Hans Schoutens

The use of ultraproducts in commutative algebra

October 4, 2008

Springer

Contents

Chapter 1
Introduction

Unbeknownst to the majority of algebraists, ultraproducts have been around in model-theory for more than half a century, since their first appearance in a paper by Łoś ([51]), although the construction goes even further back, to work of Skolem in 1938 on non-standard models of arithmetic. Through Kochen's seminal paper [49] and his joint work [9] with Ax, ultraproducts also found their way into algebra. They did not leave a lasting impression on the algebraic community though, shunned perhaps because there were conceived as non-algebraic, belonging to the alien universe of set-theory and non-standard arithmetic, a universe in which most mathematicians did not, and still do not feel too comfortable.

The present book intends to debunk this common perception of ultraproducts: when applied to algebraic objects, their construction is quite natural, yet very powerful, and requires hardly any knowledge of model-theory. In particular, when applied to a collection of rings A_w, where w runs over some infinite index set W, the construction is entirely algebraic:[1] the ultraproduct of the A_w is realized as a certain residue ring of the Cartesian product $A_\infty := \prod A_w$ modulo the so-called *null-ideal* (see below). Any ring arising in this way will be denoted $A_\natural$, and called an *ultra-ring*;[2] and the A_w are then called *approximations* of this ultra-ring. As this terminology suggests, we may think of ultraproducts as certain kinds of limits. This is the perspective of [78], which I will not discuss in these notes.

Whereas the classical Cartesian product performs a parallel computation, so to speak, within each A_w, the ultraproduct, on the other hand, computes things generically: elements in the ultraproduct $A_\natural$ satisfy certain algebraic relations if and only if their corresponding entries satisfy the same relations in the approximations A_w *with probability one*. To make this latter condition explicit, an ostensibly extrinsic component has to be introduced: we must impose some (degenerated) probability measure on the index set W of the family. The classical way is to choose a (non-principal) ultrafilter on W, and then say that an *event holds with probability one* (or, more informally, *almost always*) if the set of indices for which it holds belongs

[1] For a construction with a more geometrical flavor, see Project 2.7.

[2] For the rather unorthodox notation, see below.

to the ultrafilter. Fortunately, the dependence on the choice of ultrafilter/probability measure turns out to be, for all intents and purposes, irrelevant, and so ultraproducts behave almost as if they were intrinsically defined.[3]

Once we have chosen a (non-principal) ultrafilter, we can define the ultraproduct $A_\natural$ as the residue ring of the Cartesian product $A_\infty := \prod_w A_w$ modulo the null-ideal of *almost zero elements*, that is to say, those elements in the product almost all of whose entries are zero. However, we can make this construction entirely algebraic, without having to rely on an ultrafilter/probablity measure (although the latter perspective is more useful when we have to prove things about ultraproducts). Namely, let us call an element in the product A_∞ a *strong idempotent* if each of its entries is either zero or one. Fix a prime ideal $\mathfrak{P}$ of A_∞ and let $\mathfrak{P}^\circ$ be the ideal generated by all strong idempotents in $\mathfrak{P}$. Then $\mathfrak{P}^\circ$ is a null-ideal, with respect to some choice of ultrafilter, and hence $A_\natural := A_\infty/\mathfrak{P}^\circ$ is an ultra-ring. Moreover, all possible ultraproducts of the A_w arise in this way (see §2.5). Principal null-ideals, corresponding to principal ultrafilters, have one of the A_w as residue rings, and therefore are of little use. Hence from now on, when talking about ultra-rings, we always assume that the null-ideal is not principal—it follows that it is then infinitely generated—and this is equivalent with the ultrafilter containing all co-finite subsets, and also with the defining prime ideal $\mathfrak{P}$ containing the direct sum $\bigoplus A_w$. This construction simplifies further in case all A_w are domains: their ultraproduct is then the coordinate ring of an irreducible component of $\operatorname{Spec}(A_\infty)$, that is to say, $A_\natural = A_\infty/\mathfrak{G}$ with $\mathfrak{G}$ a minimal prime ideal of A_∞, and any minimal prime defines one of the possible ultraproducts.

We already alluded to the main property of ultraproducts: they have the same (first-order) properties than almost all their approximations A_w; this is known to model-theorists as Łos' Theorem. Although it may not always be easy to determine whether a property carries over, that is to say, is first-order, this is the case if it is expressible in arithmetic terms. *Arithmetical* here refers to algebraic formulas between ring elements, 'first-order objects,' but not between 'higher-order objects,' like ideals or modules. For instance, properties such as being a domain, reduced, normal, local, or Henselian, are easily seen to be preserved. Among those that do not carry over, is, unfortunately, the Noetherian property. Ultra-rings, therefore, are hardly ever Noetherian; the ultraproduct construction takes us outside our category! In particular, tools from commutative algebra seem no longer applicable. However, as we will show, there is still an awful lot, especially in the local case, that does carry through, with a few minor adaptations of the definitions. In fact, we will introduce two variant constructions that are designed to overcome altogether this obstacle. I have termed these *chromatic products*, for they, too, are denoted using musical notation: the *protoproduct* $A_\flat$, and the *cataproduct* $A_\sharp$. The latter is defined as soon all A_w are Noetherian local rings of bounded embedding dimension (that is to say, whose maximal ideal is generated by n elements, for some n independent from w). Its main advantage over the ultraproduct itself, of which it is a further residue ring, is that a cataproduct is always Noetherian and complete. To define protoproducts, we need some additional data on the approximations, namely, some uniform grading, analo-

[3] This does not mean that ultraproducts of the same rings, but with respect to different ultrafilters, are necessarily isomorphic.

gous to polynomial degree. Although protoproducts do not need to be Noetherian, they often are. In case both are defined, we get a *chromatic scale of homomorphisms* $A_\flat \to A_\natural \to A_\sharp$.

However, as we shall see, it is in combination with certain flatness results that ultraproducts, and more generally chromatic products, acquire their real power. Already in their 1984 paper [65], Schmidt and van den Dries observed how a certain flatness property of ultraproducts, discovered five years prior to this by van den Dries in [20], translates into the existence of uniform bounds in polynomial rings (see our discussion in §8.2). This paper was soon followed by others exploiting this new method: [10, 18, 64]. The former two papers brought in a third theme that we will encounter in this book on occasion: Artin Approximation (see §11.1). So, germane to almost every single application of ultraproducts is flatness, to which we therefore devote a separate chapter, Chapter 6. In order to do this properly, we also need to review some more basic commutative algebra.

Consequently, the first part of this book has been designed as a primer in commutative algebra for the benefit of the reader who is less familiar with this field. Most of the material in this part is standard, except perhaps some of the material on flatness, and can easily be skipped by the experienced algebraist. Incidentally, there is an additional reason why our approach is primarily algebraic, even when dealing with geometrical issues: the ultraproduct of schemes, even affine ones, is in general no longer a scheme. The exact formalism to describe these *ultra-schemes* has yet to be developed, and so we restrict our attention to ultra-rings, which are at least always rings.

In the second part, we then apply our tools from commutative algebra to these ultra-rings, to obtain several deeper results in commutative algebra. As already mentioned, flatness abounds these methods. Since an ultraproduct averages or captures the generic behavior of its approximations, it should not come as a surprise that as a tool, it is particularly well suited to derive uniformity results. This is done in Chapter 8, which is both thematically and chronologically the closest to its above mentioned paradigmatic forebear [65]. A second, more profound application of the method to commutative algebra is described in the subsequent chapters: we use ultraproducts to give an alternative treatment of tight closure theory in characteristic zero. Tight closure theory, introduced by Hochster and Huneke in an impressive array of beautiful articles—[34, 35, 37, 40, 38], to name only a few—is an extremely powerful tool, which relies heavily on the algebraicity of the Frobenius in positive characteristic, and as such is primarily a positive characteristic tool. Without going into details (these can be found in Chapter 9), one associates, using the p-th power Frobenius homomorphisms, to any ideal $\mathfrak{a}$ in a ring of characteristic $p > 0$, its *tight closure* $\mathfrak{a}^*$, an overideal contained in the integral closure of $\mathfrak{a}$, but often much closer or "tighter" to the original $\mathfrak{a}$. What really attracted people to the method was not only the apparent ease with which deep, known results could be reproved, but also its new, and sometimes unexpected applications, both in commutative algebra and algebraic geometry, derived all by means of fairly elementary arguments.

Although essentially a positive characteristic method, its authors also conceived of tight closure theory in characteristic zero in [41], by a generic reduction to positive characteristic. In fact, this reduction method, using Artin Approximation (our third theme emerges again!), as well as the method in positive characteristic itself were both inspired by the equally impressive work of Peskin and Szpiro [57] on Intersection Conjectures, and Hochster's own early work on big Cohen-Macaulay modules ([43]) and Homological Conjectures ([31, 32]). However, to develop the method in characteristic zero some extremely deep results on Artin Approximation[4] were required, and the elegance of the positive characteristic method was entirely lost. No wonder! In characteristic zero, there is no Frobenius, nor any other algebraic endomorphism that could take over its role. To the rescue, however, come our ultraproducts. Keeping in mind that an ultraproduct is some kind of averaging process, it follows that the ultraproduct of rings of different positive characteristic is an ultra-ring of characteristic zero, for which reason we call it a *Lefschetz ring*. Furthermore, the ultraproduct of the corresponding Frobenius maps—one of the many advantages of ultraproducts, they can be taken of almost anything!—yields an *ultra-Frobenius* on this Lefschetz ring. Notwithstanding that it is no longer a power map, this ultra-Frobenius can easily fulfill the role played by the Frobenius in the positive characteristic theory. The key observation now is that many rings of characteristic zero—for instance, all Noetherian local rings, and all rings of finite type over a field—embed in a Lefschetz ring via a faithfully flat homomorphism. Flatness is essential here: it guarantees that the embedded ring preserves its ideal structure within the Lefschetz ring, which makes it possible to define the tight closure of its ideals inside that larger ring. In this manner, we can restore the elegant arguments from the positive characteristic theory, and prove the same results with the same elegant arguments as before. The present theory of characteristic zero tight closure is the easiest to develop for rings of finite type over an algebraically closed field, and this is explained in Chapter 10. The general local case is more complicated, and does require some further results on Artin Approximation, although far less deep than the ones Hochster and Huneke need for their theory. In fact, conversely, one can deduce certain Artin Approximation results from the fact that any Noetherian local ring has a faithfully flat Lefschetz extension. Chapter 11 only develops the parts necessary to derive all the desired applications; for a more thorough treatment, one can consult [6].

In a parallel development, Hochster and Huneke's work on tight closure also led them to their discovery of canonically defined, big balanced Cohen-Macaulay algebras in positive characteristic: any system of parameters in a excellent local domain of positive characteristic becomes a regular sequence in the absolute integral closure of the ring. The same statement is plainly false in characteristic zero, and the authors had to circumvent this obstruction again using complicated reduction techniques. Using ultraproducts, one constructs, quite canonically, big balanced Cohen-Macaulay algebras in characteristic zero simply by (faithfully flatly) embedding the ring inside a Lefschetz ring and then taking the ultraproduct of the absolute integral closures of the positive characteristic approximations of the Lefschetz ring. With aid of these new techniques, I was able to give new characterizations of rational

[4] The controversy initially shrouding these results is a tale on its own.

and log-terminal singularities. Furthermore, exploiting the canonical properties of the ultra-Frobenius, I succeeded in settling some of the conjectures that hitherto had remained impervious to tight closure methods. All these results, unfortunately, fall outside the scope of this book, and the reader is referred to the articles [72, 73, 77].

The next two chapters, Chapter 12 on cataproducts, and Chapter 13 on protoproducts, develop the theory of these chromatic powers. Most of the applications are on uniform bounds. In fact, in [79], characterizations of many common ring-theoretic properties of Noetherian local rings, such as being analytically unramified, Cohen-Macaulay, unmixed, etc., were obtained in terms of uniform behavior of two particular ring-invariants: order (with respect to the maximal ideal) and *degree*. This latter invariant measures to which extent an element is a parameter of the ring, and is a spin-off of our analysis of the dimension theory for ultra-rings (Krull dimension is one of the many invariants that are not preserved under ultraproducts, requiring a different approach via systems of parameters). Protoproducts, on the other hand, are designed to study rings with a generalized grading, called *proto-grading*, and most applications are again on uniform bounds in terms of these. This is in essence a formalization of the method coming out of the aforementioned [65].

In the last chapter, we discuss some open problems, commonly known as *Homological Conjectures*. Whereas these are now all settled in equal characteristic, either by the older methods, or by the recent tight closure methods, the case when the Noetherian local ring has different characteristic than its residue field, the *mixed characteristic case*, is for the most part still wide open.[5] We will settle some of them, at least *asymptotically*, meaning, for large enough residual characteristic. This is still far from a complete solution, and our asymptotic results would only gain considerable interest if the actual conjectures turned out to be false. The method is inspired by Ax and Kochen's solution of a problem posed by Artin, historically the first application of ultraproducts outside logic (see above). Their main result, generalized latter by Eršhov ([23, 24]), is that an ultraproduct of mixed characteristic discrete valuation rings of different residual characteristics is isomorphic to an ultraproduct of equal characteristic discrete valuation rings. So, we can transfer results from equal characteristic, the known case, to results in mixed characteristic. However, the fact that properties only hold with probability one in an ultraproduct accounts for the asymptotic nature of our results. These limitations of the method, which is in essence a protoproduct argument, probably will never allow for a solution of the full conjectures. In §14.3, I propose a variant method, using cataproducts instead. Here the asymptotic nature can also be expressed in terms of the ramification index (= the order of p), rather than just the residual characteristic. Although this gives often more general results, in terms of more natural invariants, some of the homological problems still elude treatment. As discussed in [79, §12.11], such results, however, could potentially lead to a positive solution of the corresponding full conjecture.

Guidelines for the reader This book started as lecture notes for a course I taught at the CUNY Graduate Center in Fall 2006: *The use of ultraproducts in commutative algebra*. It was listed officially as an advanced Algebraic Model-theory course,

[5] Some recent strides in dimension three have been made by Heitman ([29]) and Hochster ([33]).

but was designed to be an hybrid course for logic and algebra graduate students. I think this also best describes the present book. Its intended audience are advanced graduate students and researchers in Model-theory, Commutative Algebra, or Algebraic Geometry. The more specialized topics, or those topics tangential to the main discussion, are typographically distinguished from the others, and can safely be skipped during a first reading. There are also plenty of exercises, with some (partial) solutions at the back of the book.

Every effort has been made to keep the book as self-contained as possible. A general background in elementary algebra though is assumed (like [7, 47]), but not much more.[6] Whereas the first part is a survey of some classical algebraic topics (dimension theory, singulairities, completion, and flatness), the second part contains mostly my own work, except for the chapter on tight closure in positive characteristic. The material on uniform bounds and tight closure in characteristic zero has already been published elsewhere, and I have only extracted those results that could be treated within the limitations of this publication. The material in the last three chapters, on chromatic products, has not yet been published at the time of writing, and some of this is still work-in-progress.

Notations and conventions We follow the common convention to let $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_p$, $\mathbb{Q}$, $\mathbb{Q}_p$, $\mathbb{R}$, and $\mathbb{C}$ denote respectively, the natural numbers, the integers, the ring of p-adic integers, the field of rational, of p-adic, of real, and of complex numbers. The q-element field, for q a power of a prime number, will be denoted $\mathbb{F}_q$. The complement of a set $D \subset W$ is denoted $-D$, and more generally, the difference between two subsetes $D,E \subseteq W$ is denoted $D-E$.

All rings are assumed to be commutative. More often than not, the image of an element $a \in A$ under a ring homomorphism $A \to B$ is still denoted a. In particular, IB denotes the ideal generated by the images of elements in the ideal $I \subseteq A$, and $J \cap A$ denotes the ideal of all elements whose image lies in the ideal $J \subseteq B$.

[6] That is not to say, of course, that some experience with model-theory, algebraic geometry, or more advanced commutative algebra would certainly help.

Part I
Prelude

Chapter 2
Ultraproducts and Łos' Theorem

In this chapter, W denotes an infinite set, always used as an index set, on which we fix a non-principal ultrafilter. Given any collection of (first-order) structures indexed by W, we can define their ultraproduct. However, in this book, we will be mainly concerned with the construction of an ultraproduct of rings, an *ultra-ring* for short, which is then defined as a certain residue ring of their Cartesian product. From this point of view, the construction is purely algebraic, although it is originally a model-theoretic one (we only provide some supplementary background on the model-theoretic perspective). We review some basic properties (deeper theorems will be proved in the later chapters), the most important of which is Łos' Theorem, relating properties of the approximations with their ultraproduct. When applied to algebraically closed fields, we arrive at a result that is pivotal in most of our applications: the Lefschetz Principle (Theorem 2.4.3), allowing us to transfer many properties between positive and zero characteristic.

2.1 Ultraproducts

Non-principal ultrafilters. By a *non-principal ultrafilter* $\mathscr{U}$ on W, we mean a collection of infinite subsets of W closed under finite intersection, with the property that for any subset $D \subseteq W$, either D or its complement $-D$ belongs to $\mathscr{U}$. In particular, the empty set does not belong to $\mathscr{U}$, and if $D \in \mathscr{U}$ and E is an arbitrary set containing D, then also $E \in \mathscr{U}$, for otherwise $-E \in \mathscr{U}$, whence $\emptyset = D \cap -E \in \mathscr{U}$, contradiction. Since every set in $\mathscr{U}$ must be infinite, it follows that any co-finite set belongs to $\mathscr{U}$. The existence of non-principal ultrafilters is equivalent with the Axiom of Choice, and we make this set-theoretic assumption henceforth. It follows that for any infinite subset of W, we can find a non-principal ultrafilter containing this set. If we drop the requirement that all sets in $\mathscr{U}$ must infinite, then some singleton must belong to $\mathscr{U}$; such an ultrafilter is called *principal*.

In the remainder of these notes, unless stated otherwise, we fix a non-principal ultrafilter $\mathscr{U}$ on W, and (almost always) omit reference to this fixed ultrafilter from our notation. No extra property of the ultrafilter is assumed, with the one exception described in Remark 12.1.5, which is nowhere used in the rest of our work anyway. Non-principal ultrafilters play the role of a decision procedure on the collection of subsets of W by declaring some subsets 'large' (those belonging to $\mathscr{U}$) and declaring the remaining ones 'small'. More precisely, let o_w be elements indexed by $w \in W$, and let $\mathscr{P}$ be a property. We will use the expressions *almost all* o_w *satisfy property* $\mathscr{P}$ or o_w *satisfies property* $\mathscr{P}$ *for almost all* w as an abbreviation of the statement that there exists a set D in the ultrafilter $\mathscr{U}$, such that property $\mathscr{P}$ holds for the element o_w, whenever $w \in D$. Note that this is also equivalent with the statement that the set of all $w \in W$ for which o_w has property $\mathscr{P}$, lies in the ultrafilter (read: *is large*). Similarly, we say that the o_w *almost never satisfy property* $\mathscr{P}$ (or *almost no* o_w *satisfies* $\mathscr{P}$), if almost all o_w do not satisfy property $\mathscr{P}$.

Ultraproducts. Let O_w be sets, for $w \in W$. We define an equivalence relation on the Cartesian product $O_\infty := \prod O_w$, by calling two sequences (a_w) and (b_w), for $w \in W$, equivalent, if a_w and b_w are equal for almost all w. In other words, if the set of indices $w \in W$ for which $a_w = b_w$ belongs to the ultrafilter. We will denote the equivalence class of a sequence (a_w) by

$$\underset{w\to\infty}{\mathrm{ulim}}\, a_w, \quad \text{or} \quad \mathrm{ulim}\, a_w, \quad \text{or} \quad a_\natural.$$

The set of all equivalence classes on $\prod O_w$ is called the *ultraproduct* of the O_w and is denoted

$$\underset{w\to\infty}{\mathrm{ulim}}\, O_w, \quad \text{or} \quad \mathrm{ulim}\, O_w, \quad \text{or} \quad O_\natural.$$

Note that the element-wise and set-wise notations are reconciled by the fact that

$$\underset{w\to\infty}{\mathrm{ulim}}\{o_w\} = \{\underset{w\to\infty}{\mathrm{ulim}}\, o_w\}.$$

The more common notation for an ultraproduct one usually finds in the literature is O^*; in the past, I also have used O_∞, which in this book is reserved to denote Cartesian products. The reason for using the particular notation $O_\natural$ in these notes is because we will also introduce the remaining "chromatic" products $O_\flat$ and $O_\sharp$ (at least for certain local rings; see Chapters 13 and 12 respectively).

We wil also often use the following terminology: if o is an element in an ultraproduct $O_\natural$, then any choice of elements $o_w \in O_w$ with ultraproduct equal to o will be called an *approximation* of o. Although an approximation is not uniquely determined by the element, any two agree almost everywhere. Below we will extend our usage of the term approximation to include other objects as well.

Properties of ultraproducts. For the following properties, the easy proofs of which are left as an exercise, let O_w be sets with ultraproduct $O_\natural$.

2.1.1 *If Q_w is a subset of O_w for each w, then $\mathrm{ulim}\, Q_w$ is a subset of $\mathrm{ulim}\, O_w$.*

In fact, $\mathrm{ulim}\, Q_w$ consists of all elements of the form $\mathrm{ulim}\, o_w$, with almost all o_w in Q_w.

2.1.2 *If each O_w is the graph of a function $f_w\colon A_w \to B_w$, then $O_\natural$ is the graph of a function $A_\natural \to B_\natural$, where $A_\natural$ and $B_\natural$ are the respective ultraproducts of A_w and B_w. We will denote this function by*

$$\operatorname*{ulim}_{w\to\infty} f_w \quad \text{or} \quad f_\natural.$$

Moreover, we have an equality

$$\operatorname*{ulim}_{w\to\infty}(f_w(a_w)) = (\operatorname*{ulim}_{w\to\infty} f_w)(\operatorname*{ulim}_{w\to\infty} a_w), \tag{2.1}$$

for $a_w \in A_w$.

2.1.3 *If each O_w comes with an operation $*_w\colon O_w \times O_w \to O_w$, then*

$$*_\natural := \operatorname*{ulim}_{w\to\infty} *_w$$

is an operation on $O_\natural$. If all (or, almost all) O_w are groups with multiplication $*_w$ and unit element 1_w, then $O_\natural$ is a group with multiplication $*_\natural$ and unit element $1_\natural := \operatorname{ulim} 1_w$. If almost all O_w are Abelian groups, then so is $O_\natural$.

2.1.4 *If each O_w is a (commutative) ring under the addition $+_w$ and the multiplication $\cdot_w$, then $O_\natural$ is a (commutative) ring with addition $+_\natural$ and multiplication $\cdot_\natural$.*

In fact, in that case, $O_\natural$ is just the quotient of the product $O_\infty := \prod O_w$ modulo the *null-ideal*, the ideal consisting of all sequences (o_w) for which almost all o_w are zero (for more on this ideal, see §2.5 below). From now on, we will drop subscripts on the operations and denote the ring operations on the O_w and on $O_\natural$ simply by $+$ and $\cdot$.

2.1.5 *If almost all O_w are fields, then so is $O_\natural$.*

Just to give an example of how to work with ultraproducts, let me give the proof: if $a \in O_\natural$ is non-zero, with approximation a_w (recall that this means that $\operatorname{ulim} a_w = a$), then by the previous description of the ring structure on $O_\natural$, almost all a_w will be non-zero. Therefore, letting b_w be the inverse of a_w whenever this makes sense, and zero otherwise, one verifies that $\operatorname{ulim} b_w$ is the inverse of a. □

2.1.6 *If C_w are rings and O_w is an ideal in C_w, then $O_\natural$ is an ideal in $C_\natural := \operatorname{ulim} C_w$. In fact, $O_\natural$ is equal to the subset of all elements of the form $\operatorname{ulim} o_w$ with almost all $o_w \in O_w$. Moreover, the ultraproduct of the C_w/O_w is isomorphic to $C_\natural/O_\natural$.*

In other words, the ultraproduct of ideals $O_w \subseteq C_w$ is equal to the image of the ideal $\prod O_w$ in the product $C_\infty := \prod C_w$ under the canonical residue homomorphism $C_\infty \to C_\natural$.

2.1.7 *If $f_w\colon A_w \to B_w$ are ring homomorphisms, then the ultraproduct $f_\natural$ is again a ring homomorphism. In particular, if σ_w is an endomorphism on A_w, then the ultraproduct $\sigma_\natural$ is a ring endomorphism on $A_\natural := \operatorname{ulim} A_w$.*

2.2 Model-theory in rings

The previous examples are just instances of the general principle that 'algebraic structure' carries over to the ultraproduct. The precise formulation of this principle is called *Łos' Theorem* (Łos is pronounced 'wôsh') and requires some terminology from model-theory. However, for our purposes, a weak version of Łos' Theorem (namely Theorem 2.3.1 below) suffices in almost all cases, and its proof is entirely algebraic. Nonetheless, for a better understanding, the reader is invited to indulge in some elementary model-theory, or rather, an ad hoc version for rings only (if this not satisfies him/her, (s)he should consult any textbook, such as [44, 52, 61]).

Formulae. By a *quantifier free formula without parameters* in the free variables $\xi = (\xi_1,\dots,\xi_n)$, we will mean an expression of the form

$$\varphi(\xi) := \bigvee_{j=1}^{m} f_{1j} = 0 \wedge \ldots \wedge f_{sj} = 0 \wedge g_{1j} \neq 0 \wedge \ldots \wedge g_{tj} \neq 0, \tag{2.2}$$

where each f_{ij} and g_{ij} is a polynomial with integer coefficients in the variables ξ, and where $\wedge$ and $\vee$ are the logical connectives *and* and *or*. If instead we allow the f_{ij} and g_{ij} to have coefficients in a ring R, then we call $\varphi(\xi)$ a *quantifier free formula with parameters in R*. We allow all possible degenerate cases as well: there might be no variables at all (so that the formula simply declares that certain elements in $\mathbb{Z}$ or in R are zero and others are non-zero) or there might be no equations or no negations or perhaps no conditions at all. Put succinctly, a quantifier free formula is a Boolean combination of polynomial equations using the connectives $\wedge$, $\vee$ and $\neg$ (negation), with the understanding that we use distributivity and De Morgan's Laws to rewrite this Boolean expression in the (disjunctive normal) form (2.2).

By a *formula without parameters* in the free variables ξ, we mean an expression of the form

$$\varphi(\xi) := (\mathrm{Q}_1\, \zeta_1)\cdots(\mathrm{Q}_p\, \zeta_p)\, \psi(\xi,\zeta),$$

where $\psi(\xi,\zeta)$ is a quantifier free formula without parameters in the free variables ξ and $\zeta = (\zeta_1,\dots,\zeta_p)$ and where Q_i is either the universal quantifier $\forall$ or the existential quantifier $\exists$. If instead $\psi(\xi,\zeta)$ has parameters from R, then we call $\varphi(\xi)$ a *formula with parameters in R*. A formula with no free variables is called a *sentence*.

Satisfaction. Let $\varphi(\xi)$ be a formula in the free variables $\xi = (\xi_1,\dots,\xi_n)$ with parameters from R (this includes the case that there are no parameters by taking $R = \mathbb{Z}$ and the case that there are no free variables by taking $n = 0$). Let A be an R-algebra and let $\mathbf{a} = (a_1,\dots,a_n)$ be a tuple with entries from A. We will give meaning to the expression $\mathbf{a}$ *satisfies the formula $\varphi(\xi)$ in A* (sometimes abbreviated to $\varphi(\mathbf{a})$ *holds in A* or *is true in A*) by induction on the number of quantifiers. Suppose first that $\varphi(\xi)$ is quantifier free, given by the Boolean expression (2.2). Then $\varphi(\mathbf{a})$ holds in A, if for some j_0, all $f_{ij_0}(\mathbf{a}) = 0$ and all $g_{ij_0}(\mathbf{a}) \neq 0$. For the general case, suppose $\varphi(\xi)$ is of the form $(\exists\zeta)\,\psi(\xi,\zeta)$ (respectively, $(\forall\zeta)\,\psi(\xi,\zeta)$), where the satisfaction relation is already defined for the formula $\psi(\xi,\zeta)$. Then $\varphi(\mathbf{a})$ holds in A, if there is some $b \in A$ such that $\psi(\mathbf{a},b)$ holds in A (respectively, if $\psi(\mathbf{a},b)$ holds in A, for all $b \in A$). The subset of A^n consisting of all tuples satisfying $\varphi(\xi)$ will be called the *subset defined by* φ, and will be denoted $\varphi(A)$. Any subset that arises in such way will be called a *definable subset* of A^n.

Note that if $n = 0$, then there is no mention of tuples in A. In other words, a sentence is either true or false in A. By convention, we set A^0 equal to the singleton $\{\emptyset\}$ (that is to say, A^0 consists of the empty tuple $\emptyset$). If φ is a sentence, then the set defined by it is either $\{\emptyset\}$ or $\emptyset$, according to whether φ is true or false in A.

Constructible Sets. There is a connection between definable sets and Zariski-constructible sets, where the relationship is the most transparent over algebraically closed fields, as we will explain below. In general, we can make the following observations. Note, however, that the material in this section already assumes the terminology from Chapter 3 below.

Let R be a ring. Let $\varphi(\xi)$ be a quantifier free formula with parameters from R, given as in (2.2). Let $\Sigma_{\varphi(\xi)}$ denote the constructible subset of $\mathbb{A}^n_R$ (see page 40) consisting of all prime ideals $\mathfrak{p}$ of $\operatorname{Spec}(R[\xi])$ which, for some j_0, contain all f_{ij_0} and do not contain any g_{ij_0}. In particular, if $n=0$, so that $\mathbb{A}^0_R$ is by definition $\operatorname{Spec}(R)$, then the constructible subset Σ_φ associated to φ is a subset of $\operatorname{Spec}(R)$.

Let A be an R-algebra and assume moreover that A is a domain (we will never use constructible sets associated to formulae if A is not a domain). For an n-tuple $\mathbf{a}$ over A, let $\mathfrak{p}_\mathbf{a}$ be the (prime) ideal in $A[\xi]$ generated by the $\xi_i - a_i$, where $\xi = (\xi_1,\dots,\xi_n)$. Since $A[\xi]/\mathfrak{p}_\mathbf{a} \cong A$, we call such a prime ideal an *A-rational point* of $A[\xi]$. It is not hard to see that this yields a bijection between n-tuples over A and A-rational points of $A[\xi]$, which we therefore will identify with one another. In this terminology, $\varphi(\mathbf{a})$ holds in A if and only if the corresponding A-rational point $\mathfrak{p}_\mathbf{a}$ lies in the constructible set $\Sigma_{\varphi(\xi)}$ (strictly speaking, we should say that it lies in the base change $\Sigma_{\varphi(\xi)} \times_{\operatorname{Spec}(R)} \operatorname{Spec}(A)$, but for notational clarity, we will omit any reference to base changes). If we denote the collection of A-rational points of the constructible set $\Sigma_{\varphi(\xi)}$ by $\Sigma_{\varphi(\xi)}(A)$, then this latter set corresponds to the definable subset $\varphi(A)$ under the identification of A-rational points of $A[\xi]$ with n-tuples over A. If φ is a sentence, then Σ_φ is a constructible subset of $\operatorname{Spec}(R)$ and hence its base change to $\operatorname{Spec}(A)$ is a constructible subset of $\operatorname{Spec}(A)$. Since A is a domain, $\operatorname{Spec}(A)$ has a unique A-rational point (corresponding to the zero-ideal) and hence φ holds in A if and only if this point belongs to Σ_φ.

Conversely, if Σ is an R-constructible subset of $\mathbb{A}^n_R$, then we can associate to it a quantifier free formula $\varphi_\Sigma(\xi)$ with parameters from R as follows. However, here there is some ambiguity, as a constructible set is more intrinsically defined than a formula. Suppose first that Σ is the Zariski closed subset $\operatorname{V}(I)$, where I is an ideal in $R[\xi]$. Choose a system of generators, so that $I = (f_1,\dots,f_s)R[\xi]$ and set $\varphi_\Sigma(\xi)$ equal to the quantifier free formula $f_1(\xi) = \dots = f_s(\xi) = 0$. Let A be an R-algebra without zero-divisors. It follows that an n-tuple $\mathbf{a}$ is an A-rational point of Σ if and only if $\mathbf{a}$ satisfies the formula φ_Σ. Therefore, if we make a different choice of generators $I = (f'_1,\dots,f'_s)R[\xi]$, although we get a different formula φ', it defines in any R-algebra A without zero-divisors the same definable set, to wit, the collection of A-rational points of Σ. To associate a formula to an arbitrary constructible set, we do this recursively by letting $\varphi_\Sigma \wedge \varphi_\Psi$, $\varphi_\Sigma \vee \varphi_\Psi$ and $\neg\varphi_\Sigma$ correspond to the constructible sets $\Sigma \cap \Psi$, $\Sigma \cup \Psi$ and $-\Sigma$ respectively.

We say that two formulae $\varphi(\xi)$ and $\psi(\xi)$ in the same free variables $\xi = (\xi_1,\dots,\xi_n)$ are *equivalent over a ring* A, if they hold on exactly the same tuples from A (that is to say, if they define the same subsets in A^n). In particular, if φ and ψ are sentences, then they are equivalent in A if they are simultaneously true or false in A. If $\varphi(\xi)$ and $\psi(\xi)$ are equivalent for all rings A in a certain class $\mathscr{K}$, then we say that $\varphi(\xi)$ and $\psi(\xi)$ are *equivalent modulo the class* $\mathscr{K}$. In particular, if Σ is a constructible set in $\mathbb{A}^n_R$, then any two formulae associated to it are equivalent modulo the class of all R-algebras without zero-divisors. In this sense, there is a one-one correspondence between constructible subsets of $\mathbb{A}^n_R$ and quantifier free formulae with parameters from R upto equivalence.

Quantifier Elimination. For certain rings (or classes of rings), every formula is equivalent to a quantifier free formula; this phenomenon is known under the name *Quantifier Elimination*. We will only encounter it for the following class.

Theorem 2.2.1 (Quantifier Elimination for algebraically closed fields). *If $\mathscr{K}$ is the class of all algebraically closed fields, then any formula without parameters is equivalent modulo $\mathscr{K}$ to a quantifier free formula without parameters.*

More generally, if F is a field and $\mathscr{K}(F)$ the class of all algebraically closed fields containing F, then any formula with parameters from F is equivalent modulo $\mathscr{K}(F)$ to a quantifier free formula with parameters from F.

Proof (Sketch of proof). These statements can be seen as translations in model-theoretic terms of Chevalley's Theorem which says that the projection of a constructible set is again constructible. I will only explain this for the first assertion. As already observed, a quantifier free formula $\varphi(\xi)$ (without parameters) corresponds to a constructible set $\Sigma_{\varphi(\xi)}$ in $\mathbb{A}^n_{\mathbb{Z}}$ and the tuples in K^n satisfying $\varphi(\xi)$ are precisely the K-rational points $\Sigma_{\varphi(\xi)}(K)$ of $\Sigma_{\varphi(\xi)}$. The key observation is now the following. Let $\psi(\xi,\zeta)$ be a quantifier free formula and put $\gamma(\xi) := (\exists\zeta)\,\psi(\xi,\zeta)$, where $\xi = (\xi_1,\dots,\xi_n)$ and $\zeta = (\zeta_1,\dots,\zeta_m)$. Let $\Psi := \psi(K)$ be the subset of K^{n+m} defined by $\psi(\xi,\zeta)$ and let $\Gamma := \gamma(K)$ be the subset of K^n defined by $\gamma(\xi)$. Therefore, if we identify K^{n+m} with the collection of K-rational points of $\mathbb{A}^{n+m}_K$, then

$$\Psi = \Sigma_{\psi(\xi,\zeta)}(K).$$

Moreover, if $p\colon \mathbb{A}^{n+m}_K \to \mathbb{A}^n_K$ is the projection onto the first n coordinates then $p(\Psi) = \Gamma$. By Chevalley's Theorem (see for instance [22, Corollary 14.7] or [28, II. Exercise 3.19]), $p(\Sigma_{\psi(\xi,\zeta)})$ (as a subset in $\mathbb{A}^n_{\mathbb{Z}}$) is again constructible, ands therefore, by our previous discussion, of the form $\Sigma_{\chi(\xi)}$ for some quantifier free formula $\chi(\xi)$. Hence $\Gamma = \Sigma_{\chi(\xi)}(K)$, showing that $\gamma(\xi)$ is equivalent modulo K to $\chi(\xi)$. Since $\chi(\xi)$ does not depend on K, we have in fact an equivalence of formulae modulo the class $\mathscr{K}$. To get rid of an arbitrary chain of quantifiers, we use induction on the number of quantifiers, noting that the complement of a set defined by $(\forall\zeta)\,\psi(\xi,\zeta)$ is the set defined by $(\exists\zeta)\neg\psi(\xi,\zeta)$, where $\neg(\cdot)$ denotes negation.

For some alternative proofs, see [44, Corollary A.5.2] or [52, Theorem 1.6]. □

2.3 Łos' Theorem

Thanks to Quantifier Elimination (Theorem 2.2.1), when dealing with algebraically closed fields, we may forget altogether about formulae and use constructible sets instead. However, we will not always be able to work just in algebraically closed fields and so we need to formulate a general transfer principle for ultraproducts. For most of our purposes, the following version suffices:

Theorem 2.3.1 (Equational Łos' Theorem). *Suppose each A_w is an R-algebra, and let $A_\natural$ denote their ultraproduct. Let ξ be an n-tuple of variables, let $f \in R[\xi]$, and let $\mathbf{a}_w$ be n-tuples in A_w with ultraproduct $\mathbf{a}_\natural$. Then $f(\mathbf{a}_\natural) = 0$ in $A_\natural$ if and only if $f(\mathbf{a}_w) = 0$ in A_w for almost all w.*

Moreover, instead of a single equation $f = 0$, we may take in the above statement any system of equations and negations of equations over R.

Proof. Let me only sketch a proof of the first assertion. Suppose $f(\mathbf{a}_\natural) = 0$. One checks (do this!), making repeatedly use of (2.1), that $f(\mathbf{a}_\natural)$ is equal to the ultraproduct of the $f(\mathbf{a}_w)$. Hence the former being zero simply means that almost all $f(\mathbf{a}_w)$ are zero. The converse is proven by simply reversing this argument. □

On occasion, we might also want to use the full version of Łos' Theorem, which requires the notion of a formula as defined above. Recall that a sentence is a formula without free variables.

Theorem 2.3.2 (Łos' Theorem). *Let R be a ring and let A_w be R-algebras. If φ is a sentence with parameters from R, then φ holds in almost all A_w if and only if φ holds in the ultraproduct $A_\natural$.*

More generally, let $\varphi(\xi_1,\dots,\xi_n)$ be a formula with parameters from R and let $\mathbf{a}_w$ be an n-tuple in A_w with ultraproduct $\mathbf{a}_\natural$. Then $\varphi(\mathbf{a}_w)$ holds in almost all A_w if and only if $\varphi(\mathbf{a}_\natural)$ holds in $A_\natural$.

The proof is tedious but not hard; one simply has to unwind the definition of formula (see [44, Theorem 9.5.1] for a more general treatment). Note that $A_\natural$ is naturally an R-algebra, so that it makes sense to assert that φ is true or false in $A_\natural$. Applying Łos' Theorem to a quantifier free formula proves Theorem 2.3.1.

2.4 Ultra-rings

An *ultra-ring* is simply an ultraproduct of rings. Probably the first examples of ultra-rings appearing in the literature are the so-called *non-standard integers*, that is to say, the ultrapowers $\mathbb{Z}_\natural$ of $\mathbb{Z}$.[1] Ultra-rings will be our main protagonists, but for the moment we only establish some very basic facts about them.

Ultra-fields. Let K_w be a collection of fields and $K_\natural$ their ultraproduct, which is again a field by 2.1.5 (or by an application of Łos' Theorem). Any field which arises in this way is called an *ultra-field*.[2] Since an ultraproduct is either finite or uncountable, $\mathbb{Q}$ is an example of a field which is not an ultra-field.

2.4.1 *If for each prime number p, only finitely many K_w have characteristic p, then $K_\natural$ has characteristic zero.*

Indeed, for every prime number p, the equation $p\xi - 1 = 0$ has a solution in all but finitely many of the K_w and hence it has a solution in $K_\natural$, by Theorem 2.3.1. We will call an ultra-field $K_\natural$ of characteristic zero which arises as an ultraproduct

[1] Logicians study these under the guise of *models of Peano arithmetic*, where, instead of $\mathbb{Z}_\natural$, one traditionally looks at the sub-semi-ring $\mathbb{N}_\natural$, the ultrapower of $\mathbb{N}$.

[2] In case the K_w are finite but of unbounded cardinality, their ultraproduct $K_\natural$ is also called a *pseudo-finite field*; in these notes, however, we prefer the usage of the prefix *ultra-*, and so we would call such fields instead *ultra-finite fields*

of fields of positive characteristic, a *Lefschetz field* (the name is inspired by Theorem 2.4.3 below); and more generally, an ultra-ring of characteristic zero given as the ultraproduct of rings of positive characteristic will be called a *Lefschetz ring* (see page 169 for more).

2.4.2 *If almost all K_w are algebraically closed fields, then so is $K_\natural$.*

The quickest proof is by means of Łos' Theorem, although one could also give an argument using just Theorem 2.3.1 (which is no surprise in light of Exercise 2.6.17).

Proof. For each $n \geq 2$, consider the sentence σ_n given by

$$(\forall \zeta_0, \ldots, \zeta_n)\,(\exists \xi)\,\zeta_n = 0 \,\vee\, \zeta_n \xi^n + \cdots + \zeta_1 \xi + \zeta_0 = 0.$$

This sentence is true in any algebraically closed field, whence in almost all K_w, and therefore, by Łos' Theorem, in $K_\natural$. However, a field in which every σ_n holds is algebraically closed. □

We have the following important corollary which can be thought of as a model theoretic Lefschetz Principle (here $\mathbb{F}_p^{\mathrm{alg}}$ denotes the algebraic closure of the p-element field; and, more generally, $\mathbb{F}^{\mathrm{alg}}$ denotes the algebraic closure of a field F).

Theorem 2.4.3 (Lefschetz Principle). *Let W be the set of prime numbers, endowed with some non-principal ultrafilter. The ultraproduct of the fields $\mathbb{F}_p^{alg}$ is isomorphic with the field $\mathbb{C}$ of complex numbers, that is to say, we have an isomorphism*

$$\operatorname*{ulim}_{p \to \infty} \mathbb{F}_p^{alg} \cong \mathbb{C}.$$

Proof. Let $\mathbb{F}_\natural$ denote the ultraproduct of the fields $\mathbb{F}_p^{\mathrm{alg}}$. By 2.4.2, the field $\mathbb{F}_\natural$ is algebraically closed, and by 2.4.1, its characteristic is zero. Using elementary set theory, one calculates that the cardinality of $\mathbb{F}_\natural$ is equal to that of the continuum. The theorem now follows since any two algebraically closed fields of the same uncountable cardinality and the same characteristic are (non-canonically) isomorphic by Steinitz's Theorem (see [44] or Theorem 2.4.5 below). □

Remark 2.4.4. We can extend the above result as follows: any algebraically closed field K of characteristic zero and cardinality 2^κ, for some infinite cardinal κ, is a Lefschetz field. Indeed, for each p, choose an algebraically closed field K_p of characteristic p and cardinality κ. Since the ultraproduct of these fields is then an algebraically closed field of characteristic zero and cardinality 2^κ, it is isomorphic to K by Steinitz's Theorem (Theorem 2.4.5). Under the generalized Continuum Hypothesis, any uncountable cardinal is of the form 2^κ, and hence any uncountable algebraically closed field of characteristic zero is then a Lefschetz field. We will tacitly assume this, but the reader can check that nowhere this assumption is used in an essential way.

Theorem 2.4.5 (Steinitz's Theorem). *If K and L are algebraically closed fields of the same characteristic and the same uncountable cardinality, then they are isomorphic.*

Proof *(Sketch of proof).* Let k be the common prime field of K and L (that is to say, either $\mathbb{Q}$ in characteristic zero, or $\mathbb{F}_p$ in positive characteristic p). Let Γ and Δ be respective transcendence bases of K and L over k. Since K and L have the same uncountable cardinality, Γ and Δ have the same cardinality, and hence there exists a bijection $f\colon \Gamma \to \Delta$. This naturally extends to a field isomorphism $k(\Gamma) \to k(\Delta)$. Since K is the algebraic closure of $k(\Gamma)$, and similarly, L of $k(\Delta)$, this isomorphism then extends to an isomorphism $K \to L$. □

Ultra-rings. Let A_w be a collection of rings. Their ultraproduct $A_\natural$ will be called, as already mentioned, an *ultra-ring*.

2.4.6 *If each A_w is local with maximal ideal $\mathfrak{m}_w$ and residue field $k_w := A_w/\mathfrak{m}_w$, then $A_\natural$ is local with maximal ideal $\mathfrak{m}_\natural := \operatorname{ulim}\mathfrak{m}_w$ and residue field $k_\natural := \operatorname{ulim} k_w$.*

Indeed, a ring is local if and only if the sum of any two non-units is again a non-unit. This statement is clearly expressible by means of a sentence, so that by Łos' Theorem (Theorem 2.3.2), $A_\natural$ is local. Again we can prove this also directly, or using the equational version, Theorem 2.3.1. The remaining assertions now follow easily from 2.1.6. In fact, the same argument shows that the converse is also true: if $A_\natural$ is local, then so are almost all A_w.

2.4.7 *If A_w are local rings of embedding dimension e, then so is $A_\natural$.*

Recall that the *embedding dimension* of a local ring is the minimal number of generators of its maximal ideal. Hence, by assumption almost all $\mathfrak{m}_w$ are generated by e elements x_{iw}. It follows from 2.1.6 that $\mathfrak{m}_\natural$ is generated by the e ultraproducts $x_{i\natural}$.

2.4.8 *Almost all A_w are domains (respectively, reduced) if and only if $A_\natural$ is a domain (respectively, reduced).*

Indeed, being a domain is captured by the fact that the equation $\xi\zeta = 0$ has no solution by non-zero elements; and being reduced by the fact that the equation $\xi^2 = 0$ has no non-zero solutions. In particular, using 2.1.6, we see that an ultraproduct of ideals is a prime (respectively, radical, maximal) ideal if and only if almost all ideals are prime (respectively, reduced, maximal).

2.4.9 *If I_w are ideals in the local rings $(A_w, \mathfrak{m}_w)$, such that in $(A_\natural, \mathfrak{m}_\natural)$, their ultraproduct $I_\natural$ is $\mathfrak{m}_\natural$-primary, then almost all I_w are $\mathfrak{m}_w$-primary.*

Recall that an ideal I in a local ring $(R, \mathfrak{m})$ is called $\mathfrak{m}$*-primary* if its radical is equal to $\mathfrak{m}$. Note that here the converse may fail to hold: not every ultraproduct of $\mathfrak{m}_w$-primary ideals need to be $\mathfrak{m}_\natural$-primary (see Exercise 2.6.10).

As will become apparent later on, the following ideal plays an important role in the study of local ultra-rings.

Definition 2.4.10 (Ideal of infinitesimals). For an arbitrary local ring $(R,\mathfrak{m})$, define its *ideal of infinitesimals*, denoted $\mathfrak{I}_R$, as the intersection

$$\mathfrak{I}_R := \mathfrak{m}^\infty := \bigcap_{n\geq 0} \mathfrak{m}^n.$$

The $\mathfrak{m}$-adic topology (see page 101) on R is Hausdorff (=separated) if and only if $\mathfrak{I}_R = 0$. Therefore, we will refer to the residue ring $R/\mathfrak{I}_R$ as the *separated quotient* of R. In commutative algebra, the ideal of infinitesimals hardly ever appears simply because of:

Theorem 2.4.11 (Krull's Intersection Theorem). *If R is a Noetherian local ring, then $\mathfrak{I}_R = 0$.*

Proof. This is an immediate consequence of the Artin-Rees Lemma (for which see [54, Theorem 8.5] or [7, Proposition 10.9]), or of its weaker variant proven in Theorem 12.2.1 below. Namely, for $x \in \mathfrak{I}_R$, there exists, according to the latter theorem, some c such that $xR \cap \mathfrak{m}^c \subseteq x\mathfrak{m}$. Since $x \in \mathfrak{m}^c$ by assumption, we get $x \in x\mathfrak{m}$, that is to say, $x = ax$ with $a \in \mathfrak{m}$. Hence $(1-a)x = 0$. As $1-a$ is a unit in R, we get $x = 0$. □

Corollary 2.4.12. *In a Noetherian local ring $(R,\mathfrak{m})$, every ideal is the intersection of $\mathfrak{m}$-primary ideals.*

Proof. For $I \subseteq R$ an ideal, an application of Theorem 2.4.11 to the ring R/I shows that I is the intersection of all $I + \mathfrak{m}^n$, and the latter are indeed $\mathfrak{m}$-primary. □

Most local ultra-rings have a non-zero ideal of infinitesimals.

2.4.13 *If R_w are local rings with non-nilpotent maximal ideal, then the ideal of infinitesimals of their ultraproduct $R_\natural$ is non-zero. In particular, $R_\natural$ is not Noetherian.*

Indeed, by assumption, we can find non-zero $a_w \in \mathfrak{m}^w$ (let us for the moment assume that the index set is equal to $\mathbb{N}$) for all w. Hence their ultraproduct $a_\natural$ is non-zero and lies inside $\mathfrak{I}_{R_\natural}$.

Ultra-exponentation. Let $A_\natural$ be an ultra-ring, given as the ultraproduct of rings A_w. Let $\mathbb{N}_\natural$ be the ultrapower of the natural numbers, and let $\alpha \in \mathbb{N}_\natural$ with approximations α_w. The *ultra-exponentation map* on A with exponent α is given by sending $x \in A$ to the ultraproduct, denoted x^α, of the $x_w^{\alpha_w}$, where x_w is an approximation of x. One easily verifies that this definition does not depend on the choice of approximation of x or α. If A is local and x a non-unit, then x^α is an infinitesimal for any α in $\mathbb{N}_\natural$ not in $\mathbb{N}$. In these notes, the most important instance will be the ultra-exponentation map obtained as the ultra-product of Frobenius maps. More precisely, let $A_\natural$ be a Lefschetz ring, say, realized as the ultraproduct of rings A_p of characteristic p (here we assumed for simplicity that the underlying index set is just the set of prime numbers, but this is not necessary). On each A_p, we have an action of the *Frobenius*, given as $\mathbf{F}_p(x) := x^p$ (for more, see §9.1).

Definition 2.4.14 (Ultra-Frobenius). The ultraproduct of these Frobenii yields an endomorphism $\mathbf{F}_\infty$ on $A_\natural$, called the *ultra-Frobenius*, given by $\mathbf{F}_\infty(x) := x^\pi$, where $\pi \in \mathbb{N}_\natural$ is the ultraproduct of all prime numbers.

2.5 Algebraic definition of ultra-rings

Let A_w, for $w \in W$, be rings with Cartesian product $A_\infty := \prod_w A_w$ and direct sum $A_{(\infty)} := \bigoplus A_w$. Note that $A_{(\infty)}$ is an ideal in A_∞. Call an element $a \in A_\infty$ a *strong idempotent* if each of its entries is either zero or one. For any ideal $\mathfrak{I} \subseteq A_\infty$, let $\mathfrak{I}^\circ$ be the ideal generated by all strong idempotents in $\mathfrak{I}$. Let $\mathfrak{P}$ be a prime ideal of A_∞, and let $\mathscr{U}_\mathfrak{P}$ be the collection of $D \subseteq W$ such that $1 - 1_D \in \mathfrak{P}$, where 1_D denotes the characteristic function of D, that is to say, the strong idempotent whose entries are one for $w \in D$ and zero otherwise (note that $1 = 1_W$).

2.5.1 *Each $\mathscr{U}_\mathfrak{P}$ is an ultrafilter, which is principal if and only if the ideal $\mathfrak{P}^\circ$ is principal, if and only if $\mathfrak{P}$ does not contain the ideal $A_{(\infty)}$.*

Indeed, given an idempotent e, its *complement* $1-e$ is again idempotent, and the product of both is zero. It follows that any prime ideal contains exactly one among e and $1-e$. Hence $\mathscr{U}_\mathfrak{P}$ also consists of those subsets $D \subseteq W$ such that $1_D \notin \mathfrak{P}$. Since $1 - 1_D$ is the characteristic function of the complement of D, it follows that either D or its complement belongs to $\mathscr{U}_\mathfrak{P}$. Moreover, if $D \in \mathscr{U}_\mathfrak{P}$ and $D \subseteq E$, then $1_D \cdot 1_E = 1_D$ does not belong to $\mathfrak{P}$, whence neither does 1_E, showing that $E \in \mathscr{U}_\mathfrak{P}$. This proves that $\mathscr{U}_\mathfrak{P}$ is an ultrafilter. It is not hard to see that if $\mathfrak{P}^\circ$ is principal, then it must be generated by the characteristic function of the complement of a singleton, and hence $\mathscr{U}_\mathfrak{P}$ must be principal (the other direction is immediate). For the last equivalence, see Exercise 2.6.14. □

We can now formulate the following entirely algebraic characterization of an ultra-ring.

2.5.2 *The ultraproduct of the A_w with respect to the ultrafilter $\mathscr{U}_\mathfrak{P}$ is equal to $A_\infty/\mathfrak{P}^\circ$, that is to say, $\mathfrak{P}^\circ$ is the null-ideal determined by $\mathscr{U}_\mathfrak{P}$. Furthermore, any ultra-ring having the A_w as approximations is of this form, for some prime ideal containing the direct sum ideal $A_{(\infty)}$.*

Let $\mathfrak{I}$ be the null-ideal determined by $\mathscr{U}_\mathfrak{P}$. If $D \in \mathscr{U}_\mathfrak{P}$, then almost all entries of $1 - 1_D$ are zero, and hence $1 - 1_D \in \mathfrak{I}$. Since this is a typical generator of $\mathfrak{P}^\circ$, we get $\mathfrak{P}^\circ \subseteq \mathfrak{I}$. Conversely, suppose $a = (a_w) \in \mathfrak{I}$. Hence $a_w = 0$ for all w belonging to some $D \in \mathscr{U}_\mathfrak{P}$. Since $1 - 1_D \in \mathfrak{P}^\circ$ and $a = a(1 - 1_D)$, we get $a \in \mathfrak{P}^\circ$.

Conversely, if $\mathscr{U}$ is an ultrafilter with corresponding null-ideal $\mathfrak{I} \subseteq A_\infty$, then any prime ideal $\mathfrak{P}$ containing $\mathfrak{I}$ satisfies $\mathfrak{I} = \mathfrak{P}^\circ$ (Exercise 2.6.13). □

In fact, if $\mathfrak{P} \subseteq \mathfrak{Q}$ then $\mathfrak{P}^\circ = \mathfrak{Q}^\circ$, showing that already all minimal prime ideals of A_∞ determine all possible ultrafilters (see Exercise 2.6.13). For the geometric notions mentioned in the next result, see Chapter 3.

Corollary 2.5.3. *If all A_w are domains, then $A_\natural$ is the coordinate ring of an irreducible component of* $\operatorname{Spec}(A_\infty)$*. More precisely, the residue rings $A_\infty/\mathfrak{G}$, for $\mathfrak{G} \subseteq A_\infty$ a minimal prime, are precisely the ultraproducts having the domains A_w for approximations. Moreover, these ireducible components are then also the connected components of* $\operatorname{Spec}(A_\infty)$*, that is to say, they are mutually disjoint.*

Proof. Since the ultraproduct $A_\natural$ determined by $\mathfrak{G}$ is equal to $A_\infty/\mathfrak{G}^\circ$, and a domain by 2.4.8 or Łos' Theorem, $\mathfrak{G}^\circ$ is also a prime ideal. By minimality, $\mathfrak{G}^\circ = \mathfrak{G}$. To prove the last assertion, let $\mathfrak{G}_1$ and $\mathfrak{G}_2$ be two distinct minimal prime ideals of A_∞. Suppose $\mathfrak{G}_1 + \mathfrak{G}_2$ is not the unit ideal. Hence there exists a maximal ideal $\mathfrak{M} \subseteq A_\infty$ such that $\mathfrak{G}_1, \mathfrak{G}_2 \subseteq \mathfrak{M}$, and hence

$$\mathfrak{G}_1 = \mathfrak{G}_1^\circ = \mathfrak{M}^\circ = \mathfrak{G}_2^\circ = \mathfrak{G}_2,$$

contradiction. Hence $\mathfrak{G}_1 + \mathfrak{G}_2 = 1$. This shows that any two irreducible components of $\operatorname{Spec}(A_\infty)$ are disjoint. □

In the following structure theorem, $\mathbb{Z}_\infty := \mathbb{Z}^W$ denotes the Cartesian power of $\mathbb{Z}$. Any Cartesian product $A_\infty := \prod A_w$ is naturally a $\mathbb{Z}_\infty$-algebra.

Theorem 2.5.4. *Any ultra-ring is a base change of a ring of non-standard integers $\mathbb{Z}_\natural$. More precisely, the ultra-rings with approximation A_w are precisely the rings of the form $A_\infty/\mathfrak{G}A_\infty$, where $\mathfrak{G}$ is a minimal prime of $\mathbb{Z}_\infty$ containing the direct sum ideal.*

Proof. If $\mathfrak{P}$ is a prime ideal in A_∞ containing the direct sum ideal, then the generators of $\mathfrak{P}^\circ$ already live in $\mathbb{Z}_\infty$, and generate the null-ideal in $\mathbb{Z}_\infty$ corresponding to the non-principal ultrafilter $\mathscr{U}_{\mathfrak{P}}$. By Corollary 2.5.3, the latter ideal therefore is a minimal prime ideal $\mathfrak{G} \subseteq \mathbb{Z}_\infty$, and hence $\mathfrak{G}A_\infty = \mathfrak{P}^\circ$, so that one direction is clear from 2.5.2. Conversely, again by Corollary 2.5.3, any minimal prime ideal $\mathfrak{G} \subseteq \mathbb{Z}_\infty$ is the null-ideal determined by the ultrafilter $\mathscr{U}_{\mathfrak{G}}$, and one easily checks that the same is therefore true for its extension $\mathfrak{G}A_\infty$. □

2.6 Exercises

Ex 2.6.1

Prove properties 2.1.1–2.1.7.

Ex 2.6.2

Prove 2.4.6 in detail, using only Theorem 2.3.1. Show that if $\mathfrak{p}_w$ are prime ideals in A_w, then their ultraproduct $\mathfrak{p}_\natural$ is a prime ideal in $A_\natural$, and the ultraproduct of the $(A_w)_{\mathfrak{p}_w}$ is equal to $(A_\natural)_{\mathfrak{p}_\natural}$.

Ex 2.6.3

Show that an ultrafilter on W is the same as a filter which is maximal (with respect to inclusion) among all filters containing the Frechet filter. Recall that a filter *on a set W is a collection of non-empty sets closed under finite intersection and supersets, and that the* Frechet filter *is the collection of all co-finite subsets, that is to say, all subsets whose complement is finite.*
Use this to show that any collection of subsets of W having the finite intersection property *(meaning that the intersection of finitely many is never empty) is contained in some ultrafilter. If any finite intersection is infinite, then we can choose this ultrafilter to be non-principal.*

Ex 2.6.4

In the statement of 2.4.1, we tacitly assume that the underlying set is countable. Prove the following more general version which works over an arbitrary infinite index set: if for each prime number p, almost no field K_w has characteristic p, then their ultraproduct $K_\natural$ has characteristic zero, whence is a Lefschetz field.

*Ex 2.6.5

Fill in the details in the proof of the following result due to Ax ([8]): If a polynomial map $\mathbb{C}^n \to \mathbb{C}^n$ is injective, then it is surjective.
Here we call a map $\phi \colon \mathbb{C}^n \to \mathbb{C}^n$ polynomial *if there exist n polynomials $p_1(\xi), \dots, p_n(\xi) \in \mathbb{C}[\xi]$ in the n variables $\xi := (\xi_1, \dots, \xi_n)$ such that $\phi(\mathbf{u}) = (p_1(\mathbf{u}), \dots, p_n(\mathbf{u}))$ for all $\mathbf{u} \in \mathbb{C}^n$ (in the language of Chapter 3 this is just a morphism of affine space $\mathbb{A}^n_{\mathbb{C}}$ to itself).*

Proof. *By the Pigeon Hole Principle, the result is true if we replace $\mathbb{C}$ by any finite field; since $\mathbb{F}_p^{alg}$ is a union of finite fields, the assertion also holds upon replacing $\mathbb{C}$ by $\mathbb{F}_p^{alg}$; hence we are done by Theorem 2.4.3.* □

Ex 2.6.6

True or false: any homomorphic image of an ultra-ring is again an ultra-ring (you may want to take a peek at the next exercise).

Ex 2.6.7

Suppose $I_w \subseteq A_w$ are ideals, and let $I_\natural \subseteq A_\natural$ be their ultraproduct. Show that if H_w is a set of generators of I_w, then the ultraproduct $H_\natural := \operatorname{ulim} H_w$ generates $I_\natural$. Suppose next that all H_w are finite, say $H_w = \{f_{1w}, \dots, f_{m(w),w}\}$, and for each $i \in \mathbb{N}$, let $f_{i\natural}$ be the ultraproduct of the f_{iw}, where we put $f_{iw} := 0$ whenever $m(w) < i$. Let m be the supremum of all $m(w)$ (allowing $m = \infty$). Show that if $m < \infty$, then the $f_{i\natural}$ for $i = 1, \dots, m$ generate $I_\natural$. Use the example $I_w := (\xi, \zeta)^w A_w$ (with $W = \mathbb{N}$) where $A_w := K[\xi, \zeta]$, to show that the same statement is false if $m = \infty$.
Conclude that any finitely generated ideal in an ultra-ring A is an ultra-ideal. Moreover, if I is a finitely generated ideal in a ring A, then its ultrapower in the ultrapower $A_\natural$ of A is equal to $IA_\natural$. Give a counterexample to this assertion if I is not finitely generated.

Ex 2.6.8

Prove the following more general version of the last assertion in Exercise 2.6.7: let $N \subseteq M$ be modules and let $N_\natural$ and $M_\natural$ be their ultrapowers. If N is finitely generated, then $N_\natural$ is equal to the submodule of $M_\natural$ generated by N.

Ex 2.6.9

Let $A \to B$ be a finite, injective homomorphism. Show, using induction on the number of A-algebra generators of B, that if A is an ultra-ring, then so is B.

Ex 2.6.10

Show that the ultraproduct of rings of length l is again a ring of length l (see page 52 for the notion of length). Use this to prove 2.4.9. Give a counterexample to the converse of 2.4.9.

Ex 2.6.11

Show that if the ideal of infinitesimals in an ultraproduct of Noetherian local rings is finitely generated, then it is zero. Give an example where the latter case occurs. Also show the following generalization of 2.4.13: any ultraproduct of local rings of unbounded nilpotency degree has a non-zero infinitesimal, where the nilpotency degree *of a local ring $(R,\mathfrak{m})$ is the largest n such that $\mathfrak{m}^n \neq 0$ (with the understanding that it is ∞ when no power is zero).*

Ex 2.6.12

By an ultra-discrete valuation ring*, we mean an ultraproduct of discrete valuation rings. Show that the ideal of infinitesimals $\mathfrak{I}_V$ of an ultra-discrete valuation ring V is an infinitely generated prime ideal. Show that an ultra-discrete valuation ring is a* valuation domain *(=a domain such that for all a in the field of fractions of V, at least one of a or $1/a$ belongs to V). Show that the separated quotient $V/\mathfrak{I}_V$ is a discrete valuation ring—in Chapter 12 we will call this a* cataproduct *of discrete valuation rings.*

Ex 2.6.13

Show that if $\mathfrak{I} \subseteq A_\infty := \prod A_w$ is the null-ideal determined by an ultrafilter $\mathscr{U}$, and if $\mathfrak{P}$ is a prime ideal containing $\mathfrak{I}$, then $\mathscr{U}_{\mathfrak{P}} \subseteq \mathscr{U}$, whence both must be equal, and $\mathfrak{I} = \mathfrak{P}^\circ$. Show that if $\mathfrak{P} \subseteq \mathfrak{Q}$ are prime ideals in A_∞, then $\mathfrak{P}^\circ = \mathfrak{Q}^\circ$, so that they determine the same ultraproduct.

Ex 2.6.14

Given a prime ideal $\mathfrak{P}$ in an infinite product $A_\infty = \prod A_w$, show that $\mathfrak{P}^\circ$ is not principal if and only if $\mathfrak{P}$ contains the direct sum ideal $A_{(\infty)} := \bigoplus A_w$, in which case it is infinitely generated.

Ex 2.6.15

Use the characterization of 2.5.2 to prove 2.1.5 without relying on Łos' Theorem as follows: a Cartesian product of fields has the property that any element has an idempotent multiple (this is basically stating that the product is von Neuman regular), and any idempotent is strong. In particular, $\mathfrak{I} = \mathfrak{I}^\circ$ for any ideal $\mathfrak{I}$ in the product, and the result follows from Exercise 2.6.13.

Ex 2.6.16

Theorem 2.5.4 allows us also to give an entirely algebraic definition of the ultraproduct of modules: show that if M_w are modules (over some rings A_w), then their ultraproduct $M_\natural$ is equal to $M_\infty/\mathfrak{G}M_\infty$, where $\mathfrak{G}$ is a minimal prime ideal of $\mathbb{Z}_\infty$ (containing the direct sum ideal), and where M_∞ is the Cartesian product of the M_w (with its natural structure of $\mathbb{Z}_\infty$-module).

Additional exercises.

Ex 2.6.17

Derive Łos' Theorem (Theorem 2.3.2) from its equational version, Theorem 2.3.1.

Ex 2.6.18

Give a counterexample to Theorem 2.4.5 if we allow the common cardinality to be countable. Can you formulate a version which also works in the countable case?

Ex 2.6.19

Give a detailed proof of Theorem 2.4.5.

Ex 2.6.20

Let k be a field and $k_\natural$ its ultrapower. Use Maclane's criterion for separability (see for instance [54, Theorem 26.4] or [22, Theorem A1.3]) to show that the natural extension $k \to k_\natural$ is separable.

Ex 2.6.21

Recall from model-theory that a class of structures over a language L is axiomatizable *or* first-order definable*, if there exists a theory T in the language L whose models are precisely the members of this class. Show that an axiomatizable class is closed under ultraproducts. Deduce from this and 2.4.13 that the class of Noetherian rings is not first order-definable in the language of rings.*

Ex 2.6.22

Show that all A_w for $w \in W$ are connected (=have no non-trivial idempotents) if and only if any idempotent in the Cartesian product $A_\infty := \prod A_w$ is strong.

Ex 2.6.23

For a proper ideal $\mathfrak{I}$ in a Cartesian product A_∞, define $\mathscr{U}_\mathfrak{I}$ analogously as the collection of all subsets $D \subseteq W$ such that $1 - 1_D \in \mathfrak{I}$. Show that $\mathscr{U}_\mathfrak{I}$ is a filter (see Exercise 2.6.3). Show that if $\mathfrak{I}$ contains some power of a prime ideal, then $\mathscr{U}_\mathfrak{I}$ is an ultrafilter.

Ex 2.6.24

As in Exercise 2.6.23, let $\mathfrak{I}$ be a proper ideal in a Cartesian product A_∞. The residue ring $A_\infty/\mathfrak{I}^\circ$ is called a reduced *product (and $\mathfrak{I}^\circ$ is the* null-ideal *with respect to the filter $\mathscr{U}_\mathfrak{I}$). Show that if all A_w are reduced, then $\mathfrak{I}^\circ$ is radical.*
This last property is just a special case of the following more general result due to Chang ([44, Theorem 9.4.3]): let $\varphi(\xi)$ be a Horn formula *in the n free variables ξ, that is to say, a first-order formula consisting of a (possibly empty) string of quantifiers followed by a finite conjunction of formulas of the form $\mathbf{f} = 0 \to \mathbf{g} = 0$, where $\mathbf{f}, \mathbf{g}$ are finite tuples of polynomials with integer coefficients (in some quantified variables together with the free variables ξ). Show that if $\mathbf{a}_w \in (A_w)^n$ and $D \in \mathscr{U}_\mathfrak{I}$ such that $\varphi(\mathbf{a}_w)$ holds in A_w for all $w \in D$, then $\varphi(\mathbf{a})$ holds in the reduced product $A_\infty/\mathfrak{I}^\circ$, where $\mathbf{a}$ is the product of the $\mathbf{a}_w$. (When applied to the Horn sentence $\forall \zeta : \zeta^2 = 0 \to \zeta = 0$, we get our previous assertion.)*

2.7 Project: ultra-rings as stalks

Prerequisites: sheaf-theory (for instance, [28, II.1], or the rudimentary discussion on page 37).

Let W be an infinite set and give it the discrete topology (in which all sets are open). Let $W^\vee$ be the *Stone-Čech compactification* of W consisting of all ultrafilters on W. Embed W in $W^\vee$ (and henceforth view it as a subset) by sending an element to the principal ultrafilter it generates.

2.7.1 *Show that taking for open sets all sets of the form $\tau(U)$ for $U \subseteq W$, where $\tau(U)$ consists of all ultrafilters containing U, constitutes a topology on $W^\vee$. Show that W is dense in $W^\vee$, that $W^\vee$ is compact Hausdorff, and that any continuous map $W \to X$ into a compact Hausdorff space X factors through $W^\vee$ (this then justifies $W^\vee$ being called a 'compactification').*

2.7.2 *Show that $\tau(U)$ is homeomorphic to $U^\vee$, for any infinite subset $U \subseteq W$.*

Using the ideas from §2.5, prove the following geometric realization of $W^\vee$. Let $B := \mathscr{P}(W)$ be the power set of W, viewed as a Boolean algebra (with addition given by the symmetric difference, and multiplication by intersection).

2.7.3 *Show that the assignment $\mathfrak{P} \mapsto \mathscr{U}_{\mathfrak{P}}$ defined in §2.5 yields a homeomorphism between the affine scheme $X := \operatorname{Spec}(B)$ (in its Zariski toplogy) and $W^\vee$ (Hint: B is isomorphic to the Cartesian power $\mathbb{F}_2^W$).*

Let A_w be rings, indexed by $w \in W$. Define a sheaf of rings $\mathscr{A}$ on W by taking for stalk $\mathscr{A}_w := A_w$ in each point $w \in W$ (note that since W is discrete, this completely determines the sheaf $\mathscr{A}$). Let $i\colon W \to W^\vee$ be the above embedding and let $\mathscr{A}^\vee := i_*\mathscr{A}$ be the direct image sheaf of $\mathscr{A}$ under i. By general sheaf theory, this is a sheaf on $W^\vee$.

2.7.4 *Show that the stalk of $\mathscr{A}^\vee$ in a boundary point $\mathscr{U} \in W^\vee - W$ is isomorphic to the ultraproduct $\operatorname{ulim} A_w$ with respect to the non-principal ultrafilter $\mathscr{U}$.*

Prove the following reformulation of this result in terms of schemes, using 2.7.3 and the terminology from Chapter 3. As above, we let X be the affine scheme with coordinate ring the Boolen algebra $B := \mathscr{P}(W)$.

2.7.5 *Let $\mathscr{A}$ be a sheaf on X. If the tangent space at a point $x \in X$ is infinite, then the stalk $\mathscr{A}_x$ is an ultra-ring, given as the ultraproduct of the stalks $\mathscr{A}_y$ at points $y \in X$ having finite tangent space (with respect to the ultrafilter given as the image of x under the homeomorphism $X \cong W^\vee$). Show that the set of all points of X with infinite tangent space is a closed subset with ideal of definition given by the ideal of finite subsets.*

Part II
Toccata in C minor[3]

[3] Being a minor introduction into Commutative Algebra. . .

Chapter 3
Commutative Algebra versus Algebraic Geometry

Historically, algebraic geometry was developed over the complex numbers, $\mathbb{C}$. However, because of its algebraic nature, it can be carried out over any algebraically closed field. Therefore, in this chapter, we fix an algebraically closed field K, and we let $A := K[\xi]$ be the polynomial ring in n indeterminates $\xi := (\xi_1, \dots, \xi_n)$. We start with taking a look at classical or 'naive' algebraic geometry. Gradually we then move to an algebraization of the concepts (Hilbert-Noether theory, local properties, singularities, ...), which we will study subsequently by means of the algebraic theory developed in the next chapters. Obviously, this chapter can only be a summary treatment of the vast subject that is Algebraic Geometry. It is intended mainly to provide some background for the algebraic topics discussed later in these notes.

3.1 Classical algebraic geometry

Affine space. One defines *affine n-space* over K to be the topological space whose underlying set is K^n, and in which the closed sets are the algebraic sets. Recall that by an *algebraic set* we mean any solution set of a system of polynomial equations. More precisely, given a subset $\Sigma \subseteq A$, let $\mathrm{V}(\Sigma)$ be the collection of all tuples $\mathbf{u}$ such that $p(\mathbf{u}) = 0$ for all $p \in \Sigma$. Note that if $I := \Sigma A$ denotes the ideal generated by Σ, then $\mathrm{V}(I) = \mathrm{V}(\Sigma)$, so that in the definition, we may already assume that Σ is an ideal. In particular, if $p_1, \dots, p_s$ are generators of I, then $\mathrm{V}(I) = \mathrm{V}((p_1, \dots, p_s)A) = \mathrm{V}(p_1, \dots, p_s)$. A subset of the form $\mathrm{V}(I)$, for some ideal $I \subseteq A$, is then what is called an *algebraic* set (also called a *Zariski closed* subset). That this forms indeed a topology on K^n, called the *Zariski topology*, is an immediate consequence of the next lemma (the proof of which is deferred to the exercises):

Lemma 3.1.1. *Given ideals $I, J, I_n \subseteq A$, we have*

1. $\mathrm{V}(1) = \emptyset, \quad \mathrm{V}(0) = K^n$;
2. $\mathrm{V}(I) \cup \mathrm{V}(J) = \mathrm{V}(I \cdot J) = \mathrm{V}(I \cap J)$;
3. $\mathrm{V}(I_1) \cap \mathrm{V}(I_2) \cap \dots = \mathrm{V}(I_1 + I_2 + \dots)$,

where in the last equality, the intersection and the sum are allowed to be infinite as well.

Conversely, given a closed subset $V \subseteq K^n$, we define the *ideal of definition* of V, denoted $\mathfrak{I}(V)$, to be the collection of all $p \in A$ such that p is identical zero on V. We have:

3.1.2 *The set $\mathfrak{I}(V)$ is a radical ideal, $\mathrm{V}(\mathfrak{I}(V)) = V$, and $\mathfrak{I}(V)$ is maximal among all ideals I such that $\mathrm{V}(I) = V$.*

Recall that an ideal $I \subseteq R$ is called *radical* if $x^n \in I$ implies $x \in I$. This is equivalent with R/I being *reduced*, that is to say, without nilpotent elements. The *radical* of an ideal I, denoted $\operatorname{rad}(I)$, is the ideal of all $x \in R$ such that some power belongs to I. Immediately from 3.1.2 we get:

3.1.3 *Every singleton in K^n is closed, and its ideal of definition is a maximal ideal.*

Indeed, let $\mathbf{u} := (u_1, \dots, u_n) \in K^n$. Let $\mathfrak{m}_{\mathbf{u}}$ be the ideal in A generated by the linear polynomials $\xi_i - u_i$. One verifies that the "evaluation at $\mathbf{u}$" map $A \to K\colon p \mapsto p(\mathbf{u})$ is surjective and has kernel equal to $\mathfrak{m}_{\mathbf{u}}$. Hence $A/\mathfrak{m}_{\mathbf{u}} \cong K$, showing that $\mathfrak{m}_u$ is a maximal ideal. Clearly, $\mathrm{V}(\mathfrak{m}_{\mathbf{u}}) = \{\mathbf{u}\}$. □

Noetherian spaces. A topological space X is called *Noetherian* if there are no infinite strictly descending chains of closed subsets (one says: *X admits the descending chain condition on closed subsets*). A topological space X is called *irreducible* if it is not the union of two proper closed subsets. We call a subset $V \subseteq X$ *irreducible* if it so in the topology induced from X. An easy but important fact of Noetherian spaces is:

Proposition 3.1.4. *Any closed subset V of a Noetherian space X is a finite union of irreducible closed subsets.*

Proof. The argument is typical for Noetherian spaces, and often is therefore referred to as *Noetherian induction*. Namely, in a Noetherian space, every collection of closed subsets has a minimal element (prove this!). Now, if the assertion is false, let V be a minimal closed counterexample. In particular, V cannot be irreducible, and hence can be written as $V = V_1 \cup V_2$, with $V_1, V_2 \subsetneq V$ closed. By minimality, each V_i is a finite union of irreducible closed subsets, but then so is their union $V = V_1 \cup V_2$, contradiction. □

Hence any closed subset V admits an *irreducible decomposition* $V = V_1 \cup \cdots \cup V_s$ with the V_i irreducible closed subsets. We may always omit any V_i that is contained in some other V_j, and hence arrive at a *minimal* irreducible decomposition. One can show (see Exercise 3.6.2) that such a decomposition is unique (up to a renumbering of its components), and the V_i in this decomposition are then called the *irreducible components* of V.

Definition 3.1.5 (Dimension). The *dimension* of a Noetherian space X is the maximal length[1] of a chain of irreducible closed subsets (this can be infinite), and is denoted $\dim(X)$.

3.2 Hilbert-Noether theory

To develop (classical) algebraic geometry, three results are of crucial importance. We will prove them after first reformulating them as algebraic problems.

Hilbert's basis theorem. Hilbert proved the following result by a constructive method. We will provide a more streamlined version of this below.

Theorem 3.2.1. *Affine n-space is a Noetherian space of dimension n.*

In particular, any collection of Zariski closed subsets has a minimal element, any chain of irreducible Zariski closed subsets has length at most n, and any Zariski closed subset is the finite union of irreducible closed subsets. In order to prove Hilbert's basis theorem, we will translate it into an algebraic result (Theorem 3.3.5 below).

Nullstellensatz. We have already seen that a closed subset is given by an ideal as the locus $\mathrm{V}(I)$, and conversely, to a closed subset V is associated its ideal of definition $\mathfrak{I}(V)$. The next result, also due to Hilbert, describes the precise correspondence:

Theorem 3.2.2. *The operator $\mathfrak{I}(\cdot)$ induces an (order-reversing) bijection between (singletons of) K^n and maximal ideals of A; between closed subsets of K^n and radical ideals of A; and between irreducible closed subsets of K^n and prime ideals of A.*

More generally, if $V \subseteq K^n$ is a closed subset, and $I := \mathfrak{I}(V)$ its ideal of definition, then under the above correspondence, points in V correspond to maximal ideals containing I; closed subsets in V to radical ideals containing I; and irreducible closed subsets of V to prime ideals containing I.

Affine varieties and coordinate rings. The 'algebraic leap' to make now is that the three collections of ideals described in the second part of Theorem 3.2.2 correspond naturally to respectively the maximal, radical and prime ideals of the ring A/I (verify this!). We call A/I the *coordinate ring* of V and denote it $K[V]$ (see Exercise 3.6.4 for a justification of this notation). But this then again prompts us to view V as an object on its own, without immediate reference to its ambient affine space. Therefore, we will call any closed subset of K^n, for some n, an *affine variety*[2] over K, and we view it as a topological space via the induced topology.

---

[1] Whenever one talks about the *length of a chain* one means one less than the number of distinct sets in the chain.

[2] Be aware that some authors, unlike me, insist that varieties should also be irreducible.

The previous definition brings to the fore an algebraic object closely associated to a variety, to wit, its coordinate ring. To study it, we introduce some further terminology. By an *affine algebra* over K, or a K-*affine ring* or *algebra*, we mean a finitely generated K-algebra. Later on, we will work over other base rings than just fields, so it is apt to generalize this definition already now: let Z be an arbitrary ring. By a Z-*affine* ring or algebra we mean a finitely presented Z-algebra, that is to say, a Z-algebra of the form $Z[\xi]/I$ with ξ a finite tuple of indeterminates and I a finitely generated ideal. It follows from (the algebraic version of) Theorem 3.2.1 that both our definitions agree in the case Z is a field. If Z is moreover a local ring with maximal ideal $\mathfrak{p}$, then by a *local* Z-*affine* ring (or algebra) R we mean a localization of a Z-affine ring with respect to a prime ideal containing $\mathfrak{p}$, that is to say, $R \cong (Z[\xi]/I)_{\mathfrak{P}}$ with I finitely generated and $\mathfrak{P}$ a prime ideal of $Z[\xi]$ containing $\mathfrak{p}$. In particular, $Z \to R$ is a local homomorphism. By a *homomorphism* of Z-affine rings $A \to B$, we mean a Z-algebra homomorphism making B into an A-affine algebra (that is to say, the homomorphism $A \to B$ itself is of *finite type*). Similarly, by a *local homomorphism* of local Z-affine rings $R \to S$, we mean a local homomorphism of Z-algebras making S into a local R-affine ring (such a homomorphism is also said to be *essentially of finite type*).

Returning to our discussion about coordinate rings, we see that each $K[V]$ is a reduced K-affine ring. In Exercise 3.6.6, you will show that every reduced K-affine ring arises as a coordinate ring, and that different affine varieties have different coordinate rings. Hence we established the following 'duality' between geometric and algebraic objects:

3.2.3 *Associating the coordinate ring to an affine variety yields a one-one correspondence between affine varieties over* K *and reduced* K*-affine rings.*

To make this into an equivalence of categories, we must define morphisms between affine varieties. First off, a *morphism* between affine spaces is a polynomial map $\phi\colon K^n \to K^m$, that is to say, a map given by m polynomials $p_1(\xi),\dots,p_m(\xi) \in A$, sending an n-tuple $\mathbf{u}$ to the m-tuple

$$\phi(\mathbf{u}) := (p_1(\mathbf{u}),\dots,p_m(\mathbf{u})).$$

Note that ϕ also induces a K-algebra homomorphism $\varphi\colon B \to A$ by mapping ζ_i to p_i, where $B :=: K[\zeta]$ and $\zeta := (\zeta_1,\dots,\zeta_m)$ are the indeterminates on K^m. Now, let V and W be affine varieties, that is to say, V is a closed subset of K^n and W a closed subset of K^m, say. Then a *morphism* $V \to W$ is the restriction of a polynomial map $\phi\colon K^n \to K^m$ for which $\phi(V) \subseteq W$, which we will just denote again as $\phi\colon V \to W$. Let $I := \mathfrak{I}(V) \subseteq A$ and $J := \mathfrak{I}(W) \subseteq B$ be the respective ideals of definition. We already noticed that ϕ induces a K-algebra homomorphism $\varphi\colon B \to A$. One verifies that if $\phi\colon V \to W$ is a morphism, then $\varphi(J) \subseteq I$, so that we get an induced K-algebra homomorphism $K[W] = B/J \to K[V] = A/I$. With this notion of morphism, 3.2.3 gives an anti-equivalence of categories ('anti' since the morphisms $V \to W$ yield homomorphisms $K[W] \to K[V]$ going the other way). An *isomorphism* of affine varieties, as always, is a morphism admitting an inverse which is also a morphism. It follows that $V \to W$ is an isomorphism if and only if so is the K-algebra homomorphism $K[W] \to K[V]$.

The *Krull dimension* of a ring R is by definition the maximal length of a chain of prime ideals in R (see §4.1). Using Theorem 3.2.2, we therefore get:

Corollary 3.2.4. *For every affine variety V, its dimension is equal to the Krull dimension of its coordinate ring $K[V]$.* □

Noether normalization. To formulate the last of our 'great' theorems, we call a morphism of affine varieties $V \to W$ *finite* if the induced homomorphism $K[W] \to K[V]$ is finite (meaning that $K[V]$ is finitely generated as a module over $K[W]$).

Theorem 3.2.5. *Each variety V admits a finite and surjective morphism onto some affine space K^d.*

Proof. We will actually prove the slightly stronger algebraic form of this statement: any K-affine ring C (not necessarily reduced) admits a finite and injective homomorphism $K[\zeta_1,\dots,\zeta_d] \subseteq C$ (see 4.3.7 below). We prove this by induction on n, the number of variables ξ used to define C. Write C as A/I for some ideal I with $A := K[\xi]$. There is nothing to show if I is zero, so assume f is a non-zero polynomial in I. The trick is to find a change of coordinates such that f becomes monic in the last coordinate ξ_n, that is to say, when viewed as a polynomial in $A'[\xi_n]$, the highest degree term of f is equal to ξ_n^s, where $A' := K[\xi']$ and $\xi' := (\xi_1,\dots,\xi_{n-1})$. Such a change of coordinates does indeed exist (Exercise 3.6.23), and in fact, can be taken to be linear in case K is infinite (which is the case if K is algebraically closed). So we may assume f is monic in ξ_n of degree s. By Euclidean division in $A'[\xi_n]$, any polynomial g can be written as $g = fq + r$ with $q, r \in A$ such that the ξ_n-degree of r is at most $s-1$. This means that A/fA is generated as an A'-module by $1, \xi_n, \dots, \xi_n^{s-1}$. Let $I' := I \cap A'$. It follows that the extension $A'/I' \subseteq A/I$ is again finite. By induction, A'/I' is a finite $K[\zeta]$-module for some tuple of variables $\zeta := (\zeta_1,\dots,\zeta_d)$. Hence the composition $K[\zeta] \subseteq A'/I' \subseteq A/I = C$ is the desired *Noether normalization* of C. □

We will see later (in Corollary 4.3.9) that d is actually equal to the dimension of V. In particular, this then proves the second statement in Theorem 3.2.1 (see also Corollary 4.3.3); the first statement will be covered in Theorem 3.3.5 below. One calls a surjective morphism of affine varieties sometimes a *cover*, and hence we may paraphrase the above result as: *an affine variety has dimension d if and only if it is a finite cover of some affine d-space.*

Next, we prove the Nullstellensatz. We start with:

Corollary 3.2.6 (Weak Nullstellensatz). *If $E \subseteq F$ is an extension of fields such that F is finitely generated as an E-algebra, then $E \subseteq F$ is a finite extension.*

Proof. By Theorem 3.2.5, we can find a finite, injective homomorphism $E[\zeta] \subseteq F$. The result now follows from Lemma 3.2.7, since the only way $E[\zeta]$ can be a field is for ζ to be the empty tuple of variables, showing that $E \subseteq F$ itself is finite, as claimed. □

Lemma 3.2.7. *If $R \subseteq F$ is a finite, injective homomorphism (or more generally, an integral extension) with F a field, then R is also a field.*

Proof. Let a be a non-zero element of R. By assumption, $1/a \in F$ is integral over R, whence satisfies an equation

$$(1/a)^d + r_1(1/a)^{d-1} + \cdots + r_d = 0$$

with $r_i \in R$. Multiplying with a^d, we get $1 + a(r_1 + r_2 a + \cdots + r_d a^{d-1}) = 0$, showing that a has an inverse in R. □

Proof of the Nullstellensatz, Theorem 3.2.2

We already observed (in 3.1.3) that $\mathfrak{I}(\mathbf{u}) = \mathfrak{m}_{\mathbf{u}}$ is a maximal ideal of A. So we need to prove conversely that any maximal ideal of A is realized in this way. Let $\mathfrak{m}$ be a maximal ideal. By Corollary 3.2.6, the field $A/\mathfrak{m}$ is a finite extension of K, and since K is algebraically closed, it must in fact be equal to it. If u_i denotes the image of ξ_i under the composition $A \to A/\mathfrak{m} \cong K$, then $\mathfrak{m}_{\mathbf{u}} \subseteq \mathfrak{m}$ for $\mathbf{u} := (u_1, \dots, u_n)$, whence both ideals must be equal as they are maximal. This proves the one-one correspondence between K^n and the maximal ideals of A. By 3.1.2, the operator $\mathfrak{I}$ is injective. To prove it is surjective, we have to show that $I = \mathfrak{I}(\mathrm{V}(I))$ for any radical ideal $I \subseteq A$. In fact, the stronger equality

$$\mathfrak{I}(\mathrm{V}(I)) = \mathrm{rad}(I), \tag{3.1}$$

holds for any ideal $I \subseteq A$. Equality (3.1) translates (do this!) into the fact that $\mathrm{rad}(I)$ is equal to the intersection of all maximal ideals containing I. Replacing A by $A/\mathrm{rad}(I)$, we reduce to showing that the Jacobson radical of a reduced K-affine ring C is zero (one says that C is a *Jacobson* ring), where the *Jacobson radical* of C is by definition the intersection of all of its maximal ideals. This amounts to showing that given any non-zero element f of C, there exists a maximal ideal not containing f. By Theorem 3.2.5, we can find a finite, injective homomorphism $B := K[\zeta] \subseteq C$. Let

$$f^s + b_1 f^{s-1} + \cdots + b_s = 0 \tag{3.2}$$

be an integral equation of minimal degree with all $b_i \in B$. By minimality, $b_s \neq 0$. By Exercise 3.6.23, there exists $\mathbf{v}$ such that $b_s(\mathbf{v}) \neq 0$. In other words, $\mathfrak{m}_{\mathbf{v}}$ is a maximal ideal of B not containing b_s. Since $\mathfrak{m}_{\mathbf{v}}C$ is not the unit ideal by Nakayama's Lemma, we can find a maximal ideal $\mathfrak{m}$ of C containing $\mathfrak{m}_{\mathbf{v}}$. In particular, $\mathfrak{m}_{\mathbf{v}} \subseteq \mathfrak{m} \cap B$ and hence this must be an equality by maximality. In particular, it follows then from (3.2) that $f \notin \mathfrak{m}$.

This establishes the one-one correspondence between closed subsets and radical ideals. In Exercise 3.6.2 you are asked to show that $\mathfrak{I}(V)$ is a prime ideal if and only if V is irreducible. This then concludes the proof of the first part of Theorem 3.2.2. The second part, however, simply follows from this by identifying ideals of A/I with the ideals of A containing I. □

3.3 Affine schemes

There are several motivations for generalizing the classical perspective, by introducing a larger class of 'geometric' objects. Let us look at two of these motivations.

Generic points. Firstly, geometers often reason by 'general' or 'generic' points. They will for instance say that a "general point on a variety is non-singular" (see 3.5.5 below for the exact meaning of this phrase). But what is a 'generic' point? We can give a topological definition:

Definition 3.3.1 (Generic point). A point x of an irreducible topological space X is called *generic* if the closure of $\{x\}$ is all of X.

More generally, for X an arbitrary Noetherian topological space, one calls $x \in X$ generic, if its closure (or more accurately, the closure of the singleton determined by x) is an irreducible component (see page 28) of X.

In view of 3.1.3, the only closed subsets of K^n having a generic point are the singletons themselves. So how do we get generic points? There is a simple topological construction. Given a Noetherian space X, let $\mathfrak{Irr}(X)$ be the collection of all irreducible closed subsets of X. Define a topology on $\mathfrak{Irr}(X)$ by taking for closed subsets the sets of the form $\mathfrak{Irr}(V)$ for $V \subseteq X$ closed. There is a continuous map $X \to \mathfrak{Irr}(X)$ sending a point $x \in X$ to its closure (note that the closure of a singleton is always irreducible). Exercise 3.6.7 explores how this creates plenty of generic points.

If we apply this construction to K^n, then by Theorem 3.2.2, the resulting space $\mathfrak{Irr}(K^n)$ is equal to $|\mathrm{Spec}(A)|$, the collection of all prime ideals of A.[3] A (*Zariski*) closed subset of $|\mathrm{Spec}(A)|$ is then a closed subset in the above defined topology, and hence is of the form $\mathrm{V}(I)$, for some ideal I, where $\mathrm{V}(I)$ denotes the collection of all prime ideals containing I. In particular, if $\mathfrak{p}$ is a prime ideal, then $\mathfrak{p}$ is the unique generic point of $\mathrm{V}(\mathfrak{p})$.

More generally, given a ring R, let $|\mathrm{Spec}(R)|$ be the collection of all its prime ideals and make this into a topological space by taking for closed subsets the $\mathrm{V}(I)$ for $I \subseteq R$. Note that each $\mathrm{V}(I)$ is naturally identified with $|\mathrm{Spec}(R/I)|$, and often we will equate both subsets. That this forms indeed a topology, the so-called *Zariski topology*, follows by the same argument that proves Lemma 3.1.1. We call $\mathfrak{Irr}(K^n)$ the *enhanced affine n-space*. It has a unique generic point given by the zero ideal (check this). This extends by Theorem 3.2.2 to any affine variety:

3.3.2 *Given an affine variety V with coordinate ring $K[V]$, the space $\mathfrak{Irr}(V)$ is homeomorphic to $|\mathrm{Spec}(K[V])|$, where the latter carries the Zariski topology. The generic points of the* enhanced affine variety $\mathfrak{Irr}(V)$ *then correspond to the minimal primes of $K[V]$.*

Henceforth, we will therefore identify $\mathfrak{Irr}(V)$ with $|\mathrm{Spec}(K[V])|$. The canonical map $V \to \mathfrak{Irr}(V) = |\mathrm{Spec}(K[V])|$ is given by identifying a point $\mathbf{u} \in V$ with its (maximal) ideal of definition $\mathfrak{m}_{\mathbf{u}}$; it is easily seen to be injective. A point in $|\mathrm{Spec}(K[V])|$ coming from V is called a *closed* point. Indeed, these are the only points which are equal to their closure. Note that the intersection of the minimal primes of $K[V]$ is equal to the zero ideal (recall that $K[V]$ is reduced). At this point, there is no need to stick to K-affine rings, and so we call any topological space of the form $|\mathrm{Spec}(R)|$

[3] The reason for the awkward notation will become clear in the next section.

with R any ring, an *enhanced affine variety*. A *closed* point then corresponds to a maximal ideal of R; and a generic point to a minimal prime.

Base change Coming back to our discussion of generic points, 3.3.2 shows that every enhanced affine variety has only finitely many generic points, which is not what we would expect of a 'general' point. To get around this obstruction, we need to work over a larger algebraically closed field L containing K. The *base change* of an affine variety V over K to L is defined as the (Zariski) closure V_L of V in L^n. One shows (Exercise 3.6.10) that if V has ideal of definition $I \subseteq A$, then $IL[\xi]$ is the ideal of definition of V_L. In particular, V_L is an affine variety over L, and its coordinate ring is

$$L[V_L] = L[\xi]/IL[\xi] = K[V] \otimes_K L.$$

We use:

3.3.3 *If $R \to S$ is a (ring) homomorphism, then $|\mathrm{Spec}(S)| \to |\mathrm{Spec}(R)|$ given by the rule $\mathfrak{q} \mapsto \mathfrak{q} \cap R$ is a continuous map of topological spaces.*

Note that we have used the slightly misleading notation $J \cap R$ for the *contraction* of an ideal $J \subseteq S$ to R (even if R is not a subset of S); by definition $J \cap R$ is the ideal of all $r \in R$ such that the image of r in S lies inside J. Hence if φ denotes the homomorphism $R \to S$, then $J \cap R$ is actually $\varphi^{-1}(J)$. Returning to our discussion on generic points, the natural homomorphism $K[\xi] \to L[\xi]$ (called the *base change*) induces a homomorphism $K[V] \to L[V_L]$, whence a map of enhanced affine varieties

$$\mathfrak{Irr}(V_L) = |\mathrm{Spec}(L[V_L])| \to \mathfrak{Irr}(V) = |\mathrm{Spec}(K[V])|.$$

Now, a point $\mathbf{v} \in V_L$ is *generic with respect to K* if its image under the above map is a generic point of $\mathfrak{Irr}(V)$. This is equivalent with $\mathfrak{m}_{\mathbf{v}} \cap K[V]$ being a minimal prime of $K[V]$.

Example 3.3.4. The point with coordinates (e, π) is (probably) a generic point of the affine plane over $\mathbb{Q}^{\mathrm{alg}}$. Similarly, the point $(0, \pi)$ is a generic point over $\mathbb{Q}^{\mathrm{alg}}$ of the y-axis.

Using 3.3.2, we can now also prove Theorem 3.2.1 as it translates immediately to the following algebraic result (recall that a ring is *Noetherian* if there exists no infinite strictly ascending chain of ideals, or equivalently, if every ideal is finitely generated):

Theorem 3.3.5 (Hilbert Basis Theorem–algebraic form). *The polynomial ring A over a field K in n variables is Noetherian.*

Proof. We induct on n, where the case $n = 0$ is trivial, so that we may assume $n > 0$. Let $\mathfrak{a}$ be a non-zero ideal of A and let $f \in \mathfrak{a}$ be non-zero. By Theorem 3.2.5, there exists a finite extension $B := K[\zeta] \subseteq A/fA$, where ζ is a tuple of variables of length at most $n-1$ (and in fact equal to $n-1$). By induction, B is Noetherian. Since A/fA is a finite B-module, it too is Noetherian (see for instance [7, Proposition 6.5]). In particular, $\mathfrak{a}(A/fA)$ is finitely generated, and hence so is $\mathfrak{a}$ (by the liftings of the generators of $\mathfrak{a}(A/fA)$ together with f). □

Nilpotent structure. A second draw-back of the classical approach is that if we intersect two closed subsets, the resulting closed subset does not take into account the finer structure of this intersection. For instance, a circle C in the affine plane with radius one and center $(0,1)$ intersects the x-axis L in a single point, the origin O. However, if we look at equations (or, equivalently, ideals of definitions), where C is given by $I := (\xi^2 + \zeta^2 - 2\zeta)A$, and L by $J := \zeta A$, then we get a system of equations which reduces to $\xi^2 = 0, \zeta = 0$ (equivalently, the ideal $I + J = (\xi^2, \zeta)A$), which suggests that we should count the intersection point O twice (accounting for the tangency of L to C). Hence, instead of looking at the ideal $\mathrm{rad}(I+J) = \mathrm{rad}(\xi^2, \zeta) = (\xi, \zeta)A$, or equivalently, to the coordinate ring $K[O] = A/(\xi, \zeta)A = K$, we should not 'forget' the nilpotent structure of $A/(I+J)$. However, enhanced affine varieties cannot capture this phenomenon. Namely, if B is an arbitrary K-affine ring, then as a topological spaces $|\mathrm{Spec}(B)|$ and $|\mathrm{Spec}(B_{\mathrm{red}})|$ are homeomorphic, where $B_{\mathrm{red}} := B/\mathrm{nil}(B)$ and $\mathrm{nil}(B) := \mathrm{rad}(0)$ is the *nil-radical* of B. In particular, $|\mathrm{Spec}(A/(I+J))|$ and $|\mathrm{Spec}(K)|$ are the same. To resolve this problem, we have to resort to a finer structure, that of an (affine) scheme. Roughly speaking, an affine scheme is an enhanced affine variety X together with a sheaf of functions $\mathscr{O}_X$. I will only provide a sketch of the general definitions. To this end, we must first discuss Zariski open subsets.

Open subsets. Let R be a ring and f an element in R. The localization of R at f, denoted R_f or $R[1/f]$, is the ring $R[\xi]/(f\xi - 1)R[\xi]$ obtained by inverting f (this includes the degenerate case that f is zero, or, more generally, nilpotent, in which case R_f is the zero ring). Equivalently, it is the collection of all fractions r/f^n with $r \in R$ up to the equivalence relation identifying two fractions r/f^n and s/f^m, if there exists some k such that $f^{k-n}r = f^{k-m}s$ in R. This definition becomes much more straightforward if we assume $f \neq 0$ and R to be a domain: R_f is then the subring of the field of fractions $\mathrm{Frac}(R)$ of R consisting of all fractions r/f^n with $r \in R$. Let $V := |\mathrm{Spec}(R)|$ be an enhanced affine variety and let $f \in R$. Let $\mathrm{D}(f)$ be the complement of the closed subset $\mathrm{V}(fR) = |\mathrm{Spec}(R/fR)|$ of V. We refer to $\mathrm{D}(f)$ as a *basic* open subset. Indeed, given an arbitrary open subset U, say given as the complement of a closed subset $\mathrm{V}(I)$, we have

$$U = V - \mathrm{V}(I) = \bigcup_{f \in I} \mathrm{D}(f). \tag{3.3}$$

In particular, if R is Noetherian, then any open subset is a finite union of basic open subsets.

3.3.6 *The basic open* $\mathrm{D}(f)$ *is homeomorphic with* $\left|\mathrm{Spec}(R_f)\right|$, *whence in particular is an enhanced affine variety.*

See Exercise 3.6.15. Note that not every open subset can be realized as an (enhanced) affine variety: for instance the plane with the origin removed is an open which is not affine (see Exercise 3.6.5). Here is an example of a basic open subset with some additional structure.

Example 3.3.7. Let $\mathrm{GL}(K,n)$ be the *general linear group* consisting of all invertible $n \times n$-matrices over K. If we identify an $n \times n$-matrix with a tuple in K^{n^2}, then $\mathrm{GL}(K,n)$ is the open subset $\mathrm{D}(\det)$, where $\det(\cdot)$ is the polynomial representing the determinant function. In particular, we may view $\mathrm{GL}(K,n)$ as an enhanced affine variety. In Exercise 3.6.16, you will show that the multiplication map $\mathrm{GL}(K,n) \times \mathrm{GL}(K,n) \to \mathrm{GL}(K,n)$ is a morphism, and so is the map sending a matrix to its inverse.

Sections. To define sections, let us first look at these on an affine variety $V \subseteq K^n$. We already observed that any $f \in K[V]$ induces a function $\sigma_f \colon V \to K \colon \mathbf{u} \mapsto f(\mathbf{u})$. We call such a map a *section* on V. If f is identically zero, or more generally, if $f \in \mathfrak{I}(V)$, then σ_f is just the zero section. So assume $f \notin \mathfrak{I}(V)$, that is to say, f is non-zero in $K[V]$. If $f(\mathbf{u}) \neq 0$, then $1/f(\mathbf{u})$ is defined. Hence $1/f$ can be viewed as a section on $\mathrm{D}(f) \cap V$. More generally, we see that every element of R_f is a section on $\mathrm{D}(f)$.

For an arbitrary enhanced affine variety $V := |\mathrm{Spec}(R)|$, the definition of a section is more involved. We need a definition:

Definition 3.3.8 (Residue field). Given a point $x \in V$ with corresponding prime ideal $\mathfrak{p}_x \subseteq R$, its *residue field* $\kappa(x)$ is by definition the field of fractions of the domain $R/\mathfrak{p}_x$.

Note that if R is a K-affine ring, and x a closed point, then $\kappa(x) = K$ by Theorem 3.2.2. However, in general the various residue fields are no longer the same (they even may have different characteristic; see Exercise 3.6.12). Hence we cannot expect a section to take values in a fixed field. Let $Q(V)$ be the disjoint union of all $\kappa(x)$ where x runs over all points $x \in V$.

A (*reduced*) *section* $\sigma \colon V \to Q(V)$ is a map such that $\sigma(x) \in \kappa(x)$ for every point $x \in V$. Let us denote the collection of all sections on an enhanced affine variety V by $\mathrm{Sect}(V)$, which we may view as a ring, since we can add and multiply sections. Any element $f \in R$ induces a section σ_f on V, simply by letting $\sigma_f(x)$ be the image of f in $\kappa(x)$. More generally, any element of R_f induces a section on $\mathrm{D}(f)$, since f is invertible in $\kappa(x)$ for $x \in \mathrm{D}(f)$. In particular, we have a homomorphism $R_f \to \mathrm{Sect}(\mathrm{D}(f))$. However, in general this map can have a kernel (see Exercise 3.6.15):

3.3.9 *The kernel of $R \to \mathrm{Sect}(|\mathrm{Spec}(R)|)$ is the nil-radical of R.*

To define a scheme structure on V, we now have to declare, for each open subset $U \subseteq V$, which sections are to be viewed as 'continuous' sections on U. But we also want to incorporate nilpotent elements, which are 'invisible' in $\mathrm{Sect}(U)$ by 3.3.9. So for each open U, we define a ring $\Gamma(U, \mathscr{O}_V)$ (also denoted $\mathscr{O}_V(U)$) and a surjective homomorphism $\Gamma(U, \mathscr{O}_V) \to \mathrm{Sect}(U)$. Without given all the details, we declare $\Gamma(V, \mathscr{O}_V)$ to be R (the so-called *global sections* of V), and we put

$$\Gamma(\mathrm{D}(f), \mathscr{O}_V) := R_f \tag{3.4}$$

(note that the first case is just a special case of (3.4), by taking $f = 1$). For each open U the elements of $\Gamma(U, \mathscr{O}_V)$ are still called *sections* on U (in fact, this is the correct terminology in view of our discussion below on page 45).

Sheafs.

Of course, the sections on the various open subsets of V have to be related to one another. The correct definition is that $\mathscr{O}_V$ has to be a *sheaf* on X. In general, a *sheaf of rings* (or of groups, sets, ...) $\mathscr{A}$ on a topological space X is a functor associating to each open subset $U \subseteq X$ a ring (group, set, etc.) $\mathscr{A}(U)$ (also denoted $\Gamma(U, \mathscr{A})$), and to each inclusion $U \subseteq U'$ a *restriction homomorphism* sending $f \in \mathscr{A}(U')$ to an element $f|_U \in \mathscr{A}(U)$ (being a *functor* means, among other things, that if $U \subseteq U' \subseteq U''$ then the composition of the restriction maps $\mathscr{A}(U'') \to \mathscr{A}(U') \to \mathscr{A}(U)$ is equal to the restriction map $\mathscr{A}(U'') \to \mathscr{A}(U)$), satisfying the following two additional properties for every open subset $U \subseteq X$ and every open covering $\{U_i\}$ of U:

1. if $f, g \in \mathscr{A}(U)$ are such that their restriction to each U_i is the same, then $f = g$;
2. if $f_i \in \mathscr{A}(U_i)$ are given such that the restriction of f_i and f_j to $U_i \cap U_j$ coincide, for all i, j, then there exists $f \in \mathscr{A}(U)$ such that $f|_{U_i} = f_i$ for all i.

One can show that there exists a unique sheaf $\mathscr{O}_V$ on $V = |\mathrm{Spec}(R)|$ for which conditions (3.4) hold, that is to say, such that $\Gamma(\mathrm{D}(f), \mathscr{O}_V) = R_f$. Moreover, each $g \in \Gamma(U, \mathscr{O}_V)$ then induces a section on U, that is to say, we have a homomorphism $\Gamma(U, \mathscr{O}_V) \to \mathrm{Sect}(U)$. In fact, this gives rise to a natural transformation $\Gamma(\cdot, \mathscr{O}_V) \to \mathrm{Sect}(\cdot)$ of functors. For the 'official' definition of $\mathscr{O}_V$, see page 45 below.

The category of affine schemes. An *affine scheme* $X = \mathrm{Spec}(R)$, therefore, is an enhanced affine variety $|\mathrm{Spec}(R)|$ (with R an arbitrary ring) together with a sheaf of sections $\mathscr{O}_X$ on $|\mathrm{Spec}(R)|$ satisfying (3.4), called the *structure sheaf* of X. Note that we can recover R from its associated affine scheme as the ring of global sections $R = \Gamma(X, \mathscr{O}_X)$. We often refer to R still as the *coordinate ring* of X. A *morphism* $Y \to X$ between affine schemes $X := \mathrm{Spec}(R)$ and $Y := \mathrm{Spec}(S)$ is given by a ring homomorphism $R \to S$: it induces a continuous map $\phi\colon\ |\mathrm{Spec}(S)| \to |\mathrm{Spec}(R)|$ by 3.3.3, as well as ring homomorphisms $\mathscr{O}_X(U) \to \mathscr{O}_Y(\phi^{-1}(U))$, for every open $U \subseteq |\mathrm{Spec}(R)|$. To define the latter, it suffices to do this on a basic open subset $\mathrm{D}(f)$, where it just the induced homomorphism $R_f \to S_f$, for any $f \in R$. Observe that $\varphi^{-1}(\mathrm{D}(f))$ is the basic open subset $\mathrm{D}(f)$ in $|\mathrm{Spec}(S)|$. In particular, on X, the induced ring homomorphism between global sections is the original homomorphism $R \to S$. Moreover, these homomorphisms are compatible with the restriction maps. The morphism $Y \to X$ is called of *finite type* if the corresponding homomorphism $A \to B$ is of finite type, that is to say, if B is finitely generated as an A-algebra. Note that any K-affine ring R induces a morphism $X := \mathrm{Spec}(R) \to \mathrm{Spec}(K)$ of finite type, sometimes called the *structure map* of X. Note that the underlying set of $\mathrm{Spec}(K)$ is just a singleton, and hence $|X| \to |\mathrm{Spec}(K)|$ is the trivial map. One additional advantage to this formalism is that there is no need anymore to have K algebraically closed: we can define affine schemes of finite type over any field. Generalizing 3.2.3 we now get:

3.3.10 *Associating to an affine scheme X its ring of global sections $\Gamma(X, \mathscr{O}_X)$ induces an anti-equivalence of categories between the category of affine schemes and the category of rings. Under this anti-equivalence, affine schemes of finite type over a field K correspond to K-affine rings.*

Here is one more reason why we should work with the enhanced space of all prime ideals of a ring, not just its maximal ideals: namely, in general the contraction of a maximal ideal, although prime, need not be maximal. For instance in $K[[\xi]][\zeta]$ the ideal generated by $\xi\zeta - 1$ is maximal as its residue ring is the field $K((\xi))$ of Laurent series. However, its contraction to $K[[\xi]]$ is the zero ideal. In classical algebraic geometry, this complication however is absent:

Proposition 3.3.11. *If $Y \to X$ is a morphism of finite type of affine schemes of finite type over K, then the image of a closed point is again closed.*

Proof. The algebraic translation says that if $C \to D$ is a K-algebra homomorphism of K-affine rings, and if $\mathfrak{n} \subseteq D$ is a maximal ideal, then so is $\mathfrak{m} := \mathfrak{n} \cap C$. To prove this, note that $D/\mathfrak{n}$ is again a K-affine ring, whence $K \subseteq D/\mathfrak{n}$ is finite by Corollary 3.2.6. Since $A/\mathfrak{m}$ is a subring of $D/\mathfrak{n}$, it is also finite over K, whence an Artinian domain, or, in other words, a field. □

Intersections of closed subschemes. Returning to our discussion on intersections, the correct way of viewing the intersection of two affine varieties $V, W \subseteq K^n$ with respective ideals of definition $I := \mathfrak{I}(V)$ and $J := \mathfrak{I}(W)$ is as the affine scheme $\mathrm{Spec}(A/(I+J))$. To define this also for arbitrary affine schemes, we must make precise what it means to be a 'subscheme'. The next result gives an indication of what this should mean (its proof is relegated to Exercise 3.6.17).

Lemma 3.3.12. *Let $X := \mathrm{Spec}(R)$ be an affine scheme and let V be a closed subset of $|X|$. If $I \subseteq R$ is an ideal such that $\mathrm{V}(I) = V$, then $\mathrm{Spec}(R/I)$ is an affine scheme with underlying set equal to V.*

The 'smallest' scheme structure on V is given by the ideal $\mathscr{I}(V)$ obtained by intersecting all prime ideals in V. More precisely, if Y is an affine scheme with $|Y| = V$, then there exists an injective morphism $\mathrm{Spec}(R/\mathscr{I}(V)) \to Y$. □

One refers to $\mathrm{Spec}(R/\mathscr{I}(V))$ as the *induced reduced scheme structure* on V. Note that $\mathscr{I}(V)$ is a radical ideal, and that any ideal I such that $\mathrm{V}(I) = V$ satisfies $\mathrm{rad}(I) = \mathscr{I}(V)$. More generally, we define a *closed subscheme* of an affine scheme $X := \mathrm{Spec}(R)$ as an affine scheme of the form $Y := \mathrm{Spec}(R/I)$, for some ideal $I \subseteq R$. By the previous lemma, the underlying set $|Y|$ is a closed subvariety of the underlying set $|X|$. Moreover, the inclusion $Y \subseteq X$ is a morphism of affine schemes, called a *closed immersion*. In analogy with vector spaces, we call the collection of all closed subschemes of an affine scheme X the *Grassmanian* of X and denote it $\mathrm{Grass}(X)$. We can define a (partial) order on $\mathrm{Grass}(X)$ by letting $Y \subseteq Z$ stand for 'Y is a closed subscheme of Z'. It is important to note that in spite of the notation, $Y \subseteq Z$ does not just mean an inclusion of underlying sets. In fact, if I and J are the ideals of R such that $Y = \mathrm{Spec}(R/I)$ and $Z = \mathrm{Spec}(R/J)$, then $Y \subseteq Z$ if and only if $J \subseteq I$. For this reason, we also define the *Grassmanian* $\mathrm{Grass}(R)$ of a ring R as the collection of all its ideals, ordered by reverse inclusion. Hence there is a one-one correspondence between $\mathrm{Grass}(R)$ and $\mathrm{Grass}(\mathrm{Spec}(R))$.

Given two closed subschemes $Y_k := \mathrm{Spec}(R/I_k)$ of X, for $k = 1,2$, we now define their *scheme-theoretic intersection* $Y_1 \cap Y_2$ as the closed subscheme $\mathrm{Spec}(R/(I_1 + I_2))$. In particular, $Y_1 \cap Y_2 \subseteq Y_1, Y_2$. In fact, intersection is the minimum (or join) operation in the Grassmanian $\mathrm{Grass}(X)$. Note that we have an identity

$$R/(I_1+I_2) \cong R/I_1 \otimes_R R/I_2.$$

This prompts a further definition:

Fiber products. Given two morphisms of affine schemes $Y_1 \to X$ and $Y_2 \to X$, we define the *fiber product* of Y_1 and Y_2 over X to be the affine scheme

$$Y_1 \times_X Y_2 := \operatorname{Spec}(S_1 \otimes_R S_2)$$

where $R = \Gamma(\mathscr{O}_X, X)$ and $S_k = \Gamma(Y_k, \mathscr{O}_{Y_k})$ are the corresponding rings. By Exercise 3.6.26, the fiber product is in fact a product (in the categorical sense) on the category of affine schemes over X (see below for more on this category). Note that our previous definition of scheme-theoretic intersection is a special case, where the two morphisms are just the closed immersions $Y_k \subseteq X$. Put differently, the intersection of two closed subschemes $Y_k \subseteq X$ is just their fiber product:

$$Y_1 \cap Y_2 = Y_1 \times_X Y_2.$$

Relative schemes.

The formalism of schemes immediately allows one to relativize the notion of a scheme in the following sense. Let Z be a ring. An *affine scheme over* Z or *affine* Z*-scheme* is then simply an affine scheme $\operatorname{Spec}(R)$ given by a Z-algebra R, together with the canonical morphism $\operatorname{Spec}(R) \to \operatorname{Spec}(Z)$ (induced by the natural homomorphism $Z \to R$). A *morphism* of affine Z-schemes $\operatorname{Spec}(S) \to \operatorname{Spec}(R)$, for some Z-algebra S, is then determined by a Z-algebra homomorphism $R \to S$. Note that this gives rise to a commutative diagram

$$\begin{tikzcd} & \operatorname{Spec}(Z) \arrow[dl] \arrow[dr] & \\ \operatorname{Spec}(S) \arrow[rr] & & \operatorname{Spec}(R) \end{tikzcd} \tag{3.5}$$

of morphisms of affine schemes. Of course, if we take $Z = \mathbb{Z}$, we recover the category of all affine schemes (since any ring homomorphism is a $\mathbb{Z}$-algebra homomorphism). We say that an affine scheme $\operatorname{Spec}(R)$ is of *finite type* over Z, if the morphism $\operatorname{Spec}(R) \to \operatorname{Spec}(Z)$ is of finite type, that is to say, if R is of the form $Z[\xi]/I$ for some finite tuple of indeterminates ξ and some ideal I. Recall that we called such an algebra Z-affine if I is moreover finitely generated. This double usage of the term 'affine' will hopefully not cause too much confusion.

Fibers. A morphism of affine schemes $\phi\colon Y \to X$ can also be viewed as a family of affine schemes: for each point $x \in X$, the *fiber* $\phi^{-1}(x)$ admits the structure of an affine scheme as follows. If $R \to S$ is the corresponding ring homomorphism and $\mathfrak{p}$ the prime ideal corresponding to x, then

$$\phi^{-1}(x) \cong |\operatorname{Spec}(S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}})|. \tag{3.6}$$

In view of this, we call $\mathrm{Spec}(S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}})$ the (*scheme-theoretic*) *fiber* of ϕ at $\mathfrak{p}$. Reformulated in the terminology of fiber products, (3.6) says that

$$\phi^{-1}(x) = Y \times_X \mathrm{Spec}(\kappa(x)) \tag{3.7}$$

(recall that $\kappa(x)$ is the residue field of x); see Exercise 3.6.13 for the proofs.

Example 3.3.13. The family of all circles is encoded by the following morphism. Let Y be the *hypersurface* in $\mathbb{A}^5_K$ given by the equation

$$p := (\xi - u)^2 + (\zeta - v)^2 - w^2 = 0,$$

let $X := \mathbb{A}^3_K$, and let $\phi\colon Y \to X$ be induced by the projection $K^5 \to K^3\colon \mapsto (\xi, \zeta, u, v, w) \mapsto (u, v, w)$, that is to say, given by the natural K-algebra homomorphism

$$K[u, v, w] \to K[\xi, \zeta, u, v, w]/pK[\xi, \zeta, u, v, w].$$

If P is a closed point of X corresponding to a triple $(a, b, r) \in K^3$, that is to say, given by the maximal ideal $\mathfrak{m}_P = (u - a, v - b, w - r)K[u, v, w]$, then $\phi^{-1}(P)$ is isomorphic to the circle with center (a, b) and radius r.

Constructible subsets.

Recall that a subset Σ of a toplogical space X is called *constructible* if it is a finite Boolean combination of closed subsets. It follows that any constructible set is a finite union of locally closed subsets, where we call a subset *locally closed* if it is of the form $V \cap U$ with V closed and U open.

If R is any ring, then we can now easily define *affine n-space* over R as the affine scheme $\mathbb{A}^n_R := \mathrm{Spec}\, R[\xi]$ with $\xi = (\xi_1, \dots, \xi_n)$ indeterminates. We argued on page 13 that any quantifier free formula in the variables ξ, with parameters from R, defines a constructible subset of $\mathbb{A}^n_R$, and conversely.

Rational points.

Recapitulating, given an affine variety $V \subseteq K^n$, we have embedded it as a dense subset of the enhanced affine variety $\mathfrak{Irr}(V)$, which in turn is the underlying set of the affine scheme $X := \mathrm{Spec}(K[V])$. Since $K[V]$ is a K-algebra, X is in fact an affine K-scheme. We can recover V from X as the collection of K-rational points, defined as follows. Let $X := \mathrm{Spec}(R)$ be an affine Z-scheme and let S be a Z-algebra. An *S-rational point* of X over Z is by definition a morphism $\mathrm{Spec}(S) \to X$ of Z-schemes, that is to say, an element of $\mathrm{Mor}_Z(\mathrm{Spec}(S), X)$. We denote the set of all S-rational points of X over Z also by $X_Z(S)$, or $X(S)$, when Z is clear from the context. In other words, we actually view X as a functor, namely $\mathrm{Mor}_Z(\cdot, X)$, on the category of Z-algebras (see Exercise 3.6.27). By definition of a morphism, we have an equality

$$X_Z(S) = \mathrm{Mor}_Z(\mathrm{Spec}(S), X) = \mathrm{Hom}_Z(R, S)$$

where the latter set denotes the collection of Z-algebra homomorphisms $R \to S$. Returning to our example, where we take $S = Z = K$ and $R = K[V] = A/I$ with $I := \mathfrak{I}(V)$, a K-rational point $x \in X(K)$ then corresponds to a K-algebra homomorphism $R \to K$. Now, any K-algebra homomorphism is completely determined by the image of the variables, say $\xi_i \mapsto u_i$, since the image of a polynomial p is then simply $p(\mathbf{u})$ where $\mathbf{u} = (u_1, \dots, u_n)$. To be well-defined, we must have $p(\mathbf{u}) = 0$ for all $p \in I$, that is to say, $\mathbf{u} \in \mathrm{V}(I) = V$. Conversely, substitution by any element of V induces a K-algebra homomorphism $R \to K$ whence a K-rational point of X. We therefore showed that $V = X(K)$, as claimed.

In the sequel, we will sometimes confuse the underlying set $|\mathrm{Spec}(R)|$ of an affine scheme with the scheme itself, and denote it also by $\mathrm{Spec}(R)$.

3.4 Projective schemes

Most schemes we will encounter are affine, and in fact, often we work with the associated ring of global sections, or with their local rings (see §3.5). Nonetheless, we also will need projective schemes, which are a special case of a general scheme.

The category of schemes. Roughly speaking, a *scheme* X is a topological space $|X|$ together with a structure sheaf $\mathscr{O}_X$ of sections on $|X|$, with the property that there exists an open covering $\{X_i\}$ of X by affine schemes $\mathrm{Spec}(R_i)$ (for short, an *open affine covering*) such that $\Gamma(X_i, \mathscr{O}_X) = R_i$. Put differently, a scheme is obtained by *gluing* together affine schemes (for a more precise definition, consult any textbook in algebraic geometry, such as [28] or [48]). A *morphism* of schemes $f\colon Y \to X$ is a continuous map $|Y| \to |X|$ of underlying spaces which is 'locally a morphism of affine schemes' in the sense that there exist open affine coverings $\{Y_i\}$ and $\{X_i\}$ of Y and X respectively such that f maps each $|Y_i|$ inside $|X_i|$ thereby inducing for each i a morphism $Y_i \to X_i$ of affine schemes. If $U \subseteq X$ is any open, then we define a *sheaf of sections* $\mathscr{O}_U := \mathscr{O}_X|_U$ on U by restriction: for $W \subseteq U$ open, let $\Gamma(W, \mathscr{O}_U)$ be the ring of all sections $\mathscr{O}_X(W)$ on W. From the definitions (not all of which have been stated here), the next result follows almost immediately.

3.4.1 *An open $U \subseteq X$ in a scheme X together with the restriction $\mathscr{O}_U$ is again a scheme, and the embedding $U \subseteq X$ is a morphism of schemes, called an* open immersion.

For example, the 'punctured plane' $D \subseteq \mathbb{A}^2_K$ obtained by removing the origin, is a scheme. One can show that $\Gamma(D, \mathscr{O}_D) = K[\xi, \zeta]$, showing that D is not affine (see Exercise 3.6.5).

Here is an example of an actual gluing together of two affine schemes. Let $X_k := \mathbb{A}^1_K$ for $k = 1,2$ be two copies of the affine line, and let $U \subseteq X_k$ be the open obtained by removing the origin. Note that U is again affine, namely equal to $\mathrm{Spec}(K[\xi, \xi^{-1}])$. Let X be the result of gluing together X_1 and X_2 along their common open subset U. The resulting scheme is called the *affine line with the origin doubled*. It requires some more properties of schemes to see that it is in fact not affine. A more clever choice of gluing the above data together leads to the projective line, as we will now explain.

Projective varieties. To discuss projective schemes, let us first introduce *projective n-space* over K as the set of equivalence classes $K^{n+1} \setminus \{0\}/\approx$, where $\mathbf{u} \approx \mathbf{v}$ if and only if there exists a non-zero $k \in K$ such that $\mathbf{u} = k\mathbf{v}$. An equivalence class of an $n+1$-tuple $\mathbf{u} = (u_0, \dots, u_n)$, that is to say, a point in projective n-space, will be denoted $\tilde{\mathbf{u}} = (u_0 : u_1 : \cdots : u_n)$. Alternatively, we may view projective n-space as the collection of lines in affine $n+1$-space going through the origin. The relevant algebraic counterpart, in fact the *homogeneous coordinate ring* of projective n-space, is the polynomial ring $\tilde{A} := K[\zeta_0, \dots, \zeta_n]$. However, $\tilde{A}$ cannot be viewed as ring of sections, for given $p \in \tilde{A}$, we can no longer unambiguously evaluate it at a projective point $\tilde{\mathbf{u}}$. Nonetheless, if p is homogeneous, say of degree m, then $p(k\mathbf{u}) = k^m p(\mathbf{u})$, so that p vanishes on some $n+1$-tuple if and only if it vanishes on all $n+1$-tuples $\approx$-equivalent to it. Hence, for a given projective point $\tilde{\mathbf{u}}$, it makes sense to say that it is a *zero* of the homogeneous polynomial p, if $p(\mathbf{u}) = 0$.

We can now make projective n-space into a topological space by taking for closed subsets the sets of the form $\tilde{\mathrm{V}}(I)$, where $\tilde{\mathrm{V}}(I)$ is the collection of all projective points $\tilde{\mathbf{u}}$ that are a zero of each homogeneous polynomial in the ideal I. The analogue of Lemma 3.1.1 also holds, so that we get indeed a topology. Any closed subset of projective n-space is called a *projective variety*. Given such a closed subset V of projective n-space, we define its *ideal of definition* $\tilde{\mathfrak{I}}(V)$ as the ideal generated by all homogeneous forms $p \in \tilde{A}$ that vanish on V, and we call $\tilde{A}/\tilde{\mathfrak{I}}(V)$ the *homogeneous coordinate* ring of V, denoted $\widetilde{K[V]}$. Note that $\tilde{\mathfrak{I}}(V)$ is a homogeneous ideal (an ideal I is called *homogeneous*, if $p \in I$ implies that every homogeneous component of p lies in I too).

3.4.2 *The homogeneous coordinate ring* $\widetilde{K[V]}$ *of a projective variety* V *is a graded ring, and* V *has dimension equal to* $\dim(\widetilde{K[V]}) - 1$.

Recall that a ring S is called *graded*, if it admits a direct sum decomposition $S = \oplus_i S_i$ with each S_i an additive subgroup (called the i-th *graded part* of S) with the additional condition that $S_i \cdot S_j \subseteq S_{i+j}$ (meaning that if $a \in S_i$ and $b \in S_j$, then $ab \in S_{i+j}$). Here the index set of all i can in principal be any ordered, Abelian (semi-)group, but for our purposes, we will only work with $\mathbb{N}$-graded rings (with an occasional occurrence of a $\mathbb{Z}$-graded ring). In an $\mathbb{N}$-graded ring S, the zero-th part S_0 is always a subring of S, and $S_+ := \oplus_{i>0} S_i$ is an ideal such that $S/S_+ \cong S_0$. In case $S = \widetilde{K[V]}$, then $S_0 = K$, and S is generated over S_0 by finitely many linear forms. An $\mathbb{N}$-graded ring with these two properties is called a *standard graded (K-)algebra* (also called a *homogeneous* graded ring). In particular, S_+ is then a maximal ideal, called the *irrelevant maximal ideal*. The terminology comes from the fact that $\tilde{\mathrm{V}}(S_+) = \emptyset$. For example, if $S = \tilde{A}$ viewed as a (standard) graded K-algebra, then $(\zeta_0, \dots, \zeta_n)S$ is its irrelevant maximal ideal.

Projective schemes. To define *enhanced projective varieties*, let $S = \oplus_i S_i$ be a standard graded K-algebra (for this construction to work, $K = S_0$ need not be algebraically closed—although we will not treat this, S_0 does not even need to be a field), and define $|\mathrm{Proj}(S)|$ to be the collection of all homogeneous prime ideals of S not containing S_+. In analogy with the affine case, we get a topological space by taking as closed subsets the subsets $\tilde{\mathrm{V}}(I)$ of all homogeneous prime ideals containing the ideal I, for various (homogeneous) ideals I. If V is a projective variety and $S := \widetilde{K[V]}$ its projective coordinate ring, then V embeds in $|\mathrm{Proj}(S)|$ by mapping a projective point $\tilde{\mathbf{u}}$ to its ideal of definition $\tilde{\mathfrak{I}}(\tilde{\mathbf{u}})$. The latter is indeed a (homogeneous) prime ideal, generated by the linear forms $u_i\zeta_j - u_j\zeta_i$ for all $i < j$. As before, (the image of) V is dense in $|\mathrm{Proj}(S)|$, so that any projective variety determines a unique enhanced projective variety. Conversely, every (enhanced) projective variety is a closed subset of some (enhanced) projective space, since any standard graded K-algebra is of the form $\tilde{A}/I$ for some homogeneous ideal I (and some appropriate choice of n). Unfortunately, unlike the affine case, non-isomorphic standard graded algebras might give rise to isomorphic (enhanced) projective varieties.

Finally, we define the *projective scheme* associated to S, denoted as $\mathrm{Proj}\, S$, as the scheme with underlying set $|\mathrm{Proj}(S)|$ and with structure sheaf $\mathscr{O}_X$, roughly speaking, 'induced by S'. Let me only explain this, and then still omitting most details, for projective n-space $\mathbb{P}^n_K := \mathrm{Proj}(\tilde{A})$. Once more we must turn our attention to open subsets. Similarly as in the affine case, given a homogeneous element $f \in \tilde{A}$ of degree m, we define the *basic open* $\tilde{\mathrm{D}}(f)$ as the complement of $\tilde{\mathrm{V}}(f\tilde{A})$. As before, these basic opens form a basis for the topology. Define $\Gamma(\tilde{\mathrm{D}}(f), \mathscr{O}_{\mathbb{P}^n_K})$ to be the *graded localization* $\tilde{A}_{(f)}$, defined as the collection of all fractions of the form $s := p/f^l$ with p homogeneous of degree ml. Put differently, $\tilde{A}_{(f)}$ is the degree zero part of the $\mathbb{Z}$-graded localization $\tilde{A}_f$. Since we are trying to construct a structure sheaf, it should consist of sections, and this is indeed the case. Namely, given $\tilde{\mathbf{u}}$ such that $f(\tilde{\mathbf{u}}) \neq 0$, the value $s(\mathbf{u})$ is independent from the choice of representative of the projective point $\tilde{\mathbf{u}}$, for s a section as above: if $\mathbf{v} \approx \mathbf{u}$, say $\mathbf{v} = k\mathbf{u}$, then $s(\mathbf{v}) = k^{ml}p(\mathbf{u})/(k^m f(\mathbf{u}))^l = s(\mathbf{u})$. Hence we can define $s(\tilde{\mathbf{u}}) := s(\mathbf{u})$, so that $\Gamma(\tilde{\mathrm{D}}(f), \mathscr{O}_{\mathbb{P}^n_K})$ consists indeed of sections on $\tilde{\mathrm{D}}(f)$.

3.4.3 *Each basic open $\tilde{\mathrm{D}}(f)$ with f a non-zero homogeneous form is homeomorphic to the enhanced affine variety $\left|\mathrm{Spec}(\tilde{A}_{(f)})\right|$.*

Indeed, define a map $\phi\colon \tilde{\mathrm{D}}(f) \to \left|\mathrm{Spec}(\tilde{A}_{(f)})\right|$ by sending a homogeneous prime ideal $\mathfrak{p}$ not containing f to the ideal $\phi(\mathfrak{p}) := \mathfrak{p}\tilde{A}_f \cap \tilde{A}_{(f)}$. One checks that $\phi(\mathfrak{p})$ is indeed a prime ideal. We leave it as an exercise (see 3.6.15) to show that this map is a homeomorphism. In particular, if we let f be one of the variables, say ζ_0 to make our notation easy, then one checks that $A \cong \tilde{A}_{(\zeta_0)}$ by sending ξ_i to ζ_i/ζ_0. Hence each $\tilde{\mathrm{D}}(\zeta_i)$ has affine n-space as underlying set. We can now make $\mathbb{P}^n_K$ into a scheme by gluing together the $n+1$ affine schemes $\mathrm{Spec}(\tilde{A}_{(\xi_i)}) \cong \mathbb{A}^n_K$ (again we must leave details to more specialized works). A similar construction applies to any standard graded K-algebra S, thus defining the scheme structure on $\mathrm{Proj}(S)$.

Proposition 3.4.4. *For any projective scheme $X := \mathrm{Proj}(S)$ and any homogeneous element $f \in S$, we have $\Gamma(\tilde{\mathrm{D}}(f), \mathscr{O}_X) = S_{(f)}$. Moreover, $\Gamma(X, \mathscr{O}_X) = K$.*

Proof. The last assertion is a special case of the first by taking $f = 1$, since then $S_{(1)} = S_0 = K$. The first assertion is basically how we defined the scheme structure on X. □

The last assertion shows that unlike in the affine case, the global sections on a scheme in general do not determine the scheme. In fact, two non-isomorphic graded

K-algebras can give rise to isomorphic projective schemes, so that even the 'coordinate ring' S is not determined by the scheme (but also depends on the embedding of X as a closed subscheme of some $\mathbb{P}^n_K$). We will have more to say about projective schemes, and their relation to affine schemes, when we discuss singularities: see page 65.

3.5 Local theory

We have now associated to each geometric object (be it an affine variety, a projective variety or a scheme) an algebraic object, its coordinate ring, or more precisely, a collection of rings, the sheaf of sections on each open subset. If x is a closed point (that is to say, $\{x\}$ is closed) of an affine scheme $X := \operatorname{Spec}(R)$, then $\{x\}$ itself is an affine scheme by Lemma 3.3.12, with associated ring $\kappa(x) = R/\mathfrak{m}_x$, the residue field of x. Put pedantically, $x = \operatorname{Spec}(\kappa(x))$. Clearly, this point of view ignores the embedding $\{x\} \subset X$, and hence gives us no information on the nature of X in the neighborhood of x.

Local rings. We therefore introduce the *local ring* of X at an arbitrary point x, denoted $\mathscr{O}_{X,x}$, as the ring of germs of sections at x. This means that a typical element of $\mathscr{O}_{X,x}$ is a pair (U,σ) with U an open containing x and $\sigma \in \Gamma(U,\mathscr{O}_X)$, modulo the equivalence relation $(U,\sigma) \approx (U',\sigma')$ if and only if there exists a common open $x \in U'' \subseteq U \cap U'$ such that σ and σ' agree on U''.

Recall from page 37 that part of $\mathscr{O}_X$ being a sheaf is the fact that for each inclusion $U' \subseteq U$, we have a restriction homomorphism $\Gamma(U,\mathscr{O}_X) \to \Gamma(U',\mathscr{O}_X)$. Hence the $\Gamma(U,\mathscr{O}_X)$ together with the restriction homomorphisms form a direct system, and we can now state the previous definition more elegantly as

$$\mathscr{O}_{X,x} = \varinjlim_{x \in U} \Gamma(U,\mathscr{O}_X). \tag{3.8}$$

Unlike the ring of sections on an arbitrary open, the local ring at a point has a very concrete description:

Proposition 3.5.1. *If $X := \operatorname{Spec}(R)$ is an affine scheme, and x a point in X with corresponding prime ideal $\mathfrak{p}_x \subseteq R$, then $\mathscr{O}_{X,x} = R_{\mathfrak{p}_x}$. In particular, $\mathscr{O}_{X,x}$ is a local ring with residue field equal to the residue field $\kappa(x)$ of x.*

Proof. To simplify the proof, I will assume that R is moreover a domain (the general case is not much harder; see Exercise 3.6.31). In this case, each $\Gamma(U,\mathscr{O}_X)$ is a subring of the field of fractions $\operatorname{Frac}(R)$ and the direct limit (3.8) is simply a union. Since the $\mathrm{D}(f)$ are a basis of opens, it suffices to only consider the contributions in this union given by the U of the form $\mathrm{D}(f)$ with $f \notin \mathfrak{p}_x$. Hence, in view of (3.4), the local ring $\mathscr{O}_{X,x}$ is the union of all R_f with $f \notin \mathfrak{p}_x$, which is easily seen to be the localization $R_{\mathfrak{p}_x}$. The last assertion is immediate from the definition of the residue field (see Definition 3.3.8). □

The maximal ideal of $\mathscr{O}_{X,x}$, that is to say, $\mathfrak{p}_x\mathscr{O}_{X,x}$, will be denoted $\mathfrak{m}_{X,x}$.

Tangent spaces. The local ring of a point x captures quite a lot of information of the geometry of X near x. For instance, one might formally define the *tangent space* $T_{X,x}$ at x as the the dual of the $\kappa(x)$-vector space $\mathfrak{m}_{X,x}/\mathfrak{m}_{X,x}^2$. Without proof we state the following (for a proof see for instance [48, Lemma 6.3.10] or [28, I. Theorem 5.3]):

Theorem 3.5.2. *Let $X := \operatorname{Spec}(R)$ be an affine scheme of finite type over K and assume R is a domain (whence X is irreducible). Then there exists a non-empty open $U \subseteq X$ such that the tangent space $T_{X,x}$ has dimension equal to the dimension of X, for every closed point $x \in U$.*

Under the stated conditions, the local ring $\mathcal{O}_{X,x}$ of x has the same dimension as X (see Exercise 4.4.14). The dimension of this local ring, even if x is not assumed to be a closed point, is called the *local dimension of X at x*, or put less accurately, the dimension of X in the neighbourhood of x. Immediate from Nakayama's lemma, we get:

3.5.3 *The embedding dimension of the local ring $\mathcal{O}_{X,x}$ of a point x on an affine scheme X, that is to say, the local dimension of X at x, is equal to the dimension of its tangent space $T_{X,x}$.*

It follows that the dimension of the tangent space of an arbitrary point is always at least the local dimension at that point. Points were this is an equality are special enough to deserve a name (we shall return to this concept and study it in more detail in §5 below):

Definition 3.5.4 (Non-singular point). A point x on an affine scheme $X := \operatorname{Spec}(R)$ is called *non-singular* if its tangent space $T_{X,x}$ has the same dimension as the local dimension of X at the point. A point where the dimension inequality is strict is called *singular*.

Returning to a phrase quoted on page 32, we can now prove:

3.5.5 *An affine variety is non-singular at its generic points.*

Indeed, by 3.3.2, a generic point P of V corresponds to a minimal prime ideal $\mathfrak{g}$ of $B := K[V]$. Since B is reduced, $B_{\mathfrak{g}}$ is a reduced local ring of dimension zero, whence a field (see our discussion on page 52). Hence the maximal ideal of $\mathcal{O}_{V,P} = B_{\mathfrak{g}}$ is zero, whence $T_{V,P} = 0$, and the embedding dimension of $B_{\mathfrak{g}}$ is also zero. More generally, this proves that if B is a reduced ring, then the generic points of $\operatorname{Spec}(B)$ are non-singular. This also implies that any K-generic point of V_L, where V_L denotes the base change of V over an algebraically closed overfield L of K (see page 34), is non-singular, but the proof requires some deeper results beyond the scope of these notes.

Continuous sections.

We can now give a better definition of a section on an open of an affine scheme $X := \operatorname{Spec}(R)$. Instead of letting a section take values in $Q(|X|)$, the disjoint union of all residue fields, we should take for target the disjoint union $\operatorname{Loc}(X)$ of all local rings $\mathscr{O}_{X,x}$ with $x \in X$: a (*generalized*) *section* on an open $U \subseteq X$ is then a map $\sigma\colon U \to \operatorname{Loc}(X)$ such that $\sigma(x) \in \mathscr{O}_{X,x}$ for all $x \in X$. With this new notion we can now formally define $\Gamma(U, \mathscr{O}_X)$ for an arbitrary open U as the set of all continuous sections on U, where we call a section σ *continuous* if it is locally represented by a fraction, that is to say, if for each $x \in U$, we can find an open $U' \subseteq U$ containing x, and elements $a, f \in R$ such that, for all $y \in U'$, in $\mathscr{O}_{X,y}$, the element f is a unit and $\sigma(y) = a/f$.

Stalks.

One can extend the concept of a local ring to arbitrary schemes. This is just a special case of a *stalk* $\mathscr{A}_x$ of a sheaf $\mathscr{A}$ at a point x on a topological space X, defined similarly as

$$\mathscr{A}_x := \varinjlim_{x \in U} \Gamma(U, \mathscr{A}).$$

However, even if $\mathscr{A}$ is a sheaf of rings, $\mathscr{A}_x$ need not be a local ring, but it is so if X is a scheme and $\mathscr{A} = \mathscr{O}_X$ its structure sheaf. An argument similar to the one in the proof of Proposition 3.5.1 yields:

Proposition 3.5.6. *Let $X := \operatorname{Proj}(S)$ be a projective scheme and let x be a point of X corresponding to the homogeneous prime ideal $\mathfrak{p}_x$. The local ring $\mathscr{O}_{X,x}$ is equal to the degree zero part $S_{(\mathfrak{p}_x)}$ of the localization $S_{\mathfrak{p}_x}$.*

3.6 Exercises

Ex 3.6.1

Verify Lemma 3.1.1. Show that the same properties hold for the operation $\operatorname{V}(\cdot)$ on any affine scheme, and for the operation $\tilde{\operatorname{V}}(\cdot)$ on any projective scheme.

Ex 3.6.2

Show that if $V_1 \cup \cdots \cup V_s = V_1' \cup \cdots \cup V_t'$ are two minimal irreducible decompositions of a Noetherian space V, then $s = t$, and after renumbering, $V_i = V_i'$ for all i.
Show that for a closed subset $V \subseteq K^n$, its ideal of definition $\mathfrak{I}(V)$ is prime if and only if V is irreducible.

Ex 3.6.3

Show that the Zariski topology on K^n is compact Hausdorff. More generally, any affine variety is compact Hausdorff. Hint: you could use 3.3.6.

Ex 3.6.4

Let $V \subseteq K^n$ be a variety and let $I := \mathfrak{I}(V)$ be its ideal of definition. Every $p \in A$ induces a polynomial map $K^n \to K$ by the rule $\mathbf{u} \mapsto p(\mathbf{u})$. Show that the collection of restrictions $p|_V$ of polynomial maps on V is in one-one correspondence with the coordinate ring $K[V]$ of V.

Ex 3.6.5

Show that the punctured plane $K^2 \setminus \{O\}$ *(where O denotes the origin), is not an affine variety, for if it were, then its ideal of definition would be zero, contradiction. In fact, by the discussion on page 41 there is a scheme D with underlying set this punctured plane. It can be realized as the union of the two affine opens $\mathrm{D}(\xi)$ and $\mathrm{D}(\zeta)$ of $\mathbb{A}^2_K$, where $A := K[\xi, \zeta]$ is the coordinate ring of $\mathbb{A}^2_K$. Show that $\Gamma(D, \mathscr{O}_D) = A_\xi \cap A_\zeta = A$. Conclude that D is not affine.*

Ex 3.6.6

Prove 3.2.3 in detail. In particular, given a reduced K-affine ring B, construct an affine variety whose coordinate ring is B. Prove that the correspondence in 3.2.3 induces an anti-equivalence of categories. In particular, show that if two affine varieties are isomorphic, then so are their coordinate rings. Using this equivalence, show that a parabola is isomorphic to a straight line.

Ex 3.6.7

Show that if X is Noetherian, then $\mathfrak{Irr}(X)$ is a toplogical space in which every irreducible closed subset has a generic point; if X is moreover Hausdorff, then every irreducible closed subset has a unique generic point. In particular, in the latter case, the map $X \to \mathfrak{Irr}(X)$ is an embedding, and (the image of) X is dense in $\mathfrak{Irr}(X)$.

Ex 3.6.8

Let $K \subseteq L$ be an extension of algebraically closed fields. Show that a point $\mathbf{u} \in L^n$ is generic over K if and only if $K(\mathbf{u})$ has transcendence degree n over K. This shows that generic points are plentiful. Now explain the enigmatic adverb 'probably' used in Example 3.3.4.

Ex 3.6.9

Show that if R is Noetherian, then the associated enhanced affine variety $|\mathrm{Spec}(R)|$ is also Noetherian. It is irreducible if and only if R has a unique minimal prime ideal (and if R is moreover reduced, this is then equivalent to R being a domain). The Krull dimension of R is equal to the dimension of $|\mathrm{Spec}(R)|$.
Can you give an example where $|\mathrm{Spec}(R)|$ is Noetherian, yet R is not Noetherian?

Ex 3.6.10

Show that if $K \subseteq L$ is an extension of algebraically closed fields and $V \subseteq K^n$ is an affine variety over K, then its closure in L^n is an affine variety over L with coordinate ring $K[V] \otimes_K L$.

Ex 3.6.11

Let R be a domain and $X := \mathrm{Spec}(R)$ the associated affine scheme. Let η be the (unique) generic point of X. Show that the residue field $\kappa(\eta)$, the local ring $\mathscr{O}_{X,\eta}$ at η, and the field of fractions $\mathrm{Frac}(R)$ *are all equal. This field is often called the* function field *of the scheme.*

Ex 3.6.12

Calculate all residue fields of $\mathrm{Spec}(\mathbb{Z})$*. What are the residue fields of* $\mathrm{Spec}(\mathbb{R}[\xi])$ *for ξ a single variable?*

Ex 3.6.13

Prove that (3.6) is a homeomorphism. Use this to prove (3.7).

Ex 3.6.14

Show that a finite morphism of affine schemes has finite fibers.

Ex 3.6.15

Prove 3.3.6, 3.3.9 and 3.4.3.

Ex 3.6.16

Work out Example 3.3.7 in detail.

Ex 3.6.17

Prove Lemma 3.3.12.

Ex 3.6.18

Show that an ideal I in a graded ring S is homogeneous if and only if it is generated by homogeneous elements. For an arbitrary ideal I, let $\tilde{I}$ be the ideal generated by all homogeneous components of all elements in I. Show that $\tilde{\mathrm{V}}(I) = \tilde{\mathrm{V}}(\tilde{I})$.

Ex 3.6.19

Prove 3.4.2 (where you might need some results from Chapter 4 to prove the dimension equality).

Ex 3.6.20

Let V be a projective variety over K, with homogeneous coordinate ring $S := \widetilde{K[V]}$. Show that $\mathfrak{Irr}(V) = |\mathrm{Proj}(S)|$.

Ex 3.6.21

Let C be the affine scheme determined by the ring

$$R := K[\xi,\zeta]/(\xi^2 - \zeta^3)K[\xi,\zeta],$$

a so-called cusp *(see page 62). Let x be the origin, that is to say, the (closed) point determined by the maximal ideal $(\xi,\zeta)R$. Show that the tangent space $T_{C,x}$ has dimension two, whereas C itself has dimension one (showing that x is* singular*). What about the point y given by the maximal ideal $(\xi-1,\zeta-1)R$?*

Additional exercises

Ex 3.6.22

Show that the geometric form of the Noether normalization as stated in Theorem 3.2.5 is indeed equivalent to the algebraic form formulated in the proof.

Ex 3.6.23

We want to prove the assertion in the proof of Theorem 3.2.5 that states that after a change of coordinates, a polynomial becomes monic in one of the variables. Let $p \in A$ be a non-constant polynomial of degree s, and let $p_s(\xi)$ be its homogeneous part of degree s. Put $p' := p(\xi', 1)$ where $\xi' := (\xi_1, \dots, \xi_{n-1})$. Show that if K is infinite, then there exists $\mathbf{u}' := (u_1, \dots, u_{n-1}) \in K^{n-1}$ such that $p'(\mathbf{u}') \neq 0$. This is clear if $n-1 = 1$ since a non-zero polynomial has only finitely many roots. Reason by induction to show this also for more variables. Now define a change of coordinates $\xi_i \mapsto \xi_i - u_i\xi_n$ and show that the image of p under this map is monic in ξ_n.

If K is arbitrary, show that the change of variables $\xi_i \mapsto \xi_i - \xi_n^{e^i}$ for $i < n$ also transforms p into a monic polynomial if $e > s$ (examine the transforms of each monomial in p).

Ex 3.6.24

Prove the following generalization of Lemma 3.2.7: if $R \subseteq S$ is a finite (or integral) extension of domains, then R is a field if and only if S is.

Ex 3.6.25

Show that if an algebra is generated by n elements over a field, then any of its maximal ideals is also generated by at most n elements. Reduce first to the polynomial case, and then use the Weak Nullstellensatz (Corollary 3.2.6) to show that any maximal ideal is generated by n polynomials.

Ex 3.6.26

The product *of two objects M and N in a category $\mathfrak{C}$ is the (necessarily unique) object $M \times N$ together with two morphisms $M \times N \to M$ and $M \times N \to N$ (called* projections*), satisfying the following* universal property*: if $K \to M$ and $K \to N$ are morphisms, then there exists a unique morphism $K \to M \times N$ which composed with the two projections yield the original morphisms $K \to M$ and $K \to N$. Show that in the category of affine schemes over a fixed affine scheme X, the fiber product $\cdot \times_X \cdot$ is a product in the above sense.*

Ex 3.6.27

Show that given an (affine) Z-scheme X, the rule assigning to a Z-algebra S the set $X_Z(S)$ of S-rational points of X over Z, constitutes a functor on the category of Z-algebras.

Ex 3.6.28

Show that the definition of $\Gamma(U, \mathscr{O}_X)$ as all continuous sections given on page 45 makes $\mathscr{O}_X$ into a sheaf.

Ex 3.6.29

Prove Proposition 3.5.6.

Ex 3.6.30

Let $S := K[\zeta]/\zeta^2 K[\zeta]$ *be the ring of* dual numbers *over* K *(where* ζ *is a single variable). Let* X *be an affine variety of finite type over* K*. Show that to give an* S*-rational point of* X *over* K *is the same as to give a* K*-rational point* x *of* X *together with an element of the tangent space* $T_{X,x}$*.*

Ex 3.6.31

Show, without relying on Proposition 3.5.1, that if Y *is a closed subscheme of* $X := \mathrm{Spec}(R)$ *with corresponding ideal* $I \subseteq R$*, then* $\mathscr{O}_{Y,y} = \mathscr{O}_{X,y}/I\mathscr{O}_{X,y}$ *for every* $y \in Y$*. Use this then to derive the non-domain case in the proposition.*

Chapter 4
Dimension theory

Dimension is one of these intuitive notions that our scientific mind has formalized into an abstract concept in such diverse fields as geometry, algebra, analysis, topology, statistics, physics, ... Also in commutative algebra, dimension plays a primary role, and so we study its properties first. For a ring, (Krull) dimension is defined by means of its prime spectrum. Although at the face of it an abstract definition, it does correspond to the intuitive notion of geometric dimension via the duality between rings and algebraic varieties discussed in the previous chapter. We give several definitions which are equivalent, at least for Noetherian local rings. This will enable us later to extend the notion of dimension to ultra-rings. In the next chapter, we will introduce some more ring invariants and compare them with dimension; this will lead to several notions of singularities.

4.1 Krull dimension

Height. The *height* of a prime ideal $\mathfrak{p}$ in a ring R is by definition the maximal length of a proper chain of prime ideals inside $\mathfrak{p}$, and is often denoted $\mathrm{ht}(\mathfrak{p})$. Hence a prime ideal is minimal if and only if its height is zero. The supremum of the heights of all prime ideals in R is called the (*Krull*) *dimension* of R and is denoted $\dim(R)$. More generally, the *height* $\mathrm{ht}(I)$ of an ideal I is the minimum of the heights of all prime ideals containing I. The following inequality is almost immediate from the definitions (see Exercise 4.4.1).

4.1.1 *For every prime ideal $\mathfrak{p} \subseteq R$, we have an inequality*

$$\dim(R/\mathfrak{p}) + \mathrm{ht}(\mathfrak{p}) \leq \dim(R).$$

Almost immediate from the definitions (see Exercise 3.6.9), we get the following generalization of Corollary 3.2.4:

4.1.2 *The Krull dimension of a ring R is equal to the dimension of the associated enhanced affine variety $|\mathrm{Spec}(R)|$.*

Dimension, although seemingly a global invariant, has a strong local character:

4.1.3 *The height of a prime ideal $\mathfrak{p} \subseteq R$ is equal to the dimension of $R_{\mathfrak{p}}$. In particular, the dimension of R is equal to the supremum of the dimensions of its localizations $R_{\mathfrak{m}}$ at maximal ideals $\mathfrak{m}$. Similarly, the dimension of an affine variety $X := \mathrm{Spec}(R)$ is equal to the supremum of the dimensions of its local rings $\mathscr{O}_{X,x}$ at (closed) points $x \in X$.*

The first assertion is proven in Exercise 4.4.5, and the second is an immediate consequence of this (since maximal ideals have the largest height). The last assertion then follows from Proposition 3.5.1.

Artinian rings. Recall that a ring is called respectively *Noetherian* or *Artinian* if the collection of ideals satisfies the ascending or the descending chain condition respectively. Without proof we state the following structure theorem for Artinian rings (for a proof see for instance [54, Theorem 3.2] or [7, Theorems 8.5 and 8.7]):

4.1.4 *Any Artinian ring R is Noetherian, and has only finitely many prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_s$. Each $\mathfrak{p}_i$ is moreover maximal, so that R has dimension zero, and $R = R_{\mathfrak{p}_1} \oplus \dots \oplus R_{\mathfrak{p}_s}$.*

In fact, a ring R is Artinian if and only if it has finite *length* $l = \ell(R)$, meaning that any proper chain of ideals has length at most l, and there is a chain with this length. It follows that any finitely generated R-module M also has finite length, denoted $\ell(M)$, and defined as the maximal length of a proper chain of submodules. An Artinian ring of length one is a field. Length is a generalization of vector space dimension; for instance, you will be asked to prove the following characterization of length in Exercise 4.4.3:

4.1.5 *If R is finitely generated (as a module) over an algebraically closed field K, then $\ell(R)$ is equal to the vector space dimension of R over K.*

4.2 Hilbert series

Although we are interested in the study of local rings, it turns out that graded rings play an important role in dimension theory. The connection between the two is provided by the graded ring $\mathrm{Gr}(R)$ associated to a local ring R (see page 54). So we first study the graded case.

Let R be an Artinian local ring and let S be a standard graded R-algebra. Recall that this means that $S = \oplus_{i \in \mathbb{N}} S_i$ is $\mathbb{N}$-graded, the degree zero part S_0 is equal to R, and S is generated as an R-algebra by finitely many linear forms (=elements in S_1). Let M be a finitely generated $\mathbb{N}$-graded S-module, meaning that $M = \oplus_{i \in \mathbb{N}} M_i$ and $S_i M_j \subseteq M_{i+j}$ for all i, j.

4.2.1 *Every M_n is a finitely generated R-module, whence in particular has finite length.*

Indeed, we may choose homogenous generators $\mu_1, \dots, \mu_s$ of M as an S-module. If k_i is the degree of μ_i, then $M_n = S_{n-k_1}\mu_1 + \dots + S_{n-k_s}\mu_s$ (with the understanding that $S_j = 0$ for $j < 0$). Furthermore, if $a_1, \dots, a_s$ are the linear forms generating S as an R-algebra, then S_n is generated as an R-module by all monomials of degree n in the a_i. Therefore, M_n is finitely generated over R, and therefore has finite length.

Hilbert series. In view of 4.2.1, we can now define the *Hilbert series* of a finitely generated S-module M, with S a standard graded algebra over an Artinian local ring R, as the formal power series

$$\mathrm{Hilb}_M(t) := \sum_{n \geq 0} \ell(M_n)t^n. \tag{4.1}$$

As rings will be our primary objective in these notes, rather than modules, we will be mainly interested in the properties of $\mathrm{Hilb}_S(t)$. However, it is more convenient to work in the larger module setup for inductive proofs to go through. The key result on Hilbert series is:

Theorem 4.2.2. *Let S be a standard graded algebra over an Artinian local ring R. The Hilbert series of any finitely generated S-module M is rational. In fact, for some $d = d(M) \in \mathbb{N}$, the power series $(1-t)^d \cdot \mathrm{Hilb}_M(t)$ is a polynomial with integer coefficients.*

Proof. We will prove the last assertion by induction on the minimal number r of linear R-algebra generators of S. If $r = 0$, then $S = R$, so that M is a finitely generated module over an Artinian ring, whence has finite length. It follows that $M_n = 0$ for $n \gg 0$ and we are done in this case. So assume $r > 0$ and let x be one of the linear forms generating S as an R-algebra. Multiplication by x induces maps $M_n \to M_{n+1}$ for all n. Let K_n and L_{n+1} be the respective kernel and cokernel of these maps (with $L_0 := M_0$). Define two new graded S-modules $K := \oplus_n K_n$ and $L := \oplus_n L_n$. It follows that $K \subseteq M$ and $M/xM \cong L$, proving that both modules are finitely generated over S. By construction, $xK = xL = 0$, so that both K and L are actually modules over S/xS, and hence we may apply our induction hypothesis to them. Since we have an exact sequence (see page 75 for the notion of an exact sequence)

$$0 \to K_n \to M_n \xrightarrow{x} M_{n+1} \to L_{n+1} \to 0$$

we get $\ell(K_n) - \ell(M_n) + \ell(M_{n+1}) - \ell(L_{n+1}) = 0$ by Exercise 4.4.2. Multiplying this equality with t^{n+1} and adding all terms together, we get an identity

$$t\,\mathrm{Hilb}_K(t) - t\,\mathrm{Hilb}_M(t) + \mathrm{Hilb}_M(t) - \mathrm{Hilb}_L(t) = 0.$$

Using the induction hypothesis for K and L then yields the desired result. $\square$

Corollary 4.2.3. *For every finitely generated graded module M over a standard graded algebra over an Artinian local ring, there exists a polynomial $P_M(t) \in \mathbb{Z}[t]$, such that $\ell(M_n) = P_M(n)$ for all n sufficiently large.*

Proof. By Theorem 4.2.2 we can write $\mathrm{Hilb}_M(t) = q(t)/(1-t)^d$ for some polynomial $q(t) \in \mathbb{Z}[t]$. Using the Taylor expansion of $(1-t)^{-d}$ and then comparing coefficients at both sides, the result follows readily (see Exercise 4.4.8). Note that we have equality for all $n > \deg(q)$. □

Associated graded ring. For a given Noetherian ring $(R, \mathfrak{m})$, define its *associated graded ring* as

$$\mathrm{Gr}(R) := \bigoplus_{n \geq 0} \mathfrak{m}^n/\mathfrak{m}^{n+1}$$

Note that this is a standard graded algebra over the residue field $R/\mathfrak{m}$ of R (as always $\mathfrak{m}^0$ stands for the unit ideal). Applying Corollary 4.2.3 to $M = S = \mathrm{Gr}(R)$ we can find a polynomial $P_R(t)$ such that

$$P_R(n) = \ell(\mathfrak{m}^n/\mathfrak{m}^{n+1}) \tag{4.2}$$

for all $n \gg 0$. For various reasons, one often works with the 'iterate' of this function:

Hilbert-Samuel polynomial. We define the *Hilbert-Samuel function* of R as the function $n \mapsto \ell(R/\mathfrak{m}^{n+1})$. By induction, one easily shows that

$$\ell(R/\mathfrak{m}^{n+1}) = \sum_{k=0}^{n} \ell(\mathfrak{m}^k/\mathfrak{m}^{k+1}). \tag{4.3}$$

It follows from (4.2) that there then exists a polynomial $\chi_R(t)$ with integer coefficients, called the *Hilbert-Samuel polynomial*, such that

$$\ell(R/\mathfrak{m}^{n+1}) = \chi_R(n) \tag{4.4}$$

for all $n \gg 0$.

4.3 Local dimension theory

In this section, $(R, \mathfrak{m})$ denotes a local ring, which is most of the time also Noetherian. The Krull dimension of R will be denoted $\dim(R)$. We introduce two more variants, and show that they agree on Noetherian local rings.

Definition 4.3.1 (Geometric dimension). We define the *geometric dimension* of R, denoted $\mathrm{geodim}(R)$, as the least number of elements generating an $\mathfrak{m}$-primary ideal (see 2.4.9 for the definition of $\mathfrak{m}$-primary ideal). We let $\mathrm{Hilbdim}(R)$ denote the degree of the Hilbert-Samuel polynomial $\chi_R(t)$ of R given by (4.4).

As $\dim(R)$ equals the dimension of the topological space $V := |\mathrm{Spec}(R)|$, it is essentially a topological invariant. On the other hand, $\mathrm{geodim}(R)$ is the least number of hypersurfaces[1] $H_1, \dots, H_d \subseteq V$ such that $H_1 \cap \dots \cap H_d$ is a singleton (necessarily equal to the closed point x corresponding to the maximal ideal $\mathfrak{m}$), and hence is a geometric invariant. Note that the definition of geometric dimension makes sense for any local ring R (unlike the definition of Hilbert dimension which assumes the rationality of the Hilbert series), and that it is finite if and only if R has finite embedding dimension. Finally, $\mathrm{Hilbdim}(R)$ is by definition a combinatorial invariant. It follows that both geometric dimension and Hilbert dimension are finite for Noetherian local rings, but this is less obvious for Krull dimension. Nonetheless, all three seemingly unrelated invariants are always equal for Noetherian local rings (whence in particular Krull dimension is always finite):

Theorem 4.3.2. *If R is a Noetherian local ring, then*

$$\dim(R) = \mathrm{geodim}(R) = \mathrm{Hilbdim}(R).$$

Proof. It is not hard to verify this equality whenever one of them is zero: R has Krull dimension zero if and only if its maximal ideal is nilpotent (in other words, (0) is $\mathfrak{m}$-primary) if and only if its Hilbert-Samuel function is constant.

So we may assume that all three invariants are non-zero. First we show by induction on δ that

$$t := \mathrm{Hilbdim}(R) \leq \delta := \mathrm{geodim}(R). \tag{4.5}$$

Let $I := (a_1, \dots, a_\delta)R$ be an $\mathfrak{m}$-primary ideal, and put $S := R/a_1R$. It is not hard so see that then necessarily $\mathrm{geodim}(S) = \delta - 1$, so that by induction, $\mathrm{Hilbdim}(S) \leq \delta - 1$. We have, for n sufficiently large,

$$\begin{aligned}
\chi_S(n) = \ell(S/\mathfrak{m}^{n+1}S) &= \ell(R/a_1R + \mathfrak{m}^{n+1}) \\
&= \ell(R/\mathfrak{m}^{n+1}) - \ell(R/(\mathfrak{m}^{n+1} : a_1)) \\
&\geq \ell(R/\mathfrak{m}^{n+1}) - \ell(R/\mathfrak{m}^{n}) = \chi_R(n) - \chi_R(n-1)
\end{aligned}$$

(where we used (6.9) below in the second line). Note that $\chi_R(n) - \chi_R(n-1)$ has degree $t-1$ (verify this!), and hence $\chi_S(n)$, a polynomial dominating the latter difference, must have degree at least $t-1$. Putting everything together, we therefore get $t - 1 \leq \deg(\chi_S) \leq \delta - 1$, as we wanted to show.

For the remainder of the proof, we induct on the Krull dimension $d := \dim(R)$, and so we assume that the theorem is proven for rings of smaller Krull dimension. Let $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_d = \mathfrak{m}$ be a chain of prime ideals in R of maximal length. Choose x outside all minimal prime ideals but inside $\mathfrak{p}_1$. By prime avoidance (see [7, Proposition 1.11] or the more general version [22, Lemma 3.3]), such an element must exist. Put $S := R/xR$. Since $\mathfrak{p}_iS$ are distinct prime ideals, for $i > 0$, we get

[1] In these notes, a *hypersurface* in an affine variety V is any closed subset of the form $\mathrm{V}(I)$ with I a proper principal ideal (this does not mean that its ideal of definition is principal!) Be aware that some authors have a far more restrictive usage for this term.

$\dim(S) = d-1$. Hence by induction, $\operatorname{geodim}(S) = d-1$, so that there exists an $\mathfrak{m}S$-primary ideal $I \subseteq S$ generated by $d-1$ elements. Let $J := I \cap R$. Any lifting of the $d-1$ generators of I in R together with x therefore generate J. Moreover, J is clearly $\mathfrak{m}$-primary, so that we showed $\operatorname{geodim}(R) \le d-1+1 = d$.

Let $\bar{R} := R/\mathfrak{p}_0$ and $\bar{S} := S/\mathfrak{p}_0 S$. Tensoring the exact sequence

$$0 \to \bar{R} \xrightarrow{x} \bar{R} \to \bar{S} \to 0$$

with $R/\mathfrak{m}^{n+1}$, we get an exact sequence

$$0 \to H_n \to \bar{R}/\mathfrak{m}^{n+1}\bar{R} \xrightarrow{x} \bar{R}/\mathfrak{m}^{n+1}\bar{R} \to \bar{S}/\mathfrak{m}^{n+1}\bar{S} \to 0.$$

Hence, the two outer modules have the same length, so that $\chi_{\bar{S}}(n) = \ell(H_n)$ for sufficiently large n. On the other hand, using 6.6.15, we have an exact sequence

$$0 \to H_n \to \bar{R}/\mathfrak{m}^{n+1}\bar{R} \to \bar{R}/(\mathfrak{m}^{n+1}\bar{R} : x) \to 0$$

from which it follows that $\chi_{\bar{S}}(n) = \chi_{\bar{R}}(n) - \varphi(n)$, where $\varphi(n)$ denotes the length of the last module in the previous exact sequence (showing incidentally that $\varphi(n)$ too is a polynomial for $n \gg 0$). To estimate $\varphi(n)$, we use the Artin-Rees Lemma (see [54, Theorem 8.5] or [7, Proposition 10.9]).[2] By that theorem, there exists some c such that

$$\mathfrak{m}^{n+1}\bar{R} \cap x\bar{R} \subseteq \mathfrak{m}^{n+1-c}x\bar{R}$$

for all $n > c$. Hence if $s \in (\mathfrak{m}^{n+1}\bar{R} : x)$, that is to say, if $sx \in \mathfrak{m}^{n+1}\bar{R}$, then $sx \in \mathfrak{m}^{n+1-c}x\bar{R}$. Since $\bar{R}$ is a domain, this yields $s \in \mathfrak{m}^{n+1-c}\bar{R}$, and hence we have inclusions $\mathfrak{m}^{n+1}\bar{R} \subseteq (\mathfrak{m}^{n+1}\bar{R} : x) \subseteq \mathfrak{m}^{n+1-c}\bar{R}$ for all $n > c$. Therefore, for $n \gg 0$, we get inequalities

$$\chi_{\bar{R}}(n-c) \le \varphi(n) \le \chi_{\bar{R}}(n).$$

This shows that the (polynomial representing) φ has the same leading term as $\chi_{\bar{R}}$, and hence their difference, which is $\chi_{\bar{S}}$, has degree strictly less. Clearly, $\chi_{\bar{R}}(n) \le \chi_R(n)$ and hence $\operatorname{Hilbdim}(\bar{R}) \le \operatorname{Hilbdim}(R)$. Since $\bar{S}$ has dimension $d-1$ by choice of x, induction yields $\operatorname{Hilbdim}(\bar{S}) = d-1$. Putting everything together, we get $\operatorname{Hilbdim}(R) \ge d$. In summary, we proved the inequalities

$$\operatorname{geodim}(R) \le d \le \operatorname{Hilbdim}(R)$$

and hence we are done by (4.5). □

From this important theorem, various properties of dimension can now be deduced. We start with a loose end: the dimension of affine n-space (as stated in Theorem 3.2.1), or equivalently, the dimension of a polynomial ring.

Corollary 4.3.3. *If K is a field and A is either the polynomial ring or the power series ring over K in n variables ξ, then* $\dim(A) = n$.

[2] Unfortunately, the weak variant of Artin-Rees that we will prove in Theorem 12.2.1 below, is not sufficiently strong for the present argument to work.

Proof. The chain of prime ideals

$$(0) \subsetneq \xi_1 A \subsetneq (\xi_1, \xi_2)A \subsetneq \cdots \subsetneq \mathfrak{m} := (\xi_1, \ldots, \xi_n)A$$

shows that $\mathfrak{m}$ has height at least n (and, in fact, equal to n). Hence $\dim(A)$ and $\dim(A_\mathfrak{m})$ are at least n. In the power series case (so that A is local), $\mathfrak{m}$ witnesses the estimate $\operatorname{geodim}(A) \le n$. Hence we are done in the power series case by Theorem 4.3.2.

Let me only prove the polynomial case when K is algebraically closed (the general case is treated in Exercise 4.4.6). By Theorem 3.2.2, any maximal ideal is of the form $\mathfrak{m}_\mathbf{u}$ for some $\mathbf{u} \in K^n$. Hence $A_{\mathfrak{m}_\mathbf{u}} \cong A_\mathfrak{m}$ by a linear change of coordinates. Therefore, it suffices in view of 4.1.3 to show that $A_\mathfrak{m}$ has dimension n. However, again $\mathfrak{m}A_\mathfrak{m}$ witnesses that $\operatorname{geodim}(A_\mathfrak{m}) \le n$, and we are done once more by Theorem 4.3.2. □

The next application is another famous theorem due to Krull:

Theorem 4.3.4 (Hauptidealensatz/Principal Ideal Theorem). *Any proper ideal in a Noetherian ring generated by h elements has height at most h.*

Proof. Let $I \subseteq B$ be an ideal generated by h elements, let $\mathfrak{p}$ be a minimal prime of I, and put $R := B_\mathfrak{p}$. Since IR is then $\mathfrak{p}R$-primary, $\operatorname{geodim}(R) \le h$. Hence $\mathfrak{p}$ has height at most h by Theorem 4.3.2 and 4.1.3. Since this holds for all minimal primes of I, the height of I is at most h. □

Let $(R, \mathfrak{m})$ be a Noetherian local ring of dimension d. By Theorem 4.3.2, there exists a d-tuple $\mathbf{x}$ generating an $\mathfrak{m}$-primary ideal. We give a name to such a tuple:

Definition 4.3.5 (System of parameters). Any tuple of length equal to the dimension of R and generating an $\mathfrak{m}$-primary ideal will be called a *system of parameters* of R (sometimes abbreviated as *s.o.p*); the ideal it generates is then called a *parameter ideal*.

In other words, a parameter ideal is an $\mathfrak{m}$-primary ideal requiring the least possible number of generators, namely $d = \dim(R)$. The next result will enable us to construct systems of parameters. To this end, we define the *dimension* of an ideal $I \subseteq B$ as the dimension of its residue ring B/I. In particular, any d-dimensional prime ideal in a d-dimensional Noetherian local ring is a minimal prime ideal, whence there are only finitely many such ideals.

Corollary 4.3.6. *If R is a d-dimensional Noetherian local ring and x a non-unit in R, then $d - 1 \le R/xR \le d$. The lower bound is attained if and only if x lies outside all d-dimensional prime ideals of R.*

Proof. The second inequality is obvious (from the point of view of Krull dimension). Towards a contradiction, suppose $S := R/xR$ has dimension strictly less than $d - 1$. By Theorem 4.3.2 there exists a system of parameters $(x_1, \ldots, x_e)$ in S with

$e < d-1$. However, any liftings of the x_i to R together with x then generate an $\mathfrak{m}$-primary ideal, contradicting Theorem 4.3.2. It is now not hard to see that x lies in a d-dimensional prime ideal if and only if S admits a chain of prime ideals of length d, from which the last assertion follows. □

If R has dimension d, then element outside any d-dimensional prime is called a *parameter*. Since there are only finitely many d-dimensional prime ideals, parameters exist as soon as $d > 0$. We can now reformulate (see Exercise 4.4.10): $(x_1,\dots,x_d)$ is a system of parameters if and only if each x_i is a parameter in $R/(x_1,\dots,x_{i-1})R$.

Finite extensions. Recall that a homomorphism $R \to S$ is called *finite* if S is finitely generated as an R-module. Similarly, a morphism of affine schemes $Y \to X$ is called *finite* if the induced homomorphism on the coordinate rings is finite. Any surjective ring homomorphism $R \to R/I$ is finite.

4.3.7 *A finite morphism $Y \to X$ of affine schemes is surjective if the corresponding homomorphism of coordinate rings is injective.*

Indeed, assume $R \to S$ is a finite and injective homomorphism, and let $\mathfrak{p}$ be a prime ideal of R. Let $\mathfrak{n}$ be a maximal ideal in $S_\mathfrak{p} := R_\mathfrak{p} \otimes_R S$, and put $\mathfrak{m} := \mathfrak{n} \cap R_\mathfrak{p}$. Since $R_\mathfrak{p}/\mathfrak{m} \subseteq S_\mathfrak{p}/\mathfrak{n}$ is again finite, and the latter ring is a field, so is the former by Lemma 3.2.7. Hence $\mathfrak{m}$ is a maximal ideal, necessarily equal to $\mathfrak{p}R_\mathfrak{p}$. If we put $\mathfrak{q} := \mathfrak{n} \cap S$, then an easy calculation shows $\mathfrak{p} = \mathfrak{q} \cap R$ (verify this!). By 3.3.3, this means that the morphism $\operatorname{Spec}(S) \to \operatorname{Spec}(R)$ is surjective. □

Theorem 4.3.8. *Let $R \subseteq S$ be a finite homomorphism of Noetherian rings. If R has dimension d, then so does S.*

Proof. Put $d := \dim(R)$ and $e := \dim(S)$. To see the inequality $e \le d$, choose a maximal ideal $\mathfrak{n}$ in S of height e, and put $\mathfrak{m} := \mathfrak{n} \cap R$. Since $R_\mathfrak{m}$ has dimension at most d, there exists an $\mathfrak{m}R_\mathfrak{m}$-primary ideal $I \subseteq R_\mathfrak{m}$ generated by at most d elements by Theorem 4.3.2. Since $S_\mathfrak{n}/IS_\mathfrak{n}$ is then a finitely generated $R_\mathfrak{m}/I$-module, it is Artinian. Hence $IS_\mathfrak{n}$ is $\mathfrak{n}S_\mathfrak{n}$-primary, showing that $\operatorname{geodim}(S_\mathfrak{n}) \le d$. Since the left hand side is equal to e by Theorem 4.3.2, we showed $e \le d$.

We prove the converse inequality by induction on d (where the case $d = 0$ is clearly trivial). Choose a d-dimensional prime ideal $\mathfrak{p} \subseteq R$. Using 4.3.7, we can find a prime ideal $\mathfrak{q} \subseteq S$ *lying above* $\mathfrak{p}$, that is to say, $\mathfrak{p} = \mathfrak{q} \cap R$. Put $\bar{R} := R/\mathfrak{p}$ and $\bar{S} := S/\mathfrak{q}$. In particular, $\bar{R} \subseteq \bar{S}$ is again finite and injective. By the same argument, we can take a $d-1$-dimensional prime ideal $\mathfrak{P} \subseteq \bar{R}$, and a prime ideal $\mathfrak{Q} \subseteq \bar{S}$ lying above it. By the induction hypothesis applied to the finite extension $\bar{R}/\mathfrak{P} \subseteq \bar{S}/\mathfrak{Q}$, we get $d-1 = \dim(\bar{R}/\mathfrak{P}) \le \dim(\bar{S}/\mathfrak{Q})$. However, since any non-zero element in a domain is a parameter (see Corollary 4.3.6), the dimension of $\bar{S}/\mathfrak{Q}$ is strictly less than the dimension of $\bar{S}$, which itself is less than or equal to e. Hence $d-1 \le e-1$, as we wanted to show. □

Corollary 4.3.9. *If $V \to K^d$ is a Noether normalization of an affine variety V, then V has dimension d.*

Proof. By definition of Noether normalization, we have a finite, injective homomorphism $K[\zeta] \subseteq K[V]$ with $\zeta = (\zeta_1, \dots, \zeta_d)$. By Corollary 4.3.3, the first ring has dimension d, whence so does the second by Theorem 4.3.8. This in turn means that V has dimension d. □

4.4 Exercises

Ex 4.4.1

Prove the inequality in 4.1.1. In fact, this is often an equality, for instance if R is a polynomial ring over a field, but this is already a much less trivial result. Verify it when R is a polynomial ring over a field in a single indeterminate.

Ex 4.4.2

Show that length is additive *in the sense that if $0 \to K \to M \to N \to 0$ is a short exact sequence of A-modules, then $\ell(M) = \ell(K) + \ell(N)$.*

Ex 4.4.3

Prove 4.1.5. More generally, show that if R is an Artinian local ring with residue field k, then the length of R is equal to its vector space dimension over k. For the latter, you need to know that k is a subfield of R, and this is proven in Theorem 7.4.2 and Remark 7.4.3, but you can just assume for the moment that this is the case.

Ex 4.4.4

Let S be a standard graded R-algebra. Show that S is Noetherian if R is.

Ex 4.4.5

Show the first assertion in 4.1.3: the height of a prime ideal $\mathfrak{p} \subseteq R$ is equal to the dimension of $R_{\mathfrak{p}}$.

Ex 4.4.6

Use Exercise 3.6.25 to complete the proof of Corollary 4.3.3.

Ex 4.4.7

Generalize Corollary 4.3.3 by replacing the field by any Artinian local ring. Moreover, in the power series case, formulate a result with the base ring any Noetherian local ring. Such a result also holds in the polynomial case, but the proof requires some more powerful tools such as flatness, discussed in §6; for a proof, see for instance [54, Theorem 15.4].

Ex 4.4.8

Work out the details of the proof of Corollary 4.2.3.

*Ex 4.4.9

Develop the theory of Hilbert-Samuel polynomials also for finitely generated R-modules M and for $\mathfrak{m}$-primary ideals I, by using the graded algebra

$$\mathrm{Gr}_I(R) := \oplus_n I^n/I^{n+1}$$

and the graded module

$$\mathrm{Gr}_I(M) := \oplus_n I^n M/I^{n+1} M$$

.

Ex 4.4.10

Show that $(x_1,\dots,x_d)$ is a system of parameters in R if and only if x_i is a parameter in $R/(x_1,\dots,x_{i-1})R$ for every $i = 1,\dots,d$.

Ex 4.4.11

Show that if $\mathbf{x}$ is a tuple of length e in a Noetherian local ring R such that $\mathbf{x}R$ has height e, then $\mathbf{x}$ can be extended to a system of parameters of R. Using the same technique, also show that if $\mathfrak{p}$ is a prime ideal of height h, then there exists a system of parameters $(y_1,\dots,y_d)$ such that $\mathfrak{p}$ is a minimal prime of $(y_1,\dots,y_h)R$.

Ex 4.4.12

Prove the following more precise form of 4.3.7: a finite morphism $Y = \mathrm{Spec}(S) \to X = \mathrm{Spec}(R)$ is surjective if and only if the kernel of the corresponding ring homomorphism $R \to S$ is nilpotent. In fact, the only if direction is true for any morphism.

*Ex 4.4.13

For non-Noetherian rings, Krull dimension and geometric dimension need not agree; here's an example. Let R be the power series ring $K[[\xi]]$ in $d > 0$ variables ξ, and let $R_\natural$ be its ultrapower. Show that $\mathrm{geodim}(R_\natural) = d = \mathrm{Hilbdim}(R_\natural)$ but $\dim(R_\natural) > d$. To establish the latter inequality, show that the ideal of infinitesimals of $R_\natural$ is a prime ideal. In fact, $R_\natural$ has infinite Krull dimension, but proving this requires some more work.

*Ex 4.4.14

Show using Noether Normalization and Exercise 4.4.13 that any affine domain C is equidimensional*, in the sense that every maximal ideal of C has the same height.*

Additional exercises.

Ex 4.4.15

Show that a finite injective homomorphism $A \subseteq B$ satisfies the going-up theorem*, meaning that given any inclusion of prime ideals $\mathfrak{p} \subseteq \mathfrak{q} \subseteq A$ and any prime ideal $\mathfrak{P} \subseteq B$ lying over $\mathfrak{p}$, we can find a prime ideal $\mathfrak{Q} \subseteq B$ containing $\mathfrak{P}$ and lying over $\mathfrak{q}$.*

Chapter 5
Singularity theory

As the term suggests, a 'singularity' is a point where something unusual happens. We gave a formal definition of a singular point in Definition 3.5.4. In this chapter, we investigate the algebraic theory behind this phenomenon. In particular, we will identify a certain type of singularity, the Cohen-Macaulay singularity, which plays an important role in the later chapters.

5.1 Regular local rings

According to our 'algebraization paradigm', geometric properties of points are reflected by their local rings. Before we make this translation, we first explore a little the classical notion, using plane curves as example.

Multiple points on a plane curve. A *plane curve* C is an irreducible affine variety given by a non-constant, irreducible polynomial $f(\xi,\zeta) \in A := K[\xi,\zeta]$, for K some algebraically closed field, that is to say, $C = \mathrm{V}(f)$. By Corollary 4.3.6, a plane curve has dimension one. So we arrive at the more general concept of a *curve* as a one-dimensional, irreducible scheme. The degree t of f is also called the *degree* of the plane curve C. If $t = 1$, then C is just a line. So from now on, we will moreover assume $t > 1$. An easy form of Bezout's theorem states:

5.1.1 *Any line intersects the plane curve C of degree t in at most t distinct points, and there exist lines which have exactly t distinct intersection points with C.*

The proof is elementary: the general equation of a line L is $a\xi + b\zeta + c = 0$ and hence the intersection $|C \cap L|$ is given by the radical of the ideal $(a\xi + b\zeta + c, f)A$ (or, viewed as an affine scheme $C \cap L$ by the ideal itself; see page 38). In terms of equations, assuming $b = 1$ for the sake of simplicity, this means that the (ξ-values of the) intersection points are given by the equation $f(\xi, -a\xi - c) = 0$, a polynomial of degree t or less, which therefore has at most t solutions. Choosing a, b, c sufficiently general, we can moreover guarantee that this polynomial has t distinct roots. We can now state when a point P on C is singular, but to not confuse with our formal definition 45, we use a different terminology:

Definition 5.1.2. A point P on a plane curve C of degree t is called *multiple*, if every line through P intersects C in less than t distinct points. More precisely, we say that P is an *n-tuple* point on C, or $\mathrm{mult}_C(P) = n$, if n is the number of points absorbed at P in each intersection with a line, that is to say,

$$\mathrm{mult}_C(P) := \min_{L \text{ line through } P} (t - \mathrm{card}(|C \cap L|) + 1).$$

Here $|C \cap L|$ denotes the (naive) intersection as sets, not as schemes. A point which is not multiple, i.e., a 1-tuple point, is called a *simple* point.

Let us look at two examples of multiple points:

An example of a node. Let $f := \xi^2 - \zeta^2 - 3\zeta^3$ and let P be the origin. Hence a line L_a through P has equation $\zeta = a\xi$ for some $a \in K$ (for sake of simplicity, we ignore the ζ-axis; the reader should check that this makes no difference in what follows). Substituting this in the equation, the intersection points with C are given by the equations $\zeta = a\xi$ and $\xi^2 - (a\xi)^2 - 3(a\xi)^3 = 0$. The second equation reduces to $\xi = 0$ or $\xi = (1-a^2)/3a^3$, thus giving only two intersection points, contrary to the expected value of three. In conclusion, P is a double point. One can check that it is the only multiple point on C (check this for instance for the point with coordinates $(2,1)$).

Moreover, note that the two diagonals $L_{\pm 1}$ intersect C in exactly one point, that is to say, the lines $y = \pm x$ have even *higher contact* with C; they are often refered to as the *tangent lines* of C at P. To formally define a tangent line, one needs to introduce the intersection number $i(L,C;P)$ of a line L with C at P, and then call L a *tangent line* if $i(L,C;P) > \mathrm{mult}_C(P)$. One way of doing this is by defining the *intersection number* $i(L,C;P)$ as the length of R/LR, where $R := (A/fA)_{\mathfrak{m}}$ is the local ring of P at C and where we identify the line L with its defining linear equation. One checks that $i(L_a,C;P)$ equals two for $a \neq \pm 1$, and three for $a = \pm 1$.

To calculate the tangent space $T_{C,P}$ as defined on page 45, let $\mathfrak{m} := (\xi,\zeta)A$ be the maximal ideal corresponding to the origin. Since $\mathfrak{m}R$ is generated by two elements, the embedding dimension of R is two, whence so is the dimension of the tangent space $T_{C,P}$ by 3.5.3. Hence, since the tangent space has higher dimension than the scheme, P is singular on C.

An example of a cusp. For our next example, let $f := \xi^4 - \zeta^3$, a curve of degree four, and let P be the origin as before. The intersection with L_a is given by the equation $\xi^4 - (a\xi)^3 = 0$, which yields two intersection points: namely P and (a^3, a^4). Hence P is a triple point of C. Moreover, there is now only one value of a which leads to a higher contact, namely $a = 0$, showing that the ξ-axis is the only tangent line (double-check that the ζ-axis does not have higher contact). A multiple point with a unique tangent line is called a *cusp*. A similar calculation as before shows that $T_{C,P}$ is again two-dimensional, whence P is singular. Let us now prove this in general:

Proposition 5.1.3. *A point on a plane curve is a multiple point if and only if it is singular.*

Proof. Let f be the equation, of degree t, defining the curve C, and let P be a point on C. After a change of coordinates, we may assume P is the origin, defined by the maximal ideal $\mathfrak{m} := (\xi,\zeta)A$. If P is non-singular, then the embedding dimension of $\mathscr{O}_{C,P} = (A/fA)_{\mathfrak{m}}$ is one. Hence either ξ or ζ generates $\mathfrak{m}R$. So, after interchanging ξ and ζ if necessary, we can write ζ as a fraction $(\xi g + f\tilde{g})/h$ in $A_{\mathfrak{m}}$, for some $g, \tilde{g}, h \in A$ with $h \notin \mathfrak{m}$. Hence the intersection with L_a is given by $\zeta = a\xi$ and

$$a\xi = \frac{\xi g(\xi, a\xi) + f(\xi, a\xi)\tilde{g}(\xi, a\xi)}{h(\xi, a\xi)}.$$

Since f has no constant term, we may divide out ξ, so that the last equation becomes

$$ah(\xi, a\xi) = g(\xi, a\xi) + \tilde{f}(\xi) \tag{5.1}$$

for some $\tilde{f} \in K[\xi]$. If P would be a multiple point of C, then $\xi = 0$ should still be a solution of (5.1). However, this can only happen if $a = (g(0,0) + \tilde{f}(0))/h(0,0)$ (note that $h(0,0) \neq 0$ by assumption). In other words, a general line has only one intersection point at P, and hence P is a simple point. Note that it has exactly one tangent line, given by the above exceptional value of a.

Conversely, assume P is simple, and write $f = u\xi + v\zeta + \tilde{f}$ with $u, v \in K$ and $\tilde{f} \in \mathfrak{m}^2$. By assumption, the equation $u\xi + va\xi + \tilde{f}(\xi, a\xi) = 0$ should have in general $t-1$ solutiuons different from $\xi = 0$. For this to be true, at least one of u or v must be non-zero. So assume, without loss of generality, that $u \neq 0$, and then multiplying with its inverse, we may even assume $u = 1$. It follows that $\xi = -v\zeta - \tilde{f}$ in R, showing that $\mathfrak{m}R = \zeta R$ by Nakayama's Lemma, and therefore that R has embedding dimension one. $\square$

By the above argument, in order for P to be simple, $A_{\mathfrak{m}}/fA_{\mathfrak{m}}$ has to have embedding dimension one, which by Nakayama's lemma is equivalent with f being a minimal generator of $\mathfrak{m}A_{\mathfrak{m}}$, that is to say, $f \in \mathfrak{m}A_{\mathfrak{m}} - \mathfrak{m}^2A_{\mathfrak{m}}$. In Exercise 5.3.4 you will prove the following generalization:

5.1.4 *A point P is an n-tuple point on a plane curve $C := \mathrm{V}(f)$ if and only if n is the maximum of all k such that $f \in \mathfrak{m}^k A_{\mathfrak{m}}$, where $\mathfrak{m} := \mathfrak{m}_P$ is the maximal ideal of P.*

Geometrically, a closed point x is singular on an affine variety, or more generally, on an affine scheme X, if the dimension of its tangent space is larger than the local dimension of X at x. In particular, singularity is a local property, completely captured by the local ring of the point. Since the dimension of the tangent space is equal to embedding dimension of the local ring by 3.5.3, we can now formulate non-singularity entirely algebraically:

Definition 5.1.5 (Regular local ring). We call a Noetherian local ring $(R,\mathfrak{m})$ *regular* if and only if its dimension is equal to its embedding dimension.

In view of Theorem 4.3.2, regularity is equivalent with the maximal ideal being generated by the least possible number of elements. In particular, some system of parameters generates the maximal, and any such system is called a *regular system of parameters*. Geometrically, a point x on a scheme X is *regular*, or *non-singular*, if $\mathcal{O}_{X,x}$ is regular. An Artinian local ring is regular if and only if it is a field. By Corollary 4.3.3, a power series ring over a field is regular. Using that same theorem in conjunction with the Nullstellensatz (Theorem 3.2.2), we also get a similar result over an algebraically closed field K (for a more general version, see Exercise 5.3.6):

5.1.6 *Each closed point of affine n-space $\mathbb{A}^n_K$ is regular.*

To formulate a stronger result, let us call a ring B *regular* if each localization at a maximal ideal is regular. Similarly, we call a scheme X *regular* if all of its closed points are regular. Hence we may reformulate 5.1.6 as: $\mathbb{A}^n_K$ is regular. This begs the question: what about the non-closed points of $\mathbb{A}^n_K$? As it turns out, they too are regular, and in fact, this is a general property of regular rings:

5.1.7 *Any localization of a regular ring is again regular.*

To prove this, however, one needs a different characterization, homological in nature, of regular rings due to Serre (it was only after he proved his theorem that the above result became available). We will not provide all details, but 5.1.7 will be proved in Corollary 6.5.8 below. Another property is more readily available: geometric intuition predicts that at an intersection point of two distinct components, the scheme ought to be singular. Put differently, a variety should be irreducible in 'the neighbourhood of' a non-singular point. This translates into the following property of the local ring of the point:

5.1.8 *A regular local ring is a domain.*

To prove this, we need another characterization of regular local rings:

Theorem 5.1.9. *Let $(R,\mathfrak{m})$ be a d-dimensional Noetherian local ring with residue field k, and let $S := \mathrm{Gr}(R)$ be its associated graded ring. Then R is regular if and only if S is isomorphic to a polynomial ring over k in d variables.*

Proof. Let $A := k[\xi]$ with $\xi := (\xi_1,\dots,\xi_d)$, viewed as a standard graded k-algebra in the obvious way. If $A \cong S$, then $A_1 \cong S_1$ has k-vector space dimension d. Since $S_1 = \mathfrak{m}/\mathfrak{m}^2$, Nakayama's lemma shows that R has embedding dimension d, whence is regular. To prove the converse, assume R is regular, and we need to show that $S \cong A$. By assumption, $\mathfrak{m}$ is generated by d elements, $x_1,\dots,x_d$. Define a homomorphism $\varphi\colon k[\xi] \to S$ of graded k-algebras by the rule $\xi_i \mapsto x_i$. Since $\mathfrak{m} = (x_1,\dots,x_d)R$, the homomorphism φ is surjective (verify this!). Let I be its kernel. Hence $A/I \cong S$. Now, A has dimension d by Corollary 4.3.3. I claim that S has dimension at least d. However, if $I \neq 0$, then by Corollary 4.3.6, the dimension of A/I is strictly less than d. Hence $I = 0$, as we wanted to show (and S has actually dimension equal to d).

To prove the claim, it suffices to show that the maximal ideal $\mathfrak{n} := S_+$ has height d. Since $\mathfrak{n}^{n+1} = \oplus_{k>n} S_k$, we get $S/\mathfrak{n}^{n+1} \cong S_0 \oplus \cdots \oplus S_n$, and its length is equal to $\ell(R/\mathfrak{m}^{n+1})$ by (4.3). Since $S/\mathfrak{n}^{n+1} \cong S_\mathfrak{n}/\mathfrak{n}^{n+1}S_\mathfrak{n}$ (check this!), we see that R and $S_\mathfrak{n}$ have the same Hilbert-Samuel polynomial, whence the same dimension by Theorem 4.3.2, as we wanted to show. □

Incidentally, in the last part of the proof, we did not use our hypothesis on the regularity of the ring, so that we showed one inequality in the next result; the converse will not be needed here and can be found in for instance [54, Theorem 13.9].

5.1.10 *The dimension of a Noetherian local ring is equal to the dimension of its associated graded ring.*

Proof of 5.1.8. Given two non-zero elements $a, b \in R$, we need to show that their product is non-zero too. By Theorem 2.4.11, there exist $k, l \in \mathbb{N}$ such that $a \in \mathfrak{m}^k \setminus \mathfrak{m}^{k+1}$ and $b \in \mathfrak{m}^l \setminus \mathfrak{m}^{l+1}$. Hence a and b induce two non-zero elements $\bar{a} \in S_k$ and $\bar{b} \in S_l$ respectively. Since S is a domain by Theorem 5.1.9, their product $\bar{a}\bar{b} \in S_{k+l}$ is non-zero, whence a fortiori so is ab. □

Why we need projective space. Above, we have seen examples of plane curves having a multiple point. Of course, some curves are regular. The simplest example is obviously a line. Another is given by the so-called *elliptic curves*, defined by an equation

$$\zeta^2 = \xi(\xi - 1)(\xi - u)$$

with $u \neq 0, 1$. You can use the criterion from Exercise 5.3.3 to show that every point on an elliptic curve is simple, provided the characteristic of K is not 2, whence regular by Proposition 5.1.3 (see also Exercise 5.3.9). Another example of a regular curve is the one defined by the equation $\xi\zeta^2 = 1$ (again easily verified by means of Exercise 5.3.3). However, in this latter case, we are overlooking the 'points at infinity'. More precisely, recall that $\mathbb{P}^2_K$ is obtained by glueing together three copies of $\mathbb{A}^2_K$ (see page 43), each corresponding by inverting one of the 'projective' variables. So we may view $\mathbb{A}^2_K$, with coordinates (ξ, ζ) as the copy corresponding to inverting the last variable, and embed it in $\mathbb{P}^2_K$. Given a plane curve $C = \mathrm{V}(f)$ (or rather, the affine scheme $\mathrm{Spec}(B)$ with $B := A/fA$ determined by it), let $\bar{C}$ be the closure of C inside $\mathbb{P}^2_K$. We can endow $\bar{C}$ with the structure of a projective variety as follows: let $\tilde{f}$ be the *homogenization* of f, that is to say, if f has degree t, then

$$\tilde{f}(\xi, \zeta, \eta) := \eta^t f(\xi/\eta, \zeta/\eta). \tag{5.2}$$

I claim that the underlying space of $\tilde{C} := \mathrm{Proj}(\tilde{B})$ is equal to $\bar{C}$, where $\tilde{A} := K[\xi, \zeta, \eta]$ and $\tilde{B} := \tilde{A}/\tilde{f}\tilde{A}$. Since $\tilde{A}_{(\eta)} \cong A$ by 3.4.3, we get $\tilde{B}_{(\eta)} \cong B$ by (5.2), showing that

$$\mathbb{A}^2_K \cap \tilde{C} = \tilde{\mathrm{D}}(\eta) \cap \tilde{C} = C.$$

Our claim now follows, since the closure of $\mathbb{A}^2_K$ is just $\mathbb{P}^2_K$. We call $\tilde{C}$ the *projectification* or *completion* of C.

Returning to our question on singularities: any point of $\tilde{C} \setminus C$ will be called a *point at infinity* of C. To check whether such a point is non-singular, we have to 're-coordinatize', that is to say, look at one of the two other copies of $\mathbb{A}^2_K \subseteq \mathbb{P}^2_K$. Let us do this on the example with equation $f := \xi\zeta^2 - 1$. Following the recipe in (5.2), we get $\tilde{f} = \xi\zeta^2 - \eta^3$. On the copy $\tilde{\mathrm{D}}(\xi) = \mathbb{A}^2_K$, the intersection with $\tilde{C}$ is the affine scheme given by $\zeta^2 - \eta^3$, the equation of a cusp with a singular point at $\zeta = \eta = 0$ (note that it is straightforward to undo the homogenization (5.2): just replace the pertinent variable, here ξ, by 1). Hence $\tilde{C}$ is not regular. In Exercise 5.3.10, you will show that in contrast, the projectification of any elliptic curve remains regular.

In the above discussion, we used curves merely as an illustration: a similar treatment can be given for higher dimensional affine schemes as well (see Exercise 5.3.11): any closed affine subscheme $X \subseteq \mathbb{A}^n_K$ can be projectified to a projective scheme $\tilde{X} \subseteq \mathbb{P}^n_K$. So, even if an affine scheme itself is regular, it might not be as 'good' as we believe it to be, as we do not see its points at infinity. For that we need to go to its projectification.

5.2 Cohen-Macaulay rings

Algebraic geometry has developed for a large part in an attempt to gain a better understanding of singularities, and if possible, to classify them. As it turns out, certain singularities have nicer properties than others. Our goal is to identify such a class of singularities, or equivalently, by passing to their local ring, such a class of Noetherian local rings, which are more amenable to algebraic methods: the 'Cohen-Macaulay' singularities. In order to do this, we must first study an invariant called 'depth'.

Regular sequences. Recall that an element in a ring R is called a *non-zero divisor* if multiplication with this element is injective; more generally, an element x is a *non-zero divisor* on an R-module M if multiplication by x is injective on M. Recall that a prime ideal in a Noetherian ring R is called an *associated prime* of R (respectively, of a finitely generated R-module M), if it is of the form $\mathrm{Ann}_R(x)$ for some $x \in R$ (respectively, of the form $\mathrm{Ann}_R(\mu)$ for some $\mu \in M$). Moreover, R (respectively, M) admits only finitely many associated prime ideals, among which are all the minimal prime ideals, and an element is a non-zero divisor if and only if it is not contained in any associated prime ideal (for all this, see for instance [54, §6]).

A non-zero divisor of R which is not a unit is called a *regular element* in R, or *R-regular* (do not confuse with the notion of a regular local ring!). Similarly, we say that x is *M-regular* if it is a non-zero divisor on M and $xM \neq M$ (be aware that some authors might use a slightly different definition for these notions). More generally, a sequence $(x_1, \dots, x_d)$ is called a *regular sequence* in R, or *R-regular*, (respectively, *M-regular*) if each x_i is regular in $R/(x_1, \dots, x_{i-1})R$ (respectively, in $M/(x_1, \dots, x_{i-1})M$) for $i = 1, \dots, d$. Here, and elsewhere, we do not distinguish notationally between an element in a ring R and its image in any residue ring R/I, or for that matter, in any R-algebra S. If $(x_1,\dots,x_d)$ is an R-regular sequence, then by assumption $(x_1,\dots,x_d)R$ is a proper ideal of R. In particular, if R is local, then all x_i belong to the maximal ideal. To be a regular sequence in a local ring is quite a strong property:

5.2.1 *In a Noetherian local ring R, any regular sequence can be enlarged to a system of parameters. In particular, a regular sequence can have length at most* $\dim(R)$. *In fact, if $\mathbf{x}$ is a regular sequence of length e, then $\mathbf{x}R$ has height e.*

To see this, we only need to show by induction on the length of the sequence that a regular element generates a height one prime ideal and is a parameter. However, since a regular element x does not belong to any associated prime, whence in particular not to any minimal prime, the ideal xR has height one by Theorem 4.3.4. Since x then neither belongs to any prime ideal of maximal dimension, it is a parameter. Using this in conjunction with Corollary 4.3.6, we get:

5.2.2 *If $\mathbf{x}$ is a regular sequence of length e in a d-dimensional Noetherian local ring R, then $R/\mathbf{x}R$ has dimension $d-e$.*

Cohen-Macaulay local rings. A d-dimensional Noetherian local ring is called *Cohen-Macaulay* if it admits a regular sequence of length d. Trivially, any Artinian local ring is Cohen-Macaulay. The next result justifies calling the Cohen-Macaulay property a type of singularity.

Proposition 5.2.3. *Any regular local ring is Cohen-Macaulay.*

Proof. Let us induct on the dimension d of the regular local ring R. The case $d=0$ is trivial since R is then a field. By assumption, the maximal ideal $\mathfrak{m}$ is generated by d elements $x_1,\dots,x_d$. I will show by induction on d that $(x_1,\dots,x_d)$ is in fact a regular sequence. Since R is a domain by 5.1.8, the element x_1 is regular. Put $R_1 := R/x_1R$. It is a Noetherian local ring of dimension $d-1$ by Corollary 4.3.6, and its maximal ideal $\mathfrak{m}R_1$ is generated by at most $d-1$ elements. Hence R_1 is again regular. By induction, $(x_2,\dots,x_d)$ is a regular sequence in R_1, from which it follows that $(x_1,\dots,x_d)$ is a regular sequence in R. $\square$

Depth. As we will see, being Cohen-Macaulay is a natural property, and many non-regular local rings are still Cohen-Macaulay. Since the notion hinges upon the length of a regular sequence, let us give this a name: the maximal length of a regular sequence in a Noetherian local ring R is called the *depth* of R, and is denoted $\operatorname{depth}(R)$. More generally, the *depth* of an ideal I is the maximal length of a regular sequence lying in I. We proved $\operatorname{depth}(R) \leq \dim(R)$ with equality precisely when R is Cohen-Macaulay. Immediately from our discussion on associated primes, we get:

5.2.4 *A Noetherian local ring has depth zero if and only if its maximal ideal is an associated prime.*

In particular, the one-dimensional local ring $R/(\xi^2,\xi\zeta)R$ is not Cohen-Macaulay, where $R := A_{\mathfrak{m}}$ is the local ring of the origin in $\mathbb{A}^2_K$.

5.2.5 *A one-dimensional Noetherian local domain is Cohen-Macaulay. In particular, any closed point on a (plane) curve is Cohen-Macaulay.*

As the reader might have surmised, we call a point x on a scheme X *Cohen-Macaulay* if $\mathscr{O}_{X,x}$ is Cohen-Macaulay. For an example of a non-Cohen-Macaulay local domain, necessarily of dimension at least two, see Exercise 5.3.14.

If R is Cohen-Macaulay, and $\mathbf{x}$ is a regular sequence of length $d := \dim(R)$, then $\mathbf{x}$ is automatically a system of parameters by 5.2.1. This raises the following question: what about arbitrary systems of parameters?

Theorem 5.2.6. *In a Cohen-Macaulay local ring, every system of parameters is a regular sequence. In particular, any regular sequence is* permutable*, meaning that an arbitrary permuation is again regular.*

Proof. The second statement is immediate from the first since in a system of parameters, order plays no role. However, we need it to prove the first assertion. And before we can prove this, we need to establish yet another special case of the first assertion: taking powers of the elements in a regular sequence gives again a regular sequence, and for this to hold, we do not even need the ring to be Cohen-Macaulay. Although both results have relatively elementary proofs, the combinatorics are a little involved, and so we will only present the argument for $d = 2$. Hence assume (x,y) is a regular sequence in some Noetherian local ring S. We claim that both (x^k, y^l) and (y^l, x^k) are S-regular sequences, for any $k,l \geq 1$. We first show that (x^k, y) is S-regular, for all $k \geq 1$. By induction, we only need to treat the case $k = 2$. Clearly, x^2 is S-regular, so we need to show that y is S/x^2S-regular. Hence suppose $by \in x^2S$, say $by = ax^2$. Since y is S/xS-regular, $b \in xS$, say $b = cx$. Hence, $cxy = ax^2$, and using that x is S-regular, $cy = ax$. Using again that y is S/xS-regular then yields $c \in xS$, which proves that $b = cx \in x^2S$, as we wanted to show.

Next, we show that (y,x) is S-regular. To show that y is S-regular, let $by = 0$. By our previous result, (x^n, y) is a regular sequence for every n, which means that y is S/x^nS-regular. Applied to $by = 0$, we get $b \in x^nS$. Since this holds for all n, we get $b \in \mathfrak{I}_S = 0$ by Theorem 2.4.11. So remains to show that x is S/yS-regular. Suppose $ax \in yS$, say $ax = by$. Since y is S/xS-regular, $b \in xS$, say, $b = cx$. From $ax = cxy$ and the fact that x is S-regular, we get $a = cy$, as we needed to show. Finally, to prove that (x^k, y^l) and (y^l, x^k) are S-regular, observe that the following sequences are S-regular: (x^k, y) by the first property, (y, x^k) by the second, (y^l, x^k) by the first, and finally (x^k, y^l) by the second.

So, with these two properties proven for $d = 2$, and assuming them for arbitrary d, let us turn to the proof of the theorem. Let $(R, \mathfrak{m})$ be a Cohen-Macaulay local ring of dimension d, and let $(x_1, \dots, x_d)$ be a regular sequence. We prove by induction on d that any system of parameters $(y_1, \dots, y_d)$ is a regular sequence. There is nothing to show if $d = 0$, so assume $d > 0$. Put $I := (x_1, \dots, x_{d-1})R$. Since x_d is by assumption R/I-regular, $\mathfrak{m}(R/I)$ is not an associated prime. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ be prime ideals in R such that their image in R/I are precisely the associated primes of the latter ring. Since $J := (y_1, \dots, y_d)R$ is $\mathfrak{m}$-primary, it cannot be contained in any of the $\mathfrak{p}_i$, whence by prime avoidance, we can find $y \in J$ notin $\mathfrak{m}J$ and not in any $\mathfrak{p}_i$. In particular, $y = \sum u_i y_i$ with at least one u_i a unit in R. After renumbering, we may assume that u_d is a unit. It follows that $(y_1, \dots, y_{d-1}, y)$ is again a system of parameters. Moreover, y is R/I-regular, showing that $(x_1, \dots, x_{d-1}, y)$ is a regular sequence. Since we established already that any permutation is again a regular sequence, $(y, x_1, \dots, x_{d-1})$ is R-regular. Hence $(x_1, \dots, x_{d-1})$ is R/yR-regular. Since

R/yR has dimension $d-1$ by Corollary 4.3.6, it is therefore Cohen-Macaulay. Hence $(y_1,\dots,y_{d-1})$, being a system of parameters in this ring, is by induction a regular sequence. In other words, $(y,y_1,\dots,y_{d-1})$ is a regular sequence, whence so is the permuted sequence $(y_1,\dots,y_{d-1},y)$. Finally, we show that y_d is R/J'-regular with $J' := (y_1,\dots,y_{d-1})R$, which then completes the proof that $(y_1,\dots,y_d)$ is a regular sequence. So assume $ay_d \in J'$. Since $y \equiv u_d y_d \mod J'$, we get $au_d y \in J'$. Since we already showed that y is R/J'-regular, we get $u_d a \in J'$, and since u_d is a unit, we finally get $a \in J'$, proving our claim. □

Corollary 5.2.7. *Let R be a Noetherian local ring, and let $\mathbf{x}$ be a regular sequence of length e. Then R is Cohen-Macaulay if and only if $R/\mathbf{x}R$ is.*

Proof. Let $d := \dim(R)$. By 5.2.2, the residue ring $R/\mathbf{x}R$ has dimension $d-e$. If it is Cohen-Macaulay, then there exists a regular sequence $\mathbf{y}$ of that length, and then $(\mathbf{x},\mathbf{y})$ (where we still write $\mathbf{y}$ for some lifting of that tuple to R) is a regular sequence of length d, showing that R is Cohen-Macaulay. Conversely, if R is Cohen-Macaulay, let $\mathbf{y}$ be a system of parameters in $R/\mathbf{x}R$. It follows that $(\mathbf{x},\mathbf{y})$ is a system of parameters in R, whence is a regular sequence by Theorem 5.2.6. Hence $\mathbf{y}$ is a regular sequence in $R/\mathbf{x}R$ of maximal length, proving that $R/\mathbf{x}R$ is Cohen-Macaulay. □

Corollary 5.2.8. *A Cohen-Macaulay local ring has no embedded primes, that is to say, any associated prime is minimal.*

Proof. Let R be a Cohen-Macaulay local ring and $\mathfrak{p}$ an associated prime. If $\mathfrak{p}$ has positive height, we can find $x \in \mathfrak{p}$ such that xR has height one. By Exercise 4.4.11, we can extend x to a system of parameters of R, which is then a regular sequence by Theorem 5.2.6. In particular, x is R-regular, contradicting that it belongs to an associated prime. □

In fact, Corollary 5.2.7 holds in far more greater generality: without assuming that R is Cohen-Macaulay, we have that the depth of R is equal to the depth of $R/\mathbf{x}R$ plus e. However, to prove this, one needs a different characterization of depth (using Ext functors), which we will not discuss in these notes. Another property that we can now prove is that any localization of a Cohen-Macaulay local ring is again Cohen-Macaulay (recall that we also still have to resolve this issue with regards to being regular).

Corollary 5.2.9. *If R is a Cohen-Macaulay local ring, then so is any localization $R_\mathfrak{p}$ at a prime ideal $\mathfrak{p} \subseteq R$.*

Proof. Let h be the height of $\mathfrak{p}$. Let us show by induction on h that $\mathfrak{p}$ contains a regular sequence of length h (that is to say, $\mathfrak{p}$ has depth h). It is not hard to check that the image of this sequence is then a regular sequence in $R_\mathfrak{p}$, showing that the latter is Cohen-Macaulay. Obviously, we may take $h > 0$. Since $\mathfrak{p}$ cannot be contained in an associated prime of R by Corollary 5.2.8, it contains an R-regular element x. Put $S := R/xR$, which is again Cohen-Macaulay by Corollary 5.2.7. As $\mathfrak{p}S$ has height $h-1$ (check this), it contains an S-regular sequence $\mathbf{y}$ of length $h-1$. But then $(x,\mathbf{y})$ is an R-regular sequence inside $\mathfrak{p}$, as we wanted to show. □

We can now say that a Noetherian ring A is *Cohen-Macaulay* if every localization at a maximal ideal is Cohen-Macaulay, and this is then equivalent by the last result with every localization being Cohen-Macaulay. Similarly, a scheme X is Cohen-Macaulay, if every local ring $\mathcal{O}_{X,x}$ at a (closed) point $x \in X$ is Cohen-Macaulay. In particular, any reduced curve is Cohen-Macaulay.

Independent sequences A sequence $\mathbf{x} := (x_1, \dots, x_d)$ in a ring R is said to be *independent (in the sense of Lech)*, if $a_1x_1 + \cdots + a_dx_d = 0$ for some $a_i \in R$ implies that all a_i lie in the ideal $I := \mathbf{x}R$. In fact, this is really a property of the ideal I. Namely, I/I^2 is free as an R/I-module if and only if I is generated by an independent sequence. For R a Noetherian local ring, a result of Vasconcelos [86] yields that a sequence $\mathbf{x}$ is regular if and only if it is independent and $\mathbf{x}R$ is a proper ideal of finite projective dimension.

Proposition 5.2.10. *Let $(R, \mathfrak{m})$ be a Noetherian local ring and $\mathbf{x} := (x_1, \dots, x_d)$ a sequence in R. If $(x_1^n, \dots, x_d^n)$ is independent for infinitely many n, then $\mathbf{x}$ is an R-regular sequence.*

Proof. For each n, put $I_n := (x_1^n, \dots, x_d^n)R$. I first claim that if $(x_1^n, \dots, x_d^n)$ is independent, then so is $(x_1^l, x_2^n, \dots, x_d^n)$, for each $l < n$. Indeed, suppose

$$a_1x_1^l + \sum_{i=2}^{d} a_i x_i^n = 0$$

for some $a_i \in R$. Multiplying this equation with x_1^{n-l} and using that $(x_1^n, \dots, x_d^n)$ is independent, we get $a_1, a_2x_1^{n-l}, \dots, a_dx_1^{n-l} \in I_n$. Hence, a_1 lies in $(x_1^l, x_2^n, \dots, x_d^n)R$, and we want to show the same for the a_i with $i \geq 2$. Write $a_ix_1^{n-l} = b_ix_1^n + c_i$ for some $b_i \in R$ and $c_i \in (x_2^n, \dots, x_d^n)R$. Multiplying with x_1^l gives $(b_ix_1^l - a_i)x_1^n + x_1^lc_i = 0$, so that using once more independence, we get $b_ix_1^l - a_i \in I_n$, showing that a_i lies in $(x_1^l, x_2^n, \dots, x_d^n)R$, thus completing the proof of the claim.

Secondly, I claim that x_1 is R-regular. Indeed, suppose $ax_1 = 0$, for some $a \in R$. Hence $ax_1^n = 0$ so that independence of $(x_1^n, x_2^n, \dots, x_d^n)$ yields that $a \in I_n \subseteq \mathfrak{m}^n$. Since this holds for infinitely many n, Krull's intersection theorem (Theorem 2.4.11) yields $a = 0$, proving the second claim.

We now turn to the proof of the assertion, for which we use induction on d. The case $d = 1$ follows from our second claim, so assume $d > 1$. By the second claim, x_1 is R-regular. Moreover, by the first claim, (the image of) $(x_2^n, \dots, x_d^n)$ is independent in R/x_1R for infinitely many n, so that $(x_2, \dots, x_n)$ is (R/x_1R)-regular by induction. Hence $(x_1, \dots, x_n)$ is R-regular, as we wanted to show. □

Immediately from this, we may deduce the following Cohen-Macaulay criterium.

Corollary 5.2.11. *A Noetherian local ring is Cohen-Macaulay if and only if every system of parameters is independent.* □

5.3 Exercises

Ex 5.3.1

Verify all the claims made on page 62 about the given node and cusp.

***Ex 5.3.2**

Prove the following more general version of Bezout's theorem: if $C := \mathrm{V}(f)$ and $D := \mathrm{V}(g)$ are two distinct plane curves of degree t and u respectively, then their scheme-theoretic intersection, given by the (Artinian) K-algebra $A/(f,g)A$ has K-vector space dimension tu. To do this, carry out effectively the proof of Noether Normalization, to get a handle on this vector space dimension.
To see how this implies the usual statement of Bezout's theorem, namely that the set-theoretic intersection $|C \cap D|$ has cardinality at most tu, show that any Artinian ring of length l has at most l maximal ideals.

Ex 5.3.3

From the proof of Proposition 5.1.3, you can extract the following criterion for f to have a simple point at the origin: its linear part should not vanish. Use this to prove that a point P on a plane curve $C := \mathrm{V}(f)$ is a multiple point if and only if $\partial f/\partial \xi$ and $\partial f/\partial \zeta$ both vanish on P. Conclude that a plane curve has at most finitely many multiple points, and find an upperbound for their number (you will need some elimination theory for this, as given, for instance, in [22, pp. 308-309]).

Ex 5.3.4

Extend the argument in the proof of Proposition 5.1.3 to prove 5.1.4.

Ex 5.3.5

Show that if R is a regular local ring, then so is the power series ring $R[[\xi]]$ in finitely many indeterminates. Prove that the ring of convergent power series over $\mathbb{C}$ (a formal power series is called convergent *if it converges on a small open disk around the origin) is regular.*

Ex 5.3.6

Use Exercise 4.4.6 to show that we may drop the condition in 5.1.6 that K is algebraically closed.

Ex 5.3.7

From the proof of 5.1.8, it is clear that any local ring whose associated graded ring is a domain, is itself a domain. Show that the coordinate ring of a cusp gives a counterexample to the converse.

Ex 5.3.8

Show that a one-dimensional Noetherian local ring R is regular if and only if it is a discrete valuation ring, that is to say, if and only if it admits a valuation $v\colon R \setminus \{0\} \to \mathbb{Z}$.

Ex 5.3.9

Using the criterion from Exercise 5.3.3, show that a plane curve with equation $\zeta^n = f(\xi)$ with f a polynomial without double roots, defines a regular plane curve if the characteristic of K does not divide n. In particular, elliptic curves are regular in all characteristics other than 2 (and in fact, also in characteristic 2, but one needs to define them by means of a different cubic polynomial). Moreover, show that if f has a double root, then the corresponding plane curve has a singularity.

Ex 5.3.10

Use the homogenization of the equation of an elliptic curve and Exercise 5.3.3 to show that the projectification of an elliptic curve is regular if the characteristic is not 2.

***Ex 5.3.11**

Show that the discussion on page 65 generalizes to arbitrary affine schemes : if $X := \operatorname{Spec}(R) \subseteq \mathbb{A}^n_K$ is a closed affine subscheme, then the closure of $|X|$ in $\mathbb{P}^n_K$ can be endowed with the structure of a projectice scheme $\tilde{X} := \operatorname{Spec}(\tilde{R})$, such that $X = \tilde{X} \cap \mathbb{A}^n_K$ (as schemes). To this end, generalize the notion of 'homogenization' as described in (5.2) to arbitrary ideals.

Ex 5.3.12

Show that a prime ideal $\mathfrak{p}$ in a Noetherian ring B is associated if and only if there exists an injective B-algebra homomorphism $B/\mathfrak{p} \to B$.

***Ex 5.3.13**

Show that a regular ring A is a finite direct sum of regular domains as follows. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ be the minimal primes of A. Show that A is the direct sum of the $A/\mathfrak{p}_i$, and each $A/\mathfrak{p}_i$ is regular.

Ex 5.3.14

Let $B := K[\eta_1, \dots, \eta_4]$, and let $\mathfrak{p}$ be the kernel of the K-algebra homomorphism

$$B \to K[\xi, \zeta] \colon \eta_1 \mapsto \xi^4, \eta_2 \mapsto \xi^3\zeta, \eta_3 \mapsto \xi\zeta^3, \eta_4 \mapsto \zeta^4$$

and let R be the localization of $B/\mathfrak{p}$ at the maximal ideal corresponding to the origin. Clearly, R is a domain, so that η_4 is a regular element. Show that the annihilator of η_3^3 in $R/\eta_4 R$ is equal to the maximal ideal of that ring, showing that the depth of $R/\eta_4 R$ is zero. Conclude that R is not Cohen-Macaulay.

***Ex 5.3.15**

We call a tuple $\mathbf{x} := (x_1, \dots, x_n)$ in a ring A quasi-regular *if for any k and any homogeneous form of degree k in $A[\xi]$ with $\xi := (\xi_1, \dots, \xi_n)$, if $F(\mathbf{x}) \in I^{k+1}$ then all coefficients of F lie in $I := (x_1, \dots, x_n)A$. Show that a regular sequence is quasi-regular. To this end, first show that if y is a zero-divisor modulo I, then it is also a zero-divisor modulo any I^k, then show the assertion by induction on n.*
Show that $\mathbf{x}$ is quasi-regular if and only if the associated graded ring $\operatorname{Gr}_I(A) := \bigoplus_n I^n/I^{n+1}$ of I is isomorphic to $(A/I)[\xi]$. Show that a quasi-regular sequence is independent.

*Ex 5.3.16

Give a complete proof of Theorem 5.2.6 in every dimension. To this end, you must prove that powers and permutations preserve regular sequences (the former is also proven in Exercise 5.3.17 and the latter in Exercise 5.3.18).

Ex 5.3.17

Show that in a (not necessarily Noetherian) ring A, if $(x_1, \ldots, x_d)$ *is A-regular, then so is* $(x_1^{e_1}, \ldots, x_d^{e_d})$*, for any* $e_i \geq 1$.

*Ex 5.3.18

Show that in a Noetherian local ring R, a sequence $(x_1, \ldots, x_d)$ *is regular if and only if it is quasi-regular, by induction on d as follows. Only the converse requires proof, and to this end, first show that* x_1 *is R-regular by proving by induction on k that* $x_1 z = 0$ *implies* $z \in I^k$*, where* $I := (x_1, \ldots, x_d)R$*, and then using Krull's Intersection Theorem (Theorem 2.4.11). Conclude by showing that* $(x_2, \ldots, x_d)$ *is* R/x_1R*-quasi-regular.*
In particular, a regular sequence in a Noetherian local ring is permutable.

Ex 5.3.19

Use Corollary 5.2.8 to prove the 'unmixedness' theorem: if I is an ideal of height e in a Cohen-Macaulay local ring R, and if I is generated by e elements, then I has no embedded primes, that is to say, any associated prime of R/I *is minimal. Also show the converse: if a Noetherian local ring has the above unmixedness property, then it is Cohen-Macaulay.*

Chapter 6
Flatness

In this chapter we will study a very important and useful property, called 'flatness'. As a concept, however, it is neither as intuitive nor as transparent as the other concepts discussed so far. Notwithstanding, it is an extremely important phenomenon, which underlies many deeper results in commutative algebra, as will be come apparent in the later chapters.[1] With David Mumford, the great geometer, we observe:

> "The concept of flatness is a riddle that comes out of algebra, but which technically is the answer to many prayers."
>
> [17, p. 214]

Flatness is in essence a homological notion, so we start off with developing some homological algebra. We then discuss the closely related notions of faithful flatness and projective dimension, and conclude the chapter with several useful flatness criteria.

6.1 Homological algebra

The main tool of homological algebra is the 'homology of a complex', so let's define this notion first.

Complexes. Let A be a ring. By a *complex* we mean a (possibly infinite) sequence of A-module homomorphisms $M_i \xrightarrow{d_i} M_{i-1}$, for $i \in \mathbb{Z}$, such that the composition of any two consecutive maps is zero. We often simply will say that

$$\dots \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \xrightarrow{d_{i-1}} M_{i-2} \xrightarrow{d_{i-2}} \dots \qquad (M_\bullet)$$

is a complex. The d_i are called the the *boundary maps* of the complex, and often are omitted from the notation. Of special interest are those complexes in which all

[1] I know of many deep theorems and conjectures that can be reformulated as a certain flatness result.

modules from a certain point on, either on the left or on the right, are zero (which forces the corresponding maps to be zero as well). Such a complex will be called *bounded* from the left or right respectively. In that case, one often renumbers so that the first non-zero module is labeled with $i = 0$. If $M_\bullet$ is bounded from the left, one also might reverse the numbering, indicate this notationally by writing $M^\bullet$, and refer to this situation as a *co-complex* (and more generally, add for emphasis the prefix 'co-' to any object associated to it).

Homology. Since the composition $d_{i+1} \circ d_i$ is zero, we have in particular an inclusion $\mathrm{Im}(d_{i+1}) \subseteq \mathrm{Ker}(d_i)$. To measure in how far this fails to be an equality, we define the *homology* $\mathrm{H}_\bullet(M_\bullet)$ of $M_\bullet$ as the collection of modules

$$\mathrm{H}_i(M_\bullet) := \mathrm{Ker}(d_i)/\mathrm{Im}(d_{i+1}).$$

If all homology modules are zero, $M_\bullet$ is called *exact*. More generally, we say that $M_\bullet$ is *exact at* i (or at M_i) if $\mathrm{H}_i(M_\bullet) = 0$. Note that $M_1 \xrightarrow{d_1} M_0 \to 0$ is exact (at zero) if and only if d_1 is surjective, and $0 \to M_0 \xrightarrow{d_0} M_{-1}$ is exact if and only if d_0 is injective. An exact complex is often also called an *exact sequence*. In particular, this terminology is compatible with the nomenclature for short exact sequence. If $M_\bullet$ is bounded from the right (indexed so that the last non-zero module is M_0), then the *cokernel* of $M_\bullet$ is the cokernel of $d_1 \colon M_1 \to M_0$. Put differently, the cokernel is simply the zero-th homology module $\mathrm{H}_0(M_\bullet)$. We say that $M_\bullet$ is *acyclic*, if all $\mathrm{H}_i(M_\bullet) = 0$ for $i > 0$. In that case, the *augmented* complex obtained by adding the cokernel of $M_\bullet$ to the right is then an exact sequence.

6.2 Flatness

We have arrived at the main notion of this chapter. Let A be a ring and M an A-module. Recall that $\cdot \otimes_A M$, that is to say, tensoring with respect to M, is a right exact functor, meaning that given an exact sequence

$$0 \to N_2 \to N_1 \to N_0 \to 0 \tag{6.1}$$

we get an exact sequence

$$N_2 \otimes_A M \to N_1 \otimes_A M \to N_0 \otimes_A M \to 0. \tag{6.2}$$

See [7, Proposition 2.18], where one also can find a good introduction to tensor products. We now call a module M *flat* if any short exact sequence (6.1) remains exact after tensoring, that is to say, we may add an additional zero on the left of (6.2). Put differently, M is flat if and only if $N' \otimes_A M \to N \otimes_A M$ is injective whenever $N' \to N$ is an injective homomorphism of A-modules. By breaking down a long exact sequence into short exact sequences (see Exercise 6.7.1), we immediately get:

6.2.1 *If M is flat, then any exact complex $N_\bullet$ remains exact after tensoring with M.*

The easiest examples of flat modules are the free modules:

6.2.2 *Any free module, and more generally, any projective module, is flat.*

Assume first that M is a free A-module, say of the form, $M \cong A^{(I)}$, where I is a possibly infinite index set (recall that an element of $A^{(I)}$ is a sequence $\mathbf{a} := (a_i \mid i \in I)$ such that all but finitely many a_i are zero; the 'unit' vectors $\mathbf{e}_i$ form a basis of $A^{(I)}$, where all entries in $\mathbf{e}_i$ are zero except the i-th, which equals one; and, any free A-module is isomorphic to some $A^{(I)}$). For any A-module H, we have $H \otimes_A M \cong H^{(I)}$. Since direct sums preserve injectivity, we now easily conclude that M is flat. The same argument applies if M is merely *projective*, meaning that it is a direct summand of a free module, say $M \oplus M' \cong F$ with F free. This completes the proof of the assertion. In particular, $A[\xi]$, being free over A, is flat as an A-module. The same is true for power series rings, at least over Noetherian rings, but the proof is a bit more involved (see Exercise 6.7.11). Flatness is preserved under base change in the following sense (the proof is left as Exercise 6.7.3):

6.2.3 *If M is a flat A-module, then M/IM is a flat A/I-module for each ideal $I \subseteq A$. More generally, if $A \to B$ is any homomorphism, then $M \otimes_A B$ is a flat B-module.*

6.2.4 *Any localization of a flat A-module is again flat. In particular, for every prime ideal $\mathfrak{p} \subseteq A$, the localization $A_\mathfrak{p}$ is flat as an A-module.*

The last assertion follows from the first and the fact that A, being free, is flat as an A-module by 6.2.2. The first assertion is not hard and is left as Exercise 6.7.3. Our next goal is to develop a homological tool to aid us in our study of flatness.

Tor modules. Let M be an A-module. A *projective resolution* of M is a complex $P_\bullet$, bounded from the right, in which all the modules P_i are projective, and such that the *augmented complex*

$$P_i \to P_{i-1} \to \cdots \to P_0 \to M \to 0$$

is exact. Put differently, a projective resolution of M is is an acyclic complex $P_\bullet$ of projective modules whose cokernel is equal to M. Tensoring this augmented complex with a second A-module N, yields a (possibly non-exact) complex

$$P_i \otimes_A N \to P_{i-1} \otimes_A N \to \cdots \to P_0 \otimes_A N \to M \otimes_A N \to 0.$$

The homology of the non-augmented part $P_\bullet \otimes N$ (that is to say, without the final module $M \otimes N$), is denoted

$$\mathrm{Tor}_i^A(M,N) := \mathrm{H}_i(P_\bullet \otimes_A N).$$

As the notation indicates, this does not depend on the choice of projective resolution $P_\bullet$. Moreover, we have for each i an isomorphism $\mathrm{Tor}_i^A(M,N) \cong \mathrm{Tor}_i^A(N,M)$. We will not prove these properties here (the proofs are not that hard anyway, see for instance [22, Appendix 3] or [54, Appendix B]). Since tensoring is right exact, a quick calculation shows that

$$\operatorname{Tor}_0^A(M,N) \cong M \otimes_A N.$$

The next result is a general fact of 'derived functors' (Tor is indeed the *derived functor* of the tensor product as discussed for instance in [54, Appendix B]; for a proof of the next result, see Exercise 6.7.22).

6.2.5 *If*

$$0 \to N' \to N \to N'' \to 0$$

is a short exact sequence of A-modules, then we get for every A-module M a long exact sequence

$$\cdots \to \operatorname{Tor}_{i+1}^A(M,N'') \xrightarrow{\delta_{i+1}} \operatorname{Tor}_i^A(M,N') \to$$
$$\operatorname{Tor}_i^A(M,N) \to \operatorname{Tor}_i^A(M,N'') \xrightarrow{\delta_i} \operatorname{Tor}_{i-1}^A(M,N') \to \dots$$

where the δ_i are the so-called connecting homomorphisms, *and the remaining maps are induced by the original maps.*

Tor-criterion for flatness. We can now formulate a homological criterion for flatness. More flatness criteria will be discussed in §6.6 below.

Theorem 6.2.6. *For an A-module M, the following are equivalent*

1. *M is flat;*
2. $\operatorname{Tor}_i^A(M,N) = 0$ *for all $i > 0$ and all A-modules N;*
3. $\operatorname{Tor}_1^A(M,A/I) = 0$ *for all finitely generated ideals $I \subseteq A$.*

Proof. Let $P_\bullet$ be a projective resolution of N. If M is flat, then $P_\bullet \otimes_A M$ is again exact by 6.2.1, and hence its homology $\operatorname{Tor}_i^A(N,M) = \mathrm{H}_i(P_\bullet \otimes_A N)$ vanishes. Conversely, if (2) holds, then tensoring the exact sequence $0 \to N' \to N \to N/N' \to 0$ with M yields in view of 6.2.5 an exact sequence

$$0 = \operatorname{Tor}_1^A(M,N/N') \to M \otimes_A N' \to M \otimes_A N$$

showing that the latter map is injective.

Remains to show (3) ⇒ (1), which for simplicity I will only do in the case A is Noetherian; the general case is treated in Exercise 6.7.6. We must show that if $N' \subseteq N$ is an injective homomorphism of A-modules, then $M \otimes_A N' \to M \otimes_A N$ is again injective, and we already observed that this follows once we showed that $\operatorname{Tor}_1^A(M,N/N') = 0$. I claim that it suffices to show this for N finitely generated: indeed, if N is arbitrary and $t := m_1 \otimes n_1 + \cdots + m_s \otimes n_s$ is an element in $M \otimes N'$ which is sent to zero in $M \otimes N$, then by definition of tensor product, there exists a finitely generated submodule $N_1 \subseteq N$ containing all n_i such that $t = 0$ as an element of $M \otimes N_1$. In particular, t is an element of $M \otimes N_1'$, where $N_1' := N' \cap N_1$, whose image in $M \otimes N_1$ is zero. Assuming momentarily that the finitely generated case is already proven, t is therefore zero in $M \otimes N_1'$, whence a fortiori in $M \otimes N'$.

So we may assume that N is finitely generated. We prove by induction on r, the number of generators of N/N', that $\mathrm{Tor}_1^A(M, N/N') = 0$. If $r = 1$, then N/N' is of the from A/I with $I \subseteq A$ an ideal, and the result holds by assumption. For $r > 1$, let $t \in N$ be such that its image in N/N' is a minimal generator. Put $H := N' + At$, so that N/H is generated by $r-1$ elements, and H/N' is cyclic. Tensoring the short exact sequence

$$0 \to H/N' \to N/N' \to N/H \to 0$$

yields by 6.2.5 an exact sequence

$$\mathrm{Tor}_1^A(M, H/N') \to \mathrm{Tor}_1^A(M, N/N') \to \mathrm{Tor}_1^A(M, N/H).$$

By induction, the two outer modules vanish, whence so does the inner. □

For Noetherian rings we can even restrict the test in (3) to prime ideals (but see also Theorem 6.6.7 below, which reduces the test to a single ideal):

Corollary 6.2.7. *Let A be a Noetherian ring and M an A-module. If $\mathrm{Tor}_1^A(M, A/\mathfrak{p})$ vanishes for all prime ideals $\mathfrak{p} \subseteq A$, then M is flat. More generally, if, for some $i \geq 1$, every $\mathrm{Tor}_i^A(M, A/\mathfrak{p})$ vanishes for $\mathfrak{p}$ running over the prime ideals in A, then $\mathrm{Tor}_i^A(M, N)$ vanishes for all (finitely generated) A-modules N.*

Proof. The first assertion follows from the last by (3). The last assertion, for finitely generated modules, follows from the fact that every such module N admits a *prime filtration*, that is to say, a finite ascending chain of submodules

$$0 = N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots \subseteq N_e = N \tag{6.3}$$

such that each successive quotient N_j/N_{j-1} is isomorphic to the (cyclic) A-module $A/\mathfrak{p}_j$ for some prime ideal $\mathfrak{p}_j \subseteq A$, for $j = 1, \ldots, e$ (see Exercise 6.7.8). By induction on j, one then derives from the long exact sequence (6.2.5) that $\mathrm{Tor}_i^A(M, N_j) = 0$, whence in particular $\mathrm{Tor}_i^A(M, N) = 0$. To prove the same result for N arbitrary (which we will not be needing in the sequel), use an argument similar to the one in the proof of Theorem 6.2.6 (see Exercise 6.7.6). □

Corollary 6.2.8. *Let*

$$0 \to M_1 \to F \to M \to 0$$

be an exact sequence of A-modules. If F is flat, then

$$\mathrm{Tor}_i^A(M, N) \cong \mathrm{Tor}_{i-1}^A(M_1, N)$$

for all $i \geq 2$ and all A-modules N.

Proof. From the long exact sequence of Tor (see 6.2.5), we get exact sequences

$$0 = \mathrm{Tor}_i^A(F,N) \to \mathrm{Tor}_i^A(M,N) \to \mathrm{Tor}_{i-1}^A(M_1,N) \to \mathrm{Tor}_{i-1}^A(F,N) = 0$$

where the two outer most modules vanish because of Theorem 6.2.6. □

Note that in case F is actually projective in the above sequence, then M_1 is called a (first) *syzygy* of M. Therefore, the previous result is particularly useful when working with syzygies (for a typical application, see the proof of 6.5.1.)

6.3 Faithful flatness

We call an A-module M *faithful*, if $\mathfrak{m}M \neq M$ for all (maximal) ideals $\mathfrak{m}$ of A.[2] By Nakayama's Lemma, we immediately get:

6.3.1 *Any finitely generated module over a local ring is faithful.*

Of particular interest are the faithful modules which are moreover flat, called *faithfully flat* modules (see Exercise 6.7.23 for a homological characterization). It is not hard to see that any free or projective module is faithfully flat. On the other hand, no proper localization of A is faithfully flat.

6.3.2 *If M is a faithfully flat A-module, then $M \otimes_A N$ is non-zero, for every non-zero A-module N. Moreover, if $A \to B$ is an arbitrary homomorphism, then $M \otimes_A B$ is a faithfully flat B-module.*

Indeed, for the first assertion, let $N \neq 0$ and choose a non-zero element $n \in N$. Since $I := \mathrm{Ann}_A(n)$ is then a proper ideal, it is contained in some maximal ideal $\mathfrak{m} \subseteq A$. Note that $An \cong A/I$. Tensoring the induced inclusion $A/I \hookrightarrow N$ with M gives by assumption an injection $M/IM \hookrightarrow M \otimes_A N$. The first of these modules is non-zero, since $IM \subseteq \mathfrak{m}M \neq M$, whence so is the second, as we wanted to show. To prove the second assertion, $M \otimes_A B$ is flat over B by 6.2.3. Let $\mathfrak{n}$ be a maximal ideal of B, and let $\mathfrak{p} := \mathfrak{n} \cap A$ be its contraction to A. In particular, $M/\mathfrak{p}M$ is flat over $A/\mathfrak{p}$, and an easy calculation then shows that it is faithfully flat. Therefore, by the first assertion, $M/\mathfrak{p}M \otimes_{A/\mathfrak{p}} B/\mathfrak{n}$ is non-zero. As the latter is just $(M \otimes_A B)/\mathfrak{n}(M \otimes_A B)$, we showed that $M \otimes_A B$ is also faithful.

In most of our applications, the A-module has the additional structure of an A-algebra. In particular, we call a ring homomorphism $A \to B$ (*faithfully*) *flat* if B is (faithfully) flat as an A-module. Since by definition a *local homomorphism* of local rings $(R,\mathfrak{m}) \to (S,\mathfrak{n})$ is a ring homomorphism with the additional property that $\mathfrak{m} \subseteq \mathfrak{n}$, we get immediately:

6.3.3 *Any local homomorphism which is flat, is faithfully flat.* □

---

[2] The reader be warned that this is a less conventional terminology: 'faithful' often is taken to mean that the annihilator of the module is zero. However, in view of the (well-established) term 'faithfully flat', our usage seems more reasonable: faithfully flat now simply means faithful and flat.

Proposition 6.3.4. *If $A \to B$ is faithfully flat, then for every ideal $I \subseteq A$, we have $I = IB \cap A$, and hence in particular, $A \to B$ is injective.*

Proof. For I equal to the zero ideal, this just says that $A \to B$ is injective. Suppose this last statement is false, and let $a \in A$ be a non-zero element in the kernel of $A \to B$, that is to say, $a = 0$ in B. However, by 6.3.2, the module $aA \otimes_A B$ is non-zero, say, containing the non-zero element x. Hence x is of the form $ra \otimes b$ for some $r \in A$ and $b \in B$, and therefore equal to $r \otimes ab = r \otimes 0 = 0$, contradiction.

To prove the general case, note that B/IB is a flat A/I-module by 6.2.3. It is clearly also faithful, so that applying our first argument to the natural homomorphism $A/I \to B/IB$ yields that it must be injective, which precisely means that $I = IB \cap A$. □

A ring homomorphism $A \to B$ such that $I = IB \cap A$ for all ideals $I \subseteq A$ is called *cyclical pure*. Hence faithfully flat homomorphisms are cyclically pure (for an other example see 9.5.4 below). We can paraphrase this as 'faithful flatness preserves the ideal structure of a ring', that is to say, in terms of Grassmanians (see page 38), we have:

6.3.5 *If $A \to B$ is faithfully flat, or more generally, cyclically pure, then the induced map* $\mathrm{Grass}(A) \to \mathrm{Grass}(B) \colon I \mapsto IB$ *on the Grassmanians is injective.* □

Since a ring A is Noetherian if and only if its Grassmanian $\mathrm{Grass}(A)$ is well-ordered (i.e., has the descending chain condition; recall that the order on $\mathrm{Grass}(A)$ is given by reverse inclusion), we get immediately the following Noetherianity criterion from 6.3.5:

Corollary 6.3.6. *Let $A \to B$ be a faithfully flat, or more generally, a cyclically pure homomorphism. If B is Noetherian, then so is A.* □

A similar argument shows:

6.3.7 *If $R \to S$ is a faithfully flat homomorphism of local rings, and if $I \subseteq R$ is minimally generated by e elements, then so is IS.*

Clearly, IS is generated by at most e elements. By way of contradiction, suppose it is generated by strictly fewer elements. By Nakayama's lemma, we may choose these generators already in I. So there exists an ideal $J \subseteq I$, generated by less than e elements, such that $JS = IS$. However, by cyclic purity (Proposition 6.3.4), we have $J = JS \cap R = IS \cap R = I$, contradicting that I requires at least e generators. □

If $A \to B$ is a flat or faithfully flat homomorphism, then we also will call the corresponding morphism $Y := \mathrm{Spec}(B) \to X := \mathrm{Spec}(A)$ *flat* or *faithfully flat* respectively. In Exercise 6.7.14, you are asked to prove that:

6.3.8 *A morphism $f \colon Y \to X$ of affine schemes is flat if and only if for every (closed) point $y \in Y$, the induced homomorphism $\mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$ is flat.*

Theorem 6.3.9. *A morphism $Y \to X$ of affine schemes is faithfully flat if and only if it is flat and surjective.*

Proof. Let $A \to B$ be the corresponding homomorphism. Assume $A \to B$ is faithfully flat, and let $\mathfrak{p} \subseteq A$ be a prime ideal. Surjectivity of the morphism amounts to showing that there is at least one prime ideal of B lying over $\mathfrak{p}$. Now, by 6.3.2, the base change $A_\mathfrak{p} \to B_\mathfrak{p}$ is again faithfully flat, and hence in particular $\mathfrak{p}B_\mathfrak{p} \neq B_\mathfrak{p}$. In other words, the fiber ring $B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}$ is non-empty, which is what we wanted to prove (indeed, take any maximal ideal $\mathfrak{n}$ of $B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}$ and let $\mathfrak{q} := \mathfrak{n} \cap B$; then verify that $\mathfrak{q} \cap A = \mathfrak{p}$.)

Conversely, assume $Y \to X$ is flat and surjective, and let $\mathfrak{m}$ be a maximal ideal of A. Let $\mathfrak{q} \subseteq B$ be an ideal lying over $\mathfrak{m}$. Hence $\mathfrak{m}B \subseteq \mathfrak{q} \neq B$, showing that B is faithful over A. □

6.4 Flatness and regular sequences

The first fundamental fact regarding regular sequences and flat homomorphisms is:

Proposition 6.4.1. *If $A \to B$ is a flat homomorphism and $\mathbf{x}$ is an A-regular sequence, then $\mathbf{x}$ is also B-regular.*

Proof. We induct on the length n of $\mathbf{x} := (x_1, \dots, x_n)$. Assume first $n = 1$. Multiplication by x_1, that is to say, the homomorphism $A \xrightarrow{x_1} A$, is injective, whence remains so after tensoring with B by 6.2.3. It is not hard to see that the resulting homomorphism is again multiplication $B \xrightarrow{x_1} B$, showing that x_1 is B-regular. For $n > 1$, the base change $A/x_1A \to B/x_1B$ is flat, so that by induction $(x_2, \dots, x_n)$ is B/x_1B-regular. Hence we are done, since x_1 is B-regular by the previous argument. □

Tor modules behave well under deformation by a regular sequence in the following sense.

Proposition 6.4.2. *Let $\mathbf{x}$ be a regular sequence in a ring A, and let M and N be two A-modules. If $\mathbf{x}$ is M-regular and $\mathbf{x}N = 0$, then we have for each i an isomorphism*

$$\operatorname{Tor}_i^A(M,N) \cong \operatorname{Tor}_i^{A/\mathbf{x}A}(M/\mathbf{x}M, N).$$

Proof. By induction on the length of the sequence, we may assume that we have a single A-regular and M-regular element x. Put $B := A/xA$. From the short exact sequence

$$0 \to A \xrightarrow{x} A \to B \to 0$$

we get after tensoring with M, a long exact sequence of Tor-modules as in 6.2.5. Since $\operatorname{Tor}_i^A(A,M)$ vanishes for all i, so must each $\operatorname{Tor}_i^A(M,B)$ in this long exact sequence for $i > 1$. Furthermore, the initial part of this long exact sequence is

$$0 \to \operatorname{Tor}_1^A(M,B) \to M \xrightarrow{x} M \to M/xM \to 0$$

proving that $\mathrm{Tor}_1^A(M,B)$ too vanishes as x is M-regular. Now, let $P_\bullet$ be a projective resolution of M. The homology of $\bar{P}_\bullet := P_\bullet \otimes_A B$ is by definition $\mathrm{Tor}_i^A(M,B)$, and since we showed that this is zero, $\bar{P}_\bullet$ is exact, whence a projective resolution of M/xM. Hence we can calculate $\mathrm{Tor}_i^B(M/xM,N)$ as the homology of $\bar{P}_\bullet \otimes_B N$ (note that by assumption, N is a B-module). However, the latter complex is equal to $P_\bullet \otimes_A N$ (which we can use to calculate $\mathrm{Tor}_i^A(M,N)$), and hence both complexes have the same homology, as we wanted to show. □

6.5 Projective dimension

If an A-module M has a projective resolution $P_\bullet$ which is also bounded from the left, that is to say, is of the form

$$0 \to P_e \to \cdots \to P_0 \to M \to 0$$

then we say that M has *finite projective dimension*. The smallest length e of such an exact sequence is called the *projective dimension* of M and is denoted $\mathrm{projdim}(M)$; if M does not have a finite projective resolution, then we set $\mathrm{projdim}(M) := \infty$. Clearly, the projective dimension of a module is zero if and only if it is projective. The connection with Tor is immediate by virtue of the latter's definition as the homology of the tensor product with a projective resolution:

6.5.1 *If M is an A-module of projective dimension e, then $\mathrm{Tor}_i^A(M,N) = 0$ for all $i > e$ and all A-modules N. Moreover, if*

$$0 \to H \to P_e \to P_{e-1} \to \cdots \to P_0 \to M \to 0$$

is exact, with all P_e projective, then H is flat (and in fact projective).

Only the second assertion requires explanation. By Corollary 6.2.8, the vanishing of $\mathrm{Tor}_{e+1}^A(M,N)$ is equivalent with the vanishing of $\mathrm{Tor}_1^A(H,N)$. Hence H is a flat A-module by Theorem 6.2.6. To prove that it is actually projective, one needs Ext-functors, which we will not treat.

If x is an A-regular element, then A/xA has projective dimension one, as is clear from the exact sequence

$$0 \to A \xrightarrow{x} A \to A/xA \to 0. \tag{6.4}$$

In fact, this is also true for regular sequences of any length, but to prove this we need a new tool:

Minimal resolutions. A complex $M_\bullet$ over a local ring $(R,\mathfrak{m})$ is called *minimal* if the kernel of each boundary $d_i \colon M_i \to M_{i-1}$ lies inside $\mathfrak{m}M_i$. The next result is easily derived from Nakayama's lemma and induction (see Exercise 6.7.9):

6.5.2 *Every finitely generated module over a Noetherian local ring admits a minimal free resolution, consisting of finitely generated free modules.*

Corollary 6.5.3. *Over a Noetherian local ring, a finitely generated module is flat if and only if it is projective if and only if it is free.*

Proof. The converse implications are all trivial. So remains to show that if G is a finitely generated flat R-module, then it is free. By 6.5.2 (or Nakayama's lemma), we can find a finitely generated free A-module F, and a surjective map $F \to G$ whose kernel H lies inside $\mathfrak{m}F$. In other words, $F/\mathfrak{m}F \cong G/\mathfrak{m}G$. On the other hand, tensoring the exact sequence $0 \to H \to F \to G \to 0$ with $k := R/\mathfrak{m}$ yields by 6.2.5 an exact sequence

$$0 = \mathrm{Tor}_1^R(G,k) \to H/\mathfrak{m}H \to F/\mathfrak{m}F \to G/\mathfrak{m}G \to 0$$

where we used the flatness of G to obtain the vanishing of the first module. Since the last arrow is an isomorphism, $H/\mathfrak{m}H = 0$, which by Nakayama's lemma implies $H = 0$, that is to say, $F = G$ is free. □

Minimal resolutions are essentially unique:

Proposition 6.5.4. *Let $(R,\mathfrak{m})$ be a Noetherian local ring with residue field k. Let M be a finitely generated R-module, and let*

$$\ldots F_i \to F_{i-1} \to \cdots \to F_0 \to M \to 0 \qquad (F_\bullet)$$

be a minimal free resolution. For each $i \geq 0$, the i-th Betti number *of M, that is to say, the k-vector space dimension of* $\mathrm{Tor}_i^R(M,k)$, *is equal to the rank of F_i.*

Moreover, the projective dimension of M is equal to the supremum of all i for which $\mathrm{Tor}_i^R(M,k) \neq 0$, *and hence is less than or equal to* $\mathrm{projdim}(k)$.

Proof. By definition, $\mathrm{Tor}_i^R(M,k)$ is the homology of $F_\bullet \otimes_R k$. Since $F_\bullet$ is minimal, the boundaries in $F_\bullet \otimes_R k$ are all zero, so that $\mathrm{H}_i(F_\bullet \otimes_R k) = F_i \otimes_R k$. This shows that the Betti numbers of M coincide with the ranks of the free modules in $F_\bullet$ (and hence the latter are uniquely determined). The second assertion follows immediately from this and from 6.5.1. □

Put differently, the previous result yields a criterion for a finitely generated module to have finite projective dimension, namely that some Betti number be zero. We can now prove (6.4) for any regular sequence:

Corollary 6.5.5. *If $\mathbf{x}$ is a regular sequence in a Noetherian local ring R, then $R/\mathbf{x}R$ has finite projective dimension.*

Proof. We prove by induction on the length l of the sequence that $R/\mathbf{x}R$ has projective dimension at most l, where the case $l = 1$ is (6.4). Write $\mathbf{x} = (\mathbf{y}, x)$ with $\mathbf{y}$ a regular sequence of length $l - 1$. The short exact sequence

$$0 \to R/\mathbf{y}R \xrightarrow{x} R/\mathbf{y}R \to R/\mathbf{x}R \to 0$$

when tensored with the residue field k yields by 6.2.5 a long exact sequence

$$\mathrm{Tor}_i^R(R/\mathbf{y}R,k) \to \mathrm{Tor}_i^R(R/\mathbf{x}R,k) \to \mathrm{Tor}_{i-1}^R(R/\mathbf{y}R,k)$$

For $i-1 \geq l$, both outer modules are zero by induction and Proposition 6.5.4, whence so is the inner module. Using Proposition 6.5.4 once more, we see that $R/\mathbf{x}R$ therefore has projective dimension at most l. □

In fact, the projective dimension of $R/\mathbf{x}R$ is exactly l. Moreover, this result remains true if the ring is not local, nor even Noetherian. This more general result is proven by means of a complex called the *Koszul complex*, whose homology actually measures the failure of a sequence being regular. For all this, see for instance [54, §16] or [22, §17].

Theorem 6.5.6 (Serre). *A d-dimensional Noetherian local ring R is regular if and only if its residue field k has finite projective dimension (equal to d). If this is the case, then any module has projective dimension at most d.*

Proof (partim). Regarding the first statement, we will only prove the direct implication. Since a regular local ring R is Cohen-Macaulay by Proposition 5.2.3, its maximal ideal is generated by a regular sequence $\mathbf{x}$. Hence $k = R/\mathbf{x}R$ has finite projective dimension by Corollary 6.5.5. To prove the converse, some additional tools (like Ext-functors) are required, and we refer the reader to the literature (see for instance [54, Theorem 19.2] or [22, Theorem 19.12]).

The second assertion for finitely generated modules now follows immediately from the first and Proposition 6.5.4. To also prove this for non-finitely generated modules, again Ext-functors are needed (see for instance [54, §19 Lemma 2] or [22, Theorem A3.18]). □

Although we did not give a complete proof, we did prove most of what we will use, with the most notable exception Corollary 6.5.8 below. We can even formulate a global version, which was first proven by Hilbert in the case A is a polynomial ring over a field.

Theorem 6.5.7. *Over a d-dimensional regular ring A, any finitely generated A-module M has projective dimension at most d.*

Proof. Choose an exact sequence

$$0 \to H \to A^{n_d} \to \dots A^{n_1} \to A^{n_0} \to M \to 0$$

for some n_i and some finitely generated module H, the *d-th syzygy* of M, given as the kernel of the homomorphism $A^{n_d} \to A^{n_{d-1}}$. Since $A_\mathfrak{m}$ is flat over A, for $\mathfrak{m}$ a maximal ideal of A, we get an exact sequence

$$0 \to H_\mathfrak{m} \to A_\mathfrak{m}^{n_d} \to \dots A_\mathfrak{m}^{n_1} \to A_\mathfrak{m}^{n_0} \to M_\mathfrak{m} \to 0.$$

By Theorem 6.5.6, the $A_\mathfrak{m}$-module $M_\mathfrak{m}$ has finite projective dimension, and hence, $H_\mathfrak{m}$ is flat by 6.5.1. Therefore, H is projective by Exercise 6.7.16. □

Corollary 6.5.8. *If A is a regular ring, then so is any of its localizations.*

Proof. A moment's reflection yields that we only need to prove this when A is already local, and $\mathfrak{p}$ is some (non-maximal) prime ideal. By Theorem 6.5.6, the residue ring $A/\mathfrak{p}$ admits a finite free resolution. Since localization is flat, tensoring this resolution with $A_\mathfrak{p}$ gives a finite free resolution of $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ viewed as an $A_\mathfrak{p}$-module. Hence $A_\mathfrak{p}$ is regular by Theorem 6.5.6 (this is the one spot where we use the unproven converse from that theorem). □

6.6 Flatness criteria

Because flatness will play such a crucial role in our later work, we want several ways of detecting it. In this section, we will see five such criteria.

Equational criterion for flatness Our first criterion is very useful in applications (see for instance Theorem 8.4.3), and works without any hypothesis on the ring or module. To give a streamlined presentation, let us introduce the following terminology: given an A-module N, and tuples $\mathbf{b}_i$ in A^n, by an *N-linear combination* of the $\mathbf{b}_i$, we mean a tuple in N^n of the form $n_1\mathbf{b}_1 + \cdots + n_s\mathbf{b}_s$ where $n_i \in N$. Of course, if N has the structure of an A-algebra, this is just the usual terminology. Given a (finite) homogeneous linear system of equations

$$L_1(t) = \cdots = L_s(t) = 0 \tag{$\mathscr{L}$}$$

over A in the n variables t, we denote the A-submodule of N^n consisting of all solutions of $(\mathscr{L})$ in N by $\mathrm{Sol}_N(\mathscr{L})$, and we let $f_\mathscr{L}\colon N^n \to N^s$ be the map given by substitution $\mathbf{x} \mapsto (L_1(\mathbf{x}), \ldots, L_s(\mathbf{x}))$. In particular, we have an exact sequence

$$0 \to \mathrm{Sol}_N(\mathscr{L}) \to N^n \xrightarrow{f_\mathscr{L}} N^s. \tag{$\dagger_{\mathscr{L}/N}$}$$

Theorem 6.6.1. *A module M over a ring A is flat if and only if every solution in M of a homogeneous linear equation in finitely many variables over A is an M-linear combination of solutions in A. Moreover, instead of a single linear equation, we may take any finite system of linear equations in the above criterion.*

Proof. We will only prove the first assertion, and leave the second for the exercises (Exercise 6.7.10). Let $L = 0$ be a homogeneous linear equation in n variables with coefficients in A. If M is flat, then the exact sequence $(\dagger_{L/A})$ remains exact after tensoring with M, that is to say,

$$0 \to \mathrm{Sol}_A(L) \otimes_A M \to M^n \xrightarrow{f_L} M,$$

and hence by comparison with $(\dagger_{L/M})$, we get

$$\mathrm{Sol}_M(L) = \mathrm{Sol}_A(L) \otimes_A M.$$

From this it follows easily that any tuple in $\mathrm{Sol}_M(L)$ is an M-linear combination of tuples in $\mathrm{Sol}_A(L)$, proving the direct implication.

Conversely, assume the condition on the solution sets of linear forms holds. To prove that M is flat, we will verify condition (3) in Theorem 6.2.6. To this end, let $I := (a_1, \dots, a_k)A$ be a finitely generated ideal of A. Tensor the exact sequence $0 \to I \to A \to A/I \to 0$ with M to get by 6.2.5 an exact sequence

$$0 = \mathrm{Tor}_1^A(A,M) \to \mathrm{Tor}_1^A(A/I,M) \to I \otimes_A M \to M. \tag{6.6}$$

Suppose y is an element in $I \otimes M$ that is mapped to zero in M. Writing $y = a_1 \otimes m_1 + \dots + a_k \otimes m_k$ for some $m_i \in M$, we get $a_1m_1 + \dots + a_km_k = 0$. Hence by assumption, there exist solutions $\mathbf{b}^{(1)}, \dots, \mathbf{b}^{(s)} \in A^k$ of the linear equation $a_1t_1 + \dots + a_kt_k = 0$, such that

$$(m_1, \dots, m_k) = n_1\mathbf{b}^{(1)} + \dots + n_s\mathbf{b}^{(s)}$$

for some $n_i \in M$. Letting $b_i^{(j)}$ be the i-th entry of $\mathbf{b}^{(j)}$, we see that

$$y = \sum_{i=1}^{k} a_i \otimes m_i = \sum_{i=1}^{k}\sum_{j=1}^{s} a_i \otimes n_j b_i^{(j)} = \sum_{j=1}^{s}(\sum_{i=1}^{k} a_i b_i^{(j)}) \otimes n_j = \sum_{j=1}^{s} 0 \otimes n_j = 0.$$

Hence $I \otimes_A M \to M$ is injective, so that $\mathrm{Tor}_1^A(A/I,M)$ must be zero by (6.6). Since this holds for all finitely generated ideals $I \subseteq A$, we proved that M is flat by Theorem 6.2.6(3). □

It is instructive to view the previous result from the following perspective. To a homogeneous linear equation $L = 0$, we associated an exact sequence $(\dagger_{L/N})$. The image of f_L is of the form IN where I is the ideal generated by the coefficients of the linear form defining L. In case $N = B$ is an A-algebra, this leads to the following extended exact sequence

$$0 \to \mathrm{Sol}_B(L) \to B^n \xrightarrow{f_L} B \to B/IB \to 0. \tag{$\ddagger_{IB}$}$$

This justifies calling $\mathrm{Sol}_B(L)$ the *module of syzygies* of IB (one checks that it only depends on the ideal I). Therefore, we may paraphraze the equational flatness criterion for algebras as follows:

6.6.2 *A ring homomorphism $A \to B$ is flat if and only if taking syzygies commutes with extension in the sense that the module of syzygies of IB is the extension to B of the module of syzygies of I.*

Here is one application of the equational flatness criterion.

Corollary 6.6.3. *The canonical embedding of a Noetherian ring inside its ultrapower is faithfully flat.*

Proof. Let A be a ring and $A_\natural$ an ultrapower of A. Recall that $A \to A_\natural$ is given by sending an element $a \in A$ to the ultraproduct $\mathrm{ulim}_{w\to\infty} a$ of the constant sequence. If $\mathfrak{m} \subseteq A$ is a maximal ideal, then $\mathfrak{m}A_\natural$ is its ultraproduct (since $\mathfrak{m}$ is finitely generated) whence again maximal, showing that $A_\natural$ is faithful. To show it is also flat, we use the equational criterion. Let $L = 0$ be a homogeneous linear equation with coefficients in A. Let $\mathbf{a} \in A_\natural^n$ be a solution of $L = 0$ in $A_\natural$. Write $\mathbf{a}$ as an ultraproduct of tuples $\mathbf{a}_w \in A^n$. By Łos' Theorem (Theorem 2.3.1), almost each $\mathbf{a}_w \in \mathrm{Sol}_A(L)$. Hence $\mathbf{a}$ lies in the ultrapower of $\mathrm{Sol}_A(L)$. By Noetherianity, $\mathrm{Sol}_A(L)$ is finitely generated, and hence, its ultrapower is simply the $A_\natural$-module generated by $\mathrm{Sol}_A(L)$ (see Exercise 2.6.8), so that we are done by Theorem 6.6.1. □

Coherency criterion

We can turn this into a criterion for coherency. Recall that a ring A is called *coherent*, if the solution set of any homogeneous linear equation over A is finitely generated. Clearly, Noetherian rings are coherent. We have:

Theorem 6.6.4. *A ring A is coherent if and only if the canonical embedding into one of its ultrapowers is flat.*

Proof. The direct implication is proven by the same argument that proves Corollary 6.6.3, since we really only used that A is coherent in that argument. Conversely, suppose $A \to A_\natural$ is flat. Towards a contradiction, assume L is a linear form (in n indeterminates) over A whose solution set $\mathrm{Sol}_A(L)$ is infinitely generated. In particular, we can choose a sequence $\mathbf{a}_w$ in $\mathrm{Sol}_A(L)$ which is contained in no finitely generated submodule of $\mathrm{Sol}_A(L)$ (see Exercise 6.7.25). The ultraproduct $\mathbf{a}_\natural \in A_\natural^n$ of this sequence lies in $\mathrm{Sol}_{A_\natural}(L)$ by Łos' Theorem. Hence, by Theorem 6.6.1, there exists a finitely generated submodule $H \subseteq \mathrm{Sol}_A(L)$ such that $\mathbf{a}_\natural \in H \cdot A_\natural$. Therefore, almost all $\mathbf{a}_j$ lie in H by Łos' Theorem, contradiction. □

Quotient criterion for flatness. The next criterion is derived from our Tor-criterion (Theorem 6.2.6):

Theorem 6.6.5. *Let $A \to B$ be a flat homomorphism, and let $I \subseteq B$ be an ideal. The induced homomorphism $A \to B/I$ is flat if and only if $\mathfrak{a}B \cap I = \mathfrak{a}I$ for all finitely generated ideals $\mathfrak{a} \subseteq A$.*

Moreover, if A is Noetherian, we only need to check the above criterion for $\mathfrak{a}$ a prime ideal of A.

Proof. From the exact sequence $0 \to I \to B \to B/I \to 0$ we get after tensoring with $A/\mathfrak{a}$ an exact sequence

$$0 = \mathrm{Tor}_1^A(B, A/\mathfrak{a}) \to \mathrm{Tor}_1^A(B/I, A/\mathfrak{a}) \to I/\mathfrak{a}I \to B/\mathfrak{a}B$$

where we used the flatness of B for the vanishing of the first module. The kernel of $I/\mathfrak{a}I \to B/\mathfrak{a}B$ is easily seen to be $(\mathfrak{a}B \cap I)/\mathfrak{a}I$. Hence $\mathrm{Tor}_1^A(B/I, A/\mathfrak{a})$ vanishes if and only if $\mathfrak{a}B \cap I = \mathfrak{a}I$. This proves by Theorem 6.2.6 the stated equivalence in the first assertion; the second assertion follows by the same argument, this time using Corollary 6.2.7. □

To put this criterion to use, we need another definition (for further applications, see Theorem 12.2.1 and Exercise 12.3.14 below). The (A-)*content* of a polynomial $f \in A[\xi]$ (or a power series $f \in A[[\xi]]$) is by definition the ideal generated by its coefficients.

Corollary 6.6.6. *Let A be a Noetherian ring, let ξ be a finite tuple of indeterminates, and let B denote either $A[\xi]$ or $A[[\xi]]$. If $f \in B$ has content one, then B/fB is flat over A.*

Proof. By 6.2.2 or Exercise 6.7.11, the natural map $A \to B$ is flat. To verify the second criterion in Theorem 6.6.5, let $\mathfrak{p} \subseteq A$ be a prime ideal. The forward inclusion in the to be proven equality $\mathfrak{p}fB = \mathfrak{p}B \cap fB$ is immediate. To prove the other, take $g \in \mathfrak{p}B \cap fB$. In particular, $g = fh$ for some $h \in B$. Since $\mathfrak{p} \subseteq A$ is a prime ideal, so is $\mathfrak{p}B$ (this is a property of polynomial or power series rings, not of flatness!). Since f has content one, $f \notin \mathfrak{p}B$ whence $h \in \mathfrak{p}B$. This yields $g \in \mathfrak{p}fB$, as we needed to prove. □

Local criterion for flatness.

For finitely generated modules, we have the following criterion:

Theorem 6.6.7 (Local flatness theorem–finitely generated case). *Let R be a Noetherian local ring with residue field k. If M is a finitely generated R-module whose first Betti number vanishes, that is to say, if $\operatorname{Tor}_1^R(M,k) = 0$, then M is flat.*

Proof. Take a minimal free resolution

$$\cdots \to F_1 \to F_0 \to M \to 0.$$

of M. By Proposition 6.5.4, the rank of F_1 is zero, so that $M \cong F_0$ is free whence flat. □

There is a much stronger version of this result, where we may replace the condition that M is finitely generated over R by the condition that M is finitely generated over a Noetherian local R-algebra S. Since we will not really need this result, we refer the reader either to the literature (see for instance [54, Theorem 22.3] or [22, Theorem 6.8]), or to Project 6.8.

Cohen-Macaulay criterion for flatness. To formulate our next criterion, we need a definition.

Definition 6.6.8 (Big Cohen-Macaulay modules). Let R be a Noetherian local ring, and let M be an arbitrary R-module. We call M a *big Cohen-Macaulay module*, if there exists a system of parameters on R which is M-regular. If moreover every system of parameters is M-regular, then we call M a *balanced big Cohen-Macaulay*.

It has become tradition to add the somehow redundant adjective ‘big’ to emphasize that the module is not necessarily finitely generated. It is one of the greatest open problems in homological algebra to show that every Noetherian local ring has at least one big Cohen-Macaulay module, and this is known to be the case for any

Noetherian local ring containing a field (see §10.4 and §11.4).[3] A Cohen-Macaulay local ring is clearly a balanced big Cohen-Macaulay module over itself, so the problem of the existence of these modules is only important for deriving results over Noetherian local rings with 'worse than Cohen-Macaulay' singularities.

Once one has a big Cohen-Macaulay module, one can always construct, using completion (for which, see Chapter 7), a balanced big Cohen-Macaulay module from it (see for instance [15, Corollary 8.5.3]). Here is a criterion for a big Cohen-Macaulay module to be balanced taken from [6, Lemma 4.8]; its proof is a simple modification of the proof of Theorem 5.2.6 and is worked out in Exercise 6.7.12 (recall that a regular sequence is called *permutable* if any permutation is again regular).

Proposition 6.6.9. *A big Cohen-Macaulay module M over a Noetherian local ring is balanced, if every M-regular sequence is permutable.*

If R is a Cohen-Macaulay local ring, and M a flat R-module, then M is a balanced big Cohen-Macaulay module, since every system of parameters in R is R-regular by Theorem 5.2.6, whence M-regular by Proposition 6.4.1. We have the following converse:

Theorem 6.6.10. *If M is a balanced big Cohen-Macaulay module over a regular local ring, then it is flat. More generally, over an arbitrary local Cohen-Macaulay ring, if M is a balanced big Cohen-Macaulay module of finite projective dimension, then it is flat.*

Proof. The first assertion is indeed a special case of the second by Theorem 6.5.6. For simplicity, we will just prove the first, and refer to Exercise 6.7.13 for the second. So let M be a balanced big Cohen-Macaulay module over the d-dimensional regular local ring R. Since a finitely generated R-module N has finite projective dimension by the (proven part of) Theorem 6.5.6, all $\operatorname{Tor}_i^R(M,N) = 0$ for $i \gg 0$ by 6.5.1. Let e be maximal such that $\operatorname{Tor}_e^R(M,N) \neq 0$ for some finitely generated R-module N. If $e = 0$, then we are done by Theorem 6.2.6. So, by way of contradiction, assume $e \geq 1$. By Corollary 6.2.7, there exists a prime ideal $\mathfrak{p} \subseteq R$ such that $\operatorname{Tor}_e^R(M, R/\mathfrak{p}) \neq 0$. Let h be the height of $\mathfrak{p}$. By Exercise 4.4.11, we can choose a system of parameters $(x_1,\dots,x_d)$ in R such that $\mathfrak{p}$ is a minimal prime of $I := (x_1,\dots,x_h)R$. Since (the image of) $\mathfrak{p}$ is then an associated prime of R/I, we can find by Exercise 5.3.12 a short exact sequence

$$0 \to R/\mathfrak{p} \to R/I \to C \to 0$$

for some finitely generated R-module C. The relevant part of the long exact Tor sequence from 6.2.5, obtained by tensoring the above exact sequence with M, is

[3] A related question is even open in these cases: does there exist a 'small' Cohen-Macaulay module, i.e., a finitely generated one, if the ring is moreover complete? For the notion of a complete local ring, see §7.2; there are counterexamples to the existence of a small Cohen-Macaulay module if the ring is not complete.

$$\mathrm{Tor}^R_{e+1}(M,C) \to \mathrm{Tor}^R_e(M,R/\mathfrak{p}) \to \mathrm{Tor}^R_e(M,R/I). \tag{6.8}$$

The first module in (6.8) is zero by the maximality of e. The last module is zero too since it is isomorphic to $\mathrm{Tor}^{R/I}_e(M/IM,R/I) = 0$ by Proposition 6.4.2 and the fact that $(x_1,\dots,x_d)$ is by assumption M-regular. Hence the middle module in (6.8) is also zero, contradiction. □

We derive the following criterion for Cohen-Macaulayness:

Corollary 6.6.11. *If X is an irreducible affine scheme of finite type over an algebraically closed field K, and $\phi\colon X \to \mathbb{A}^d_K$ is a Noether normalization, that is to say, a finite and surjective morphism, then X is Cohen-Macaulay if and only if ϕ is flat.*

Proof. Suppose $X = \mathrm{Spec}(B)$, so that ϕ corresponds to a finite and injective homomorphism $A \to B$, with $A := K[\xi_1,\dots,\xi_d]$ (see our discussion on page 31) and B a d-dimensional affine domain. Let $\mathfrak{n}$ be a maximal ideal of B, and let $\mathfrak{m} := \mathfrak{n} \cap A$ be its contraction to A. Since $A/\mathfrak{m} \to B/\mathfrak{n}$ is finite and injective, and since the second ring is a field, so is the former by Lemma 3.2.7. Hence $\mathfrak{m}$ is a maximal ideal of A, and $A_\mathfrak{m}$ is regular by 5.1.6. By Exercise 4.4.14, the height of $\mathfrak{n}$ is d. Choose an ideal $I := (x_1,\dots,x_d)A$ whose image in $A_\mathfrak{m}$ is a parameter ideal. Since the natural homomorphism $A/I \to B/IB$ is finite, the latter ring is Artinian since the former is (note that $A/I = A_\mathfrak{m}/IA_\mathfrak{m}$). It follows that $IB_\mathfrak{n}$ is a parameter ideal in $B_\mathfrak{n}$.

Now, if B, whence also $B_\mathfrak{n}$ is Cohen-Macaulay, then $(x_1,\dots,x_d)$, being a system of parameters in $B_\mathfrak{n}$, is $B_\mathfrak{n}$-regular by Theorem 5.2.6. This proves that $B_\mathfrak{n}$ is balanced big Cohen-Macaulay module over $A_\mathfrak{m}$, whence is flat by Theorem 6.6.10. Hence ϕ is flat by 6.3.8.

Conversely, assume $X \to \mathbb{A}^d_K$ is flat. Therefore, $A_\mathfrak{m} \to B_\mathfrak{n}$ is flat, and hence $(x_1,\dots,x_d)$ is $B_\mathfrak{n}$-regular by Proposition 6.4.1. Since we already showed that this sequence is a system of parameters, we see that $B_\mathfrak{n}$ is Cohen-Macaulay. Since this holds for all maximal prime ideals of B, we proved that B is Cohen-Macaulay. □

Remark 6.6.12. The above argument proves the following more general result in the local case: if $A \subseteq B$ is a finite and faithfully flat extension of local rings with A regular, then B is Cohen-Macaulay. For the converse, we can even formulate a stronger criterion.

Theorem 6.6.13. *Let $(R,\mathfrak{m}) \to (S,\mathfrak{n})$ be a local homomorphism of Noetherian local rings. If R is regular of dimension d, if S is Cohen-Macaulay of dimension e, and if $S/\mathfrak{m}S$ has dimension $e-d$, then $R \to S$ is flat.*

Proof. Let $(x_1,\dots,x_d)$ be a system of parameters of R. Since $S/\mathfrak{m}S$ has dimension $e-d$, there exist $x_{d+1},\dots,x_e$ in S such that their image in $S/\mathfrak{m}S$ is a system of parameters. Hence $(x_1,\dots,x_e)$ is a system of parameters in S, whence is S-regular by Theorem 5.2.6. In particular, $(x_1,\dots,x_d)$ is S-regular, showing that S is a balanced big Cohen-Macaulay R-module, and therefore is flat by Theorem 6.6.10. □

The residue ring $S/\mathfrak{m}S$ is called the *closed fiber* of $R \to S$. Note that the affine scheme defined by it is indeed the fiber of $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ of the unique closed point of $\mathrm{Spec}(R)$; see (3.6). Exercise 6.7.17 establishes that flatness in turn forces the dimension equality in the theorem, without any singularity assumptions on the rings. We conclude with an application of the above Cohen-Macaulay criterion:

Corollary 6.6.14. *Any hypersurface in $\mathbb{A}^n_K$ is Cohen-Macaulay.*

Proof. Recall that a hypersurface Y is an affine closed subscheme of the form $\mathrm{Spec}(A/fA)$ with $A := K[\xi_1, \dots, \xi_n]$ and $f \in A$. Moreover, Y has dimension $n-1$ (by an application of Corollary 4.3.6), whence its Noether normalization is of the form $Y \to \mathbb{A}^{n-1}_K$. In fact, after a change of coordinates (see the proof of Theorem 3.2.5), we may assume that f is monic in ξ_n of degree d. It follows that A/fA is free over $A' := K[\xi_1, \dots, \xi_{n-1}]$ with basis $1, \xi_n, \dots, \xi_n^{d-1}$. Hence A/fA is flat over A' by 6.2.2, whence Cohen-Macaulay by Corollary 6.6.11. □

Colon criterion for flatness. Recall that $(I : a)$ denotes the *colon* ideal of all $x \in A$ such that $ax \in I$. Colon ideals are related to cyclic modules in the following way:

6.6.15 *For any ideal $I \subseteq A$ and any element $a \in A$, we have an isomorphism $a(A/I) \cong A/(I : a)$.*

Indeed, the homomorphism $A \to A/I \colon x \mapsto ax$ has image $a(A/I)$ whereas its kernel is $(I : a)$. We already saw that faithfully flat homomorphisms preserve the ideal structure of a ring (see 6.3.5). Using colon ideals, we can even give the following criterion:

Theorem 6.6.16. *A homomorphism $A \to B$ is flat if and only if*

$$(IB : a) = (I : a)B$$

for all elements $a \in A$ and all (finitely generated) ideals $I \subseteq A$.

Proof. Suppose $A \to B$ is flat. In view of 6.6.15, we have an exact sequence

$$0 \to A/(I : a) \to A/I \to A/(I + aA) \to 0 \tag{6.9}$$

which, when tensored with B gives the exact sequence

$$0 \to B/(I : a)B \to B/IB \xrightarrow{f} B/(IB + aB) \to 0.$$

However, the kernel of f is easily seen to be $a(B/IB)$, which is isomorphic to $B/(IB : a)$ by 6.6.15. Hence the inclusion $(I : a)B \subseteq (IB : a)$ must be an equality.

For the converse, we need in view of Theorem 6.2.6 to show that $\mathrm{Tor}_1^A(B, A/J) = 0$ for every finitely generated ideal $J \subseteq A$. We induct on the minimal number s of generators of J, where the case $s = 0$ trivially holds. Write $J = I + aA$ with I an ideal generated by $s - 1$ elements. Tensoring (6.9) with B, we get from 6.2.5 an exact sequence

$$0 = \mathrm{Tor}_1^A(B, A/I) \to \mathrm{Tor}_1^A(B, A/J) \xrightarrow{\delta} B/(I : a)B \to B/IB \xrightarrow{g} B/JB \to 0,$$

where the first module vanishes by induction. As above, the kernel of g is easily seen to be $B/(IB:a)$, so that our assumption on the colon ideals implies that δ is the zero map, whence $\mathrm{Tor}_1^A(B, A/J) = 0$ as we wanted to show. □

Here is a nice 'descent type' application of this criterion:

Corollary 6.6.17. *Let $A \to B \to C$ be homomorphisms whose composition is flat. If $B \to C$ is cyclically pure, then $A \to B$ is flat. In fact, it suffices that $B \to C$ is* cyclically pure with respect to ideals extended from A, *that is to say, that $JB = JC \cap B$ for all ideals $J \subseteq A$.*

Proof. Given an ideal $I \subseteq A$ and an element $a \in A$, we need to show in view of Theorem 6.6.16 that $(IB : a) = (I : a)B$. One inclusion is immediate, so take y in $(IB : a)$. By the same theorem, we have $(IC : a) = (I : a)C$, so that y lies in $(I : a)C \cap B$ whence in $(I : a)B$ by cyclical purity. □

The next criterion will be useful when dealing with non-Noetherian algebras in the next chapter. Here we call an ideal J in a ring B *finitely related*, if it is of the form $J = (I : b)$ with $I \subseteq B$ a finitely generated ideal and $b \in B$.

Theorem 6.6.18. *Let A be a Noetherian ring and B an arbitrary A-algebra. Suppose $\mathscr{P}$ is a collection of prime ideals in B such that every proper, finitely related ideal of B is contained in some prime ideal belonging to $\mathscr{P}$. If $A \to B_{\mathfrak{p}}$ is flat for every $\mathfrak{p} \in \mathscr{P}$, then $A \to B$ is flat.*

Proof. By Theorem 6.6.16, we need to show that $(IB : a) = (I : a)B$ for all $I \subseteq A$ and $a \in A$. Put $J := (I : a)$. Towards a contradiction, let x be an element in $(IB : a)$ but not in JB. Hence $(JB : x)$ is a proper, finitely related ideal, and hence contained in some $\mathfrak{p} \in \mathscr{P}$. However, $(IB_{\mathfrak{p}} : a) = JB_{\mathfrak{p}}$ by flatness and another application of Theorem 6.6.16, so that $x \in JB_{\mathfrak{p}}$, contradicting that $(JB : x) \subseteq \mathfrak{p}$. □

6.7 Exercises

Ex 6.7.1

Show that if $N_\bullet$ is an exact sequence, then there exist short exact sequences $0 \to Z_{i+1} \to N_i \to Z_i \to 0$ for some submodules $Z_i \subseteq N_i$ and all i. Use this to deduce 6.2.1.

Ex 6.7.2

Give a complete proof of 6.2.2, including the infinitely generated case.

Ex 6.7.3

Prove 6.2.3 and 6.2.4.

Ex 6.7.4

Show that if $A \to B$ is flat, and $I, J \subseteq A$ are ideals, then $IB \cap JB = (I \cap J)B$.

Ex 6.7.5

Show that if $A \to B$ is a flat homomorphism and M, N are A-modules, then

$$\operatorname{Tor}_i^A(M,N) \otimes_A B \cong \operatorname{Tor}_i^B(M \otimes_A B, N \otimes_A B)$$

for all i.

Ex 6.7.6

Show directly that for a given A-module M, if $I \otimes_A M \to M$ is injective for every finitely generated ideal I, then the same holds for every ideal. Use this to give a proof of (3) $\Rightarrow$ (1) in Theorem 6.2.6 in case A is not Noetherian. Prove the infinitely generated case in Corollary 6.2.7 by using syzygies and Corollary 6.2.8, in combination with a modification of the argument in Theorem 6.2.6.

Ex 6.7.7

Show that a homomorphism $A \to B$ is cyclically pure with respect to prime ideals, meaning that $\mathfrak{p}B \cap A = \mathfrak{p}$ for all prime ideals $\mathfrak{p} \subseteq A$, if and only if the induced map of affine schemes $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is surjective.

Ex 6.7.8

Show using Exercise 5.3.12 that any finitely generated module N over a Noetherian ring admits a prime filtration (6.3). Use this to work out the details in the proof of Corollary 6.2.7.

Ex 6.7.9

Prove 6.5.2 by constructing inductively a minimal resolution using Nakayama's lemma.

Ex 6.7.10

Generalize the proof of the first part of Theorem 6.6.1 to prove the second assertion in that theorem.

Ex 6.7.11

Mimic the proof of Corollary 6.6.3 to show that any power series ring in finitely many indeterminates over a Noetherian ring is flat.

Ex 6.7.12

Modify the argument in the last part of the proof of Theorem 5.2.6 to prove Proposition 6.6.9.

Ex 6.7.13

Make the necessary adjustments in the proof of the first assertion of Theorem 6.6.10 to derive the second.

Ex 6.7.14

Show that an A-module M is flat if and only if $M_{\mathfrak{m}}$ is flat as an $A_{\mathfrak{m}}$-module for every maximal ideal $\mathfrak{m} \subseteq A$. Prove 6.3.8 (note that if X is moreover Noetherian, then this follows already from Theorem 6.6.18).

Ex 6.7.15

By 4.1.4, any Artinian ring is a finite direct sum of local rings. This no longer holds true for an arbitrary Noetherian semi-local *ring S, that is to say, a Noetherian ring with finitely many maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_s$. Show that nonetheless there is always a natural homomorphism $S \to S_{\mathfrak{m}_1} \oplus \cdots \oplus S_{\mathfrak{m}_s}$, which is moreover faithfully flat.*

*Ex 6.7.16

Show that if M is a finitely generated module over a Noetherian ring A such that $M_{\mathfrak{m}}$ is flat over $A_{\mathfrak{m}}$, for every maximal ideal $\mathfrak{m}$, then M is projective as an A-module.

*Ex 6.7.17

Show that if $A \to B$ is a flat homomorphism, then the going-down *theorem holds for $A \to B$, meaning that if $\mathfrak{p} \subsetneq \mathfrak{q}$ is a chain of prime ideals in A, and if $\mathfrak{Q}$ is a prime ideal in B lying over $\mathfrak{q}$, then there exists a prime ideal $\mathfrak{P} \subsetneq \mathfrak{Q}$ lying over $\mathfrak{p}$. Use this to prove that if $(R, \mathfrak{m}) \to (S, \mathfrak{n})$ is a flat and local homomorphism of Noetherian local rings, then*

$$\dim(R) + \dim(S/\mathfrak{m}S) = \dim(S).$$

Ex 6.7.18

Use the Colon criterion, Theorem 6.6.16, to show that every overring without zero-divisors, or more generally, any torsion-free overring, of a discrete valuation ring is flat.

Ex 6.7.19

Show that every finitely related ideal in an ultra-ring is an ultra-ideal.

*Ex 6.7.20

Prove a version of Theorem 6.6.16 for modules, that is to say, by replacing the A-algebra B by an A-module M.

Additional exercises.

Ex 6.7.21

Show that a module P is projective (=direct summand of a free module) if and only if any map $P \to N/N'$ lifts to a map $P \to N$, where $N' \subseteq N$ are arbitrary modules.

Ex 6.7.22

Show that if

$$0 \to M'_\bullet \xrightarrow{f} M_\bullet \xrightarrow{g} M''_\bullet \to 0$$

is an exact sequence of complexes, meaning that for each i, we have an exact sequence

$$0 \to M'_i \xrightarrow{f_i} M_i \xrightarrow{g_i} M''_i \to 0,$$

such that the maps f_i and g_i commute with the maps in the various complexes, then we get a long exact sequence

$$\dots \xrightarrow{\delta_{i+1}} \mathrm{H}_i(M'_\bullet) \xrightarrow{f_i} \mathrm{H}_i(M_\bullet) \xrightarrow{g_i} \mathrm{H}_i(M''_\bullet) \xrightarrow{\delta_i} \mathrm{H}_{i-1}(M'_\bullet) \to \dots$$

where the f_i and g_i are used to denote the corresponding induced homomorphisms, and where the δ_i are the connecting homomorphisms defined as follows: for $\bar{u} \in H_i(M''_\bullet)$, choose a lifting $u \in \mathrm{Ker}(d''_i) \subseteq M''_i$ and an element $v \in M_i$ such that $g_i(v) = u$. Since $g(d_i(v)) = 0$, there exists a well-defined $w \in M'_{i-1}$ for which $f_{i-1}(w) = d_i(v)$ and $d_{i-1}(w) = 0$. Show that assigning the class of w in $H_{i-1}(M'_\bullet)$ to $\bar{u}$ gives a well-defined homomorphism δ_i, making the above sequence exact.
Use this result to now give a complete proof of 6.2.5.

Ex 6.7.23

Show that for an A-module M to be faithfully flat, it is necessary and sufficient that an arbitrary complex $N_\bullet$ is exact if and only if $N_\bullet \otimes_A M$ is exact.

Ex 6.7.24

Let $A \to B \to C$ be homomorphisms. Show that if $A \to C$ is flat, then $A \to B$ is cyclically pure. Show using Exercise 6.7.23 that if both $A \to C$ and $B \to C$ are faithfully flat, then so is $A \to B$.

Ex 6.7.25

Show that a module is finitely generated if and only if any countably generated submodule is contained in a finitely generated submodule.

Ex 6.7.26

Prove the following version of a theorem due to Chase ([16]): a ring is coherent if and only if every finitely related ideal is finitely generated. The direct implication is a simple application of the coherency condition; for the converse use Theorem 6.6.4 and the Colon Criterion for flatness, Theorem 6.6.16.
Use this to extend Theorem 6.6.18 to the case that A is only assumed to be coherent.

Ex 6.7.27

Show that an ultra-Dedekind domain R, that is to say, an ultraproduct of Dedekind domains, is coherent. In fact, prove the stronger fact that any finitely related ideal in R is generated by two elements, and then use Exercise 6.7.26.

6.8 Project: local flatness criterion via nets

Let $(R,\mathfrak{m})$ be a Noetherian local ring with residue field k, and let $\mathbf{mod}_R$ be the class of all finitely generated R-modules (up to isomorphism). In [71], a subset $\mathbf{N} \subseteq \mathbf{mod}_R$ is called a *net* if it is closed under *extension* (i.e., if $0 \to H \to M \to N \to 0$ is an exact sequence in $\mathbf{mod}_R$ with $H,N \in \mathbf{N}$, then also $M \in \mathbf{N}$), and under *direct summands* (i.e., if $M \cong H \oplus N$ belongs to $\mathbf{N}$, then so do H and N). Clearly, $\mathbf{mod}_R$ itself is a net.

6.8.1 *Show that any intersection of nets is again a net. Conclude that any class $\mathbf{K} \subseteq \mathbf{mod}_R$ sits inside a smallest net, called the* net generated *by* $\mathbf{K}$.

6.8.2 *Show that the net generated by the singleton $\{k\}$ consists of all modules of finite length. Show that $\mathbf{mod}_R$ is generated as a net by all $R/\mathfrak{p}$ with $\mathfrak{p} \subseteq R$ a prime ideal.*

A net $\mathbf{N}$ is called *deformational*, if for every $M \in \mathbf{mod}_R$ and every M-regular element x, if $M/xM \in \mathbf{N}$ then $M \in \mathbf{N}$.

6.8.3 *Show that the deformational net generated by the singleton $\{k\}$ is equal to* $\mathbf{mod}_R$.

The goal is to prove the following version of the local flatness criterion:

6.8.4 *If $R \to S$ is a local homomorphism of Noetherian local rings, and Q a finitely generated S-module such that $\operatorname{Tor}_1^R(Q,k) = 0$, then Q is flat as an R-module.*

To this end, for $M \in \mathbf{mod}_R$, put $F(M) := \operatorname{Tor}_1^R(Q,M)$. In view of Theorem 6.2.6, we need to show that F is zero on $\mathbf{mod}_R$.

6.8.5 *Show that $F(M)$ carries a natural structure of an S-module, and as such is finitely generated, for any finitely generated R-module M.*

6.8.6 *Show that if F is zero on a class $\mathbf{K} \subseteq \mathbf{mod}_R$, then F is zero on the net generated by $\mathbf{K}$, and, in fact, even zero on the deformational net generated by $\mathbf{K}$. For the first assertion, use 6.2.5, and for the second, show that for any $N \in \mathbf{mod}_R$ and any $x \in \mathfrak{m}$, if $xF(N) = F(N)$ then $F(N) = 0$, using 6.8.5. Finally, conclude the proof of 6.8.4 by using 6.8.3.*

Chapter 7
Completion

A very important algebraic tool in studying local properties of a variety, or equivalently, properties of Noetherian local rings, is the completion of a Noetherian local ring. As the name suggests, we can put a canonical metric on any such ring R, and then take its topological completion $\widehat{R}$. This is again a Noetherian local ring, which inherits many of the properties of the original ring, and in fact, there is natural homomorphism $R \to \widehat{R}$, which is flat and unramified (the latter means that the maximal ideal of R extends to the maximal ideal of its completion $\widehat{R}$); see Theorem 7.3.4. Whereas there is no known classification of arbitrary Noetherian local rings, we do have many structure theorems, due mostly to Cohen, for *complete* Noetherian local rings. In particular, the equal characteristic complete regular local rings are completely classified by their residue field k and their dimension d: any such ring is isomorphic to the power series ring $k[[\xi_1,\dots,\xi_d]]$; see Theorem 7.4.5. Also extremely useful is the fact that we have an analogue of Noether Normalization for complete Noetherian local rings: any such ring admits a regular subring over which it is finite (Theorem 7.4.6).

7.1 Complete normed rings

Normed rings. In these notes, a *quasi-normed ring* $(A, ||\cdot||)$ will mean a ring A together with a real-valued function $A \to [0,1]\colon a \mapsto ||a||$ such that $||0|| = 0$ and such that for all $a, b \in A$ we have

1. $||a+b|| \leq \max\{||a||, ||b||\}$;
2. $||ab|| \leq ||a|| \cdot ||b||$.

We normally exclude the case that $||\cdot||$ is identical zero (the so-called *degenerated* case). Inequality (1) is called the *non-archimedean triangle inequality*, as opposed to the usual, weaker triangle inequality in the reals (note that (1) implies indeed that $||a+b|| \leq ||a|| + ||b||$). An immediate consequence of this triangle inequality is:

3. if $||a|| < ||b||$, then $||a+b|| = ||b||$,

which often is paraphrased by saying that "every triangle is isosceles". If moreover $||a|| = 0$ implies $a = 0$, then we call $(A, ||\cdot||)$ a *normed ring* (or, we simply say that $||\cdot||$ is a norm). The value $||a||$ will also be called the *norm* of a, even if $||\cdot||$ is only a quasi-norm. If in (2) we always have equality, then we call the norm *multiplicative* (be aware that some authors tacitly assume that a norm is always multiplicative; moreover, it is common to allow elements to also have norm bigger than one). Some immediate consequences of this definition (see Exercise 7.5.1):

7.1.1 *Any unit in a quasi-normed ring has norm equal to one. The elements of norm equal to zero form an ideal I_0; and those of norm strictly less than one form an ideal I_1^-, called the* center *of $||\cdot||$. If $||\cdot||$ is multiplicative, then I_0 and I_1^- are prime. In particular, a multiplicatively normed ring is a domain.*

There is also a very canonical procedure to turn a quasi-norm into a norm:

7.1.2 *If A is a quasi-normed ring, and I_0 its ideal of elements of norm zero, then $||\cdot||$ factors through A/I_0, making the latter into a normed ring.*

Indeed, using (3) we have $||a|| = ||a+w||$ for all $w \in I_0$, so that letting $||\bar{a}|| := ||a||$ is well-defined, where $\bar{a}$ denotes the image of a in A/I_0. The remaining properties are now easily checked. The normed ring A/I_0 is called the *Hausdorffication* or *separated quotient* of A. The name is justified by the following considerations: any quasi-normed ring inherits a topology, called the *norm topology*, simply by taking for opens the inverse images of the opens of $[0,1]$ under the norm map $A \to [0,1]$. Now, by Exercise 7.5.4, the topology on A is Hausdorff if and only if $||\cdot||$ is a norm.

Let $(A, ||\cdot||_A)$ and $(B, ||\cdot||_B)$ be two quasi-normed rings. A homomorphism $A \to B$ is called a *homomorphism of quasi-normed rings* if $||a||_B \leq ||a||_A$ for all a. We may also express this fact by saying that B is a *quasi-normed A-algebra*. If $I \subseteq A$ is an ideal, define a quasi-norm on A/I by letting $||a+I||$ be the infimum of all $||a+i||$ with $i \in I$. By Exercise 7.5.5, we have

7.1.3 *For any ideal $I \subseteq A$, the pair $(A/I, ||\cdot||)$ is a quasi-normed ring, and the residue map $A \to A/I$ is a homomorphism of quasi-normed rings.*

Cauchy sequences. Let $(A, ||\cdot||)$ be a quasi-normed ring. We will represent sequences in A as functions $\mathbf{a}\colon \mathbb{N} \to A$. Any element $a \in A$ defines a sequence, the *constant sequence* with value a defined as $\mathbf{a}(n) := a$. We will identify an element $a \in A$ with the constant sequence it defines.

We say that a sequence $\mathbf{a}$ is a *null-sequence* if for each $\varepsilon > 0$, there exists $N := N(\varepsilon)$ such that $||\mathbf{a}(n)|| \leq \varepsilon$ for all $n \geq N$. In particular, a constant sequence a is null if and only if $||a|| = 0$. The *twist* $\mathbf{a}^+$ of a sequence $\mathbf{a}$ is the sequence defined by $\mathbf{a}^+(n) := \mathbf{a}(n+1)$. We say that $\mathbf{a}$ is a *Cauchy sequence*, if $\mathbf{a} - \mathbf{a}^+$ is a null-sequence. We say that an element $b \in A$ is a *limit* of a sequence $\mathbf{a}$, if $\mathbf{a} - b$ is a null-sequence. A sequence admitting a limit is called a *converging* sequence. We have:

7.1.4 *Any converging sequence is Cauchy. If b is a limit of a sequence $\mathbf{a}$, then so is $b+w$ for any w of norm zero. In particular, if $||\cdot||$ is a norm, then a Cauchy sequence has at most one limit.*

If the converse also holds, that is to say, if any Cauchy sequence is convergent, then we say that $(A, ||\cdot||)$ is *quasi-complete*. We call $(A, ||\cdot||)$ *complete* if it is quasi-complete and $||\cdot||$ is a norm, that is to say, if any Cauchy sequence has a unique limit.

7.1.5 *If A is quasi-complete and $I \subseteq A$ is a proper ideal, then A/I is again quasi-complete.*

This is proven in Exercise 7.5.5. In particular, we can turn any quasi-complete ring into a complete one: simply consider its Hausdorffication A/I_0. A sequence $\mathbf{b}$ is called a *subsequence* of a sequence $\mathbf{a}$ if there exists some strictly increasing function $f\colon \mathbb{N} \to \mathbb{N}$ such that $\mathbf{a}(f(n)) = \mathbf{b}(n)$ for all n. The following is left as an exercise (Exercise 7.1.6):

7.1.6 *Any subsequence of a Cauchy sequence is a Cauchy sequence, and any limit of a sequence is also a limit of any of its subsequences. Moreover, for a Cauchy sequence to be convergent it suffices that some subsequence is convergent.*

Note that a (non-Cauchy) sequence can very well have a converging subsequence without itself being convergent.

Adic norms. Let A be any ring, and I an ideal. We can associate a quasi-norm to this situation, called the *I-adic quasi-norm* defined as $||a||_I := \exp(-n)$ where n is the supremum of all k for which $a \in I^k$. We allow for this supremum to be infinite, with the understanding that $\exp(-\infty) = 0$. By Exercise 7.5.7 this is indeed a quasi-norm, which is degenerated if and only if I is the unit ideal. Hence $||\cdot||_I$ is a norm if and only if the intersection I^∞ of all I^k is zero. The only case of interest to us is when $(R, \mathfrak{m})$ is local viewed in its $\mathfrak{m}$-adic quasi-norm, which we then call the *canonical* quasi-norm of R, or when there is no confusion, *the* quasi-norm of R. By what we just said, the quasi-norm of $(R, \mathfrak{m})$ is a norm if and only if its ideal of infinitesimals, $\mathfrak{I}_R := \mathfrak{m}^\infty$ (see Definition 2.4.10), is equal to zero. By Exercise 7.5.7, we have:

7.1.7 *Any polynomial $f \in A[\xi]$ in a single indeterminate ξ defines a continuous function $A \to A\colon a \mapsto f(a)$ in the topology induced by an I-adic quasi-norm.*

If $A \to B$ is a homomorphism and $I \subseteq A$ an ideal, then $A \to B$ is a homomorphism of quasi-normed rings if we take the I-adic quasi-norm on A and the IB-adic quasi-norm on B.

7.2 Complete local rings

We call a local ring R (*quasi-*)*complete*, if it is (quasi-)complete with respect to its $\mathfrak{m}$-adic quasi-norm. By Exercise 7.5.8, we have

7.2.1 *A local ring $(R,\mathfrak{m})$ is quasi-complete if and only if every sequence $\mathbf{a}$ satisfying $\mathbf{a}(n) \equiv \mathbf{a}(n+1) \mod \mathfrak{m}^n$, for all n, has a limit, and for this it suffices that we can find a subsequence $\mathbf{b}$ of $\mathbf{a}$ and an element $b \in R$ such that $b \equiv \mathbf{b}(n) \mod \mathfrak{m}^n$.*

Fields are obviously complete local rings, and more generally, so are Artinian local rings. Any power series ring over a field (or an Artinian local ring) in finitely many indeterminates is complete. This follows by induction from the following more general result.

Proposition 7.2.2. *If R is a quasi-complete local ring, then so is $R[[\xi]]$ with ξ a single variable.*

Proof. The maximal ideal $\mathfrak{n}$ of $R[[\xi]]$ is generated by ξ and the maximal ideal $\mathfrak{m}$ of R. By (7.2.1), we need to show that a sequence $\mathbf{f}$ in $R[[\xi]]$ such that

$$\mathbf{f}(k) \equiv \mathbf{f}(k+1) \mod \mathfrak{n}^k \tag{7.1}$$

for all k, has a limit. Write each $\mathbf{f}(n) = \sum_j \mathbf{a}_j(n)\xi^j$. Expanding (7.1) and comparing coefficients, we get $\mathbf{a}_j(k) \equiv \mathbf{a}_j(k-1) \mod \mathfrak{m}^{k-j}$ for all $j \leq k$. In particular, each $\mathbf{a}_j$ is Cauchy, whence admits a limit $b_j \in R$. I claim that $g(\xi) := \sum_j b_j \xi^j$ is a limit of $\mathbf{f}$. To verify this, fix some k. By assumption, there exists, for each j, some $N_j(k)$ such that $b_j \equiv \mathbf{a}_j(n) \mod \mathfrak{m}^k$ for all $n \geq N_j(k)$. Let $N(k)$ be the maximum of all $N_j(k)$ with $j < k$. For $n \geq N(k)$, the terms in $g - \mathbf{f}(n)$ of degree at least k clearly lie inside $\mathfrak{n}^k$. The coefficient of the term of degree $j < k$ is $b_j - \mathbf{a}_j(n)$, which lies in $\mathfrak{m}^k$ by the choice of $N(k)$. Hence $g \equiv \mathbf{f}(n) \mod \mathfrak{n}^k$ for all $n \geq N(k)$, proving the claim. □

Immediately from 7.1.5 we get:

7.2.3 *Any homomorphic image of a quasi-complete local ring is again quasi-complete.*

In particular, the Hausdorffication of a quasi-complete local ring R, that is to say, the separated quotient $R/\mathfrak{I}_R$, is a complete local ring.

Hensel's lemma. The next result is a formal version of Newton's method for finding approximate roots.

Theorem 7.2.4. *Let $(R,\mathfrak{m})$ be a complete local ring with residue field k. Let $f \in R[\xi]$ be a monic polynomial in the single variable ξ, and let $\bar{f} \in k[\xi]$ denote its reduction modulo $\mathfrak{m}R[\xi]$. For every simple root $u \in k$ of $\bar{f} = 0$, we can find $a \in R$ such that $f(a) = 0$ and u is the image of a in k.*

Proof. Let $a_1 \in R$ be any lifting of u. Since $\bar{f}(u) = 0$, we get $f(a_1) \equiv 0 \mod \mathfrak{m}$. We will define elements $a_n \in R$ recursively such that $f(a_n) \equiv 0 \mod \mathfrak{m}^n$ and $a_n \equiv a_{n-1} \mod \mathfrak{m}^{n-1}$ for all $n > 1$. Suppose we already defined $a_1, \dots, a_n$ satisfying the above conditions. Consider the Taylor expansion

$$f(a_n + \xi) = f(a_n) + f'(a_n)\xi + \xi^2 g_n(\xi) \tag{7.2}$$

where $g_n \in R[\xi]$ is some polynomial. Since the image of a_n in k is equal to u, and since $\bar{f}'(u) \neq 0$ by assumption, $f'(a_n)$ does not lie in $\mathfrak{m}$ whence is a unit, say, with inverse u_n. Define $a_{n+1} := a_n - u_n f(a_n)$. Substituting $\xi = -u_n f(a_n)$ in (7.2), we get

$$f(a_{n+1}) \in (u_n f(a_n))^2 R \subseteq \mathfrak{m}^{2n},$$

as required.

To finish the proof, note that the sequence $\mathbf{a}$ given by $\mathbf{a}(n) := a_n$ is by construction Cauchy, and hence by assumption admits a limit $a \in R$ (whose residue is necessarily again equal to u). By continuity, $f(a)$ is equal to the limit of the $f(a_n)$ whence is zero. □

There are sharper versions of this result, where the root in the residue field need not be simple (See Exercise 7.5.15), or even involving systems of equations. Any local ring satisfying the hypothesis of the above theorem is called a *Henselian* ring. From a model-theoretic point of view, it is sometimes more convenient to work with Henselian local rings than with complete ones, since they form a first-order definable class (as is clear from the defining condition).

As with completion (see §7.3 below), there exists a 'smallest' Henselian overring. More precisely, for each Noetherian local ring R, there exists a Noetherian local R-algebra $R^\sim$, its *Henselization*, satisfying the following universal property: any local homomorphism $R \to H$ with H a Henselian local ring, factors uniquely through an R-algebra homomorphism $R^\sim \to H$. The existence of such a Henselization will be proven in Project 7.6. Note that Theorem 7.2.4 and the universal property imply that $R^\sim$ is a subring of $\widehat{R}$ (see 7.3.3), and in particular, the latter is the completion of the former.

Let $A := k[\xi]$ be a polynomial ring over a field k. For simplicity, we will denote the Henselization of the localization of A with respect to the variables also by $A^\sim$. It can be shown that $A^\sim = k[[\xi]]^{\mathrm{alg}}$, the ring of *algebraic power series* over k, where we call a power series in $k[[\xi]]$ *algebraic* if it is algebraic over $k[\xi]$, that is to say, satisfies a non-zero polynomial equation with coefficients in $k[\xi]$ (for a discussion see [2] or 7.6.4 below).

Lifting generators. The next property of quasi-complete local rings, a generalization of Nakayama's lemma, is also quite useful.

Theorem 7.2.5. *Let $(R, \mathfrak{m})$ be a quasi-complete local ring, and let M be an R-module which is $\mathfrak{m}$-adically Hausdorff, in the sense that the intersection of all $\mathfrak{m}^n M$ is zero. If $M/\mathfrak{m}M$ has vector space dimension e over the residue field $R/\mathfrak{m}$, then M is generated as an R-module by e elements. In fact, any lifting of a set of generators of $M/\mathfrak{m}M$ generates M.*

Proof. Let $\nu_1, \dots, \nu_e \in M$ be liftings of the generators of $M/\mathfrak{m}M$ and let N be the submodule they generate. In particular, $M = N + \mathfrak{m}M$. Take an arbitrary $\mu \in M$. We can find some $a_i^{(0)} \in A$ such that $\mu = \sum_i a_i^{(0)} \nu_i + \mu^{(1)}$ with $\mu^{(1)} \in \mathfrak{m}M$. Applying the same to $\mu^{(1)}$, we can find $a_i^{(1)} \in \mathfrak{m}$ such that $\mu^{(1)} = \sum_i a_i^{(1)} \nu_i + \mu^{(2)}$ with $\mu^{(2)} \in \mathfrak{m}^2 M$. Continuing this way, we find $a_i^{(n)} \in \mathfrak{m}^n$ such that

$$\mu \equiv \sum_{i=1}^{s} (\sum_{j=0}^{n} a_i^{(j)}) v_i \mod \mathfrak{m}^{n+1} M. \tag{7.3}$$

Putting $\mathbf{b}_i(n) := \sum_{j \leq n} a_i^{(j)}$, it follows that each $\mathbf{b}_i$ is a Cauchy sequence, whence has a limit $a_i \in R$. Using (7.3), one easily verifies that $\mu - \sum a_i v_i$ lies in every $\mathfrak{m}^n M$ whence is zero, showing that $\mu \in N$, and therefore $M = N$. □

7.3 Completions

We have seen in the previous section that complete local rings satisfy many good properties. In this section, we will describe how to construct complete local rings from arbitrary local rings. Let again start in a more general setup.

Quasi-completion of a quasi-norm. Let $(A, ||\cdot||)$ be a quasi-normed ring. Let $\mathscr{C}(A)$ be the collection of all Cauchy sequences. We make $\mathscr{C}(A)$ into a ring by adding and multiplying sequences coordinate wise. In this way, $\mathscr{C}(A)$ becomes an A-algebra, via the canonical map $A \to \mathscr{C}(A)$ sending an element to the constant sequence it determines. Note that this is in fact an embedding.

7.3.1 *A sequence* $\mathbf{a}$ *in* A *is Cauchy if and only if* $||\mathbf{a}(n)||$ *converges in* $\mathbb{R}$ *as* $n \to \infty$. *This latter limit is denoted* $||\mathbf{a}||$; *it induces a quasi-norm on* $\mathscr{C}(A)$ *extending the norm on* A. *A Cauchy sequence has norm zero if and only if it is a null-sequence.*

From now on, we view $\mathscr{C}(A)$ as a quasi-normed ring with the above norm.

Proposition 7.3.2. *The ring of Cauchy sequences* $\mathscr{C}(A)$ *of* A *is quasi-complete. Moreover,* A *is dense in* $\mathscr{C}(A)$*, and the following universal property holds: if we have a homomorphism of quasi-normed rings* $A \to B$ *with* B *complete, then* $A \to B$ *extends uniquely to a homomorphism* $\mathscr{C}(A) \to B$ *of quasi-normed rings.*

Proof. For clarity, we let $j\colon A \to \mathscr{C}(A)$ denote the canonical homomorphism sending an element $a \in A$ to the constant sequence $j(a)$, and we distinguish between the norms on A and $\mathscr{C}(A)$ by adding a subscript to the norm symbol. Let $\mathbf{a}$ be a Cauchy sequence in A, that is to say, an element in $\mathscr{C}(A)$. It follows that the limit of $||j(\mathbf{a}(n)) - \mathbf{a}||_{\mathscr{C}(A)}$ is zero, for $n \mapsto \infty$. Hence, the Cauchy sequence $\mathbf{D}$ in $\mathscr{C}(A)$ defined as $\mathbf{D}(n) := j(\mathbf{a}(n))$ converges to the element $\mathbf{a} \in \mathscr{C}(A)$, showing that A (or, rather, $j(A)$) is dense in $\mathscr{C}(A)$.

Let $\mathbf{B}$ be a Cauchy sequence in $\mathscr{C}(A)$. Hence, $\mathbf{B}(m)$ is a Cauchy sequence in A, for each m, with n-th entry $\mathbf{B}(m)(n)$. Replacing $\mathbf{B}$ by a subsequence if necessary, we may assume $||\mathbf{B}(m) - \mathbf{B}(m+1)||_{\mathscr{C}(A)} \leq \exp(-m)$ for all m. By the previous observation, for each m, there exists $g(m)$ such that

$$||j(\mathbf{B}(m)(g(m))) - \mathbf{B}(m)||_{\mathscr{C}(A)} \leq \exp(-m).$$

Define a sequence $\mathbf{c}$ by the rule $\mathbf{c}(m) := \mathbf{B}(m)(g(m))$. Since $||\mathbf{c}(m) - \mathbf{c}(m+1)||_A$ is equal to

$$||j(\mathbf{c}(m)) - \mathbf{B}(m) + \mathbf{B}(m) - \mathbf{B}(m+1) + \mathbf{B}(m+1) - j(\mathbf{c}(m+1))||_{\mathscr{C}(A)} \leq \exp(-m)$$

we conclude that $\mathbf{c}$ is a Cauchy sequence in A. In particular, for a fixed n, we can find $N \geq n$ such that $||j(\mathbf{c}(m)) - \mathbf{c}||_{\mathscr{C}(A)} \leq \exp(-n)$, for all $m \geq N$. To show that $\mathbf{c}$ is the limit of $\mathbf{B}$, we use the estimate

$$\begin{aligned} ||\mathbf{B}(m) - \mathbf{c}||_{\mathscr{C}(A)} &= ||\mathbf{B}(m) - j(\mathbf{c}(m)) + j(\mathbf{c}(m)) - \mathbf{c}||_{\mathscr{C}(A)} \\ &\leq \max\{\exp(-m), \exp(-n)\} = \exp(-n), \end{aligned}$$

for all $m \geq N$. This proves that $\mathbf{c}$ is the limit of $\mathbf{B}$.

To prove the last assertion, we define $\varphi \colon \mathscr{C}(A) \to B$ as follows. Let $\mathbf{a}$ be a Cauchy sequence in A. From the definition of homomorphism of quasi-normed rings, it follows that $\mathbf{a}$ is a Cauchy sequence in B. Since B is complete, $\mathbf{a}$ has a unique limit $b \in B$. The assignment $\mathbf{a} \mapsto b$ is now easily seen to be an A-algebra homomorphism of quasi-normed rings. □

In view of this result, we call $\mathscr{C}(A)$ the *quasi-completion* of A. The *completion* of A is then the Hausdorffication of $\mathscr{C}(A)$, that is to say, the ring $\mathscr{C}(A)/\mathscr{I}_0$, where $\mathscr{I}_0$ is the ideal of all null-sequences. If the quasi-norm is understood, as will be the case with the canonical quasi-norm of a local ring, we denote the completion by $\widehat{A}$. From Proposition 7.3.2, we get the following universal property of completion:

7.3.3 *If B is a normed A-algebra which is complete, then there exists a unique A-algebra homomorphism of normed rings $\widehat{A} \to B$.*

Completion of a Noetherian local ring. We now apply the previous theory to the canonical norm on a Noetherian local ring R. Its completion $\mathscr{C}(R)/\mathscr{I}_0$ is denoted $\widehat{R}$. It is easy to see that $\mathfrak{m}\mathscr{C}(R)$ cannot be the unit ideal, whence neither is $\mathfrak{m}\widehat{R}$. We will shortly show that $\widehat{R}$ is in fact a Noetherian local ring with maximal ideal $\mathfrak{m}\widehat{R}$, and in its adic norm, it is complete. Moreover, the norm inherited from the norm on $\mathscr{C}(R)$ is identical to the $\mathfrak{m}\widehat{R}$-adic norm. To prove all these claims, we resort to flatness.

Theorem 7.3.4. *The canonical homomorphism $R \to \widehat{R}$ of a Noetherian local ring into its completion is faithfully flat. Moreover, $\widehat{R}$ is a Noetherian local ring with the same residue field as R.*

Proof. Since $\mathfrak{m}\widehat{R} \neq \widehat{R}$, it suffices to show that $R \to \widehat{R}$ is flat. Let $\mathbf{x} := (x_1, \dots, x_e)$ generate the maximal ideal $\mathfrak{m}$ of R, and let $\xi := (\xi_1, \dots, \xi_e)$ be a tuple of indeterminates. Define an R-algebra homomorphism $S := R[[\xi]] \to \widehat{R}$ as follows. Let f be a power series and let f_n be is its truncation consisting of all terms up to degree n. The sequence $\mathbf{a}$ defined by $\mathbf{a}(n) := f_n(\mathbf{x})$ is easily seen to be a Cauchy sequence in R, whence has a unique limit in $\widehat{R}$, which we simply denote by $f(\mathbf{x})$. The homomorphism $S \to \widehat{R}$ is given by the rule $f \mapsto f(\mathbf{x})$. A moment's reflection shows that its kernel is $I := (\xi_1 - x_1, \dots, \xi_e - x_e)S$. I claim that $S \to \widehat{R}$ is surjective, so that

$\widehat{R} = S/I$, showing already that $\widehat{R}$ is a Noetherian local ring with the same residue field as R. To prove surjectivity, let $\mathbf{a}$ be a Cauchy sequence, that is to say, an element of $\mathscr{C}(R)$. Since any subsequence of $\mathbf{a}$ has the same image in $\widehat{R}$, we may assume that $\mathbf{a}(n) \equiv \mathbf{a}(n+1) \mod \mathfrak{m}^n$ for all n. Hence we can write

$$\mathbf{a}(n+1) = \mathbf{a}(n) + \sum_{|\nu|=n} r_\nu \mathbf{x}^\nu$$

where the sum runs over all e-tuples ν such that $|\nu| := \nu_1 + \cdots + \nu_e = n$. Define

$$f(\xi) := \mathbf{a}(0) + \sum_\nu r_\nu \xi^\nu$$

where the sum is now over all non-zero e-tuples ν. Hence $f_n(\mathbf{x}) = \mathbf{a}(n)$ for all n (where as before f_n is the n-th degree truncation of f), showing that $f(\mathbf{x}) = \mathbf{a}$.

Since $R \to S$ is flat by Exercise 6.7.11, the flatness of $R \to \widehat{R}$ will follow from Thereom 6.6.5 once we show that $I \cap \mathfrak{a}S = \mathfrak{a}I$ for every ideal $\mathfrak{a} \subseteq R$. Let $\mathfrak{a} := (a_1, \dots, a_n)R$. Let $f \in I \cap \mathfrak{a}S$ so that we can write it in two different ways as

$$f = a_1 s_1 + \cdots + a_n s_n = t_1(\xi_1 - x_1) + \cdots + t_e(\xi_e - x_e) \tag{7.4}$$

for some $s_i, t_i \in S$. We want to show that $s_i \in I$. By Taylor expansion, we can write each s_i as $s_i = b_i + s_i'$ with $b_i \in R$ and $s_i' \in I$. Hence $f \equiv c \mod \mathfrak{a}I$ where $c := a_1 b_1 + \cdots + a_n b_n$. However, $R \to \widehat{R}$ is injective (since $\mathfrak{I}_R = 0$), so that $I \cap R = (0)$. Since c lies in $I \cap R$ it is therefore zero, showing that $f \in \mathfrak{a}I$. □

Corollary 7.3.5. *Let $(R, \mathfrak{m})$ be a Noetherian local ring with completion $\widehat{R}$. For all n, we have an isomorphism $R/\mathfrak{m}^n R \cong \widehat{R}/\mathfrak{m}^n \widehat{R}$. In particular, $\widehat{R}$ is a complete Noetherian local ring, that is to say, is complete in its canonical $\mathfrak{m}\widehat{R}$-adic norm, of the same dimension as R.*

Proof. Let $R_n := R/\mathfrak{m}^n$, and let $S_n := \widehat{R}/\mathfrak{m}^n \widehat{R}$. Note that R_n is Artinian, whence complete. As $S_n/\mathfrak{m}S_n$ is equal to the residue field of R whence of R_n by Theorem 7.3.4, we get $S_n \cong R_n$ by Theorem 7.2.5. In particular, R and $\widehat{R}$ have the same Hilbert-Samuel polynomial, whence the same dimension by Theorem 4.3.2.

I claim that if $\mathbf{a}$ is a Cauchy sequence such that $\mathbf{a}(k) \in \mathfrak{m}^n$ for all $k \gg 0$, then $\mathbf{a} \in \mathfrak{m}^n \widehat{R}$. Indeed, by what we just proved, we have $\widehat{R} = R + \mathfrak{m}^n \widehat{R}$. Hence if we choose generators $\mathbf{x}$ for $\mathfrak{m}$, then we can write

$$\mathbf{a} = r + \sum_{|\nu|=n} \mathbf{x}^\nu \mathbf{b}_\nu \tag{7.5}$$

with $r \in R$ and $\mathbf{b}_\nu \in \widehat{R}$. Substituting k such that $\mathbf{a}(k) \in \mathfrak{m}^n$ in (7.5) shows that $r \in \mathfrak{m}^n \widehat{R}$. Since $\mathfrak{m}^n \widehat{R} \cap R = \mathfrak{m}^n$ by faithful flatness (or the above isomorphism), we get $\mathbf{a} \in \mathfrak{m}^n \widehat{R}$, as claimed. It follows that the $\mathfrak{m}\widehat{R}$-adic norm of an element is at most its norm as a Cauchy sequence. The converse is easy, thus proving the last assertion.

□

Immediate from 7.2.3 we get:

7.3.6 *If I is an ideal in a Noetherian local ring R, then $\widehat{R}/I\widehat{R}$ is the completion of R/I.*

Another extremely useful property of completion is that it "transfers singularities" in the following sense:

Corollary 7.3.7. *A Noetherian local ring is regular or Cohen-Macaulay if and only if its completion is.*

Proof. Let $(R,\mathfrak{m})$ be a d-dimensional Noetherian local ring. The completion $\widehat{R}$ of R also has dimension d by Corollary 7.3.5. If R is regular, then $\mathfrak{m}$ is generated by d elements, whence so is $\mathfrak{m}\widehat{R}$, showing that $\widehat{R}$ is regular. Conversely, if $\widehat{R}$ is regular, so that $\mathfrak{m}\widehat{R}$ is generated by a d-tuple $\mathbf{x}$, then by Nakayama's lemma, we may choose these generators already in $\mathfrak{m}$. From $\mathbf{x}\widehat{R} = \mathfrak{m}\widehat{R}$, the cyclic purity of faithfully flat homomorphisms (Proposition 6.3.4) yields $\mathbf{x}R = \mathfrak{m}$, showing that R is regular. If R is Cohen-Macaulay and $\mathbf{x}$ is an R-regular sequence of length d, then $\mathbf{x}$ is also $\widehat{R}$-regular by faithful flatness and Proposition 6.4.1, showing that $\widehat{R}$ is also Cohen-Macaulay. Conversely, assume $\widehat{R}$ is Cohen-Macaulay, and let $\mathbf{x} := (x_1,\dots,x_d)$ be a system of parameters of R. Using Corollary 7.3.5, we get $R/\mathbf{x}R \cong \widehat{R}/\mathbf{x}\widehat{R}$, showing that $\mathbf{x}$ is also a system of parameters in $\widehat{R}$, whence $\widehat{R}$-regular. Since $R/(x_1,\dots,x_e)R \hookrightarrow \widehat{R}/(x_1,\dots,x_e)\widehat{R}$ for all e by faithful flatness and Proposition 6.3.4, it follows easily that $\mathbf{x}$ is also R-regular. □

For those that know inverse limits (also called projective limits), one can give the following alternative construction of the completion:

Proposition 7.3.8. *The completion of a Noetherian local ring $(R,\mathfrak{m})$ is equal to the inverse limit $\varprojlim R/\mathfrak{m}^n$.*

Proof. Here we view the $R_n := R/\mathfrak{m}^n$ as an inverse system via the canonical residue maps $R_m \to R_n$ for all $m \geq n$. A typical element of the inverse limit is represented by a sequence $\mathbf{a}$ in R such that $\mathbf{a}(m) + \mathfrak{m}^m$ is mapped to $\mathbf{a}(n) + \mathfrak{m}^n$ under the residue map $R_m \to R_n$ for all $m \geq n$; two sequences $\mathbf{a}$ and $\mathbf{a}'$ then give rise to the same element in the inverse limit if $\mathbf{a}(m) \equiv \mathbf{a}'(m) \mod \mathfrak{m}^m$ for all m. The first of these conditions simply translates into $\mathbf{a}(m) \equiv \mathbf{a}(n) \mod \mathfrak{m}^n$ for all $m \geq n$, showing that $\mathbf{a}$ is a Cauchy sequence; the second condition says that $\mathbf{a} - \mathbf{a}'$ is a null-sequence. Hence we have a map $\varprojlim R_n \to \mathscr{C}(R)/\mathscr{I}_0 = \widehat{R}$. The reader can check that this gives indeed an isomorphism of rings. □

7.4 Complete Noetherian local rings

Classifying Noetherian local rings is a daunting task, but under the additional completeness assumption, we can say much more, as we will now explore. This will even aid us in the study of non-complete Noetherian local rings by the faithful flatness of completion proven in Theorem 7.3.4.

Cohen's structure theorem. A local ring $(R,\mathfrak{m})$ may or may not contain a field. In the former case, we say that R has *equal characteristic*; the remaining case is refered to as *mixed characteristic*. The name is justified in Exercise 7.5.11: a ring has equal characteristic if and only if has the same characteristic as its residue field. A subfield $\kappa \subseteq R$ which under the canoncial residue map $R \to k := R/\mathfrak{m}$ maps surjectively, whence isomorphically, onto k, is called a *coefficient field*. These might not always exist, but we do have a weaker version:

Lemma 7.4.1. *Let R be an equal characteristic local ring with residue field k. Then there exists a subfield $\kappa \subseteq R$, such that k is algebraic over the image $\pi(\kappa)$ of κ under the residue map $\pi\colon R \to k$.*

Proof. The collection of subfields of R is non-empty by assumption, and is clearly closed under chains. Hence by Zorn's lemma there exists a maximal subfield $\kappa \subseteq R$. Let u be an arbitrary element in $k \setminus \pi(\kappa)$, and choose $a \in R$ with $\pi(a) = u$. In particular, $a \notin \kappa$. Put $S := \kappa[a]$, the κ-subalgebra of R generated by a, and let $\mathfrak{p} := \mathfrak{m} \cap S$. Since $S_{\mathfrak{p}} \subseteq R$, it cannot be a field by maximality of κ, and hence $\mathfrak{p} \neq 0$. Choose a non-zero element $b \in \mathfrak{p}$, and write it as $b = f(a)$ for some $f \in \kappa[\xi]$. If we let $f^{\pi} \in \pi(k)[\xi]$ be the (non-zero) polynomial obtained from f by applying π to its coefficients, then $f^{\pi}(u) = 0$, showing that u is algebraic over $\pi(\kappa)$. $\square$

Theorem 7.4.2 (Equal characteristic). *Let $(R,\mathfrak{m})$ be a local ring of equal characteristic. If R is complete, then it admits a coefficient field κ. If R has moreover finite embedding dimension e, then R is Noetherian, and in fact isomorphic to a homomorphic image of a power series ring in e variables over k.*

Proof. To prove the existence of a coefficient field in positive characteristic, one normally resorts to the theory of etale extensions (as the proof in [54, Theorem 28.3]) or differential bases (as in [22, Theorem 16.14]); an alternative proof is given below in Remark 7.4.3. Here I will only give the proof in equal characteristic zero, that is to say, when the residue field of k has characteristic zero. By (the proof of) Proposition 7.4.1, if $\kappa \subseteq R$ is a maximal subfield, then k is algebraic over $\pi(\kappa)$, where $\pi\colon R \to k$ is the residue map. Towards a contradiction, assume there is some $u \in k \setminus \pi(\kappa)$. Let $f \in \kappa[\xi]$ be such that f^{π} is a minimal polynomial of u. Since we are in characteristic zero, u must be a simple root of f^{π}. Hence by Hensel's Lemma, Theorem 7.2.4, we can find $a \in R$ such that $f(a) = 0$ and $\pi(a) = u$. Since clearly $a \notin \kappa$, the strictly larger field $\kappa(a) \cong \kappa[\xi]/f\kappa[\xi]$ embeds into R, violating the maximality of κ.

To prove the last assertion (in either characteristic), assume the maximal ideal is finitely generated, say, $\mathfrak{m} = (x_1,\dots,x_e)R$. By Exercise 7.5.12, every element of R can be expanded as a power series in $(x_1,\dots,x_e)$ with coefficients in κ. In particular, R is a homomorphic image of the regular local ring $\kappa[[\xi_1,\dots,\xi_e]]$ (for the regularity of this latter ring, see Exercise 5.3.5). $\square$

Remark 7.4.3. Suppose $(R,\mathfrak{m})$ is a complete local ring of equal characteristic p. We want to show that it contains a subfield mapping onto its residue field k. Assume first that R is Artinian, or, more generally, admits a nilpotent maximal ideal. We will induct on the smallest power q of p such that $\mathfrak{m}^q = 0$, where there is nothing to show if $q = 1$. Suppose first $q = p$. Let $\mathbf{F}_p(R)$ denote the subring of all p-th powers in R. I claim that $\mathbf{F}_p(R)$ is a subfield of R. Indeed, let a^p be a non-zero element in $\mathbf{F}_p(R)$, for some $a \in R$. Since the square of any non-unit is zero, a must be a unit in R, with inverse, say, b. Since $a^p b^p = 1$, we conclude that a^p is invertible in $\mathbf{F}_p(R)$. Let κ be a maximal subfield of R containing $\mathbf{F}_p(R)$, and assume towards a contradiction that $\pi(\kappa)$ is a proper subfield of k. Let $S := \kappa + \mathfrak{m}$. It is easy to verify that this is a (proper) local subring of R with residue field κ and maximal ideal $\mathfrak{m}$. Choose some a in R outside S. Hence $c := a^p$ belongs to $\mathbf{F}_p(R) \subseteq \kappa$. Suppose $c = d^p$ for some $d \in \kappa$. Hence $(a-d)^p = 0$, showing that $a - d \in \mathfrak{m}$ whence $a \in S$, contradiction. In conclusion, c is not a p-th power in κ, or put differently, $h(\xi) := \xi^p - c$ is an irreducible polynomial over κ. Hence $\kappa[\xi]/h\kappa[\xi]$ embeds into R by sending ξ to a, contradicting the maximality of κ.

For $q > p$, let $\mathfrak{n} := \mathfrak{m}^{q/p}$ and let $\pi\colon R \to R/\mathfrak{n}$ be the residue homomorphism. By induction, we can find an embedding $\iota\colon k \to R/\mathfrak{n}$. Let $S := \pi^{-1}(\iota(k))$. Clearly $\mathfrak{n} \subseteq S$ and $S/\mathfrak{n} \cong \iota(k)$, showing that $\mathfrak{n}$ is a maximal ideal of S. In fact, $\mathfrak{n}^p = 0$, so that S is local. By induction, k embeds in S, whence also in R, as we wanted to show.

For an arbitrary complete Noetherian local ring $(R,\mathfrak{m})$ of equal characteristic p, its residue field k embeds in each $R_n := R/\mathfrak{m}^n$ by the above argument. Moreover, analyzing the above inductive argument, we see that we can choose these embeddings to be compatible with the residue maps $R_m \to R_n$ for $m \geq n$. Hence we get a homomorphism $k \to \varprojlim R_n$. This gives the required embedding, since $\varprojlim R_n$ is equal to $\widehat{R} = R$ by Proposition 7.3.8.

The analogue in mixed characteristic requires even more work, and so again we only quote the result here (see [54, Theorem 29.4] for a proof).

Theorem 7.4.4 (Mixed characteristic). *Let $(R,\mathfrak{m})$ be a complete local ring of mixed characteristic, with residue field k of characteristic $p > 0$. If R has embedding dimension e, then there exists a complete discrete valuation ring V with with maximal ideal pV and residue field k, and there exists an ideal $I \subseteq V[[\xi]]$ with $\xi = (\xi_1, \dots, \xi_{e-1})$ such that $R \cong V[[\xi]]/I$. In particular, R is Noetherian.*

The complete discrete valuation ring V from the statement is in fact uniquely determined by p and k, and called the *complete p-ring* with residue field k (see [54, Theorem 29.2 and Corollary]).

Immediately some important corollaries follow from these structure theorems.

Theorem 7.4.5. *A complete regular local ring of equal characteristic is isomorphic to a power series ring over a field.*

Proof. Let R be a d-dimensional complete regular local ring with residue field k. By definition, R has embedding dimension d, so that $R \cong k[[\xi]]/I$ by Theorem 7.4.2, with $\xi = (\xi_1, \dots, \xi_d)$ and $I \subseteq k[[\xi]]$. Since $k[[\xi]]$ has dimension d by Corollary 4.3.3, the ideal I must be zero by Corollary 4.3.6. $\square$

There is also a structure theorem for complete regular local rings of mixed characteristic, but it is less straightforward and we will omit it.

Cohen normalization. The next result is the analogue for complete local rings of Noether normalization. Again we will only give the proof in equal characteristic.

Theorem 7.4.6. *If R is a d-dimensional Noetherian local ring of equal characteristic, then there exists a (complete) d-dimensional regular local subring $S \subseteq R$ over which R is finite.*

Proof. Assume R has equal characteristic, and view its residue field k as a coefficient field of R (see Theorem 7.4.2). Let $\mathbf{x} := (x_1, \ldots, x_d)$ be a system of parameters of R. Let $k[[\xi]] \to R$ be the k-algebra homomorphism given by $\xi_i \mapsto x_i$, where $\xi = (\xi_1, \ldots, \xi_d)$, let I be the kernel of this homomorphism, and let S be its image. Hence $S \cong k[[\xi]]/I$. Since $R/\mathbf{x}R$ is Artinian by definition of system of parameters, it is a finite dimensional vector space over $S/\xi S = k$. Since S is also complete, R is a finite S-module by Theorem 7.2.5 (notice that $\mathfrak{I}_R = 0$ by Theorem 2.4.11 so that the Hausdorff condition is satisfied). In particular, by Theorem 4.3.8, both rings have the same dimension d. However, this then forces by Corollaries 4.3.3 and 4.3.6 that $I = 0$, so that S is regular (by Exercise 5.3.5). □

The same result is true in mixed characteristic if we moreover assume that R is a domain, or more generally, if the prime p is a multiplier of R in the sense of page 131; see [54, Theorem 29.4 and Remark] or [74, Theorem 1.1]. Here are some examples were the assertion fails: the Artinian local ring $\mathbb{Z}/4\mathbb{Z}$, which even has non-prime characteristic, or the complete Noetherian local ring $\mathbb{Z}_p[[\xi]]/p\xi\mathbb{Z}_p[[\xi]]$, containing the discrete valuation ring $\mathbb{Z}_p$, the p-adic integers, over which it is not finite (see also Exercise 7.5.16).

Complete scalar extensions. Sometimes it is desirable to have a residue field with some additional properties. We finish with discussing a technique of extending the residue field in equal characteristic (for the mixed characteristic case, we refer to [78]).

Theorem 7.4.7. *Let $(R, \mathfrak{m})$ be a Noetherian local ring of equal characteristic with residue field k. Every extension $k \subseteq K$ of fields can be lifted to a faithfully flat extension $R \to R^{\widehat{}}_K$, inducing the given extension on the residue fields, with $R^{\widehat{}}_K$ a complete local ring with maximal ideal $\mathfrak{m}R^{\widehat{}}_K$ and residue field K. In fact, $R^{\widehat{}}_K$ is a solution to the following universal property: any complete Noetherian local R-algebra T with residue field K has a unique structure of a local $R^{\widehat{}}_K$-algebra. In particular, $R^{\widehat{}}_K$ is uniquely determined by R and K up to isomorphism, and is called the* complete scalar extension *of R along K.*

Proof. By Theorem 7.4.2, the completion $\widehat{R}$ of R is isomorphic to $k[[\xi]]/I$ for some ideal I and some tuple of indeterminates ξ. Put $R^{\widehat{}}_K := K[[\xi]]/IK[[\xi]]$. By Theorem 7.3.4 and base change, S has all the required properties.

To prove the universal property, let T be any complete Noetherian local R-algebra, given by the local homomorphism $R \to T$. By the universal property of completions, we have a unique extension $k[[\xi]]/I \cong \widehat{R} \to T$, and by the universal property of tensor products, this uniquely extends to a homomorphism $R^{\widehat{}}_K = K[[\xi]]/IK[[\xi]] \to T$. □

Note that complete scalar extension is actually a functor, that is to say, any local homomorphism $R \to S$ of Noetherian local rings whose residue fields are subfields of K extends to a local homomorphism $R^{\widehat{}}_K \to S^{\widehat{}}_K$. In particular, complete scalar extension commutes with homomorphic images:

$$(R/I)^{\widehat{}}_K \cong R^{\widehat{}}_K / IR^{\widehat{}}_K, \tag{7.6}$$

for all ideals $I \subseteq R$. By Exercise 7.5.13, the complete scalar extension $R^{\widehat{}}_K$ has the same dimension as R, and one is respectively regular or Cohen-Macaulay if and only if the other is.

7.5 Exercises

Ex 7.5.1

Prove the statements in 7.1.1. Show moreover that the set I_r of all elements of norm at most r, and the set I_r^- of all elements of norm strictly less than r, are ideals, for all $r \in [0,1]$ (called norm-ideals*).*

Ex 7.5.2

Prove that if A is I-adically complete, then I lies in the Jacobson *radical (=intersection of all maximal ideals) of A. Conclude that if A is complete with respect to a maximal ideal, then it is local.*

Ex 7.5.3

Show that the canonical norm on a regular local ring is multiplicative.

Ex 7.5.4

Show that all norm-ideals (see Exercise 7.5.1) in a quasi-normed ring A are open in the norm topology. Show that A is Hausdorff if and only if $||\cdot||$ is a norm.

Ex 7.5.5

Prove the statements in 7.1.3 and 7.1.5. Prove that I is closed in the norm topology if and only if the quasi-norm on A/I is a norm.

Ex 7.5.6

Prove 7.1.6.

Ex 7.5.7

Show that the I-adic quasi-norm $||\cdot||_I$ is indeed a quasi-norm. Show that I and any of its powers define equivalent quasi-norms, in the sense that both norms are mutually bounded. Prove 7.1.7.

Ex 7.5.8

Prove 7.2.1 by finding for each Cauchy sequence an appropriate subsequence satisfying the hypothesis, and a subsequence of this satisfying the conclusion.

***Ex 7.5.9**

Show that the Jacobson radical *(:=intersection of all maximal ideals) in a quasi-complete ring is the ideal of all elements of norm strictly less than one.*

Ex 7.5.10

Formulate, and then prove a generalization of Theorem 7.2.5 which works for any ring which is quasi-complete in its I-adic quasi-norm. In fact, you can even formulate a version for any quasi-complete ring $(A, ||\cdot||)$.

Ex 7.5.11

Show that a local ring R has equal characteristic if and only if it has the same characteristic as its residue field.

Ex 7.5.12

Show that if κ is a coefficient field of a local ring $(R, \mathfrak{m})$ and $\mathfrak{m} = \mathbf{x}R$ is finitely generated, then for every $a \in R$ and each $n \in \mathbb{N}$, we can find a polynomial $f_n \in \kappa[\xi]$ such that $a \equiv f_n(\mathbf{x}) \mod \mathfrak{m}^n$. Deduce from this the assertion about power series expansions in the last paragraph of the proof of Theorem 7.4.2.

Ex 7.5.13

Show using Exercise 6.7.17 that R and its complete scalar extension $\widehat{R_K}$ have the same dimension. Prove that R is regular or Cohen-Macaulay if and only if $\widehat{R_K}$ is.

Additional exercises.

Ex 7.5.14

We can also use the formalism of norms to define ultrarings. Let us call a quasi-norm positive*, if the product of any two elements of norm one has positive norm. Let A_w for $w \in \mathbb{W}$ be rings, with Cartesian product A_∞. Given a positive quasi-norm $||\cdot||$ on A_∞, let I° be the ideal generated by all strong idempotents (see §2.5) of norm strictly less than one. Show that A_∞/I° is an ultraring, by showing that the collection of all subsets having a characteristic function of norm one is an ultrafilter, with respect to which one calculates this ultraproduct. To connect this with the construction given in §2.5, show that any quasi-norm with center a prime ideal is positive.*

Ex 7.5.15

Show the following more general version of Hensel's lemma for a complete local ring R: if $f \in R[\xi]$, $c \in \mathbb{N}$ and $a \in R$ are such that $f(a)$ lies in the ideal $f'(a)^2\mathfrak{m}^c$, then there exists $b \in R$ with $f(b) = 0$ and $b \equiv a \mod \mathfrak{m}^c$.

Ex 7.5.16

Let V be a complete discrete valuation ring with uniformizing parameter π. Show that there can be no regular local subring S inside $R := V[[\xi]]/\pi\xi V[[\xi]]$ over which R is finite.

7.6 Project: Henselizations

There are many ways to construct Henselizations (see for instance [55, 56, 59]), most of which rely on some more sophisticated notions, such as etale extensions, etc. There is, however, also a direct construction, which we will now discuss. Let $(R, \mathfrak{m})$ be a Noetherian local ring. By a *Hensel system* over R of size N, we mean a pair $(\mathscr{H}, \mathbf{u})$ consisting of a system $(\mathscr{H})$ of N polynomial equations $f_1, \dots, f_N \in R[t]$ in the N unknowns $t := (t_1, \dots, t_N)$, and an approximate solution $\mathbf{u}$ modulo $\mathfrak{m}$ in R (meaning that $f_i(\mathbf{u}) \equiv 0 \mod \mathfrak{m}$ for all i), such that associated Jacobian matrix

$$\mathrm{Jac}(\mathscr{H}) := \begin{pmatrix} \partial f_1/\partial t_1 & \partial f_1/\partial t_2 & \dots & \partial f_1/\partial t_N \\ \partial f_2/\partial t_1 & \partial f_2/\partial t_2 & \dots & \partial f_2/\partial t_N \\ \vdots & \vdots & \ddots & \vdots \\ \partial f_N/\partial t_1 & \partial f_N/\partial t_2 & \dots & \partial f_N/\partial t_N \end{pmatrix} \tag{7.7}$$

evaluated at $\mathbf{u}$ is invertible over R (that is to say, its determinant is a unit in R). An N-tuple $\mathbf{x}$ in some local R-algebra S is called a *solution* of the Hensel system $(\mathscr{H}, \mathbf{u})$, if it is a solution of the system $(\mathscr{H})$ and $\mathbf{x} \equiv \mathbf{u} \mod \mathfrak{m}S$. Note that a Hensel system of size $N = 1$ is just a Hensel equation together with a solution in the residue field, as in the statement of Hensel's lemma. In fact, R is Henselian (that is to say, satisfies Hensel's lemma) if and only if any Hensel system over R has a solution in R. The proof of this equivalence is not that easy (one can give for instance a proof using standard etale extensions; see [55] or [22, Exercise 7.26]). However, you can modify the proof of Theorem 7.2.4 to show that complete local rings have this property. In fact, using multivariate Taylor expansion, show the following stronger version (it is instructive to try this first for a single Hensel equation).

7.6.1 *Any Hensel system $(\mathscr{H}, \mathbf{u})$ over R admits a unique solution in the completion $\widehat{R}$.*

We call an element $s \in \widehat{R}$ a *Hensel element* if there exists a Hensel system $(\mathscr{H}, \mathbf{u})$ over R such that s is the first entry of the (unique) solution of this system in $\widehat{R}$. Let $R^{\sim}$ be the subset of $\widehat{R}$ of all Hensel elements. For given Hensel elements s and t, construct from their associated Hensel systems a new Hensel system for $s + t$ (respectively, for st), and use this to prove:

7.6.2 *The collection of all Hensel elements is a local ring $R^{\sim}$ with maximal ideal $\mathfrak{m}R^{\sim}$. Moreover, $R^{\sim}$ is Henselian, with completion equal to $\widehat{R}$.*

It is unfortunately less easy to prove that $R^{\sim}$ is also Noetherian. One way is to first show that $R^{\sim} \to \widehat{R}$ is faithfully flat, and then use this to deduce the Noetherianity of $R^{\sim}$ from that of $\widehat{R}$.

7.6.3 *Show that $R^{\sim}$ satisfies the universal property of Henselization: any Henselian local R-algebra S admits a unique structure of $R^{\sim}$-algebra.*

You could also try to prove:

7.6.4 *A power series over a field k in n indeterminates ξ is a Hensel element over the localization of $k[\xi]$ with respect to the maximal ideal generated by the ξ if and only if it is algebraic over that ring. In other words, $k[\xi]^{\sim} = k[[\xi]]^{alg}$.*