Homological Methods in Commutative Algebra

Olivier Haution

Ludwig-Maximilians-Universität München

Sommersemester 2017

Contents

Chapter 1. Associated primes 3
1. Support of a module 3
2. Associated primes 5
3. Support and associated primes 7

Chapter 2. Krull dimension 9
1. Dimension of a module 9
2. Length of a module 9
3. Principal ideal Theorem 11
4. Flat base change 12

Chapter 3. Systems of parameters 15
1. Alternative definition of the dimension 15
2. Regular local rings 16

Chapter 4. Tor and Ext 19
1. Chain complexes 19
2. Projective Resolutions 20
3. The Tor functor 23
4. Cochain complexes 25
5. The Ext functor 25

Chapter 5. Depth 27
1. M-regular sequences 27
2. Depth 27
3. Depth and base change 30

Chapter 6. Cohen-Macaulay modules 33
1. Cohen-Macaulay modules 33
2. Cohen-Macaulay rings 34
3. Catenary rings 36

Chapter 7. Normal rings 37
1. Reduced rings 37
2. Locally integral rings 37
3. Normal rings 39

Chapter 8. Projective dimension 43
1. Projective dimension over a local ring 43
2. The Auslander-Buchsbaum formula 45

Chapter 9. Regular rings 47
1. Homological dimension 47
2. Regular rings 47

Chapter 10. Factorial rings 51
1. Locally free modules 51
2. The exterior algebra 52
3. Factorial rings 53

Bibliography 57

CHAPTER 1

Associated primes

Basic references are [**Bou98, Bou06, Bou07**], [**Ser00**], and [**Mat89**].

All rings are commutative, with unit, and noetherian. A local ring is always nonzero.

We will use the convention that R will denote a (noetherian, commutative, unital) ring, A a local ring, $\mathfrak{m}$ its maximal ideal, and k its residue field. The letter M will either denote a R-module, or an A-module. A prime will mean a prime ideal of R, or of A. When $\mathfrak{p}$ is a prime, we denote by $\kappa(\mathfrak{p})$ the field $R_\mathfrak{p}/(\mathfrak{p}R_\mathfrak{p})$, or $A_\mathfrak{p}/(\mathfrak{p}A_\mathfrak{p})$.

1. Support of a module

Definition 1.1.1. Let M be an R-module, and $m \in M$. The *annihilator* $\operatorname{Ann}(m)$ is the set of elements $x \in R$ such that $xm = 0$. This is an ideal of R. We write $\operatorname{Ann}(M)$, or $\operatorname{Ann}_R(M)$, for the intersection of the ideals $\operatorname{Ann}(m)$, where $m \in M$.

Definition 1.1.2. The set of prime ideals of R is denoted $\operatorname{Spec}(R)$. The *support* of an R-module M, denoted $\operatorname{Supp}(M)$, or $\operatorname{Supp}_R(M)$, is the subset of of $\operatorname{Spec}(R)$ consisting of those primes $\mathfrak{p}$ such that $M_\mathfrak{p} \neq 0$.

Observe that if $\mathfrak{p} \in \operatorname{Supp}(M)$ and $\mathfrak{q} \in \operatorname{Spec}(R)$ with $\mathfrak{p} \subset \mathfrak{q}$, then $\mathfrak{q} \in \operatorname{Supp}(M)$.

Lemma 1.1.3. *The support of M is the set of primes containing the annihilator of some element of M.*

Proof. Let $\mathfrak{p} \in \operatorname{Spec}(R)$. Then $M_\mathfrak{p} \neq 0$ if and only if there exists $m \in M$ such that $tm \neq 0$ for all $t \notin \mathfrak{p}$, or equivalently $\operatorname{Ann}(m) \subset \mathfrak{p}$. □

Lemma 1.1.4. *Let M be a finitely generated R-module. Then $\operatorname{Supp}(M)$ is the set of primes containing $\operatorname{Ann}(M)$.*

Proof. Since for any $m \in M$, we have $\operatorname{Ann}(M) \subset \operatorname{Ann}(m)$, it follows from Lemma 1.1.3 that any element of $\operatorname{Supp}(M)$ contains $\operatorname{Ann}(M)$ (we did not use the assumption that M is finitely generated).

Conversely assume that M is finitely generated, and let $\mathfrak{p}$ be a prime containing $\operatorname{Ann}(M)$. We claim that there is $m \in M$ such that $\operatorname{Ann}(m) \subset \mathfrak{p}$; by Lemma 1.1.3 this will show that $\mathfrak{p} \in \operatorname{Supp}(M)$. Assuming the contrary, let $m_1, \cdots, m_n$ be a finite generating family for M. We can find $s_i \in \operatorname{Ann}(m_i)$ such that $s_i \notin \mathfrak{p}$, for $i = 1, \cdots, n$. Then the product $s_1 \cdots s_n$ belongs to $\operatorname{Ann}(M)$, hence to $\mathfrak{p}$. Since $\mathfrak{p}$ is prime, it follows that $s_j \in \mathfrak{p}$ for some j, a contradiction. □

Lemma 1.1.5. *Consider an exact sequence of R-modules:*

$$0 \to M' \to M \to M'' \to 0.$$

Then $\operatorname{Supp}(M) = \operatorname{Supp}(M') \cup \operatorname{Supp}(M'')$.

PROOF. For every prime $\mathfrak{p}$, we have an exact sequence

$$0 \to M'_{\mathfrak{p}} \to M_{\mathfrak{p}} \to M''_{\mathfrak{p}} \to 0,$$

and therefore $M_{\mathfrak{p}} = 0$ if and only if $M'_{\mathfrak{p}} = 0$ and $M''_{\mathfrak{p}} = 0$. $\square$

LEMMA 1.1.6 (Nakayama's Lemma). *Let $(A, \mathfrak{m})$ be a local ring, and M a finitely generated A-module. If $\mathfrak{m}M = M$ then $M = 0$.*

PROOF. Assume that $M \neq 0$. Let M' be a maximal proper (i.e. $\neq M$) submodule of M, and $M'' = M/M'$ (if no proper submodule were maximal, then we could build an infinite ascending chain of submodules in M, a contradiction since A is noetherian and M finitely generated). Then by maximality of M, the module M'' is simple, i.e. has exactly two submodules (0 and M''). But a simple module is isomorphic to $A/\mathfrak{m}$ (it is generated by a single element, hence is of the type A/I for an ideal I; but A/I is simple if and only if $I = \mathfrak{m}$). Therefore $\mathfrak{m}M'' = 0$, hence $\mathfrak{m}M \subset M'$. This is a contradiction with $\mathfrak{m}M = M$. $\square$

DEFINITION 1.1.7. If $(A, \mathfrak{m})$ and $(B, \mathfrak{n})$ are two local rings, a ring morphism $\phi\colon A \to B$ is called a *local morphism* if $\phi(\mathfrak{m}) \subset \mathfrak{n}$.

LEMMA 1.1.8. *Let $A \to B$ be a local morphism of local rings, and M a finitely generated A-module. If $M \otimes_A B = 0$, then $M = 0$.*

PROOF. Assume that $M \neq 0$ and let k be the residue field of A. By Nakayama's Lemma 1.1.6, the k-vector space $M \otimes_A k$ is nonzero hence admits a one-dimensional quotient. This gives a surjective morphism of A-modules $M \to k$. Then $k \otimes_A B$ vanishes, being a quotient of $M \otimes_A B$. But since $A \to B$ is local, the residue field of B is a quotient of $k \otimes_A B$, a contradiction. $\square$

PROPOSITION 1.1.9. *Let $\varphi\colon R \to S$ be a ring morphism, and M a finitely generated R-module. Then*

$$\operatorname{Supp}_S(M \otimes_R S) = \{\mathfrak{q} \in \operatorname{Spec}(S) \mid \varphi^{-1}\mathfrak{q} \in \operatorname{Supp}_R(M)\}.$$

PROOF. Let $\mathfrak{q} \in \operatorname{Spec}(S)$ and $\mathfrak{p} = \varphi^{-1}\mathfrak{q}$. Then the morphism $R_{\mathfrak{p}} \to S_{\mathfrak{q}}$ is local. We have an isomorphism of $S_{\mathfrak{q}}$-modules $(M \otimes_R S)_{\mathfrak{q}} \simeq M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} S_{\mathfrak{q}}$, and the result follows from Lemma 1.1.8. $\square$

COROLLARY 1.1.10. *Let M be a finitely generated R-module, and I an ideal of R. Then*

$$\operatorname{Supp}_R(M/IM) = \{\mathfrak{p} \in \operatorname{Supp}(M) \mid I \subset \mathfrak{p}\}.$$

PROOF. Let $\varphi\colon R \to R/I$ be the quotient morphism. Any prime $\mathfrak{p}$ containing I may be written as $\varphi^{-1}\mathfrak{q}$ for some $\mathfrak{q} \in \operatorname{Spec}(R/I)$. If in addition $\mathfrak{p} \in \operatorname{Supp}(M)$, then by Proposition 1.1.9 we have $\mathfrak{q} \in \operatorname{Supp}_{R/I}(M/IM)$. By Lemma 1.1.3 there is $m \in M/IM$ such that $\operatorname{Ann}_{R/I}(m) \subset \mathfrak{q}$, hence $\operatorname{Ann}_R(m) = \varphi^{-1} \operatorname{Ann}_{R/I}(m) \subset \varphi^{-1}\mathfrak{q} = \mathfrak{p}$, proving that $\mathfrak{p} \in \operatorname{Supp}_R(M/IM)$. This proves one inclusion. The other inclusion is clear. $\square$

2. Associated primes

DEFINITION 1.2.1. A prime $\mathfrak{p}$ of R is an *associated prime of* M if there is $m \in M$ such that $\mathfrak{p} = \mathrm{Ann}(m)$. The set of associated primes is written $\mathrm{Ass}(M)$, or $\mathrm{Ass}_R(M)$.

In other words we have $\mathfrak{p} \in \mathrm{Ass}(M)$ if and only if there is an injective R-module morphism $R/\mathfrak{p} \to M$.

PROPOSITION 1.2.2. *Any maximal element of the set* $\{\mathrm{Ann}(m)|m \in M, m \neq 0\}$, *ordered by inclusion, is prime.*

PROOF. Let $I = \mathrm{Ann}(m)$ be such a maximal element. Let $x, y \in R$, and assume that $xy \in I$. If $y \notin I$, then $ym \neq 0$. Then $I = \mathrm{Ann}(m) \subset \mathrm{Ann}(ym)$. By maximality $I = \mathrm{Ann}(ym)$. Since $xym = 0$, we have $x \in \mathrm{Ann}(ym)$, hence $x \in I$. □

COROLLARY 1.2.3. *We have* $M \neq 0$ *if and only if* $\mathrm{Ass}(M) \neq \varnothing$.

PROOF. Since R is noetherian, the set of Proposition 1.2.2 admits a maximal element as soon as it is not empty. □

LEMMA 1.2.4. *Let* $\mathfrak{p}$ *be a prime in* R. *Then* $\mathrm{Ass}_R(R/\mathfrak{p}) = \{\mathfrak{p}\}$.

PROOF. Let $m \in R/\mathfrak{p}$ be a nonzero element. Then $\mathfrak{p} \subset \mathrm{Ann}_R(m)$. Conversely, let $x \in \mathrm{Ann}_R(m)$. If $r \in R - \mathfrak{p}$ is the preimage of $m \in R/\mathfrak{p}$, we have $xr \in \mathfrak{p}$, and since $\mathfrak{p}$ is prime, it follows that $x \in \mathfrak{p}$. Thus $\mathfrak{p} = \mathrm{Ann}_R(m)$. □

PROPOSITION 1.2.5. *Consider an exact sequence of* R*-modules:*

$$0 \to M' \to M \to M'' \to 0.$$

Then $\mathrm{Ass}(M') \subset \mathrm{Ass}(M) \subset \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$.

PROOF. If $\mathfrak{p} \in \mathrm{Ass}(M')$, then M' contains a module isomorphic to $R/\mathfrak{p}$. Since $M' \subset M$, it follows that M also contains such a module, hence $\mathfrak{p} \in \mathrm{Ass}(M)$.

Now let $\mathfrak{p} \in \mathrm{Ass}(M)$. Then M contains a submodule E isomorphic to $R/\mathfrak{p}$. By Lemma 1.2.4 we have $\mathrm{Ass}(E) = \{\mathfrak{p}\}$. Let $F = M' \cap E$. The inclusion proved above implies that

$$\mathrm{Ass}(F) \subset \mathrm{Ass}(E) = \{\mathfrak{p}\} \quad \text{and} \quad \mathrm{Ass}(F) \subset \mathrm{Ass}(M').$$

If $F \neq 0$, we have $\mathrm{Ass}(F) \neq \varnothing$ by Corollary 1.2.3, so that $\mathrm{Ass}(F) = \{\mathfrak{p}\}$, and therefore $\mathfrak{p} \in \mathrm{Ass}(M')$. If $F = 0$, then the morphism $E \to M''$ is injective, so that $\{\mathfrak{p}\} = \mathrm{Ass}(E) \subset \mathrm{Ass}(M'')$. □

LEMMA 1.2.6. *Let* M_α *be a family of submodules of* M *such that* $M = \cup_\alpha M_\alpha$. *Then*

$$\mathrm{Ass}(M) = \bigcup_\alpha \mathrm{Ass}(M_\alpha).$$

PROOF. Since $M_\alpha \subset M$, we have $\mathrm{Ass}(M_\alpha) \subset \mathrm{Ass}(M)$. Conversely if $\mathfrak{p} = \mathrm{Ann}(m) \in \mathrm{Ass}(M)$, then there is α such that $m \in M_\alpha$. Then $\mathfrak{p} \in \mathrm{Ass}(M_\alpha)$. □

PROPOSITION 1.2.7. *Let* $\Phi \subset \mathrm{Ass}(M)$. *Then there is a submodule* N *of* M *such that* $\mathrm{Ass}(N) = \Phi$ *and* $\mathrm{Ass}(M/N) = \mathrm{Ass}(M) - \Phi$.

Proof. Consider the set Σ of submodules P of M such that $\operatorname{Ass}(P) \subset \Phi$. This set is non-empty since $0 \in \Sigma$, and ordered by inclusion. Moreover Σ is stable under taking reunions of totally ordered subsets by Lemma 1.2.6. By Zorn's lemma, we can find a maximal element $N \in \Sigma$ (when M is finitely generated over the noetherian ring R, we do not need Zorn's lemma). Let $\mathfrak{p} \in \operatorname{Ass}(M/N)$. Then M/N contains a submodule isomorphic to $R/\mathfrak{p}$, of the form N'/N with $N \subsetneq N' \subset M$. By Proposition 1.2.5 and Lemma 1.2.4, we have

$$\operatorname{Ass}(N') \subset \operatorname{Ass}(N) \cup \operatorname{Ass}(N'/N) \subset \Phi \cup \{\mathfrak{p}\}.$$

By maximality of N, we have $\operatorname{Ass}(N') \not\subset \Phi$. It follows that $\mathfrak{p} \notin \Phi$ and $\mathfrak{p} \in \operatorname{Ass}(N')$. Since N' is a submodule of M, we have $\operatorname{Ass}(N') \subset \operatorname{Ass}(M)$, and therefore $\mathfrak{p} \in \operatorname{Ass}(M) - \Phi$. Thus we have inclusions

$$\operatorname{Ass}(M/N) \subset \operatorname{Ass}(M) - \Phi \quad \text{and} \quad \operatorname{Ass}(N) \subset \Phi.$$

Since $\operatorname{Ass}(M) \subset \operatorname{Ass}(N) \cup \operatorname{Ass}(M/N)$ by Proposition 1.2.5, the above inclusions are in fact equalities. $\square$

Definition 1.2.8. An element of R is called a *zerodivisor in M* if it annihilates a nonzero element of M, a *nonzerodivisor* otherwise.

Any element of an associated prime of M is a zerodivisor in M. The converse is true:

Lemma 1.2.9. *The set of zerodivisors in M is the union of the associated primes of M.*

Proof. Assume that $r \in \operatorname{Ann}(x)$ with $x \in M - 0$. Then $\operatorname{Ann}(x)$ is contained in a maximal element of the set $\{\operatorname{Ann}(m) | m \in M, m \neq 0\}$ (otherwise we could construct an ascending chain of ideals in the noetherian ring R). Proposition 1.2.2 says that this maximal element is an associated prime of M. $\square$

Recall that when S is a multiplicatively closed subset of R, the map $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ induces a bijection

$$\{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \cap S = \varnothing\} \xrightarrow{\sim} \operatorname{Spec}(S^{-1}R).$$

Proposition 1.2.10. *Let S be a multiplicatively closed subset of R. Then*

$$\operatorname{Ass}_{S^{-1}R}(S^{-1}M) = \{S^{-1}\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Ass}_R(M) \text{ and } \mathfrak{p} \cap S = \varnothing\}.$$

Proof. If M contains an R-submodule isomorphic to $R/\mathfrak{p}$, then (by exactness of the localisation) $S^{-1}M$ contains an $(S^{-1}R)$-submodule isomorphic to $S^{-1}(R/\mathfrak{p})$. The latter is isomorphic to $(S^{-1}R)/(S^{-1}\mathfrak{p})$.

Conversely, as recalled above any element of $\operatorname{Ass}_{S^{-1}R}(S^{-1}M)$ is of the form $S^{-1}\mathfrak{p}$ for a unique $\mathfrak{p} \in \operatorname{Spec}(R)$ satisfying $S \cap \mathfrak{p} = \varnothing$. We need to prove that $\mathfrak{p} \in \operatorname{Ass}_R(M)$. Let $m \in M$ and $s \in S$ be such that $S^{-1}\mathfrak{p} = \operatorname{Ann}_{S^{-1}R}(m/s)$. Let $p_1, \cdots, p_n$ be a set of generators of the R-module $\mathfrak{p}$. For every $i = 1, \cdots, n$, we have $p_i m/s = 0$ in $S^{-1}M$, which means that we can find $t_i \in S$ such that $t_i p_i m = 0$ in M. Let $m' = t_1 \cdots t_n m \in M$. Since each p_i belongs to $\operatorname{Ann}_R(m')$, it follows that $\mathfrak{p} \subset \operatorname{Ann}_R(m')$. Conversely if $x \in \operatorname{Ann}_R(m')$, then $xt_1 \cdots t_n/1 \in \operatorname{Ann}_{S^{-1}R}(m/s) = S^{-1}\mathfrak{p}$. Thus $uxt_1 \cdots t_n \in \mathfrak{p}$ for some $u \in S$. Since $ut_1 \cdots t_n \in S$ and $S \cap \mathfrak{p} = \varnothing$, it follows from the primality of $\mathfrak{p}$ that $x \in \mathfrak{p}$. Therefore $\operatorname{Ann}_R(m') = \mathfrak{p}$, and $\mathfrak{p} \in \operatorname{Ass}_R(M)$. $\square$

3. Support and associated primes

PROPOSITION 1.3.1. *The set* $\mathrm{Supp}(M)$ *is the set of primes of* R *containing an element of* $\mathrm{Ass}(M)$.

PROOF. If $\mathfrak{p}$ contains an associated prime $\mathrm{Ann}(m)$ for some $m \in M$, then $\mathfrak{p} \in \mathrm{Supp}(M)$ by Lemma 1.1.3.

Let now $\mathfrak{p} \in \mathrm{Supp}(M)$. Then $M_{\mathfrak{p}} \neq 0$, hence by Corollary 1.2.3 we can find a prime in $\mathrm{Ass}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}})$, which corresponds by Proposition 1.2.10 to a prime $\mathfrak{q} \in \mathrm{Ass}_R(M)$ such that $\mathfrak{q} \subset \mathfrak{p}$. □

COROLLARY 1.3.2. *We have* $\mathrm{Ass}(M) \subset \mathrm{Supp}(M)$*, and these sets have the same minimal elements.*

COROLLARY 1.3.3. *Minimal elements of* $\mathrm{Supp}(M)$ *consist of zerodivisors in* M.

PROOF. Combine Proposition 1.3.1 with Lemma 1.2.9. □

DEFINITION 1.3.4. The non-minimal elements of $\mathrm{Ass}(M)$ are called *embedded primes of* M.

PROPOSITION 1.3.5. *Assume that* M *is finitely generated. Then there is a chain of submodules*

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$$

such that $M_i/M_{i-1} \simeq R/\mathfrak{p}_i$ *with* $\mathfrak{p}_i \in \mathrm{Spec}(R)$ *for* $i = 1, \cdots, n$. *We have*

$$\mathrm{Ass}(M) \subset \{\mathfrak{p}_1, \cdots, \mathfrak{p}_n\} \subset \mathrm{Supp}(M),$$

and these sets have the same minimal elements.

PROOF. Assume that we have constructed a chain

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_j \subset M$$

such that $M_i/M_{i-1} \simeq R/\mathfrak{p}_i$ with $\mathfrak{p}_i$ prime, for $i = 1, \cdots, j$. If $M_j = M$, then the first part of the statement is proved. Otherwise, by Corollary 1.2.3 we can find $\mathfrak{p}_{j+1} \in \mathrm{Ass}(M/M_j)$. Thus M/M_j contains a submodule isomorphic to $R/\mathfrak{p}_{j+1}$, which is necessarily of the form M_{j+1}/M_j with $M_j \subsetneq M_{j+1} \subset M$. This process must stop, since R is noetherian and M finitely generated. This proves the first part.

By Proposition 1.2.5, we have $\mathrm{Ass}(M_i) \subset \mathrm{Ass}(M_{i-1}) \cup \mathrm{Ass}(R/\mathfrak{p}_i)$. We obtain that $\mathrm{Ass}(M) \subset \{\mathfrak{p}_1, \cdots, \mathfrak{p}_n\}$ using Lemma 1.2.4 and induction on i.

By Lemma 1.1.5, we have $\mathrm{Supp}(R/\mathfrak{p}_i) \cup \mathrm{Supp}(M_{i-1}) \subset \mathrm{Supp}(M_i)$. In particular $\mathfrak{p}_i \in \mathrm{Supp}(R/\mathfrak{p}_i) \subset \mathrm{Supp}(M_i)$. Since $M_i \subset M$, we have $\mathrm{Supp}(M_i) \subset \mathrm{Supp}(M)$. This proves that $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_n\} \subset \mathrm{Supp}(M)$.

The last statement follows from Proposition 1.3.1. □

COROLLARY 1.3.6. *Assume that* M *is finitely generated. Then:*

(i) The set $\mathrm{Ass}(M)$ *is finite.*
(ii) The set of minimal elements of $\mathrm{Supp}(M)$ *is finite.*

COROLLARY 1.3.7. *Assume that* M *is finitely generated and nonzero. Then* $\mathrm{Supp}(M)$ *possesses at least one minimal element.*

REMARK 1.3.8. Corollary 1.3.7 may also be proved directly using Zorn's Lemma.

CHAPTER 2

Krull dimension

1. Dimension of a module

DEFINITION 2.1.1. The length of a chain of primes $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ in R is the integer n. The *dimension* of a finitely generated R-module M is the supremum of the lengths of the chains of primes in $\operatorname{Supp}(M)$. It is denoted $\dim M$, or $\dim_R M$. The *height* of a prime $\mathfrak{p}$ of R is the supremum of the lengths n of chains $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}$ of primes in R. In other words:

$$\operatorname{height} \mathfrak{p} = \dim R_{\mathfrak{p}}.$$

The dimension of the zero module is $-\infty$. By Lemma 1.1.4, we have $\dim M = \dim R/\operatorname{Ann}(M)$.

REMARK 2.1.2. Note that $\dim R/\mathfrak{p} + \dim R_{\mathfrak{p}}$ is the supremum of the lengths of chains of primes of R with $\mathfrak{p}$ appearing in the chain, so that

$$\dim R/\mathfrak{p} + \dim R_{\mathfrak{p}} \leq \dim R.$$

Later we will provide conditions on R ensuring that it is an equality.

PROPOSITION 2.1.3. *Let $R \to S$ be a ring homomorphism. Let M be an S-module, finitely generated as an R-module. Then*

$$\dim_R M = \dim_S M.$$

PROOF. Let $m_1, \cdots, m_n$ be generators of the S-module M. The morphism of S-modules $S \to M^n$ sending s to $(sm_1, \cdots, sm_n)$ has kernel $\operatorname{Ann}_S(M)$. This makes $S/\operatorname{Ann}_S(M)$ an S-submodule of M^n, which is therefore finitely generated as an R-module (R is noetherian). The ring morphism $R/\operatorname{Ann}_R(M) \to S/\operatorname{Ann}_S(M)$ is injective, and, as we have just seen, integral. In this situation chains of primes are in bijective correspondence (see e.g. [**AM69**, Corollary 5.9 and Theorem 5.10]). □

PROPOSITION 2.1.4. *Let M be a finitely generated R-module. Then*

$$\dim M = \max_{\mathfrak{p} \in \operatorname{Ass}(M)} \dim R/\mathfrak{p} = \max_{\mathfrak{p} \in \operatorname{Supp}(M)} \dim R/\mathfrak{p}.$$

PROOF. This follows from Lemma 1.1.4 and Proposition 1.3.1. □

2. Length of a module

DEFINITION 2.2.1. The length of a chain of submodules $0 = M_0 \subsetneq \cdots \subsetneq M_n = M$ is the integer n. The chain is called *maximal* if for each i there is no submodule N satisfying $M_i \subsetneq N \subsetneq M_{i+1}$. The *length* of an R-module M is the supremum of the lengths of the chains of submodules of M. It is denoted $\operatorname{length} M$.

The zero module is the only module of length zero.

Lemma 2.2.2. *Consider an exact sequence of R-modules*

$$0 \to M' \to M \to M'' \to 0.$$

Then we have $\operatorname{length} M = \operatorname{length} M' + \operatorname{length} M''$.

Proof. If $\operatorname{length} M' = \infty$ or $\operatorname{length} M'' = \infty$, then $\operatorname{length} M = \infty$. Assume that $\operatorname{length} M' = e < \infty$ and $\operatorname{length} M = \infty$. Let n be an integer. We may find a chain $M_0 \subsetneq \cdots \subsetneq M_{n+e}$ in M. Let $M_i' = M_i \cap M'$ and $M_i'' = M_i/M_i'$. There are at least n indices i such that $M_i' = M_{i+1}'$, and for such i we have $M_i'' \subsetneq M_{i+1}''$. Thus from the family M_i'' we may extract a chain of length n of submodules of M''. This proves that $\operatorname{length} M'' \geq n$. Since n was arbitrary, we deduce that $\operatorname{length} M'' = \infty$.

So we may assume that all modules have finite length. The statement is true if $\operatorname{length} M' = \operatorname{length} M$ or if $\operatorname{length} M'' = \operatorname{length} M$, for then $M = M'$ or $M = M''$. Thus we may assume that $\operatorname{length} M' < \operatorname{length} M$ and $\operatorname{length} M'' < \operatorname{length} M$, and proceed by induction on $\operatorname{length} M$. Let $0 = M_0 \subsetneq \cdots \subsetneq M_r = M$ be a chain of maximal length, so that $r = \operatorname{length} M$. Let $N = M_{r-1}$. Then $\operatorname{length} N = \operatorname{length} M - 1$, and $\operatorname{length} M/N = 1$. Form the commutative diagram with exact rows and columns

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & N' \arrow[r] \arrow[d] & N \arrow[r] \arrow[d] & N'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M' \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & M'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & P' \arrow[r] \arrow[d] & P \arrow[r] \arrow[d] & P'' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Then $\operatorname{length} P = 1$, hence either $P' = 0$ or $P' = P$. In any case, we have

$$\operatorname{length} P' + \operatorname{length} P'' = 1.$$

Then, using induction

$$\begin{aligned}
\operatorname{length} M &= \operatorname{length} N + 1 \\
&= \operatorname{length} N' + \operatorname{length} N'' + \operatorname{length} P' + \operatorname{length} P'' \\
&= \operatorname{length} M' + \operatorname{length} M''.
\end{aligned}$$

□

Proposition 2.2.3. *The length of any maximal chain of submodules of M is equal to the length of M.*

Proof. If M contains an infinite chain, then $\operatorname{length} M = \infty$. Let $0 = M_0 \subsetneq \cdots \subsetneq M_r = M$ be a maximal chain. We prove that $r = \operatorname{length} M$ by induction on r. If $r = 0$, then $M = 0$, hence $\operatorname{length} M = 0$. Assume that $r > 0$, and let $N = M_{r-1}$. We have $\operatorname{length} M/N = 1$ by maximality of the chain. In addition, the chain $0 = M_0 \subsetneq \cdots \subsetneq$

$M_{r-1} = N$ is maximal in N, so that $\operatorname{length} N = r-1$ by induction. Therefore, by Lemma 2.2.2

$$\operatorname{length} M = \operatorname{length} N + \operatorname{length} M/N = r - 1 + 1 = r. \qquad \square$$

Lemma 2.2.4. *Let R be an integral domain. Then R has finite length as an R-module if and only if it is a field.*

Proof. If R is a field, it has exactly two ideals (0 and R), and thus has length 1.

Now assume that R has finite length, and let $x \in R - \{0\}$. The sequence of ideals $\cdots \subset x^{i+1}R \subset x^i R \subset \cdots \subset R$ must stabilise, hence $x^n = ax^{n+1}$ for some $n \in \mathbb{N}$ and some $a \in R$. Thus $x^n(1 - ax) = 0$. If R is an integral domain then $ax = 1$, showing that x is invertible in R. $\square$

Lemma 2.2.5. *Assume that M is finitely generated. Then* $\dim M = 0$ *if and only if M is nonzero and has finite length.*

Proof. We may assume that $M \neq 0$. Let us choose $M_i, \mathfrak{p}_i$ as in Proposition 1.3.5. Then by induction M has finite length if and only if each $R/\mathfrak{p}_i$ has finite length. This is so if and only if each $\mathfrak{p}_i$ is a maximal ideal of R by Lemma 2.2.4. Since $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_n\}$ and $\operatorname{Supp}(M)$ have the same minimal elements, each $\mathfrak{p}_i$ is maximal if and only if $\operatorname{Supp}(M)$ consists of maximal ideals of R, or equivalently $\dim M = 0$. $\square$

3. Principal ideal Theorem

Definition 2.3.1. When S is a subset of R, and $\mathfrak{p} \in \operatorname{Spec}(R)$, we say that $\mathfrak{p}$ is *minimal over S* if it is a minimal element of the set of primes containing S.

Theorem 2.3.2 (Krull). *Assume that R is an integral domain. Let $x \in R - \{0\}$, and $\mathfrak{p}$ be a prime minimal over $\{x\}$. Then* $\operatorname{height} \mathfrak{p} = 1$.

Proof. The ring $R_{\mathfrak{p}}$ is an integral domain, and the image of x in $R_{\mathfrak{p}}$ is nonzero. Thus we may replace R with $R_{\mathfrak{p}}$, and assume that R is local with maximal ideal $\mathfrak{p}$. Let $\mathfrak{q}$ be a prime such that $\mathfrak{q} \subsetneq \mathfrak{p}$. It will suffice to prove that $\mathfrak{q} = 0$. We view R as a subring of $R_{\mathfrak{q}}$. For each integer $n \geq 0$, we consider the ideal of R defined as

$$\mathfrak{q}_n = (\mathfrak{q}^n R_{\mathfrak{q}}) \cap R = \{u \in R \mid su \in \mathfrak{q}^n \text{ for some } s \in R - \mathfrak{q}\},$$

(and called the n-th symbolic power of the ideal $\mathfrak{q}$). The ring R/xR has dimension zero by minimality of $\mathfrak{p}$, hence finite length by Lemma 2.2.5. It follows that the chain of ideals $\cdots \subset \mathfrak{q}_{n+1}/(\mathfrak{q}_{n+1} \cap xR) \subset \mathfrak{q}_n/(\mathfrak{q}_n \cap xR) \subset \cdots$ of R/xR must stabilise. Therefore we can find an integer n such that $\mathfrak{q}_n \subset \mathfrak{q}_{n+1} + xR$. Thus for any $y \in \mathfrak{q}_n$, we may find $a \in R$ such that $y - ax \in \mathfrak{q}_{n+1}$. Note that $x \notin \mathfrak{q}$ by minimality of $\mathfrak{p}$, hence x becomes invertible in $R_{\mathfrak{q}}$. But $ax \in \mathfrak{q}_n \subset \mathfrak{q}^n R_{\mathfrak{q}}$, and therefore $a = axx^{-1} \in \mathfrak{q}^n R_{\mathfrak{q}}$. Since $a \in R$, it follows that $a \in \mathfrak{q}_n$. We have proved that

$$\mathfrak{q}_n = \mathfrak{q}_{n+1} + x\mathfrak{q}_n.$$

Consider the finitely generated R-module $N = \mathfrak{q}_n/\mathfrak{q}_{n+1}$. We have $xN = N$ with x in the maximal ideal $\mathfrak{p}$ of R. Applying Nakayama's Lemma 1.1.6 we obtain that $N = 0$, or equivalently $\mathfrak{q}_n = \mathfrak{q}_{n+1}$. Observe that $\mathfrak{q}_m R_{\mathfrak{q}} = \mathfrak{q}^m R_{\mathfrak{q}} = (\mathfrak{q}R_{\mathfrak{q}})^m$ for any m. Thus $(\mathfrak{q}R_{\mathfrak{q}})^n = (\mathfrak{q}R_{\mathfrak{q}})^{n+1}$. We now apply Nakayama's Lemma 1.1.6 to the finitely generated $R_{\mathfrak{q}}$-module $(\mathfrak{q}R_{\mathfrak{q}})^n$ and conclude that $(\mathfrak{q}R_{\mathfrak{q}})^n = 0$. This shows that any element of the maximal ideal $\mathfrak{q}R_{\mathfrak{q}}$ of $R_{\mathfrak{q}}$ is nilpotent; but $R_{\mathfrak{q}}$ is a domain, so that $\mathfrak{q}R_{\mathfrak{q}} = 0$, and finally $\mathfrak{q} = 0$. $\square$

Lemma 2.3.3. *Let* $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ *be a chain of primes, and let* $x \in \mathfrak{p}_n$*. Then we can find a chain of primes* $\mathfrak{p}'_0 \subsetneq \cdots \subsetneq \mathfrak{p}'_n$ *with* $\mathfrak{p}_0 = \mathfrak{p}'_0$*,* $\mathfrak{p}_n = \mathfrak{p}'_n$*, and* $x \in \mathfrak{p}'_1$*.*

Proof. We proceed by induction on n, and we may assume that $n \geq 2$. It will suffice to find a prime $\mathfrak{p}'_{n-1}$ containing x and such that $\mathfrak{p}_{n-2} \subsetneq \mathfrak{p}'_{n-1} \subsetneq \mathfrak{p}_n$ (then we find by induction a chain of primes $\mathfrak{p}'_0 \subsetneq \cdots \subsetneq \mathfrak{p}'_{n-2}$ such that $\mathfrak{p}_0 = \mathfrak{p}'_0$, $\mathfrak{p}'_{n-2} \subsetneq \mathfrak{p}'_{n-1}$, and $x \in \mathfrak{p}'_1$). If $x \in \mathfrak{p}_{n-1}$, we may take $\mathfrak{p}'_{n+1} = \mathfrak{p}_{n+1}$. Thus we assume that $x \notin \mathfrak{p}_{n-1}$. Then we can find a prime $\mathfrak{p}'_{n-1}$ containing $\{x\} \cup \mathfrak{p}_{n-2}$, contained in $\mathfrak{p}_n$, and minimal for these properties (it corresponds to a minimal element of the support of the $R_{\mathfrak{p}_n}$-module $R_{\mathfrak{p}_n}/(\mathfrak{p}_{n-2}R_{\mathfrak{p}_n} + xR_{\mathfrak{p}_n})$, which exists by Corollary 1.3.7 since $\mathfrak{p}_{n-2}R_{\mathfrak{p}_n} + xR_{\mathfrak{p}_n} \subset \mathfrak{p}_n R_{\mathfrak{p}_n} \neq R_{\mathfrak{p}_n}$). Then the prime ideal $\mathfrak{p}'_{n-1}/\mathfrak{p}_{n-2}$ of $R/\mathfrak{p}_{n-2}$ is minimal over the image of x in $R/\mathfrak{p}_{n-2}$, and therefore has height 1 by Theorem 2.3.2. Since the prime ideal $\mathfrak{p}_n/\mathfrak{p}_{n-2}$ of $R/\mathfrak{p}_{n-2}$ has height ≥ 2, it cannot be equal to $\mathfrak{p}'_{n-1}/\mathfrak{p}_{n-2}$. Thus we have $\mathfrak{p}_{n-2} \subsetneq \mathfrak{p}'_{n-1} \subsetneq \mathfrak{p}_n$, with $x \in \mathfrak{p}'_{n-1}$, as required. □

Proposition 2.3.4. *Let* $(A, \mathfrak{m})$ *be a local ring,* $x \in \mathfrak{m}$*, and* M *a finitely generated* A*-module. Then*

$$\dim M/xM \geq \dim M - 1,$$

with equality if and only x *belongs to no prime* $\mathfrak{p} \in \operatorname{Supp}(M)$ *such that* $\dim A/\mathfrak{p} = \dim M$*.*

Proof. Let $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ be a chain of primes in $\operatorname{Supp}(M)$. Replacing $\mathfrak{p}_n$ with $\mathfrak{m}$, we may assume that $\mathfrak{p}_n = \mathfrak{m}$. By Lemma 2.3.3 we can assume that $x \in \mathfrak{p}_1$. This gives a chain of primes $\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ of length $n-1$ in $\operatorname{Supp}(M) \cap \operatorname{Supp}(A/xA) = \operatorname{Supp}(M/xM)$ (the last equality follows from Corollary 1.1.10), which proves that $\dim M/xM \geq n-1$.

Now a prime $\mathfrak{p} \in \operatorname{Supp}(M)$ contains x if and only if $\mathfrak{p} \in \operatorname{Supp}(M/xM)$ by Corollary 1.1.10. Thus the second statement follows from Proposition 2.1.4 applied to the module M/xM. □

Corollary 2.3.5. *Let* $(A, \mathfrak{m})$ *be a local ring and* M *a finitely generated* A*-module. Let* $x \in \mathfrak{m}$ *be a nonzerodivisor in* M*. Then* $\dim M/xM = \dim M - 1$*.*

Proof. This follows from Corollary 1.3.3 and Proposition 2.3.4. □

4. Flat base change

Definition 2.4.1. An R-module M is called *flat* if for every exact sequence of R-modules $N_1 \to N_2 \to N_3$ the induced sequence $M \otimes_R N_1 \to M \otimes_R N_2 \to M \otimes_R N_3$ is exact. We say that a ring morphism $R \to S$ is flat if S is flat as an R-module.

Lemma 2.4.2. *Let* $\varphi \colon (A, \mathfrak{m}) \to (B, \mathfrak{n})$ *be a flat local morphism. Then*

(i) For any A*-module* M*, the morphism* $M \to B \otimes_A M$ *is injective.*
(ii) The morphism $\operatorname{Spec} B \to \operatorname{Spec} A$ *is surjective.*

Proof. (i): Let $m \in M - \{0\}$. The ideal $I = \operatorname{Ann}(m)$ is contained in $\mathfrak{m}$. The exact sequence $I \to A \xrightarrow{m} M$ induces by flatness an exact sequence $B \otimes_A I \to B \xrightarrow{1 \otimes m} B \otimes_A M$. The image of $B \otimes_A I \to B$ is the ideal J generated by $\varphi(I)$ in B. Since φ is local and $I \subset \mathfrak{m}$, we have $J \subset \mathfrak{n}$. If $1 \otimes m = 0 \in B \otimes_A M$, then $B = J$, a contradiction.

(ii): Let $\mathfrak{p} \in \operatorname{Spec}(A)$. Then $\kappa(\mathfrak{p}) \to B \otimes_A \kappa(\mathfrak{p})$ is injective by (i), hence $B \otimes_A \kappa(\mathfrak{p}) \neq 0$. Thus $\operatorname{Spec}(B \otimes_A \kappa(\mathfrak{p})) \neq \varnothing$, which means that there is $\mathfrak{q} \in \operatorname{Spec} B$ such that $\varphi^{-1}\mathfrak{q} = \mathfrak{p}$ (by the description of the set of primes in a quotient or a localisation). □

Proposition 2.4.3 (Going down). *Let $\rho\colon R \to S$ be a flat ring morphism. Let $\mathfrak{q} \in \operatorname{Spec}(S)$ and $\mathfrak{p}' \in \operatorname{Spec}(R)$ be such that $\mathfrak{p}' \subset \rho^{-1}\mathfrak{q}$. Then we may find $\mathfrak{q}' \in \operatorname{Spec}(S)$ such that $\mathfrak{q}' \subset \mathfrak{q}$ and $\rho^{-1}\mathfrak{q}' = \mathfrak{p}'$.*

Proof. The morphism $R_{\mathfrak{p}} \to S_{\mathfrak{q}}$ is flat and local. Therefore by Lemma 2.4.2 (ii) the prime $\mathfrak{p}'R_{\mathfrak{p}}$ has a preimage in $\operatorname{Spec}(S_{\mathfrak{q}})$, necessarily of the form $\mathfrak{q}'S_{\mathfrak{q}}$ with $\mathfrak{q}' \subset \mathfrak{q}$. The primes $\rho^{-1}\mathfrak{q}'$ and $\mathfrak{p}'$ coincide because they are contained in $\mathfrak{p}$ and localise to the same prime of $R_{\mathfrak{p}}$. □

Corollary 2.4.4. *Let $R \to S$ be a flat ring morphism and M a finitely generated R-module. Then the morphism $\operatorname{Spec} S \to \operatorname{Spec} R$ sends minimal elements of $\operatorname{Supp}_S(S \otimes_R M)$ to minimal elements of $\operatorname{Supp}_R(M)$.*

Proof. Let $\mathfrak{q}$ be a minimal element $\operatorname{Supp}_S(S \otimes_R M)$. Then its image $\mathfrak{p} \in \operatorname{Spec}(R)$ belongs to $\operatorname{Supp}_R(M)$ by Proposition 1.1.9. If $\mathfrak{p}' \in \operatorname{Supp}_R(M)$ is such that $\mathfrak{p}' \subset \mathfrak{p}$, then by Proposition 2.4.3 we may find a preimage $\mathfrak{q}'$ of $\mathfrak{p}'$ such that $\mathfrak{q}' \subset \mathfrak{q}$. Then $\mathfrak{q}' \in \operatorname{Supp}_S(S \otimes_R M)$ by Proposition 1.1.9, hence $\mathfrak{q}' = \mathfrak{q}$ by minimality of $\mathfrak{q}$. Thus $\mathfrak{p}' = \mathfrak{p}$, proving that $\mathfrak{p}$ is a minimal element of $\operatorname{Supp}_R(M)$. □

Proposition 2.4.5 (Prime avoidance). *Let $I, \mathfrak{p}_1, \cdots, \mathfrak{p}_n$ be ideals of R. Assume that $\mathfrak{p}_i$ is prime for $i \geq 3$. If $I \subset \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$ then $I \subset \mathfrak{p}_i$ for some $i \in \{1, \cdots, n\}$.*

Proof. We assume that I is contained in no $\mathfrak{p}_i$ and find $x \in I$ belonging to no $\mathfrak{p}_i$. This is clear for $n = 0, 1$. If $n = 2$, we $x_i \in I - \mathfrak{p}_i$ for $i = 1, 2$. We may assume that $x_1 \in \mathfrak{p}_2$ and $x_2 \in \mathfrak{p}_1$ (otherwise the statement is proved). Then $x = x_1 + x_2$ works.

Now assume that $n > 2$, and proceed by induction on n. For each $j = 1, \cdots, n$, we can find by induction $x_j \in I$ which is in none of the $\mathfrak{p}_i$ for $i \neq j$, and we may assume as above that $x_j \in \mathfrak{p}_j$. Then $x = x_n + x_1 x_2 \cdots x_{n-1}$ works, since $\mathfrak{p}_n$ is prime ($n \geq 3$). □

Proposition 2.4.6. *Let $\varphi\colon A \to B$ be a local morphism of local rings and M a finitely generated A-module. Let $\mathfrak{m}$ be the maximal ideal of A, and k its residue field. Then*

$$\dim_B B \otimes_A M \leq \dim_A M + \dim_B B \otimes_A k,$$

with equality if B is flat as an A-module.

Proof. We may assume that $M \neq 0$, and proceed by induction on $\dim_A M$. First assume that $\dim_A M = 0$. Then $\{\mathfrak{m}\} = \operatorname{Supp}_A(M) = \operatorname{Supp}_A(k)$, hence $\operatorname{Supp}_B(B \otimes_A M) = \operatorname{Supp}_B(B \otimes_A k)$ by Proposition 1.1.9 and thus $\dim_B B \otimes_A M = \dim B \otimes_A k$, proving the statement in this case.

Assume that $\dim_A M > 0$. Then $\mathfrak{m}$ is not a minimal element of $\operatorname{Supp}_A(M)$. By prime avoidance (Proposition 2.4.5) and finiteness of the set of minimal primes (Corollary 1.3.6), we may find $x \in \mathfrak{m}$ belonging to no minimal primes of $\operatorname{Supp}_A(M)$. By Proposition 2.3.4 we have $\dim_A M/xM = \dim_A M - 1$, so that we may use the induction hypothesis for the module M/xM and obtain

$$\dim_B B \otimes_A (M/xM) \leq \dim_A M - 1 + \dim_B B \otimes_A k, \tag{2.4.a}$$

with equality if φ is flat. Applying Proposition 2.3.4 to the B-module $B \otimes_A M$ and the element $\varphi(x) \in B$, we obtain

$$\dim_B B \otimes_A M \leq \dim_B B \otimes_A (M/xM) + 1, \tag{2.4.b}$$

with equality if $\varphi(x)$ belongs to no minimal primes of $\mathrm{Supp}_B(B \otimes_A M)$. The latter condition is fulfilled if φ is flat by Corollary 2.4.4. The statement follows by combining (2.4.a) and (2.4.b). $\square$

CHAPTER 3

Systems of parameters

1. Alternative definition of the dimension

In this section $(A, \mathfrak{m}, k)$ is a local ring, and M a finitely generated A-module.

LEMMA 3.1.1. *The following conditions are equivalent:*

(i) $\dim M = 0$.
(ii) $\mathrm{Supp}(M) = \{\mathfrak{m}\}$.
(iii) $\mathrm{Ass}(M) = \{\mathfrak{m}\}$.
(iv) The A-module M has finite length and is nonzero.
(v) $M \neq 0$ *and there is an integer n such that* $\mathfrak{m}^n M = 0$.

PROOF. (i) $\Leftrightarrow$ (ii): Indeed, $\dim M$ is the supremum of the lengths of chains of primes in $\mathrm{Supp}(M)$, and $\mathfrak{m} \in \mathrm{Supp}(M)$ as soon as $\mathrm{Supp}(M) \neq \varnothing$.

(ii) $\Leftrightarrow$ (iii): This follows from Proposition 1.3.1.

(iv) $\Leftrightarrow$ (i): This was proved in Lemma 2.2.5.

(iv) $\Rightarrow$ (v): The sequence of submodules $\mathfrak{m}^{i+1}M \subset \mathfrak{m}^i M \subset \cdots$ must stabilise, hence there is n such that $\mathfrak{m}^{n+1}M = \mathfrak{m}^n M$. By Nakayama's Lemma 1.1.6 (applied to $\mathfrak{m}^n M$) we obtain $\mathfrak{m}^n M = 0$.

(v) $\Rightarrow$ (ii): If $\mathfrak{p} \in \mathrm{Supp}(M)$, then $\mathfrak{m}^n \subset \mathrm{Ann}(M) \subset \mathfrak{p}$. Thus for any $x \in \mathfrak{m}$ we have $x^n \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, this implies $x \in \mathfrak{p}$, proving that $\mathfrak{m} = \mathfrak{p}$. $\square$

PROPOSITION 3.1.2. *Assume that $M \neq 0$. Then $\dim M$ is finite, and coincides with the smallest integer n for which there exists elements $x_1, \cdots, x_n \in \mathfrak{m}$ such that the module $M/\{x_1, \cdots, x_n\}M$ satisfies the conditions of Lemma 3.1.1.*

PROOF. If $x_1, \cdots, x_m \in \mathfrak{m}$ are such that $\dim M/\{x_1, \cdots, x_m\}M = 0$, then $\dim M \leq m$ by Proposition 2.3.4.

If $x_1, \cdots, x_m$ is a finite set of generators of the ideal $\mathfrak{m}$ (which exists since A is noetherian), then the module $M/\{x_1, \cdots, x_m\}M = M/\mathfrak{m}M$ satisfies the condition (v) of Lemma 3.1.1, hence $\dim M \leq m < \infty$.

We prove by induction on $n = \dim M$ that we may find $x_1, \cdots, x_n \in \mathfrak{m}$ such that $\dim M/\{x_1, \cdots, x_n\}M = 0$. The case $n = 0$ being clear, let us assume that $n > 0$. By prime avoidance (Proposition 2.4.5), we may find an element $x_n \in \mathfrak{m}$ belonging to no $\mathfrak{p} \in \mathrm{Supp}(M)$ such that $\dim A/\mathfrak{p} = n$ (by Corollary 1.3.6 there are only finitely many such $\mathfrak{p}$, since they are among the minimal elements of $\mathrm{Supp}(M)$). Then $\dim M/x_n M = n - 1$ by Proposition 2.3.4. Applying the induction hypothesis to the module $N = M/x_n M$, we find $x_1, \cdots, x_{n-1} \in \mathfrak{m}$ such that $N/\{x_1, \cdots, x_{n-1}\}N = M/\{x_1, \cdots, x_n\}M$ satisfies the conditions of Lemma 3.1.1. $\square$

DEFINITION 3.1.3. A set $\{x_1, \cdots, x_n\}$ as in Proposition 3.1.2 (with $n = \dim M$) is called a *system of parameters for M*.

If V is a k-vector space, we denote by $\dim_{k-\text{vect}} V$ its dimension in the sense of linear algebra (that is, the cardinality of a k-basis).

PROPOSITION 3.1.4. *The minimal number of generators of the ideal* $\mathfrak{m}$ *is equal to* $\dim_{k-\text{vect}}(\mathfrak{m}/\mathfrak{m}^2)$.

PROOF. Let $n = \dim_{k-\text{vect}}(\mathfrak{m}/\mathfrak{m}^2)$, and $x_1, \cdots, x_n \in \mathfrak{m}$ a family which reduces modulo $\mathfrak{m}^2$ to a k-basis of $\mathfrak{m}/\mathfrak{m}^2$. Let $I \subset \mathfrak{m}$ be the ideal generated by $x_1, \cdots, x_n$. Then $\mathfrak{m} = I + \mathfrak{m}^2$. Thus the finitely generated A-module $M = \mathfrak{m}/I$ satisfies $\mathfrak{m}M = M$, hence vanishes by Nakayama's Lemma 1.1.6. This prove that $\mathfrak{m} = I$ can be generated by n elements.

Conversely if the A-module $\mathfrak{m}$ is generated by m elements, then the k-vector space $\mathfrak{m}/\mathfrak{m}^2$ is generated by their images modulo $\mathfrak{m}^2$, so that $\dim_{k-\text{vect}}(\mathfrak{m}/\mathfrak{m}^2) \leq m$. □

COROLLARY 3.1.5. *We have* $\dim_{k-\text{vect}}(\mathfrak{m}/\mathfrak{m}^2) \geq \dim A$.

PROOF. Since the A-module $k = A/\mathfrak{m}A$ satisfies the conditions of Lemma 3.1.1, this follows from Proposition 3.1.2 applied with $M = A$, and Proposition 3.1.4. □

2. Regular local rings

DEFINITION 3.2.1. We will say that a local (noetherian) ring A is *regular* if $\dim A = \dim_{k-\text{vect}}(\mathfrak{m}/\mathfrak{m}^2)$, or equivalently (Proposition 3.1.4) if $\mathfrak{m}$ can be generated by $\dim A$ elements. A system of parameters for A generating the maximal ideal is called a *regular system of parameters.*

EXAMPLE 3.2.2. A local ring of dimension zero is a regular local ring if and only if it is a field. Indeed let $\mathfrak{m}$ be its maximal ideal. Then $\dim_{k-\text{vect}}(\mathfrak{m}/\mathfrak{m}^2) = 0$ if and only if $\mathfrak{m} = \mathfrak{m}^2$. By Nakayama's Lemma 1.1.6, this condition is equivalent to $\mathfrak{m} = 0$.

EXAMPLE 3.2.3. (Exercise) A local ring of dimension one is a regular local ring if and only if it is a discrete valuation ring.

LEMMA 3.2.4. *Let* $(A, \mathfrak{m})$ *be a regular local ring, and* $x \in \mathfrak{m} - \mathfrak{m}^2$*. Then* A/xA *is a regular local ring of dimension* $\dim A - 1$.

PROOF. Consider the local ring $B = A/xA$, and let $\mathfrak{n} = \mathfrak{m}/xA$ be its maximal ideal. Note that $k = A/\mathfrak{m} = B/\mathfrak{n}$. There is a surjective morphism $\mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{n}/\mathfrak{n}^2$ of k-vector spaces whose kernel contains the 1-dimensional k-vector space generated by $x \mod \mathfrak{m}^2$. It follows that

$$\dim_{k-\text{vect}}(\mathfrak{n}/\mathfrak{n}^2) \leq \dim_{k-\text{vect}}(\mathfrak{m}/\mathfrak{m}^2) - 1 = \dim A - 1 \leq \dim B,$$

where we use Proposition 2.3.4 for the last inequality. Since $\dim_{k-\text{vect}}(\mathfrak{n}/\mathfrak{n}^2) \geq \dim B$ by Corollary 3.1.5, we conclude that $\dim_{k-\text{vect}}(\mathfrak{n}/\mathfrak{n}^2) = \dim B = \dim A - 1$. □

A partial converse is given by the following.

LEMMA 3.2.5. *Let* $(A, \mathfrak{m})$ *be a local ring, and* $x \in \mathfrak{m}$ *a nonzerodivisor in* A*. If* A/xA *is a regular local ring then so is* A.

PROOF. Let $n = \dim A$. By Corollary 2.3.5 we have $\dim A/xA = n - 1$. Let $x_1, \cdots, x_{n-1}$ be elements of $\mathfrak{m}$ reducing modulo xA to a regular system of parameters for the local ring A/xA. Then the n elements $x, x_1, \cdots, x_{n-1}$ generate the ideal $\mathfrak{m}$, and thus form a regular system of parameters for A. □

Proposition 3.2.6. *A regular local ring is an integral domain.*

Proof. Let $(A, \mathfrak{m})$ be a regular local ring. We prove that A is an integral domain by induction on $\dim A$. If $\dim A = 0$, then A is a field by Example 3.2.2, and in particular an integral domain. If $\dim A > 0$, then $\mathfrak{m} \neq 0$, hence $\mathfrak{m} \neq \mathfrak{m}^2$ by Nakayama's Lemma 1.1.6. Thus by prime avoidance (Proposition 2.4.5) we may find an element $x \in \mathfrak{m}$ not belonging to $\mathfrak{m}^2$ nor to any of the finitely many minimal primes of A (Corollary 1.3.6). The local ring A/xA is regular and has dimension $\dim A - 1$ by Lemma 3.2.4. By the induction hypothesis it is an integral domain, which means that xA is a prime ideal of A. So xA contains a minimal prime $\mathfrak{q}$; by the choice of x we have $x \notin \mathfrak{q}$. For any $y \in \mathfrak{q}$, we can write $y = xa$ for some $a \in A$. Since $\mathfrak{q}$ is prime and $x \notin \mathfrak{q}$ we have $a \in \mathfrak{q}$. Thus $\mathfrak{q} = x\mathfrak{q}$, hence $\mathfrak{q} = \mathfrak{m}\mathfrak{q}$ and by Nakayama's Lemma 1.1.6 we have $\mathfrak{q} = 0$, proving that A is an integral domain. $\square$

CHAPTER 4

Tor **and** Ext

In this section R is a commutative unital ring.

1. Chain complexes

DEFINITION 4.1.1. A *chain complex (of R-modules) C* is a collection of R-modules C_i and morphisms of R-modules $d_i^C\colon C_i \to C_{i-1}$ for $i \in \mathbb{Z}$ satisfying $d_{i-1}^C \circ d_i^C = 0$. The R-module

$$H_i(C) = \ker d_i^C / \operatorname{im} d_{i+1}^C$$

is called the *i-th homology* of the chain complex C. The chain complex C is called *exact* if $H_i(C) = 0$ for all i.

A morphism of chain complexes $f\colon C \to C'$ is a collection of morphisms $f_i\colon C_i \to C_i'$ such that $f_{i-1} \circ d_i = d_i \circ f_i$. Such a morphism induces a morphism of the homology modules $H_i(C) \to H_i(C')$. We say that the morphism $C \to C'$ is a *quasi-isomorphism* if the induced morphism $H_i(C) \to H_i(C')$ is an isomorphism for all i.

DEFINITION 4.1.2. We say that the morphisms of chain complexes $f, g\colon C \to C'$ are *homotopic* if there exists a collection of morphisms $s_i\colon C_i \to C'_{i+1}$ such that

$$f_i - g_i = d_{i+1}^{C'} \circ s_i + s_{i-1} \circ d_i^C.$$

A morphism of chain complexes $f\colon M \to N$ is a *homotopy equivalence* if there exists a morphism of chain complexes $g\colon N \to M$ such that $f \circ g$ is homotopic to id_N and $g \circ f$ is homotopic to id_M. We say that the chain complexes are *homotopy equivalent* if there exists a homotopy equivalence between them.

PROPOSITION 4.1.3. *Homotopic morphisms induce the same morphism in homology.*

PROOF. In the notations of Definition 4.1.2, the morphism $d_i^{C'} \circ s_i$ has image contained in $\operatorname{im} d_{i+1}^{C'}$ and kernel of the morphism $s_{i-1} \circ d_i^C$ contains $\ker d_i^C$. These morphisms thus induce the zero morphism in homology by construction. □

COROLLARY 4.1.4. *Homotopy equivalent chain complexes are quasi-isomorphic.*

DEFINITION 4.1.5. A sequence of chain complexes

$$0 \to C' \to C \to C'' \to 0$$

is called *exact* if the sequence

$$0 \to C_i' \to C_i \to C_i'' \to 0$$

is exact for each i.

Proposition 4.1.6. *An exact sequence of chain complexes*

$$0 \to C' \to C \to C'' \to 0$$

induces an exact sequence of modules

$$\cdots \to H_{i+1}(C'') \to H_i(C') \to H_i(C) \to H_i(C'') \to H_{i-1}(C) \to \cdots$$

Proof. We only describe the morphism $\partial \colon H_{i+1}(C'') \to H_i(C')$. Any element $x''_{i+1} \in \ker d^{C''}_{i+1}$ lifts to $x_{i+1} \in C_{i+1}$. Let $x_i = d^C_{i+1}(x_{i+1}) \in C_i$. The image of x_i in C''_i is $d^{C''}_{i+1}(x''_{i+1}) = 0$, hence x_i is the image of some $x'_i \in C'_i$. In addition the image of $d^{C'}_i(x'_i) \in C'_{i-1}$ in C_{i-1} is $d^C_i \circ d^C_{i+1}(x_i) = 0$. Since $C'_{i-1} \to C_{i-1}$ is injective, it follows that $x'_i \in \ker d^{C'}_i$. We define $\partial(x)$ as the class of $x'_i \in H_i(C') = \ker d^{C'}_i / \operatorname{im} d^{C'}_{i+1}$.

We leave it as an exercise to check that ∂ is well-defined and that the sequence is exact. □

2. Projective Resolutions

Lemma 4.2.1. *Let M be a module. Then there exists a surjective morphism $F \to M$ with F free. If M finitely generated, then F may be chosen to be finitely generated.*

Proof. First assume that $\mathcal{G} \subset M$ is a generating set for the R-module M, and let F be the free module on the basis $\{e_g | g \in \mathcal{G}\}$. Then there is a surjective morphism $F \to M$ given by $e_g \mapsto g$.

We may always take $\mathcal{G} = M$. If M is finitely generated, we may find a finite generating set $\mathcal{G}$; in this case F is finitely generated. □

Definition 4.2.2. An R-module P is *projective* if for every surjective R-module morphism $M \to M''$, the natural morphism $\operatorname{Hom}_R(P, M) \to \operatorname{Hom}_R(P, M'')$ is surjective.

Lemma 4.2.3. *A module is projective if and only if it is a direct summand of a free module.*

Proof. If P is a projective R-module, we may find a surjective R-module morphism $p \colon F \to P$ with F free by Lemma 4.2.1. Since P is projective, there is an R-module morphism $s \colon P \to F$ such that $p \circ s = \mathrm{id}_P$. This gives a decomposition $F = P \oplus \ker p$.

Let L be a free module with basis l_α, and $M \to M''$ be a surjective morphism. Let $g \colon L \to M''$ be a morphism. For each α, choose an element of $m_\alpha \in M$ mapping to $g(l_\alpha)$. Then the unique morphism $L \to M$ mapping l_α to m_α is a lifting of g. This proves that L is projective. Let now A be a direct summand of a free module L, which means that there are morphisms $A \to L$ and $L \to A$ such that the composite $A \to L \to A$ is the identity. Let $A \to M$ be a morphism. As we have just seen, the morphism $L \to A \to M$ lifts to a morphism $L \to M''$. The composite $A \to L \to M$ is then a lifting of the morphism $A \to M$. This proves that the module A is projective. □

Lemma 4.2.4. *A projective module is flat.*

Proof. Using the fact that tensor products commutes with (possibly infinite) direct sums, we see that a direct summand of a flat module is flat, and that a free module is flat. The lemma then follows from Lemma 4.2.3. □

Definition 4.2.5. Let M be an R-module. A *resolution* $C \to M$ is a chain complex C such that $C_i = 0$ for $i < 0$, together with a morphism $C_0 \to M$ such that the augmented chain complex

$$\cdots \to C_1 \to C_0 \to M \to 0$$

is exact.

This may be reformulated as follows. We denote by $C(M)$ the chain complex such that $C(M)_i = 0$ for $i \neq 0$ and $C(M)_0 = M$ (and thus $d_i^{C(M)} = 0$ for all i). A resolution of M is a chain complex C such that $C_i = 0$ for $i < 0$, together with a quasi-isomorphism $C \to C(M)$.

A resolution $C \to M$ is said to be projective, resp. free, resp. finitely generated, if each C_i is so.

Proposition 4.2.6. *Every module admits a free resolution. If R is noetherian, any finitely generated R-module admits a finitely generated free resolution.*

Proof. Let M be a module. We construct a chain complex D as follows. We let $D_i = 0$ for $i < 0$ and $D_{-1} = M$. Assuming that $D_{i-1} \to D_{i-2} \to \cdots$ is constructed for some $i \geq 0$, by Lemma 4.2.1 we may find a surjection $D_i \to \ker(D_{i-1} \to D_{i-2})$ with D_i free (resp. free and finitely generated). Then the sequence of modules $D_i \to D_{i-1} \to D_{i-2}$ is exact. The resolution $C \to M$ is obtained by letting $C_i = D_i$ for $i \neq 0$ and $C_0 = 0$. □

Proposition 4.2.7. *Let E and P be two chain complexes. Assume that*

- $P_i = E_i = 0$ *for* $i < -1$.
- P_i *is projective for* $i \geq 0$.
- E *is exact.*

Let $g \colon P_{-1} \to E_{-1}$ be a morphism of modules. Then there is a morphism of chain complexes $f \colon P \to E$ such that $f_{-1} = g$. This morphism is unique up to homotopy.

Proof. We construct f_i inductively, starting with $f_{-1} = g$. Assume that $i \geq 0$ and that f_{i-1} is constructed. The composite $f_{i-1} \circ d_i^P \colon P_i \to E_{i-1}$ lands into $\ker d_{i-1}^E$, because

$$d_{i-1}^E \circ f_{i-1} \circ d_i^P = f_{i-2} \circ d_{i-1}^P \circ d_i^P = 0.$$

By exactness of the complex E, the morphism $E_i \to \ker d_{i-1}^E$ induced by d_i^E is surjective, hence by projectivity of P_i, we may find a morphism $f_i \colon P_i \to E_i$ such that $d_i^E \circ f_i = f_{i-1} \circ d_i^P$.

Now let $f, f' \colon P \to E$ be morphisms of chain complexes extending g. We construct for each i a morphism $s_i \colon P_i \to E_{i+1}$ such that

$$f_i - f_i' = d_{i+1}^E \circ s_i + s_{i-1} \circ d_i^P$$

by induction on i. We let $s_i = 0$ for $i < -1$. Assume that s_{i-1} is constructed. Then

$$\begin{aligned} d_i^E \circ (f_i - f_i') &= (f_{i-1} - f_{i-1}') \circ d_i^P \\ &= d_i^E \circ s_{i-1} \circ d_i^P + s_{i-2} \circ d_{i-1}^P \circ d_i^P \\ &= d_i^E \circ s_{i-1} \circ d_i^P, \end{aligned}$$

so that $(f_i - f_i') - s_{i-1} \circ d_i^P \colon P_i \to E_i$ has image in $\ker d_i^E$. By exactness of the complex E, the morphism $E_{i+1} \to \ker d_i^E$ is surjective. By projectivity of P_i, we obtain a morphism $s_i \colon P_i \to E_{i+1}$ such that $d_{i+1}^E \circ s_i = (f_i - f_i') - s_{i-1} \circ d_i^P$, as required. □

Corollary 4.2.8. *Let M be an R-module, and $P \to M, P' \to M$ projective resolutions. Then there exists a morphism of chain complexes $P \to P'$ such that the composites $P_0 \to P'_0 \to M$ and $P_0 \to M$ coincide. Such a morphism is unique up to homotopy, and is a homotopy equivalence.*

Proof. By Proposition 4.2.7, the identity of M extends to morphisms of chain complexes $P \to P'$ and $P' \to P$, which are unique up to homotopy. The composite $P \to P' \to P$ and the identity of P are both extensions of the identity of M. They must be homotopic by the unicity part of Proposition 4.2.7. For the same reason, the composite $P' \to P \to P'$ is homotopic to the identity of P'. □

Lemma 4.2.9. *Let C' and C'' be chain complexes. Assume that*

- $C'_i = C''_i = 0$ *for* $i < -1$
- C''_i *is projective for* $i \geq 0$.
- C' *is exact.*

Then any exact sequence of modules

$$0 \to C'_{-1} \to M \to C''_{-1} \to 0$$

is the degree -1 part of an exact sequence of chain complexes

$$0 \to C' \to C \to C'' \to 0.$$

In addition:

(i) If the chain complex C'' is exact, then so is C.
(ii) For each $i \geq 0$, the exact sequence of modules

$$0 \to C'_i \to C_i \to C''_i \to 0$$

splits (i.e. induces a decomposition $C_i = C'_i \oplus C''_i$).
(iii) If C'_i is projective, then so is C_i.

Proof. Let us first prove (i) (ii) (iii) assume the first part of lemma.

(i): This follows from the homology long exact sequence Proposition 4.1.6.

(ii): This follows from the fact that C''_i is projective.

(iii): This follows from (ii), since a direct sum of projective modules is projective (e.g. by Lemma 4.2.3).

Let us now prove the first part of the lemma. We let $C_i = C'_i \oplus C''_i$ with the natural morphisms $C'_i \to C_i \to C''_i$. We construct by induction a morphism $d_i^C : C_i \to C_{i-1}$ such that $d_{i-1}^C \circ d_i^C = 0$ making the following diagram commute

$$\begin{tikzcd}
C'_i \arrow[r] \arrow[d] & C_i \arrow[r] \arrow[d] & C''_i \arrow[d] \\
C'_{i-1} \arrow[r] & C_{i-1} \arrow[r] & C''_{i-1}
\end{tikzcd}$$

and moreover such that the sequence

$$0 \to Z'_i \to Z_i \to Z''_i \to 0$$

is exact, where $Z_i = \ker d_i^C$, $Z'_i = \ker d_i^{C'}$, $Z''_i = \ker d_i^{C''}$.

We let $d_{-1}^C = 0$. Assume d_{i-1}^C constructed for some $i \geq 0$. The morphism $d_i^C : C_i \to Z_{i-1} \subset C_{i-1}$ is the sum of the morphism $C'_i \to Z'_{i-1} \to Z_{i-1}$ and a morphism $C''_i \to Z_{i-1}$

lifting the morphism $C''_i \to Z''_{i-1}$, which exists since C''_i is projective and $Z_{i-1} \to Z''_{i-1}$ is surjective.

It only remains to prove that $Z_i \to Z''_i$ is surjective. Any $x''_i \in Z''_i \subset C''_i$ lifts to an element $x_i \in C_i$. Let $x_{i-1} = d_i^C(x_i) \in C_{i-1}$. Then the image of x_{i-1} in C''_{i-1} is $d_i^{C''}(x''_i) = 0$, hence x_{i-1} is the image of some element of $x'_{i-1} \in C'_{i-1}$. In addition, the image of $d_{i-1}^{C'}(x'_{i-1})$ in C''_{i-2} is $d_{i-1}^C(x_{i-1}) = d_{i-1}^C \circ d_i^C(x_i) = 0$, hence $d_{i-1}^{C'}(x'_{i-1}) = 0$ by injectivity of $C'_{i-2} \to C_{i-2}$. Since the complex C' is exact, we may find $x'_i \in C'_i$ such that $d_i^{C'}(x'_i) = x'_{i-1}$. Let $y_i \in C_i$ be the image of x'_i. Then $x_i - y_i \in C_i$ maps to x''_i in C''_i, and satisfies $d_i(x_i - y_i) = 0$, i.e. belongs to Z_i. □

3. The Tor functor

When C is a chain complex, and N a module, we denote by $C \otimes_R N$ the chain complex such that that $(C \otimes_R N)_i = C_i \otimes_R N$ and $d_i^{C \otimes_R N} = d_i^C \otimes \mathrm{id}_N$. A morphism of chain complexes $f\colon C \to C'$ induces a morphism of chain complexes $f \otimes_R N\colon C \otimes_R N \to C' \otimes_R N$. If f is homotopic to g, then $f \otimes_R N$ is homotopic to $g \otimes_R N$. Thus a homotopy equivalence $C \to C'$ induces a homotopy equivalence $C \otimes_R N \to C' \otimes_R N$, and in particular a quasi-isomorphism by Corollary 4.1.4.

Definition 4.3.1. Let M, N be two modules and n an integer. Let $C \to M$ be a projective resolution. Then the module $H_n(C \otimes_R N)$ is independent of the choice of C, up to a canonical isomorphism by the discussion above and Corollary 4.2.8. We denote this module by $\mathrm{Tor}_n(M, N)$, or $\mathrm{Tor}_n^R(M, N)$. A morphism $g\colon N \to N'$ induces a morphism $\mathrm{Tor}_n(M, g)\colon \mathrm{Tor}_n(M, N) \to \mathrm{Tor}_n(M, N')$. Let now M' be another module, and $C' \to M'$ be a projective resolution. By Proposition 4.2.7 any morphism of modules $f\colon M \to M'$ extends to a morphism of complexes $C \to C'$. The latter induces a morphism $\mathrm{Tor}_n(f, N)\colon \mathrm{Tor}_n(M, N) \to \mathrm{Tor}_n(M', N)$ which does not depend on any choice by the unicity part of Proposition 4.2.7 and Proposition 4.1.3.

Proposition 4.3.2. *(i)* $\mathrm{Tor}_0(M, N) \simeq M \otimes_R N$.

(ii) $\mathrm{Tor}_n(M, N) = 0$ *for* $n < 0$.

(iii) If N *is flat, then* $\mathrm{Tor}_n(M, N) = 0$ *for* $n > 0$.

(iv) If M *is projective, then* $\mathrm{Tor}_n(M, N) = 0$ *for* $n > 0$.

(v) If $f, g\colon M \to M'$ *are two morphisms and* $\lambda \in R$*, then*

$$\mathrm{Tor}_n(f + \lambda g, N) = \mathrm{Tor}_n(f, N) + \lambda \, \mathrm{Tor}_n(g, N).$$

(vi) If $a, b\colon N \to N'$ *are two morphisms and* $\mu \in R$*, then*

$$\mathrm{Tor}_n(M, a + \mu b) = \mathrm{Tor}_n(M, a) + \mu \, \mathrm{Tor}_n(M, b).$$

Proof. If $C \to M$ is a projective resolution of M, then $M = \mathrm{coker}(C_1 \to C_0)$, hence by right-exactness of the tensor product, we have

$$M \otimes_R N = \mathrm{coker}(C_1 \otimes_R N \to C_0 \otimes_R N) = H_0(C \otimes_R N).$$

This proves (i). Since $C_n = 0$ for $n < 0$, we have $C_n \otimes_R N = 0$, and thus $H_n(C \otimes_R N) = 0$, proving (ii). If N is flat, then $C \otimes_R N \to M \otimes_R N$ is a resolution, hence $H_n(C \otimes_R N) = 0$ for $n > 0$. This proves (iii).

Now if M is projective, we may use the trivial projective resolution $C(M) \to M$ (see Definition 4.2.5) to compute $\mathrm{Tor}_n(M, N)$, so that $\mathrm{Tor}_n(M, N) = 0$ for $n > 0$. This proves (iv). The two remaining statements follow easily from the construction of the Tor functor. □

PROPOSITION 4.3.3. *Consider an exact sequence of modules*

$$0 \to M' \to M \to M'' \to 0$$

Let N be a module. Then we have an exact sequence

$$\cdots \to \mathrm{Tor}_{n+1}(M'', N) \to \mathrm{Tor}_n(M', N) \to \mathrm{Tor}_n(M, N) \to \mathrm{Tor}_n(M'', N) \to \cdots$$

PROOF. Let $C' \to M'$ and $C'' \to M''$ be projective resolutions. By Lemma 4.2.9, we find a projective resolution $C \to M$ and an exact sequence of chain complexes $0 \to C' \to C \to C'' \to 0$ extending the exact sequence of modules $0 \to M' \to M \to M'' \to 0$. Since each exact sequence $0 \to C'_i \to C_i \to C''_i \to 0$ is split, the sequence of chain complexes $0 \to C' \otimes_R N \to C \otimes_R N \to C'' \otimes_R N \to 0$ is exact. The corresponding long exact sequence (Proposition 4.1.6) is the required sequence. □

PROPOSITION 4.3.4. *Consider an exact sequence of modules*

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

Let M be a module. Then we have an exact sequence

$$\cdots \to \mathrm{Tor}_{n+1}(M, N'') \to \mathrm{Tor}_n(M, N') \to \mathrm{Tor}_n(M, N) \to \mathrm{Tor}_n(M, N'') \to \cdots$$

PROOF. Let $C \to M$ be a projective resolution. Since each C_i is projective, hence flat by Lemma 4.2.4, we have an exact sequence of complexes

$$0 \to C \otimes_R N' \to C \otimes_R N \to C \otimes_R N'' \to 0.$$

The corresponding long exact sequence (Proposition 4.1.6) is the required sequence. □

PROPOSITION 4.3.5. *The modules* $\mathrm{Tor}_n(N, M)$ *and* $\mathrm{Tor}_n(M, N)$ *are isomorphic.*

PROOF. We proceed by induction on n, the case $n = 0$ being the symmetry of the tensor product. Let $0 \to K \to P \to N \to 0$ be an exact sequence with P projective (this is possible by Lemma 4.2.1). Since P is both projective and flat (Lemma 4.2.4), so that $\mathrm{Tor}_n(P, M) = \mathrm{Tor}(P, M) = 0$ for $n > 0$ by Proposition 4.3.2.

Applying Proposition 4.3.3 and Proposition 4.3.4, we obtain a commutative diagram with exact rows (recall that $\mathrm{Tor}_1(P, M) = \mathrm{Tor}_1(M, P) = 0$)

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Tor}_1(M,N) \arrow[r] & M \otimes_R K \arrow[r] \arrow[d] & M \otimes_R P \arrow[d] \\
0 \arrow[r] & \mathrm{Tor}_1(N,M) \arrow[r] & K \otimes_R M \arrow[r] & P \otimes_R M
\end{tikzcd}$$

Since horizontal arrows are isomorphisms, we conclude that $\mathrm{Tor}_1(M, N) \simeq \mathrm{Tor}_1(N, M)$.

Let now $n > 1$. Using Proposition 4.3.3 and the vanishing of $\mathrm{Tor}_n(M, P)$ and $\mathrm{Tor}_{n-1}(M, P)$ we deduce that $\mathrm{Tor}_n(M, N) \simeq \mathrm{Tor}_{n-1}(M, K)$. Using Proposition 4.3.4 and the vanishing of $\mathrm{Tor}_n(P, M)$ and $\mathrm{Tor}_{n-1}(P, M)$ we deduce that $\mathrm{Tor}_n(N, M) \simeq \mathrm{Tor}_{n-1}(K, M)$. By induction $\mathrm{Tor}_{n-1}(M, K) \simeq \mathrm{Tor}_{n-1}(K, M)$, and the result follows. □

4. Cochain complexes

Definition 4.4.1. A *cochain complex (of R-modules) C* is a collection of R-modules C^i and morphisms of R-modules $d_C^i \colon C^i \to C^{i+1}$ for $i \in \mathbb{Z}$ satisfying $d_C^{i+1} \circ d_C^i = 0$. The R-module

$$H^i(C) = \ker d_C^i / \operatorname{im} d_C^{i-1}$$

is called the *i-th cohomology* of the cochain complex C. A morphism of cochain complexes $f \colon C \to C'$ is a collection of morphisms $f^i \colon C^i \to C'^i$ such that $f^{i+1} \circ d^i = d^i \circ f^i$. Such a morphism induces a morphism of the cohomology modules $H^i(C) \to H^i(C')$. We say that the morphism $C \to C'$ is a *quasi-isomorphism* if the induced morphism $H^i(C) \to H^i(C')$ is an isomorphism for all i.

Definition 4.4.2. We say that the morphisms of cochain complexes $f, g \colon C \to C'$ are *homotopic* if there exists a collection of morphisms $s^i \colon C^i \to C'^{i-1}$ such that

$$f^i - g^i = d_{C'}^{i-1} \circ s^i + s^{i+1} \circ d_C^i.$$

A morphism of cochain complexes $f \colon M \to N$ is a *homotopy equivalence* if there exists a morphism of cochain complexes $g \colon N \to M$ such that $f \circ g$ is homotopic to id_N and $g \circ f$ is homotopic to id_M.

Proposition 4.4.3. *Homotopic morphisms induce the same morphism in cohomology.*

Proof. In the notations of the definition, the morphism $d_{C'}^{i-1} \circ s^i$ has image contained in $\operatorname{im} d_{i-1}^{C'}$ and kernel of the morphism $s^{i+1} \circ d_C^i$ contains $\ker d_C^i$. These morphisms induce the zero morphism in cohomology by construction. □

Corollary 4.4.4. *Homotopy equivalent cochain complexes are quasi-isomorphic.*

Definition 4.4.5. A sequence of cochain complexes

$$0 \to C' \to C \to C'' \to 0$$

is called *exact* if the sequence

$$0 \to C'^i \to C^i \to C''^i \to 0$$

is exact for each i.

Proposition 4.4.6. *An exact sequence of cochain complexes*

$$0 \to C' \to C \to C'' \to 0$$

induces an exact sequence of modules

$$\cdots \to H^{i-1}(C'') \to H^i(C') \to H^i(C) \to H^i(C'') \to H^{i+1}(C) \to \cdots$$

5. The Ext functor

When M, N are two R-modules, we denote by $\operatorname{Hom}_R(M, N)$ the R-module of R-module morphisms $M \to N$. When C is a chain complex and N a module, we denote by $\operatorname{Hom}_R(C, N)$ the cochain complex such that $(\operatorname{Hom}_R(C, N))^i = \operatorname{Hom}_R(C_i, N)$ and

$$d^i_{\operatorname{Hom}_R(C,N)} \colon \operatorname{Hom}_R(C_i, N) \to \operatorname{Hom}_R(C_{i+1}, N)$$

is the morphism induced by left-composition with d_{i+1}^C.

Definition 4.5.1. Let M, N be two modules and n an integer. Let $C \to M$ be a projective resolution. Then the module $H^n(\mathrm{Hom}_R(C,N))$ is independent of the choice of C, up to a canonical isomorphism. We denote this module by $\mathrm{Ext}^n(M,N)$, or $\mathrm{Ext}^n_R(M,N)$. A morphism $g\colon N \to N'$ induces a morphism $\mathrm{Ext}^n(M,g)\colon \mathrm{Ext}^n(M,N) \to \mathrm{Ext}^n(M,N')$. A morphism $f\colon M \to M'$ induces a morphism $\mathrm{Ext}^n(f,N)\colon \mathrm{Ext}^n(M',N) \to \mathrm{Ext}^n(M,N)$.

Proposition 4.5.2. *(i)* $\mathrm{Ext}^0(M,N) \simeq \mathrm{Hom}_R(M,N)$.

(ii) $\mathrm{Ext}^n(M,N) = 0$ *for* $n < 0$.

(iii) If M *is projective, then* $\mathrm{Ext}^n(M,N) = 0$ *for* $n > 0$.

(iv) If $f, g\colon M \to M'$ *are two morphisms and* $\lambda \in R$*, then*

$$\mathrm{Ext}^n(f + \lambda g, N) = \mathrm{Ext}^n(f,N) + \lambda\,\mathrm{Ext}^n(g,N).$$

(v) If $a, b\colon N \to N'$ *are two morphisms and* $\mu \in R$*, then*

$$\mathrm{Ext}^n(M, a + \mu b) = \mathrm{Ext}^n(M,a) + \mu\,\mathrm{Ext}^n(M,b).$$

Proof. If $C \to M$ is a (projective) resolution of M, then $M = \mathrm{coker}(C_1 \to C_0)$, hence by left-exactness of the contravariant functor $\mathrm{Hom}_R(-,N)$, we have

$$\mathrm{Hom}_R(M,N) = \ker(\mathrm{Hom}_R(C_0,N) \to \mathrm{Hom}_R(C_1,N)) = H^0(\mathrm{Hom}_R(C,N)).$$

This proves the first statement. Since $C_n = 0$ for $n < 0$, we have $\mathrm{Hom}_R(C_n,N) = 0$, and thus $H^n(\mathrm{Hom}_R(C,N)) = 0$, proving the second statement. Now if M is projective, we may use the trivial projective resolution $C(M) \to M$ (see Definition 4.2.5) to compute $\mathrm{Ext}^n(M,N)$, so that $\mathrm{Ext}^n(M,N) = 0$ for $n > 0$. This proves the third statement. The two remaining statements follow easily from the construction of the Ext functor. $\square$

Proposition 4.5.3. *Consider an exact sequence of modules*

$$0 \to M' \to M \to M'' \to 0$$

Let N *be a module. Then we have an exact sequence*

$$\cdots \to \mathrm{Ext}^{n-1}(M',N) \to \mathrm{Ext}^n(M'',N) \to \mathrm{Ext}^n(M,N) \to \mathrm{Ext}^n(M',N) \to \cdots$$

Proof. Let $C' \to M'$ and $C'' \to M''$ be projective resolutions. By Lemma 4.2.9, we find a projective resolution $C \to M$ and an exact sequence of chain complexes $0 \to C' \to C \to C'' \to 0$ extending the exact sequence of modules $0 \to M' \to M \to M'' \to 0$. Since each exact sequence $0 \to C'_i \to C_i \to C''_i \to 0$ is split, the sequence of cochain complexes $0 \to \mathrm{Hom}_R(C'',N) \to \mathrm{Hom}_R(C,N) \to \mathrm{Hom}_R(C',N) \to 0$ is exact. The corresponding long exact sequence (Proposition 4.4.6) is the required sequence. $\square$

Proposition 4.5.4. *Consider an exact sequence of modules*

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

Let M *be a module. Then we have an exact sequence*

$$\cdots \to \mathrm{Ext}^{n-1}(M,N'') \to \mathrm{Ext}^n(M,N') \to \mathrm{Ext}^n(M,N) \to \mathrm{Ext}^n(M,N'') \to \cdots$$

Proof. Let $C \to M$ be a projective resolution. Since each C_i is projective, we have an exact sequence of cochain complexes

$$0 \to \mathrm{Hom}_R(C,N') \to \mathrm{Hom}_R(C,N) \to \mathrm{Hom}_R(C,N'') \to 0.$$

The corresponding long exact sequence (Proposition 4.4.6) is the required sequence. $\square$

CHAPTER 5

Depth

In this chapter $(A, \mathfrak{m})$ is a noetherian local ring, and M a finitely generated A-module.

1. M-regular sequences

Definition 5.1.1. A finite tuple $(x_1, \cdots, x_n)$ of elements of $\mathfrak{m}$ is called an *M-regular sequence* if for all i the element x_i is a nonzerodivisor in $M/\{x_1, \cdots, x_i\}M$. The integer n is the *length* of the M-regular sequence. The M-regular sequence is called *maximal* if there is no $x_{n+1} \in \mathfrak{m}$ such that $(x_1, \cdots, x_{n+1})$ is an M-regular sequence.

Lemma 5.1.2. *If $M \neq 0$, then a maximal M-regular sequence exists.*

Proof. If not, we may find $x_i \in \mathfrak{m}$ for $i \in \mathbb{N}$ such that $(x_1, \cdots, x_n)$ is an M-regular sequence for all n. By Nakayama's Lemma 1.1.6, the A-module $M/\{x_1, \cdots, x_{n-1}\}M$ is nonzero, hence we may find an element $m \in M$ such that $m \notin \{x_1, \cdots, x_{n-1}\}M$. Assume that $x_n \in \{x_1, \cdots, x_{n-1}\}A$. Then $x_n m \in \{x_1, \cdots, x_{n-1}\}M$, hence x_n is a zerodivisor in $M/\{x_1, \cdots, x_{n-1}\}M$, a contradiction. It follows that the sequence of ideals

$$\cdots \subset \{x_1, \cdots, x_n\}A \subset \{x_1, \cdots, x_{n+1}\}A \subset \cdots$$

of A is strictly increasing, which is impossible since A is noetherian. □

Definition 5.1.3. A finite subset S of $\mathfrak{m}$ is called *secant for M* if

$$\dim M/SM = \dim M - s,$$

where s is the cardinal of S. We will say that a sequence $(s_1, \cdots, s_n)$ is secant for M if the set $\{s_1, \cdots, s_n\}$ is secant for M.

Proposition 5.1.4. *Any M-regular sequence is secant.*

Proof. By induction it is enough to consider the case of a sequence of length 1, in which case the statement is Corollary 2.3.5. □

2. Depth

Definition 5.2.1. The depth of M is defined as

$$\operatorname{depth} M = \operatorname{depth}_A M = \inf\{i \in \mathbb{N} \mid \operatorname{Ext}^i(k, M) \neq 0\}.$$

This is an element of $\mathbb{N} \cup \{\infty\}$. When $M = 0$, we have $\operatorname{depth} M = \infty$.

Proposition 5.2.2. *Let $x \in \mathfrak{m}$ be a nonzerodivisor in M. Then*

$$\operatorname{depth} M/xM = \operatorname{depth} M - 1.$$

PROOF. From the exact sequence $0 \to M \xrightarrow{x} M \to M/xM \to 0$ we deduce using Proposition 4.5.4 an exact sequence

$$\cdots \to \operatorname{Ext}^{i-1}(k, M/xM) \to \operatorname{Ext}^i(k, M) \xrightarrow{x} \operatorname{Ext}^i(k, M) \to \cdots$$

In view of Proposition 4.5.2 (iv), the A-module $\operatorname{Ext}^i(k, M)$ is annihilated by $\operatorname{Ann}(k) = \mathfrak{m}$, and in particular multiplication by x is zero in this module. We obtain for each i an exact sequence

$$0 \to \operatorname{Ext}^{i-1}(k, M) \to \operatorname{Ext}^{i-1}(k, M/xM) \to \operatorname{Ext}^i(k, M) \to 0.$$

Therefore $\operatorname{Ext}^{i-1}(k, M/xM) \neq 0$ if and only if $\operatorname{Ext}^{i-1}(k, M) \neq 0$ or $\operatorname{Ext}^i(k, M) \neq 0$. The result follows. □

COROLLARY 5.2.3. *Let $(x_1, \cdots, x_n)$ be an M-regular sequence. Then*

$$\operatorname{depth}(M/\{x_1, \cdots, x_n\}M) = \operatorname{depth} M - n,$$

and in particular $\operatorname{depth} M \geq n$.

LEMMA 5.2.4. *The following conditions are equivalent:*

(i) $\operatorname{depth} M = 0$.
(ii) Every element of $\mathfrak{m}$ *is a zerodivisor in* M.
(iii) $\mathfrak{m} \in \operatorname{Ass}(M)$.

PROOF. A nonzero A-linear morphism $k \to M$ is necessarily injective, therefore $\operatorname{Ext}^0(k, M) = \operatorname{Hom}_A(k, M)$ is nonzero if and only if there is an injective A-modules morphism $k \to M$. This proves that (i) $\Leftrightarrow$ (iii).

By Lemma 1.2.9, the set of nonzerodivisors in M is the union of the associated primes of M. Since $\operatorname{Ass}(M)$ is finite (Corollary 1.3.6), we see using prime avoidance (Proposition 2.4.5) that (ii) $\Leftrightarrow$ (iii). □

LEMMA 5.2.5. *Let $(x_1, \cdots, x_n)$ be an M-regular sequence. The following conditions are equivalent:*

(i) $\operatorname{depth} M = n$.
(ii) The M-regular sequence $(x_1, \cdots, x_n)$ is maximal.
(iii) $\mathfrak{m} \in \operatorname{Ass}(M/\{x_1, \cdots, x_n\}M)$.

PROOF. In view of Corollary 5.2.3, we see that (i) is equivalent to the condition $\operatorname{depth}(M/\{x_1, \cdots, x_n\}M) = 0$. On the other hand (ii) means that every element of $\mathfrak{m}$ is a zerodivisor in $M/\{x_1, \cdots, x_n\}M$. So the lemma is just a reformulation of Lemma 5.2.4. □

PROPOSITION 5.2.6. *Assume that $M \neq 0$. Then* $\operatorname{depth} M$ *is finite, and coincides with the length of any maximal M-regular sequence.*

PROOF. If $(x_1, \cdots, x_n)$ is a maximal M-regular sequence, then $\operatorname{depth} M = n$ by Lemma 5.2.5. Such a sequence always exists by Lemma 5.1.2. □

Combining Proposition 5.2.6 and Proposition 5.1.4, we obtain:

COROLLARY 5.2.7. *If $M \neq 0$, then* $\operatorname{depth} M \leq \dim M$.

We can be more precise:

PROPOSITION 5.2.8. *We have* $\operatorname{depth} M \leq \dim A/\mathfrak{p}$ *for every* $\mathfrak{p} \in \operatorname{Ass}(M)$.

Proof. We may assume that $M \neq 0$ and proceed by induction on $\operatorname{depth} M$ (which is finite by Proposition 5.2.6), the case $\operatorname{depth} M = 0$ being clear. If $\operatorname{depth} M > 0$, then by Lemma 5.2.4 we can find $x \in \mathfrak{m}$, which a nonzerodivisor in M. Let $\mathfrak{p} \in \operatorname{Ass}(M)$, and consider the exact sequence of A-modules

$$0 \to \operatorname{Hom}_A(A/\mathfrak{p}, M) \xrightarrow{x} \operatorname{Hom}_A(A/\mathfrak{p}, M) \to \operatorname{Hom}_A(A/\mathfrak{p}, M/xM).$$

Since $\mathfrak{p} \in \operatorname{Ass}(M)$, the A-module $\operatorname{Hom}_A(A/\mathfrak{p}, M)$ is nonzero. It is also finitely generated, being a submodule of $\operatorname{Hom}_A(A, M) = M$. By Nakayama's Lemma 1.1.6, it follows that $\operatorname{Hom}_A(A/\mathfrak{p}, M)/x \operatorname{Hom}_A(A/\mathfrak{p}, M) \neq 0$, hence by the above exact sequence $\operatorname{Hom}_A(A/\mathfrak{p}, M/xM) \neq 0$. Thus the A-module M/xM contains a nonzero quotient Q of $A/\mathfrak{p}$. Let us choose an element $\mathfrak{q} \in \operatorname{Ass}(Q) \subset \operatorname{Ass}(M/xM)$ (Corollary 1.2.3). Then $\mathfrak{q} \in \operatorname{Supp}(Q) \subset \operatorname{Supp}(A/\mathfrak{p})$ (because Q is a quotient of $A/\mathfrak{p}$), hence $\mathfrak{p} \subset \mathfrak{q}$. Since $x \in \operatorname{Ann}(M/xM) \subset \operatorname{Ann}(Q) \subset \mathfrak{q}$ and $x \notin \mathfrak{p}$ (a nonzerodivisor is in no associated prime), we have $\mathfrak{p} \subsetneq \mathfrak{q}$. Thus

$$\dim A/\mathfrak{p} \geq \dim A/\mathfrak{q} + 1.$$

By Corollary 5.2.3 we have

$$\operatorname{depth} M/xM = \operatorname{depth} M - 1,$$

hence applying the induction hypothesis to the module M/xM, we know that

$$\dim A/\mathfrak{q} \geq \operatorname{depth} M/xM.$$

This concludes the proof. □

Proposition 5.2.8 may be viewed as a special case of:

Proposition 5.2.9. *For any* $\mathfrak{p} \in \operatorname{Spec}(R)$*, we have*

$$\operatorname{depth}_A M \leq \operatorname{depth}_{A_\mathfrak{p}} M_\mathfrak{p} + \dim A/\mathfrak{p}.$$

Proof. We may assume that $M \neq 0$, and proceed by induction on $\operatorname{depth} M$ (which is finite by Proposition 5.2.6), the case $\operatorname{depth} M = 0$ being clear. If $\mathfrak{p} \subset \mathfrak{q}$ for some $\mathfrak{q} \in \operatorname{Ass}(M)$, then by Proposition 5.2.8 we have

$$\operatorname{depth}_A M \leq \dim A/\mathfrak{q} \leq \dim A/\mathfrak{p} \leq \operatorname{depth}_{A_\mathfrak{p}} M_\mathfrak{p} + \dim A/\mathfrak{p}.$$

Thus we may assume that $\mathfrak{p}$ is contained in no associated prime of M. Then by prime avoidance (Proposition 2.4.5), finiteness of $\operatorname{Ass}(M)$ (Corollary 1.3.6) and Lemma 1.2.9, we may find an element $x \in \mathfrak{p}$ which is a nonzerodivisor in M. The image of x in $A_\mathfrak{p}$ is a nonzerodivisor in $M_\mathfrak{p}$ by flatness of $A \to A_\mathfrak{p}$ (since multiplication with x induces an injective endomorphism of M, multiplication with $1 \otimes x \in A_\mathfrak{p} \otimes_A A = A_\mathfrak{p}$ induces an injective endomorphism of $A_\mathfrak{p} \otimes_A M = M_\mathfrak{p}$). Therefore by Proposition 5.2.2

$$\operatorname{depth}_A M/xM = \operatorname{depth}_A M - 1 \quad \text{and} \quad \operatorname{depth}_{A_\mathfrak{p}} (M/xM)_\mathfrak{p} = \operatorname{depth}_{A_\mathfrak{p}} M_\mathfrak{p} - 1,$$

and we may conclude by applying the induction hypothesis to M/xM. □

The following observation will be used later:

Lemma 5.2.10. *Let* M, M' *be two finitely generated* A*-modules. Then*

$$\operatorname{depth}(M \oplus M') = \min(\operatorname{depth} M, \operatorname{depth} M').$$

In particular we have $\operatorname{depth} F = \operatorname{depth} A$ *for any free finitely generated nonzero* A*-module* F*.*

PROOF. Let k be the residue field. Functoriality of Ext^n implies that $\operatorname{Ext}^n(k, M \oplus M') = \operatorname{Ext}^n(k, M) \oplus \operatorname{Ext}^n(k, M')$ (exercise), and the statement follows. □

3. Depth and base change

PROPOSITION 5.3.1. *Let $\phi\colon (A, \mathfrak{m}) \to (B, \mathfrak{n})$ be a local morphism. Let M be a B-module, finitely generated as an A-module. Then*

$$\operatorname{depth}_A M = \operatorname{depth}_B M.$$

PROOF. The statement being true if $M = 0$, let us assume that $M \neq 0$. Let $(a_1, \cdots, a_n)$ be a maximal M-regular sequence, where M is viewed as an A-module, so that $\operatorname{depth}_A M = n$ by Proposition 5.2.6. Then the tuple $(\phi(a_1), \cdots, \phi(a_n))$ is an M-regular sequence, where M is viewed as a B-module. By Corollary 5.2.3, we may replace M with $M/\{a_1, \cdots, a_n\}M$, and thus assume that $\operatorname{depth}_A M = 0$. By Lemma 5.2.4, there is an element $m \in M$ such that $\operatorname{Ann}_A(m) = \mathfrak{m}$. Let N be the B-submodule of M generated by m. This is a nonzero, finitely generated A-module, which is annihilated by $\mathfrak{m}$. Hence N has finite length as an A-module (Lemma 3.1.1), and a fortiori as a B-module. Thus $\mathfrak{n} \in \operatorname{Ass}_B(N) \subset \operatorname{Ass}_B(M)$, showing that $\operatorname{depth}_B M = 0$. □

We will need the following technical lemma:

LEMMA 5.3.2. *Consider an exact sequence of finitely-generated A-modules*

$$0 \to M' \to M \to M'' \to 0.$$

If $\operatorname{depth} M'' \geq \operatorname{depth} M'$, *we have* $\operatorname{depth} M = \operatorname{depth} M'$.

PROOF (EXERCISE). Let $n = \operatorname{depth} M$ and $n' = \operatorname{depth} M'$. We have an exact sequence (Proposition 4.5.4)

$$\operatorname{Ext}^{n'-1}(k, M'') \to \operatorname{Ext}^{n'}(k, M') \to \operatorname{Ext}^{n'}(k, M).$$

By assumption, the group on the left is zero, and the group in the middle is nonzero. Thus the group on the right must be nonzero, showing that $n \leq n'$.

We have an exact sequence (Proposition 4.5.4)

$$\operatorname{Ext}^{n}(k, M') \to \operatorname{Ext}^{n}(k, M) \to \operatorname{Ext}^{n}(k, M'').$$

If $n < n'$, then the group on the left is zero. So is the group on the right by our assumption. It follows that the group in the middle vanishes, a contradiction. □

PROPOSITION 5.3.3. *Let $A \to B$ be a flat local morphism and M a finitely generated A-module. Let $\mathfrak{m}$ be the maximal ideal of A, and k its residue field. Then*

$$\operatorname{depth}_B B \otimes_A M = \operatorname{depth}_A M + \operatorname{depth}_B B \otimes_A k.$$

PROOF. We may assume that $M \neq 0$, and proceed by induction on $\dim_A M$. Assume that $\dim_A M = 0$. Thus $\operatorname{depth}_A M = 0$, and we need to prove that $\operatorname{depth}_B B \otimes_A M = \operatorname{depth}_B B \otimes_A k$. We argue by induction on $\operatorname{length}_A M$ (which is finite by Lemma 2.2.5). If $\operatorname{length}_A M = 1$, then the A-module M is isomorphic to k, and the statement is true. If $\operatorname{length}_A M > 1$, then we can find an exact sequence of A-modules

$$0 \to N \to M \to k \to 0$$

with $\operatorname{length}_A N < \operatorname{length}_A M$. Since the A-module B is flat, this gives an exact sequence of B-modules

$$0 \to B \otimes_A N \to B \otimes_A M \to B \otimes_A k \to 0.$$

In view of Lemma 5.3.2, the statement follows by using the induction hypothesis for the module N.

Assume now that $\dim_A M > 0$. Let us first assume additionally that $\mathfrak{m} \notin \operatorname{Ass}_A(M)$. Then we may find an element $x \in \mathfrak{m}$ which is a nonzerodivisor in M (by Lemma 5.2.4). Its image in B is a nonzerodivisor in $B \otimes_A M$ by flatness of $A \to B$. Thus by Proposition 5.2.2 we have $\operatorname{depth}_A M/xM = \operatorname{depth}_A M - 1$ and $\operatorname{depth}_B B \otimes_A (M/xM) = \operatorname{depth}_B B \otimes_A M - 1$. We may then conclude using the induction hypothesis for the A-module M/xM, whose dimension is $< \dim_A M$ by Corollary 2.3.5.

Thus we may assume that $\mathfrak{m} \in \operatorname{Ass}_A(M)$. Thus $\operatorname{depth}_A M = 0$, and we need to prove that $\operatorname{depth}_B B \otimes_A M = \operatorname{depth}_B B \otimes_A k$. By Proposition 1.2.7, we can find an exact sequence of A-modules

$$0 \to M' \to M \to M'' \to 0$$

such that $\operatorname{Ass}_A(M') = \{\mathfrak{m}\}$, and $\operatorname{Ass}_A(M'') = \operatorname{Ass}_A(M) - \{\mathfrak{m}\}$. Then $\dim_A M'' = \dim_A M$ and $\mathfrak{m} \notin \operatorname{Ass}_A(M'')$; we have just proved that

$$\operatorname{depth}_B B \otimes_A M'' = \operatorname{depth}_A M'' + \operatorname{depth}_B B \otimes_A k.$$

On the other hand, since $\dim_A M' = 0$, we have also proved that

$$\operatorname{depth}_B B \otimes_A M' = \operatorname{depth}_B B \otimes_A k.$$

By flatness of $A \to B$, we have an exact sequence of B-modules

$$0 \to B \otimes_A M' \to B \otimes_A M \to B \otimes_A M'' \to 0,$$

and the statement follows from Lemma 5.3.2. $\square$

CHAPTER 6

Cohen-Macaulay modules

1. Cohen-Macaulay modules

In this section $(A, \mathfrak{m})$ will be a local ring, and M a finitely generated A-module.

Definition 6.1.1. We say that M is *Cohen-Macaulay* if $\operatorname{depth} M \geq \dim M$. By Corollary 5.2.7, the module M is Cohen-Macaulay if and only if $M = 0$ or $\operatorname{depth} M = \dim M$.

Example 6.1.2. Any module of dimension zero is Cohen-Macaulay.

Proposition 6.1.3. *Assume that $M \neq 0$. The following conditions are equivalent:*

(i) M is Cohen-Macaulay,
(ii) There is an M-regular sequence which is also a system of parameters for M.
(iii) Every maximal M-regular sequence is a system of parameters for M.

Proof. (iii) $\Rightarrow$ (ii): Lemma 5.1.2.

(ii) $\Rightarrow$ (i): Assume that there is an M-regular sequence of length n which is a system of parameters. Then $\dim M = n$ by Proposition 3.1.2, and $n \leq \operatorname{depth} M$ by Lemma 5.2.5. It follows that $\dim M \geq \operatorname{depth} M$.

(i) $\Rightarrow$ (iii): Let $(x_1, \cdots, x_n)$ be a maximal M-regular sequence. Then $n = \operatorname{depth} M$ by Proposition 5.2.6, hence $n = \dim M$ by (i). It follows from Proposition 5.1.4 that $\dim M/\{x_1, \cdots, x_n\}M = 0$, proving that the set $\{x_1, \cdots, x_n\}$ is a system of parameters for M. □

Proposition 6.1.4. *Assume that M is Cohen-Macaulay. Then $\dim A/\mathfrak{p} = \dim M$ for every $\mathfrak{p} \in \operatorname{Ass}(M)$.*

Proof. Let $\mathfrak{p} \in \operatorname{Ass}(M)$. We have by Proposition 5.2.8 and Proposition 2.1.4

$$\operatorname{depth} M \leq \dim A/\mathfrak{p} \leq \dim M.$$

If M is Cohen-Macaulay, these inequalities must be equalities. □

Corollary 6.1.5. *Assume that M is Cohen-Macaulay. Then M is equidimensional ($\dim A/\mathfrak{p} = \dim M$ for every minimal prime $\mathfrak{p}$ of $\operatorname{Supp}(M)$), and has no embedded prime (every element of $\operatorname{Ass}(M)$ is minimal in $\operatorname{Supp}(M)$).*

Lemma 6.1.6. *Let $(x_1, \cdots, x_n)$ be an M-regular sequence. Then $M/\{x_1, \cdots, x_n\}M$ is Cohen-Macaulay if and only if M is so.*

Proof. We have by Corollary 5.2.3

$$\operatorname{depth} M/\{x_1, \cdots, x_n\}M = \operatorname{depth} M - n,$$

and by Proposition 5.1.4

$$\dim M/\{x_1, \cdots, x_n\}M = \dim M - n.$$ □

Proposition 6.1.7. *The following conditions are equivalent:*

(i) M is Cohen-Macaulay.
(ii) A sequence is secant for M if and only if it is M-regular.

Proof. (i) $\Rightarrow$ (ii): We proceed by induction on the length of the sequence, the case of the empty sequence being clear. Let $(x_1, \cdots, x_n)$ be a secant sequence. Then $\dim M/x_1M = \dim M - 1$, hence x_1 belongs to no $\mathfrak{p} \in \operatorname{Supp}(M)$ such that $\dim A/\mathfrak{p} = \dim M$ by Proposition 2.3.4, hence to no associated prime of M by Proposition 6.1.4. Thus x_1 is a nonzerodivisor in M (Lemma 1.2.9), and M/x_1M is Cohen-Macaulay by Lemma 6.1.6. By induction, the sequence $(x_2, \cdots, x_n)$ is M/x_1M-regular, hence the sequence $(x_1, \cdots, x_n)$ is M-regular.

(ii) $\Rightarrow$ (i): Let $n = \dim M$ and $\{x_1, \cdots, x_n\}$ a system of parameters for M. Then the sequence $(x_1, \cdots, x_n)$ is M-regular by (ii), hence $n \leq \operatorname{depth} M$ by Corollary 5.2.3, proving that M is Cohen-Macaulay. $\square$

Theorem 6.1.8 (Unmixedness theorem). *The following conditions are equivalent:*

(i) M is Cohen-Macaulay.
(ii) For every secant set S for M, the A-module M/SM has no embedded prime.

Proof. Assume that M is Cohen-Macaulay, and let $S = \{s_1, \cdots, s_n\}$ be a secant set. Then $(s_1, \cdots, s_n)$ is an M-regular sequence by Proposition 6.1.7, hence M/SM is Cohen-Macaulay by Lemma 6.1.6, and has no embedded prime by Corollary 6.1.5.

Conversely assume that for every secant subset S of A, the A-module M/SM has no embedded prime. We proceed by induction on $\dim M$, the cases $M = 0$ and $\dim M = 0$ being trivial. We thus assume that $\dim M > 0$. Taking $S = \varnothing$, we see that M has no embedded prime. The prime $\mathfrak{m}$ is not a minimal element of $\operatorname{Supp}(M)$ (because $\dim M > 0$), and therefore $\mathfrak{m} \notin \operatorname{Ass}(M)$. Thus by Lemma 5.2.4, we can find an element $x \in \mathfrak{m}$ which is a nonzerodivisor in M. Then $\dim M/xM < \dim M$ by Corollary 2.3.5. If S is a secant subset for M/xM, then $\{x\} \cup S$ is a secant subset for M; it follows that the A-module M/xM satisfies the condition of the theorem. By induction it is Cohen-Macaulay, hence M is Cohen-Macaulay by Lemma 6.1.6. $\square$

Lemma 6.1.9. *Let $A \to B$ be a local morphism. Let M be a B-module, finitely generated as an A-module. Then M is Cohen-Macaulay as an A-module if and only if it is so as a B-module.*

Proof. This follows from Proposition 5.3.1 and Proposition 2.1.3. $\square$

Proposition 6.1.10. *Let $A \to B$ be a local morphism, and M a nonzero finitely generated A-module. Let k be the residue field of A. Assume that B is flat over A.*

Then the B-module $B \otimes_A M$ is Cohen-Macaulay if and only if the A-module M and the B-module $B \otimes_A k$ are Cohen-Macaulay.

Proof. This follows from Proposition 2.4.6, Proposition 5.3.3 and Corollary 5.2.7. $\square$

2. Cohen-Macaulay rings

Lemma 6.2.1. *Let R be a ring, and M an R-module. For any $\mathfrak{p} \in \operatorname{Spec}(R)$ we have*

$$\dim_R M \geq \dim_{R_\mathfrak{p}} M_\mathfrak{p} + \dim R/\mathfrak{p}.$$

Proof. We may assume that $\mathfrak{p} \in \operatorname{Supp}(M)$. A chain of primes of $R/\mathfrak{p}$ corresponds to a chain of primes of R containing in $\mathfrak{p}$, and thus in $\operatorname{Supp}(M)$. A chain of primes in $\operatorname{Supp}_{R_\mathfrak{p}}(M_\mathfrak{p})$ corresponds to a chain of primes in $\operatorname{Supp}(M)$ contained in $\mathfrak{p}$. The concatenation of the two chains gives a chain in $\operatorname{Supp}(M)$, whose length is the sum of the two lengths. □

Proposition 6.2.2. *Let A be a local ring and M a Cohen-Macaulay A-module. Then:*

(i) For every $\mathfrak{p} \in \operatorname{Spec}(A)$, the $A_\mathfrak{p}$-module $M_\mathfrak{p}$ is Cohen-Macaulay.

(ii) For every $\mathfrak{p} \in \operatorname{Supp}(M)$, we have

$$\dim_A M = \dim_{A_\mathfrak{p}} M_\mathfrak{p} + \dim A/\mathfrak{p}.$$

Proof. If $\mathfrak{p} \notin \operatorname{Supp}(M)$, then $M_\mathfrak{p} = 0$ is a Cohen-Macaulay $A_\mathfrak{p}$-module. Assume that $\mathfrak{p} \in \operatorname{Supp}(M)$. By Proposition 5.2.9 and Lemma 6.2.1, we have

$$\operatorname{depth}_{A_\mathfrak{p}} M_\mathfrak{p} + \dim A/\mathfrak{p} \geq \operatorname{depth}_A M = \dim_A M \geq \dim_{A_\mathfrak{p}} M_\mathfrak{p} + \dim A/\mathfrak{p}.$$

Since $\operatorname{depth}_{A_\mathfrak{p}} M_\mathfrak{p} \leq \dim_{A_\mathfrak{p}} M_\mathfrak{p}$ by Corollary 5.2.7, these inequalities must be equalities, whence the statements. □

Definition 6.2.3. A ring R is called *Cohen-Macaulay* if for every $\mathfrak{p} \in \operatorname{Spec}(R)$ the $R_\mathfrak{p}$-module $R_\mathfrak{p}$ is Cohen-Macaulay.

From Proposition 6.2.2 (i) we deduce:

Corollary 6.2.4. *A ring R is Cohen-Macaulay if and only if the $R_\mathfrak{m}$-module $R_\mathfrak{m}$ is Cohen-Macaulay for every maximal ideal $\mathfrak{m}$ of R.*

Proposition 6.2.5. *A regular local ring is Cohen-Macaulay.*

Proof. Let A be a regular local ring with maximal ideal $\mathfrak{m}$. We proceed by induction on $\dim A$. Any ring of dimension zero is Cohen-Macaulay. If $\dim A > 0$, then we can find $x \in \mathfrak{m} - \mathfrak{m}^2$ by Corollary 3.1.5 (or directly by Nakayama's Lemma 1.1.6). Then A/xA is a regular local ring of dimension $< \dim A$ by Lemma 3.2.4, so is a Cohen-Macaulay ring by induction. Therefore A/xA is Cohen-Macaulay as an A/xA-module, hence as an A-module by Lemma 6.1.9. Since A is a domain by Proposition 3.2.6, the nonzero element x is a nonzerodivisor in A. By Lemma 6.1.6, it follows that A is Cohen-Macaulay as an A-module, hence is a Cohen-Macaulay ring by Corollary 6.2.4. □

Proposition 6.2.6. *Let $\rho\colon R \to S$ be a flat ring morphism. Assume that the ring R is Cohen-Macaulay and that for every prime $\mathfrak{p}$ of R, the ring $S \otimes_R \kappa(\mathfrak{p})$ is Cohen-Macaulay. Then the ring S is Cohen-Macaulay.*

Proof. Let $\mathfrak{q} \in \operatorname{Spec}(S)$, and $\mathfrak{p} = \rho^{-1}\mathfrak{q}$. By assumption $(S \otimes_R \kappa(\mathfrak{p}))_\mathfrak{q} = S_\mathfrak{q} \otimes_{R_\mathfrak{p}} \kappa(\mathfrak{p})$ is Cohen-Macaulay as a module over itself, and therefore as an $S_\mathfrak{q}$-module by Lemma 6.1.9. Thus the conditions of Proposition 6.1.10 are satisfied with $A = M = R_\mathfrak{p}$ and $B = S_\mathfrak{q}$, hence $S_\mathfrak{q}$ is Cohen-Macaulay as a module over itself. □

Proposition 6.2.7. *If the ring R is Cohen-Macaulay, then so is $R[t_1, \cdots, t_n]$.*

Proof. By induction it suffices to consider the case $n = 1$. By Proposition 6.2.6, we may assume that R is a field. Let A be the localisation of the ring $R[t_1]$ at a maximal ideal. Then A is an integral domain of dimension one. The only associated prime of A is the zero ideal, which differs from its maximal ideal. Hence $\operatorname{depth} A \geq 1 = \dim A$ by

Lemma 5.2.4, and the ring A is Cohen-Macaulay. It follows from Corollary 6.2.4 that the ring $R[t_1]$ is Cohen-Macaulay. $\square$

3. Catenary rings

Definition 6.3.1. We say that a chain of primes $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ is *saturated* if there is no prime $\mathfrak{q}$ and integer i such that $\mathfrak{p}_{i-1} \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}_i$.

We say that a ring R is *catenary* if for every pair of primes $\mathfrak{p} \subset \mathfrak{q}$ of R, all saturated chains joining $\mathfrak{p}$ to $\mathfrak{q}$ have the same length.

Lemma 6.3.2. *A quotient, or a localisation, of a catenary ring is catenary.*

Proof. This follows from the description of the primes of a quotient or a localisation. $\square$

Lemma 6.3.3. *If for every pair of primes $\mathfrak{p} \subset \mathfrak{q}$ of a ring R we have*

$$\dim R_{\mathfrak{q}} = \dim R_{\mathfrak{p}} + \dim(R_{\mathfrak{q}}/\mathfrak{p}R_{\mathfrak{q}}),$$

then R is catenary.

Proof. Let $\mathfrak{p} \subset \mathfrak{q}$ be a pair of primes of R. Let $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ a saturated chain of primes of R, with $\mathfrak{p}_0 = \mathfrak{p}$ and $\mathfrak{p}_n = \mathfrak{q}$. In order to prove the proposition, it will suffice to prove that $n = \dim(R_{\mathfrak{q}}/\mathfrak{p}R_{\mathfrak{q}})$. For each $i = 1, \cdots, n$ we have $\dim(R_{\mathfrak{p}_i}/\mathfrak{p}_{i-1}R_{\mathfrak{p}_i}) = 1$. Using the condition of the lemma for the pair $\mathfrak{p}_{i-1} \subset \mathfrak{p}_i$, we obtain

$$\dim R_{\mathfrak{p}_i} = \dim R_{\mathfrak{p}_{i-1}} + 1.$$

This gives by induction

$$\dim R_{\mathfrak{q}} = \dim R_{\mathfrak{p}} + n.$$

Now we use the condition for the pair $\mathfrak{p} \subset \mathfrak{q}$, and get

$$\dim R_{\mathfrak{p}} = \dim R_{\mathfrak{q}} + \dim(R_{\mathfrak{q}}/\mathfrak{p}R_{\mathfrak{q}}).$$

Therefore $\dim(R_{\mathfrak{q}}/\mathfrak{p}R_{\mathfrak{q}}) = n$. $\square$

Proposition 6.3.4. *A Cohen-Macaulay ring is catenary.*

Proof. Let $\mathfrak{p} \subset \mathfrak{q}$ be two primes of a Cohen-Macaulay ring R. The ring $R_{\mathfrak{q}}$ is Cohen-Macaulay by assumption. Applying Proposition 6.2.2 (ii) with $A = M = R_{\mathfrak{q}}$, for the prime $\mathfrak{p}R_{\mathfrak{q}} \in \operatorname{Supp}(R_{\mathfrak{q}})$, we obtain precisely the condition appearing in Lemma 6.3.3. $\square$

Proposition 6.3.5. *Any finitely generated algebra over a Cohen-Macaulay ring is catenary.*

Proof. Let S a be finitely generated algebra over a Cohen-Macaulay ring R. Then S is a quotient of the ring $R[t_1, \cdots, t_n]$ for some n. The latter ring is Cohen-Macaulay by Proposition 6.2.7, hence catenary by Proposition 6.3.4. It follows that S is catenary by Lemma 6.3.2. $\square$

Example 6.3.6. Any finitely generated k-algebra (k a field), or any finitely generated $\mathbb{Z}$-algebra, is catenary.

CHAPTER 7

Normal rings

In this chapters section R is a (noetherian commutative unital) ring.

1. Reduced rings

LEMMA 7.1.1. *Let A be a reduced local ring such that* $\operatorname{depth} A = 0$*. Then A is a field.*

PROOF. The maximal ideal $\mathfrak{m}$ is an associated prime of A (Lemma 5.2.4), hence $\mathfrak{m} = \operatorname{Ann}(u)$ for some $u \in A - 0$. If A is not a field, then $\mathfrak{m} \neq 0$, hence u is a zerodivisor in A. In particular u is not invertible, and so belongs to $\mathfrak{m}$. But then $u^2 = 0$. ☐

LEMMA 7.1.2. *Let N be an R-submodule of M. If $N_{\mathfrak{p}} = 0$ for every $\mathfrak{p} \in \operatorname{Ass}(M)$, then $N = 0$.*

PROOF. Let $\mathfrak{p} \in \operatorname{Ass}(N)$. Then $\mathfrak{p} \in \operatorname{Ass}(M)$ by Proposition 1.2.5, hence by assumption $N_{\mathfrak{p}} = 0$, so that $\mathfrak{p} \notin \operatorname{Supp}(N)$, a contradiction with Corollary 1.3.2. Hence $\operatorname{Ass}(N) = \varnothing$, and $N = 0$ by Corollary 1.2.3. ☐

PROPOSITION 7.1.3. *The following conditions are equivalent:*

(i) The ring R is reduced.
(ii) For every $\mathfrak{p} \in \operatorname{Ass}(R)$, the ring $R_{\mathfrak{p}}$ is a field.
(iii) For every prime $\mathfrak{p}$, the ring $R_{\mathfrak{p}}$ is reduced or has depth ≥ 1.

PROOF. (i) $\Rightarrow$ (ii): We apply Lemma 7.1.1.
(ii) $\Rightarrow$ (iii): A field is reduced.
(iii) $\Rightarrow$ (i): The set N of nilpotent elements of R is an ideal of R. We apply Lemma 7.1.2 to the submodule $N \subset M = R$. ☐

PROPOSITION 7.1.4. *A reduced ring has no embedded prime.*

PROOF. Let R be a reduced ring. If $\mathfrak{p} \subsetneq \mathfrak{q}$ are elements of $\operatorname{Ass}(R)$, then $\dim R_{\mathfrak{q}} > 0$ and $R_{\mathfrak{q}}$ is a field by Lemma 7.1.1, a contradiction. ☐

EXAMPLE 7.1.5. Let R be a reduced ring of dimension ≤ 1. Then the ring R is Cohen-Macaulay. To see this, we may assume that R is local. If $\operatorname{depth} R = 0$, then $\dim R = 0$ by Lemma 7.1.1. If $\operatorname{depth} R > 0$, then $\operatorname{depth} R \geq 1 = \dim R$.

2. Locally integral rings

LEMMA 7.2.1. *Let R be a reduced ring with exactly one minimal prime $\mathfrak{p}$. Then R is an integral domain.*

PROOF. We have $\operatorname{Ass}(R) = \{\mathfrak{p}\}$ by Proposition 7.1.4, hence $R - \mathfrak{p}$ consists of nonzerodivisors (Lemma 1.2.9), and therefore the localisation morphism $R \to R_{\mathfrak{p}}$ is injective. Since $R_{\mathfrak{p}}$ is a field by Lemma 7.1.1, its subring R is an integral domain. ☐

Remark 7.2.2. Let M be a finitely generated R-module. We say that M is *reduced* if for every $\mathfrak{p} \in \operatorname{Ass}(M)$ the $R_{\mathfrak{p}}$-module $M_{\mathfrak{p}}$ is simple (i.e. $\operatorname{length}_{R_{\mathfrak{p}}} M_{\mathfrak{p}} = 1$). We say that M is *integral* if it is reduced and has exactly one associated (or equivalently, minimal) prime.

Then a ring is reduced, resp. an integral domain, if and only if it is reduced, resp. integral, as a module over itself.

Lemma 7.2.3. *Let $f : M \to N$ be a morphism of finitely generated R-modules.*

(i) If $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective for every $\mathfrak{p}$ such that $\operatorname{depth}_{R_{\mathfrak{p}}} M_{\mathfrak{p}} = 0$*, then f is injective.*

(ii) If $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is bijective for every $\mathfrak{p}$ such that $\operatorname{depth}_{R_{\mathfrak{p}}} N_{\mathfrak{p}} = 0$ *or* $\operatorname{depth}_{R_{\mathfrak{p}}} M_{\mathfrak{p}} \leq 1$*, then f is bijective.*

Proof. (i) : Apply Lemma 7.1.2 to the submodule $\ker f \subset M$.

(ii) : We know by (i) that f is injective. Let $Q = \operatorname{coker} f$, and $\mathfrak{p} \in \operatorname{Ass}(Q)$. Then we have an exact sequence of $R_{\mathfrak{p}}$-modules (Proposition 4.5.4)

$$\operatorname{Hom}(\kappa(\mathfrak{p}), N_{\mathfrak{p}}) \to \operatorname{Hom}(\kappa(\mathfrak{p}), Q_{\mathfrak{p}}) \to \operatorname{Ext}^1(\kappa(\mathfrak{p}), M_{\mathfrak{p}}).$$

Since $Q_{\mathfrak{p}} \neq 0$, the morphism $f_{\mathfrak{p}}$ is not surjective, hence by our assumptions, the modules on the left and right of the sequence above vanish, hence so does the module in the middle. Thus $\mathfrak{p}R_{\mathfrak{p}} \notin \operatorname{Ass}_{R_{\mathfrak{p}}}(Q_{\mathfrak{p}})$, hence $\mathfrak{p} \notin \operatorname{Ass}(Q)$ by Proposition 1.2.10. Thus $\operatorname{Ass}(Q) = \varnothing$, and $Q = 0$ by Corollary 1.2.3. □

Definition 7.2.4. Let R be a ring, and S a subset of $\operatorname{Spec}(R)$. A subset of S is *closed* if its is of the form $S \cap \operatorname{Supp}(M)$, where M is a finitely generated R-module. We say that S is *connected* if it cannot be written as the disjoint union of two non-empty closed subsets.

Remark 7.2.5. One can check that this defines a topology on $\operatorname{Spec}(R)$, the *Zariski topology*. We will not use this remark.

Lemma 7.2.6. *If there are ideals $J_0, J_1 \neq R$ such that the diagonal ring morphism $f : R \to R/J_0 \times R/J_1$ is bijective, then* $\operatorname{Spec}(R)$ *is not connected.*

Proof. We have $J_0 \cap J_1 = \ker f = \{0\}$. It follows that every prime contains the product ideal $J_0 J_1$, hence one of the ideals J_i for $i \in \{0, 1\}$. This proves that $\operatorname{Supp}(R/J_0) \cup \operatorname{Supp}(R/J_1) = \operatorname{Spec}(R)$. Using the surjectivity of f, we find $x \in R$ such that $x - 1 \in J_0$ and $x \in J_1$. Thus $1 \in J_0 + J_1$, so that no prime contains both J_0 and J_1. Therefore $\operatorname{Supp}(R/J_0) \cap \operatorname{Supp}(R/J_1) = \varnothing$. □

Remark 7.2.7. The converse of Lemma 7.2.6 is true and can be deduced from the proof of Theorem 7.2.9.

Lemma 7.2.8. *The spectrum of a local ring is connected.*

Proof. Since the maximal ideal contains every prime, it is an element of every non-empty closed subset of the spectrum. Thus the latter cannot decompose as a disjoint union of non-empty closed subsets. □

Theorem 7.2.9 (Hartshorne). *Let $(A, \mathfrak{m})$ be a local ring of depth ≥ 2. Then* $\operatorname{Spec}(A) - \{\mathfrak{m}\}$ *is connected.*

PROOF. Assume that $\mathrm{Spec}(A) - \{\mathfrak{m}\}$ is not connected. Then we can find two subsets F_0 and F_1 closed in $\mathrm{Spec}(A)$, such that $F_0 \cap F_1 \subset \{\mathfrak{m}\}$ and $\mathrm{Spec}(A) - \{\mathfrak{m}\} \subset F_1 \cup F_0$. The set $\mathrm{Ass}(A)$ does not contain $\mathfrak{m}$ by assumption, hence decomposes as the disjoint union of $\mathrm{Ass}(A) \cap F_0$ and $\mathrm{Ass}(A) \cap F_1$. By Proposition 1.2.7, we can find for each $i \in \{0,1\}$ an ideal J_i such that

$$\mathrm{Ass}_A(A/J_i) = \mathrm{Ass}(A) \cap F_i \text{ and } \mathrm{Ass}_A(J_i) = \mathrm{Ass}(A) \cap F_{1-i}.$$

The subset F_i contains $\mathrm{Ass}_A(A/J_i)$ and $\mathrm{Ass}_A(J_{1-i})$. Since it is closed, it contains $\mathrm{Supp}_A(A/J_i)$ and $\mathrm{Supp}_A(J_{1-i})$. In particular $J_{1-i} \neq A$ (as $F_i \neq \mathrm{Spec}(A)$).

Consider the diagonal ring morphism $f\colon A \to A/J_0 \times A/J_1 = N$. Let $\mathfrak{p} \in \mathrm{Spec}(A)$ be such that $\mathfrak{p} \neq \mathfrak{m}$. Then there is $i \in \{0,1\}$ such that $\mathfrak{p} \notin F_i$. Thus $\mathfrak{p} \notin \mathrm{Supp}(A/J_i)$ and $\mathfrak{p} \notin \mathrm{Supp}(J_{1-i})$, and we deduce that the morphism $f_\mathfrak{p}$ is bijective. In particular, this is so when $\operatorname{depth}_{A_\mathfrak{p}} N_\mathfrak{p} = 0$ (because $\mathrm{Ass}(N) \subset \mathrm{Ass}(A)$ by Proposition 1.2.5, and $\mathfrak{m} \notin \mathrm{Ass}(A)$ by assumption), or when $\operatorname{depth} A_\mathfrak{p} \leq 1$ (by assumption). It follows from Lemma 7.2.3 (ii) that f is bijective, hence $\mathrm{Spec}(A)$ is not connected by Lemma 7.2.6. This contradicts Lemma 7.2.8. □

DEFINITION 7.2.10. A ring R is *locally integral* if the ring $R_\mathfrak{p}$ is an integral domain for every $\mathfrak{p} \in \mathrm{Spec}(R)$.

PROPOSITION 7.2.11. *The following conditions are equivalent:*

(i) The ring R is locally integral.

(ii) For every $\mathfrak{p} \in \mathrm{Spec}(R)$, the ring $R_\mathfrak{p}$ is an integral domain or has depth ≥ 2.

PROOF. (i) $\Rightarrow$ (ii) : Clear.

(ii) $\Rightarrow$ (i): We assume that R is local, and show that R is an integral domain. We know that R is reduced by Proposition 7.1.3, so it will suffice to prove that R has a unique minimal prime by Lemma 7.2.1. Assuming the contrary, the set of minimal primes decomposes as the disjoint union of two non-empty subsets M_0 and M_1. For $i \in \{0,1\}$, let $Q_i = R/J_i$ be a quotient of R such that $\mathrm{Ass}_R(Q_i) = M_i$ (Proposition 1.2.7). If $\mathfrak{q} \in \mathrm{Spec}(R)$, then $\mathfrak{q}$ contains a minimal prime, and therefore an element of $\mathrm{Ass}_R(Q_i)$ for some $i \in \{0,1\}$. It follows that $\mathfrak{q} \in \mathrm{Supp}_R(Q_i)$. Thus we have $\mathrm{Spec}(R) = \mathrm{Supp}_R(Q_0) \cup \mathrm{Supp}_R(Q_1)$. The set $\mathrm{Supp}_R(Q_0) \cap \mathrm{Supp}_R(Q_1)$ is non-empty (see Lemma 7.2.8; namely it contains the maximal ideal); let $\mathfrak{p}$ be a minimal element of this set (i.e. a prime minimal over $J_0 + J_1$), and write $X_i = \mathrm{Supp}_{R_\mathfrak{p}}((Q_i)_\mathfrak{p})$ for $i \in \{0,1\}$. If we view $\mathrm{Spec}(R_\mathfrak{p})$ as a subset of $\mathrm{Spec}(R)$, then $X_i = \mathrm{Supp}_R(Q_i) \cap \mathrm{Spec}(R_\mathfrak{p})$, hence

$$\mathrm{Spec}(R_\mathfrak{p}) = X_0 \cup X_1 \text{ and } X_0 \cap X_1 = \{\mathfrak{p}R_\mathfrak{p}\}.$$

Since $\mathfrak{p} \in \mathrm{Supp}(Q_0) \cap \mathrm{Supp}(Q_1)$, it is not a minimal prime of R, hence $X_i - \{\mathfrak{p}R_\mathfrak{p}\}$ contains M_i, and in particular is not empty. This gives a decomposition of the set $\mathrm{Spec}(R_\mathfrak{p}) - \{\mathfrak{p}R_\mathfrak{p}\}$ as the disjoint union of two non-empty closed subsets. By Theorem 7.2.9 we have $\operatorname{depth} R_\mathfrak{p} \leq 1$, hence by assumption the ring $R_\mathfrak{p}$ is an integral domain. In particular $\mathfrak{p}$ contains exactly one minimal prime of R. But for each $i \in \{0,1\}$, we have $\mathfrak{p} \in \mathrm{Supp}_R(Q_i)$, hence $\mathfrak{p}$ contains an element of M_i, a contradiction. □

3. Normal rings

DEFINITION 7.3.1. A ring is an *integrally closed domain* if it is an integral domain, and coincides with its integral closure in its fraction field. We say that a ring R is *normal* if the ring $R_\mathfrak{p}$ is an integrally closed domain for every $\mathfrak{p} \in \mathrm{Spec}(R)$.

Lemma 7.3.2. *Let A be a local integrally closed domain such that* $\operatorname{depth} A = 1$. *Then A is a discrete valuation ring.*

Proof. Let $\mathfrak{m}$ be the maximal ideal of A. Since $\mathfrak{m} \notin \operatorname{Ass}(A)$, we can find a nonzerodivisor $x \in \mathfrak{m}$. Then $\operatorname{depth}_A A/xA = 0$ by Proposition 5.2.2, hence $\mathfrak{m} \in \operatorname{Ass}_A(A/xA)$. Therefore there is an element $a \in A$ such that $a \notin xA$ and $a\mathfrak{m} \subset xA$. We let K be the fraction field of A and $t = ax^{-1} \in K$, and consider the A-submodule T of K generated by t. Then $\mathfrak{m}T \subset A$ is an ideal of A.

Assume that $\mathfrak{m}T \subset \mathfrak{m}$. Then we see by induction that for all $n \in \mathbb{N}$, the element $u_n = t^n x$ belongs to $\mathfrak{m}$. Since A is noetherian, for n large enough the element u_n is an A-linear combination of the elements u_i for $i < n$. This gives a unital polynomial p with coefficients in A such that $p(t)x = 0$ in K. Since x is invertible in K, it follows that $p(t) = 0$, showing that t is integral over A. Since A is integrally closed in K, we have $t \in A$, contradicting the choice of a.

So $\mathfrak{m}T = A$, and there is $u \in \mathfrak{m}$ such that $ut = 1$. Then

$$\mathfrak{m} = (ut)\mathfrak{m} = u(t\mathfrak{m}) \subset u(\mathfrak{m}T) = uA.$$

So $\mathfrak{m} = uA$. Moreover u is a nonzerodivisor in A, since $ua = x$ is one. This proves that A is a discrete valuation ring. $\square$

Example 7.3.3. Let R be a normal ring of dimension ≤ 2. Then R is Cohen-Macaulay. Indeed we may assume that R is local, and is an integrally closed domain. If $\operatorname{depth} R = 0$, then $\dim R = 0$ by Lemma 7.1.1. If $\operatorname{depth} R = 1$, then $\dim R = 1$ by Lemma 7.3.2. Otherwise $\operatorname{depth} R \geq 2 = \dim R$, so that in any case R is Cohen-Macaulay

Theorem 7.3.4 (Serre). *The following conditions are equivalent:*

(i) The ring R is normal.
(ii) Let $\mathfrak{p} \in \operatorname{Spec}(R)$. If $\operatorname{depth} R_{\mathfrak{p}} = 0$, *then the ring $R_{\mathfrak{p}}$ is a field. If* $\operatorname{depth} R_{\mathfrak{p}} = 1$, *then the ring $R_{\mathfrak{p}}$ is a discrete valuation ring.*
(iii) For every $\mathfrak{p} \in \operatorname{Spec}(R)$, the ring $R_{\mathfrak{p}}$ is an integrally closed domain or has depth ≥ 2.

Proof. (i) $\Rightarrow$ (ii): This follows from Lemma 7.1.1 and Lemma 7.3.2.

(ii) $\Rightarrow$ (iii): Fields and discrete valuation rings are integrally closed domains.

(iii) $\Rightarrow$ (i): We may assume that the ring R is local, and prove that it is an integrally closed domain. The ring R is an integral domain by Proposition 7.2.11. Let R' be the integral closure of R in its function field, and $\mathfrak{p} \in \operatorname{Spec}(R)$. If $\operatorname{depth} R_{\mathfrak{p}} \leq 1$, then the morphism $R_{\mathfrak{p}} \to R'_{\mathfrak{p}}$ is bijective because $R_{\mathfrak{p}}$ is integrally closed (integral closure commutes with localisation). On the hand R' is an integral domain containing R, hence $\operatorname{Ass}_R(R') = \{0\}$. Thus if $\operatorname{depth}_{R_{\mathfrak{p}}} R'_{\mathfrak{p}} = 0$, then $\mathfrak{p} = 0 \in \operatorname{Ass}(R)$, hence $\operatorname{depth} R_{\mathfrak{p}} \leq 1$, so that we are in the case considered above. It follows from Lemma 7.2.3 that $R = R'$, hence R is an integrally closed domain. $\square$

Definition 7.3.5. Let n be an integer n. We consider the following conditions on a ring R.

(Rn) : For every prime $\mathfrak{p}$ of height $\leq n$, the local ring $R_{\mathfrak{p}}$ is regular.

(Sn) : For every prime $\mathfrak{p}$, we have $\operatorname{depth} R_{\mathfrak{p}} \geq \min(\operatorname{height} \mathfrak{p}, n)$.

We have proved

Proposition 7.3.6. *Let R be a ring. Then:*

(i) R reduced $\iff$ R satisfies (R0) and (S1).

(ii) R normal $\iff$ R satisfies $(R1)$ and $(S2)$.

If R is a Cohen-Macaulay ring, then for every $\mathfrak{p}$, we have $\operatorname{height}\mathfrak{p} = \operatorname{depth} R_{\mathfrak{p}}$, so that R satisfies the condition $(\mathrm{S}n)$ for every n. Thus we obtain:

Proposition 7.3.7. *A Cohen-Macaulay ring R is*

(i) reduced if and only if the ring $R_{\mathfrak{p}}$ is so for every minimal prime $\mathfrak{p}$,
(ii) locally integral if and only if the ring $R_{\mathfrak{p}}$ is so for every prime $\mathfrak{p}$ of height ≤ 1,
(iii) normal if and only if the ring $R_{\mathfrak{p}}$ is so for every prime $\mathfrak{p}$ of height ≤ 1.

CHAPTER 8

Projective dimension

In this chapter $(A, \mathfrak{m}, k)$ is a local commutative noetherian ring.

1. Projective dimension over a local ring

PROPOSITION 8.1.1. *Let M be a finitely generated A-module. The following conditions are equivalent:*

(i) *M is free.*
(ii) *M is projective.*
(iii) *M is flat.*
(iv) $\mathrm{Tor}_1(M, k) = 0$.
(v) $\mathrm{Ext}^1(M, k) = 0$

PROOF. We have (i) $\Rightarrow$(ii) $\Rightarrow$(iii) $\Rightarrow$ (iv) and (ii) $\Rightarrow$ (v).

Let $m_1, \cdots, m_n$ be elements of M giving modulo $\mathfrak{m}M$ a k-basis of $M/\mathfrak{m}M$. This gives a morphism $\varphi\colon A^n \to M$, which is surjective by Nakayama's Lemma 1.1.6. Let Q be its kernel. We have an exact sequence

$$\mathrm{Tor}_1(M, k) \to Q \otimes_A k \to A^n \otimes_A k \xrightarrow{\varphi \otimes_A k} M \otimes_A k \to 0.$$

If $\mathrm{Tor}_1(M, k) = 0$, since $\varphi \otimes_A k$ is injective, we obtain $Q \otimes_A k = 0$, hence $Q = 0$ by Nakayama's Lemma 1.1.6. This proves (iv) $\Rightarrow$ (i).

We also have an exact sequence

$$0 \to \mathrm{Hom}_A(M, k) \xrightarrow{\varphi^*} \mathrm{Hom}_A(A^n, k) \to \mathrm{Hom}_A(Q, k) \to \mathrm{Ext}^1_A(M, k).$$

The morphism φ^* decomposes as a sequence of isomorphisms

$$\mathrm{Hom}_A(M, k) \to \mathrm{Hom}_k(M \otimes_A k, k) \xrightarrow{(\varphi \otimes_A k)^*} \mathrm{Hom}_k(A^n \otimes_A k, k) \to \mathrm{Hom}_A(A^n, k)$$

hence is an isomorphism. Thus if $\mathrm{Ext}^1_A(M, k) = 0$, then $0 = \mathrm{Hom}_A(Q, k) = \mathrm{Hom}_k(Q \otimes_A k, k)$, hence $Q \otimes_A k = 0$, and finally $Q = 0$ by Nakayama's Lemma 1.1.6. This proves (v) $\Rightarrow$ (i). $\square$

DEFINITION 8.1.2. Let R be a commutative unital ring. The *projective dimension* of an R-module M, denoted $\mathrm{projdim}_R M \in \mathbb{N} \cup \{-\infty, \infty\}$, is defined as the infimum of the lengths n of the finite projective resolutions $0 \to L_n \to \cdots \to L_0 \to M \to 0$ of M if $M \neq 0$, and as $-\infty$ if $M = 0$.

Since the functors Ext and Tor may be computed using any projective resolution of M, we see that

$$\mathrm{Tor}_n(M, -) = \mathrm{Ext}^n(M, -) = 0 \ \text{ when } \ n > \mathrm{projdim}_R M.$$

Proposition 8.1.3. *Let M be a finitely generated A-module and n an integer. The following conditions are equivalent:*

(i) $\operatorname{projdim} M \leq n$.
(ii) $\operatorname{Tor}_{n+1}(M, k) = 0$.
(iii) $\operatorname{Ext}^{n+1}(M, k) = 0$.
(iv) Let $0 \to L_n \to \cdots \to L_0 \to M \to 0$ be an exact sequence with and L_i projective for $i = 0, \cdots, n-1$. Then L_n is projective.

Proof. It is clear that (ii) $\Leftarrow$ (i) $\Rightarrow$ (iii) and that (iv) $\Rightarrow$ (i).

Let us now prove (iv) using (ii) or (iii). Let $Z_i = \operatorname{im}(L_i \to L_{i-1})$ for $i = 1, \cdots, n-1$, and let $Z_0 = M$ and $Z_n = L_n$. We have exact sequences, for $i = 0, \cdots, n-1$,

$$0 \to Z_{i+1} \to L_i \to Z_i \to 0,$$

giving exact sequences (Proposition 4.5.3)

$$\operatorname{Ext}^j(L_i, k) \to \operatorname{Ext}^j(Z_{i+1}, k) \to \operatorname{Ext}^{j+1}(Z_i, k) \to \operatorname{Ext}^{j+1}(L_i, k)$$

and (Proposition 4.3.3)

$$\operatorname{Tor}_{j+1}(L_i, k) \to \operatorname{Tor}_{j+1}(Z_i, k) \to \operatorname{Tor}_j(Z_{i+1}, k) \to \operatorname{Tor}_j(L_i, k).$$

Since for $j > 0$ the four extreme modules vanish, we obtain

$$\operatorname{Ext}^j(Z_{i+1}, k) \simeq \operatorname{Ext}^{j+1}(Z_i, k) \text{ and } \operatorname{Tor}_{j+1}(Z_i, k) \simeq \operatorname{Tor}_j(Z_{i+1}, k),$$

and we conclude that

$$\operatorname{Ext}^1(L_n, k) \simeq \operatorname{Ext}^{n+1}(M, k) \text{ and } \operatorname{Tor}_1(L_n, k) \simeq \operatorname{Tor}_{n+1}(M, k),$$

so that L_n is free by Proposition 8.1.1 under the assumption (ii) or (iii). □

Corollary 8.1.4. *Let M, M' be two finitely generated A-modules. Then*

$$\operatorname{projdim}(M \oplus M') = \max(\operatorname{projdim} M, \operatorname{projdim} M').$$

We will use the following technical lemma in the next proof.

Lemma 8.1.5. *Let R be a commutative ring. Consider an exact sequence of R-modules*

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \xrightarrow{f_3} M_4,$$

and let $x \in R$ be a nonzerodivisor in M_4. Then the sequence of R/xR-modules

$$M_1/xM_1 \to M_2/xM_2 \to M_3/xM_3$$

is exact.

Proof. The sequence is clearly a complex. Let $m_2 \in M_2$ and assume that $f_2(m_2) = xm_3$ for some $m_3 \in M_3$. We have $xf_3(m_3) = f_3 \circ f_2(m_2) = 0$. Since x is a nonzerodivisor in M_4, it follows that $f_3(m_3) = 0$, hence $m_3 = f_2(m_2')$ for some $m_2' \in M_2$. Therefore $m_2 - xm_2' = f_1(m_1)$ with $m_1 \in M_1$. This proves the statement. □

Proposition 8.1.6. *Let M be a finitely generated A-module, and $x \in \mathfrak{m}$ be a nonzerodivisor in M and in A. We have, for every n, isomorphisms of A-modules*

$$\operatorname{Tor}_n^{A/xA}(M/xM, k) \simeq \operatorname{Tor}_n^A(M, k) \quad \text{and} \quad \operatorname{Ext}^n_{A/xA}(M/xM, k) \simeq \operatorname{Ext}^n_A(M, k).$$

In particular

$$\operatorname{projdim}_{A/xA} M/xM = \operatorname{projdim}_A M.$$

Proof. Let $L \to M$ be a (possibly infinite) free resolution of the A-module M (Proposition 4.2.6). The A/xA-modules $L_n/xL_n = L_n \otimes_A (A/xA)$ are free, and fit into the complex of A/xA-modules $L/xL = L \otimes_A (A/xA)$. For every n, the element x is a nonzerodivisor in L_n and in M, hence $L/xL \to M/xM$ is a free resolution the A/xA-module M/xM by Lemma 8.1.5. Since $x \in \mathfrak{m}$, the morphisms of complexes of A-modules

$$L \otimes_A k \to (L/xL) \otimes_{A/xA} k \quad \text{and} \quad \operatorname{Hom}_{A/xA}(L/xL, k) \to \operatorname{Hom}_A(L, k)$$

are bijective in each degree, hence are quasi-isomorphisms. $\square$

2. The Auslander-Buchsbaum formula

We will use the following

Lemma 8.2.1. *Consider an exact sequence of finitely generated A-modules*

$$0 \to M' \to M \to M'' \to 0.$$

If $\operatorname{projdim} M < \operatorname{projdim} M''$, *then* $\operatorname{projdim} M' = \operatorname{projdim} M'' - 1$.

Proof. Let $n \geq \operatorname{projdim} M''$. Using the exact sequence (Proposition 4.3.3)

$$\operatorname{Tor}_{n+1}(M, k) \to \operatorname{Tor}_{n+1}(M'', k) \to \operatorname{Tor}_n(M', k) \to \operatorname{Tor}_n(M, k)$$

we see that $\operatorname{Tor}_n(M', k) \simeq \operatorname{Tor}_{n+1}(M'', k)$. Taking $n = \operatorname{projdim} M''$, we obtain $\operatorname{Tor}_n(M', k) = 0$, hence $\operatorname{projdim} M' \leq \operatorname{projdim} M'' - 1$ in view of Proposition 8.1.3. Taking $n = \operatorname{projdim} M'' - 1$, we obtain $\operatorname{Tor}_n(M', k) \neq 0$, hence $\operatorname{projdim} M' \geq \operatorname{projdim} M'' - 1$. $\square$

Theorem 8.2.2 (Auslander-Buchsbaum). *Let M be a finitely generated A-module of finite projective dimension. Then*

$$\operatorname{projdim} M + \operatorname{depth} M = \operatorname{depth} A.$$

Proof. We argue by induction on $\operatorname{projdim} M$.

If $\operatorname{projdim} M = 0$, then M is free by Proposition 8.1.1 (and nonzero), and $\operatorname{depth} M = \operatorname{depth} A$ by Lemma 5.2.10.

If $\operatorname{projdim} M = 1$, we let E be a (finite) family of elements of M whose image in $M/\mathfrak{m}M$ form a k-basis. This gives a morphism $\varphi\colon L_0 \to M$, where L_0 is the free A-module with basis E. Since $\varphi \otimes_A k$ is an isomorphism, the morphism φ is surjective by Nakayama's Lemma 1.1.6, and its kernel L_1 is contained in $\mathfrak{m}L_0$. So we have an exact sequence of A-modules

$$0 \to L_1 \xrightarrow{d} L_0 \to M \to 0$$

with $d(L_1) \subset \mathfrak{m}L_0$. By Lemma 8.2.1, we have $\operatorname{projdim} L_1 = \operatorname{projdim} M - 1 = 0$, so that the A-module L_1 is free by Proposition 8.1.1. It is also finitely generated, and we deduce that the morphism of A-modules

$$\mathfrak{m} \operatorname{Hom}_A(L_1, L_0) \to \operatorname{Hom}_A(L_1, \mathfrak{m}L_0)$$

is surjective. Thus $d = x_1 d_1 + \cdots + x_n d_n$ for some $x_j \in \mathfrak{m}$ and $d_j \in \operatorname{Hom}_A(L_1, L_0)$ for $j = 1, \cdots, n$, so that the morphism $\operatorname{Ext}^i(k, d) = x_1 \operatorname{Ext}^i(k, d_1) + \cdots + x_n \operatorname{Ext}^i(k, d_n)$ (Proposition 4.5.2 (v)) vanishes for every i (observe that $\mathfrak{m} \operatorname{Ext}^i(k, L_0) = 0$ by Proposition 4.5.2 (iv)). We obtain short exact sequences of A-modules (Proposition 4.5.4), for every i,

$$0 \to \operatorname{Ext}^i(k, L_0) \to \operatorname{Ext}^i(k, M) \to \operatorname{Ext}^{i+1}(k, L_1) \to 0.$$

Now L_0 and L_1 are free, and nonzero (because $\operatorname{projdim} M = 1$), hence $\operatorname{depth} L_1 = \operatorname{depth} L_0 = \operatorname{depth} A$ by Lemma 5.2.10. It follows that $\operatorname{depth} M = \operatorname{depth} A - 1$.

Now let us assume that $\operatorname{projdim} M \geq 2$. Choose an exact sequence of A-modules

$$0 \to N \to L \to M \to 0.$$

with L free and finitely generated (and nonzero). We have $\operatorname{projdim} N = \operatorname{projdim} M - 1$ by Lemma 8.2.1. Thus we obtain by induction

$$\operatorname{projdim} N + \operatorname{depth} N = \operatorname{depth} A.$$

In particular $\operatorname{depth} N < \operatorname{depth} A = \operatorname{depth} L$ (Lemma 5.2.10). Using the long exact sequence of A-modules

$$\operatorname{Ext}^{i-1}(k, L) \to \operatorname{Ext}^{i-1}(k, M) \to \operatorname{Ext}^{i}(k, N) \to \operatorname{Ext}^{i}(k, L),$$

we see that $\operatorname{depth} M = \operatorname{depth} N - 1$, as required. □

COROLLARY 8.2.3. *Let M be a finitely generated A-module of finite projective dimension. Then*

(i) $\operatorname{projdim} M \leq \operatorname{depth} A$, *with equality if and only if* $\mathfrak{m} \in \operatorname{Ass}(M)$.
(ii) $\operatorname{depth} M \leq \operatorname{depth} A$, *with equality if and only if M is free and nonzero.*

CHAPTER 9

Regular rings

In this chapter A is a local ring.

1. Homological dimension

Definition 9.1.1. The *homological dimension* of a commutative unital noetherian ring R is the supremum of the integers $\operatorname{projdim}_R M$, where M runs over the finitely generated R-modules. It is denoted $\operatorname{dimh} R \in \mathbb{N} \cup \{\infty\}$.

Remark 9.1.2. We can show (using Baer's criterion) that $\operatorname{dimh} R$ is the supremum $\operatorname{projdim}_R M$, where M runs over all R-modules.

Proposition 9.1.3. *Let A be a local (noetherian) ring with residue field k. Then*

$$\operatorname{dimh} A = \operatorname{projdim}_A k = \sup\{n \mid \operatorname{Tor}_n^A(k,k) \neq 0\} = \inf\{n \mid \operatorname{Tor}_{n+1}^A(k,k) = 0\}.$$

Proof. The last two equalities follow from Proposition 8.1.3. Let $m = \operatorname{projdim}_A k$, and M be a finitely generated A-module. Then $\operatorname{Tor}_{m+1}^A(k,M) = 0$, hence $\operatorname{Tor}_{m+1}^A(M,k) = 0$ by Proposition 4.3.5, and thus $\operatorname{projdim}_A M \leq m$ by Proposition 8.1.3. Therefore $\operatorname{dimh} A \leq m$; the other inequality is immediate. □

Corollary 9.1.4. *If the homological dimension of a local (noetherian) ring is finite, it is equal to its depth.*

Proof. Let A be the local ring, k its residue field. We have $\operatorname{depth}_A k = 0$. We apply the Auslander-Buchsbaum Theorem 8.2.2 to the A-module k, and obtain that $\operatorname{projdim}_A k = \operatorname{depth} A$. □

2. Regular rings

Theorem 9.2.1 (Serre). *A local ring is regular if and only if it has finite homological dimension.*

Proof. Let $(A, \mathfrak{m}, k)$ be a local ring. Assume that A is regular. We prove by induction on $n = \dim A$ that $\operatorname{projdim}_A k = n$ (see Proposition 9.1.3). This is clear when $n = 0$, because then $A = k$ by Example 3.2.2. Assume that $n > 0$. Let $\{x_1, \cdots, x_n\}$ be a regular system of parameters for A. Then the local ring A/x_nA is regular of dimension $n-1$ (Lemma 3.2.4). Since A is an integral domain by Proposition 3.2.6, the nonzero element x_n is a nonzerodivisor in A. By Proposition 6.2.5, the ring A is Cohen-Macaulay, hence by Proposition 6.1.7 the tuple $(x_1, \cdots, x_n)$ is an A-regular sequence. Thus x_n is a nonzerodivisor in $K = A/\{x_1, \cdots, x_{n-1}\}A$. By Proposition 8.1.6, it follows that $\operatorname{projdim}_A K = \operatorname{projdim}_{A/x_nA} k$. By induction we have $\operatorname{dimh} A/x_nA = n-1$, hence $\operatorname{projdim}_A K = n-1$. We have an exact sequence of A-modules

$$0 \to K \xrightarrow{x_n} K \to k \to 0.$$

This gives a long exact sequence (Proposition 4.3.3)

$$\mathrm{Tor}_i^A(K,k) \to \mathrm{Tor}_i^A(K,k) \to \mathrm{Tor}_i^A(k,k) \to \mathrm{Tor}_{i-1}^A(K,k) \to \mathrm{Tor}_{i-1}^A(K,k).$$

By Proposition 4.3.2 (vi), the morphism $\mathrm{Tor}_i^A(K,k) \to \mathrm{Tor}_i^A(K,k)$ is multiplication by x_n. Since $x_n \in \mathfrak{m}$ acts trivially on k, this morphism vanishes by Proposition 4.3.2 (vi). We obtain short exact sequences, for every i,

$$0 \to \mathrm{Tor}_i^A(K,k) \to \mathrm{Tor}_i^A(k,k) \to \mathrm{Tor}_{i-1}^A(K,k) \to 0.$$

Taking $i = n+1$, since $\mathrm{Tor}_n^A(K,k) = \mathrm{Tor}_{n+1}^A(K,k) = 0$, we see that $\mathrm{Tor}_{n+1}^A(k,k) = 0$, thus $\operatorname{projdim}_A k \leq n$ by Proposition 8.1.3. Taking $i = n$, we have $\mathrm{Tor}_{n-1}^A(K,k) \neq 0$ by Proposition 8.1.3, so that $\mathrm{Tor}_n^A(k,k) \neq 0$ and thus $\operatorname{projdim}_A k \geq n$.

For the converse, we proceed by induction on $n = \operatorname{dimh} A$. Assume that $n = 0$. Then $\operatorname{projdim}_A k = 0$, so that the A-module k is free, and (being nonzero) contains a copy of A. Thus $\mathfrak{m} = \mathrm{Ann}_A(k) = 0$, hence A is a field, hence a regular local ring (Example 3.2.2). Now we assume that $\infty > n > 0$. We have $\operatorname{depth} A = n$ by Corollary 9.1.4, and thus $\mathfrak{m} \notin \mathrm{Ass}(A)$ (Lemma 5.2.4). We have $\mathfrak{m}^2 \neq \mathfrak{m}$ by Nakayama's Lemma 1.1.6 (otherwise $\mathfrak{m} = 0$ and A is a field, a contradiction with the fact that $n > 0$). By prime avoidance (Proposition 2.4.5), we can find an element $x \in \mathfrak{m}$ which is not in $\mathfrak{m}^2$, nor in any of the finitely many associated primes of A (Corollary 1.3.6). By Lemma 1.2.9, the element x is a nonzerodivisor in A. Let $B = A/xA$, and $\mathfrak{n} = \mathfrak{m}/xA$ its maximal ideal. Consider the complex of B-modules

$$0 \to k \xrightarrow{u} \mathfrak{m}/x\mathfrak{m} \xrightarrow{v} \mathfrak{n} \to 0,$$

where u is induced by the map $A \to \mathfrak{m}, r \mapsto xr$, and v is the natural quotient $\mathfrak{m}/x\mathfrak{m} \to \mathfrak{m}/xA = \mathfrak{n}$. We claim that the sequence is exact. Indeed v is surjective and we have $\ker v = xA/x\mathfrak{m} = \operatorname{im} u$. If $a \in A$ is such that $a \mod \mathfrak{m} \in \ker u$, then $xa = xm$ for some $m \in \mathfrak{m}$. Thus $x(a-m) = 0$, and since x is a nonzerodivisor in A, we have $a = m \in \mathfrak{m}$, proving that u is injective.

The natural morphism of k-vector spaces $\mathfrak{m}/\mathfrak{m}^2 \to \mathrm{Hom}_k(\mathrm{Hom}_k(\mathfrak{m}/\mathfrak{m}^2, k), k)$ is injective (in fact bijective). Therefore since $x \neq 0 \mod \mathfrak{m}^2$, we may find a linear form $\varphi\colon \mathfrak{m}/\mathfrak{m}^2 \to k$ such that $\varphi(x) \neq 0 \in k$. Replacing φ with $(1/\varphi(x)) \cdot \varphi$, we may assume that $\varphi(x) = 1$. Composing φ with the surjection $\mathfrak{m}/x\mathfrak{m} \to \mathfrak{m}/\mathfrak{m}^2$, we obtain a morphism of B-modules $\psi\colon \mathfrak{m}/x\mathfrak{m} \to k$ sending $x \mod x\mathfrak{m}$ to 1. This gives a splitting of the exact sequence above (we have $\psi \circ u = \mathrm{id}_k$), so that we have a decomposition as B-modules

$$\mathfrak{m}/x\mathfrak{m} = k \oplus \mathfrak{n}.$$

It follows from Corollary 8.1.4 that

$$\operatorname{projdim}_B k \leq \operatorname{projdim}_B \mathfrak{m}/x\mathfrak{m}.$$

From Proposition 8.1.6, we know that

$$\operatorname{projdim}_B \mathfrak{m}/x\mathfrak{m} = \operatorname{projdim}_A \mathfrak{m}.$$

Since this quantity is smaller than $\operatorname{dimh} A = n$, we have $\operatorname{projdim}_B k < \infty$, so that B has finite homological dimension (Proposition 9.1.3). We have $\operatorname{depth} B = n-1$ by Proposition 5.2.2, hence $\operatorname{dimh} B = n-1$ by Corollary 9.1.4. By the induction hypothesis, the local ring B is regular. Therefore A is a regular local ring by Lemma 3.2.5. □

Corollary 9.2.2. *Let A be a regular local ring, and $\mathfrak{p}$ a prime of A. Then $A_\mathfrak{p}$ is a regular local ring.*

Proof. Let $n = \operatorname{projdim}_A A/\mathfrak{p}$. Then we may find an exact sequence of A-modules $0 \to L_n \to \cdots \to L_0 \to A/\mathfrak{p} \to 0$ with L_i free and finitely generated for $i = 0, \cdots, n-1$ (Lemma 4.2.1). By Proposition 8.1.3, the module L_n is projective. Since L_n is finitely generated, it is free by Proposition 8.1.1. Localising the finite resolution $0 \to L_n \to \cdots \to L_0 \to A/\mathfrak{p} \to 0$ at $\mathfrak{p}$, we obtain a finite resolution of the $A_\mathfrak{p}$-module $(A/\mathfrak{p})_\mathfrak{p} = \kappa(\mathfrak{p})$ by free, hence projective, $A_\mathfrak{p}$-modules. Thus $\operatorname{projdim}_{A_\mathfrak{p}} \kappa(\mathfrak{p}) < \infty$, hence $\operatorname{dimh} A_\mathfrak{p} < \infty$ by Proposition 9.1.3, and finally $A_\mathfrak{p}$ is regular by Theorem 9.2.1. □

Corollary 9.2.3. *A regular local ring is an integrally closed domain.*

Proof. Let A be a regular local ring, and $\mathfrak{p}$ a prime of A. The ring $A_\mathfrak{p}$ is a regular local ring by Corollary 9.2.2. If $\operatorname{depth} A_\mathfrak{p} = 0$, since $A_\mathfrak{p}$ is a reduced local ring, it is a field by Lemma 7.1.1. If $\operatorname{depth} A_\mathfrak{p} = 1$, then $A_\mathfrak{p}$ is a regular local ring of dimension one, that is, a discrete valuation ring by Example 3.2.3. It follows that A is normal by Theorem 7.3.4, and being local, is an integrally closed domain. □

Definition 9.2.4. A ring R is called *regular* if $R_\mathfrak{p}$ is a regular local ring for every prime $\mathfrak{p}$. By Corollary 9.2.2, it is equivalent to require that $R_\mathfrak{m}$ be a regular local ring for every maximal ideal $\mathfrak{m}$.

CHAPTER 10

Factorial rings

In this chapter R is a commutative unital noetherian ring.

1. Locally free modules

LEMMA 10.1.1. *An ideal of R is a free R-module of rank one if and only if it is generated by a nonzerodivisor in R.*

PROOF. If $I = iR$ with i a nonzerodivisor in R, then the surjective morphism $R \to I$, $r \mapsto ri$ must be injective, because so is the composite $R \to I \subset R$.

Conversely, if I is free and generated by i, we have an isomorphism $R \to I$, $r \mapsto ri$. The composite $R \to I \subset R$ is injective and coincides with multiplication by i in R, proving that i is a nonzerodivisor in R. $\square$

DEFINITION 10.1.2. An R-module M is *locally free* if the $R_{\mathfrak{p}}$-module $M_{\mathfrak{p}}$ is free for every $\mathfrak{p} \in \operatorname{Spec}(R)$. We say that the R-module M is *locally free of rank n* if the $R_{\mathfrak{p}}$-module $M_{\mathfrak{p}}$ is free of rank n for every $\mathfrak{p} \in \operatorname{Spec}(R)$.

LEMMA 10.1.3. *Let M, N be R-module with M finitely generated, and let S be a multiplicatively closed subset of R. Then the morphism of $S^{-1}R$-modules*

$$S^{-1} \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$$

is bijective

PROOF. Since M is finitely generated and R is noetherian we may find finitely generated free modules F_0, F_1 fitting into an exact sequence

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

We deduce a commutative diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & S^{-1} \operatorname{Hom}_R(M, N) \arrow[r] \arrow[d] & S^{-1} \operatorname{Hom}_R(F_0, N) \arrow[r] \arrow[d] & S^{-1} \operatorname{Hom}_R(F_1, N) \arrow[d] \\ 0 \arrow[r] & \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) \arrow[r] & \operatorname{Hom}_{S^{-1}R}(S^{-1}F_0, S^{-1}N) \arrow[r] & \operatorname{Hom}_{S^{-1}R}(S^{-1}F_1, S^{-1}N) \end{tikzcd}$$

A diagram chase shows that it suffices to prove that the two rightmost vertical arrows are isomorphisms. We thus reduced to assuming that M is free, in which case the statement is clear (to give a morphism from a free module consists exactly in specifying the image of a basis). $\square$

PROPOSITION 10.1.4. *If P is a finitely generated and locally free R-module, then P is projective.*

Proof. Let $M \to N$ be a surjective morphism of R-modules. To prove that the morphism of R-modules $\operatorname{Hom}_R(P, M) \to \operatorname{Hom}_R(P, N)$ is surjective, it will suffice to prove that the morphism of $R_{\mathfrak{p}}$-modules $(\operatorname{Hom}_R(P, M))_{\mathfrak{p}} \to (\operatorname{Hom}_R(P, N))_{\mathfrak{p}}$ is surjective for every $\mathfrak{p} \in \operatorname{Spec}(R)$. By Lemma 10.1.3, the latter morphism may be identified with $\operatorname{Hom}_{R_{\mathfrak{p}}}(P_{\mathfrak{p}}, M_{\mathfrak{p}}) \to \operatorname{Hom}_{R_{\mathfrak{p}}}(P_{\mathfrak{p}}, N_{\mathfrak{p}})$, which is surjective because the $R_{\mathfrak{p}}$-module $P_{\mathfrak{p}}$ is projective (being free). $\square$

Definition 10.1.5. A finitely generated R-module M is *stably free* if there is a finitely generated free R-module F such that $M \oplus F$ is a free R-module.

Lemma 10.1.6. *A finitely generated projective R-module admitting a finite resolution by finitely generated free modules is stably free.*

Proof. We prove the statement by induction on the length n of the resolution. Let M be the module, and $0 \to F_n \to \cdots \to F_0 \to M \to 0$ its resolution. Let $N = \ker(F_0 \to M)$. Then the exact sequence

$$0 \to N \to F_0 \to M \to 0$$

splits because M is projective. Since $N \oplus M \simeq F_0$ is free, it follows that N is projective. The R-module N is also finitely generated (being a quotient of F_0). We have a finite resolution $0 \to F_n \to \cdots \to F_1 \to N \to 0$ of N by finitely generated free modules of length $n-1$, hence by induction there is a finitely generated free R-module F such that $G = N \oplus F$ is free. Then $M \oplus G = M \oplus N \oplus F \simeq F_0 \oplus F$ is free, and M is stably free. $\square$

2. The exterior algebra

Definition 10.2.1. Let M be an R-module. For every integer $n \geq 0$, we define an R-module $\Lambda^n_R M = \Lambda^n M$ as the quotient of $M^{\otimes n} = M \otimes_R \cdots \otimes_R M$ by the submodule generated by the elements $m_1 \otimes \cdots \otimes m_n$ with $m_i = m_j$ for some $i \neq j$.

The morphism $M^{\otimes m} \otimes_R M^{\otimes n} \to M^{\otimes m+n}$ induces a surjective morphism $\Lambda^m M \otimes_R \Lambda^n M \to \Lambda^{m+n} M$ that we denote by $x \otimes y \mapsto x \wedge y$. This operation turns $\Lambda_R M = \Lambda M = \bigoplus_{n \geq 0} \Lambda^n R$ into an R-algebra equipped with a morphism of R-modules $M \to \Lambda M$, satisfying the following universal property. If B is an R-algebra, then any morphism of R-modules $f \colon M \to B$ such that $f(m)^2 = 0$ for any $m \in M$ extends uniquely to a morphism of R-algebras $\Lambda M \to B$.

Remark 10.2.2. We have $\Lambda^0 M \simeq R$, and $\Lambda^1 M \simeq M$.

The following results may be proved using the universal property of the exterior algebra.

Proposition 10.2.3. *(i) If $R \to S$ is a ring morphism and M an R-module, then $(\Lambda^n_R M) \otimes_R S \simeq \Lambda^n_S(M \otimes_R S)$.*

(ii) Let M, N be two R-modules. Then we have an isomorphism of graded R-algebras $\Lambda(M \oplus N) \simeq \Lambda M \otimes \Lambda N$.

Lemma 10.2.4. *Let M be a finitely generated, locally free R-module of rank one. Then $\Lambda^i M = 0$ for $i > 1$.*

Proof. It will be enough to prove that the $R_{\mathfrak{p}}$-module $(\Lambda^i M)_{\mathfrak{p}} = \Lambda^i(M_{\mathfrak{p}})$ (Proposition 10.2.3 (i)) vanishes for every $\mathfrak{p} \in \operatorname{Spec}(R)$. Thus we may assume that M is free, generated by an element m. If $x, y \in M$, and $z \in \Lambda^{i-2} M$, then x and y are scalar multiples of m, hence $x \wedge y \wedge z$ is a scalar multiple of $m \wedge m \wedge z = 0 \wedge z = 0$. $\square$

We denote by $R^m = R \oplus \cdots \oplus R$ the free R-module of rank m (with a given basis).

Lemma 10.2.5. *Let L be a finitely generated, locally free R-module of rank one. Then*

$$\Lambda^n(L \oplus R^{n-1}) \simeq L.$$

Proof. By Proposition 10.2.3 (ii), we have

$$\Lambda^n(L \oplus R^{n-1}) \simeq \bigoplus_{i_1+\ldots+i_n=n} \Lambda^{i_1}L \otimes \Lambda^{i_2}R \otimes \cdots \otimes \Lambda^{i_n}R.$$

In view of Remark 10.2.2 and Lemma 10.2.4, there is only one nonzero summand in the right hand side, namely L, when $i_1 = \cdots = i_n = 1$. □

Proposition 10.2.6. *Let L be a finitely generated, locally free R-module of rank one. If L is stably free, then L is free of rank one.*

Proof. We may assume that $R \neq 0$. There are integers m and n such that $L \oplus R^m \simeq R^n$. Choosing $\mathfrak{p} \in \operatorname{Spec}(R)$ and applying $- \otimes_R \kappa(\mathfrak{p})$ to that isomorphism, we see that $m = n - 1$ (isomorphic $\kappa(\mathfrak{p})$-vector spaces have the same dimension). Then using Lemma 10.2.5 twice (for the modules L and R), we obtain isomorphisms of R-modules

$$R \simeq \Lambda^n R^n \simeq \Lambda^n(L \oplus R^{n-1}) \simeq L.$$ □

3. Factorial rings

Definition 10.3.1. An element $x \in R$ is called *irreducible* if it is not a unit, and whenever $x = ab$ then a or b is a unit.

Lemma 10.3.2. *Any nonzero non-unit element of an integral domain decomposes as the product of finitely many irreducible elements.*

Proof. Assume that $x \in R$ does not decompose that way. We construct by induction an infinite chain of principal ideals $x_nR \subsetneq x_{n+1}R \subsetneq \cdots$, with x_n nonzero non-unit admitting no decomposition as above. This will contradict the noetherianity of R. We let $x_0 = x$. Now assume that x_n is constructed. Since x_n is nonzero, not a unit and not irreducible, it can be factored as ab with a, b non-units and nonzero. Then one element $x_{n+1} \in \{a, b\}$ does not decompose as a product of irreducible elements (otherwise x would). We have $x_nR \subset x_{n+1}R$. In case of equality, we have $x_{n+1} = x_nc$ for some $c \in R$. Then $abc \in \{a, b\}$, which implies (since R is an integral domain and a, b are nonzero) $1 \in \{bc, ac\}$, and therefore one of the elements b or a is a unit, a contradiction. □

Definition 10.3.3. A ring is a *factorial* if it is an integral domain and every ideal generated by an irreducible element is prime.

Lemma 10.3.4. *An integral domain is factorial if and only if every height one prime is principal.*

Proof. Let R be a factorial ring, and let $\mathfrak{p}$ be a prime of height one of R. Let $x \in \mathfrak{p} - \{0\}$. By Lemma 10.3.2, we may decompose x as $p_1 \cdots p_n$ with p_i irreducible elements (possibly not pairwise distinct). Then there is an index i such that $p_i \in \mathfrak{p}$. We have $0 \subsetneq p_iR \subset \mathfrak{p}$, and the ideal p_iR is prime because R is factorial. Since height $\mathfrak{p} = 1$, it follows that $p_iR = \mathfrak{p}$.

Conversely, assume that every height one prime of R is principal. Let $x \in R$ be an irreducible element. Let $\mathfrak{p}$ be a minimal prime over xR. Then by Krull's Theorem 2.3.2, the prime $\mathfrak{p}$ has height one, hence by assumption $\mathfrak{p} = pR$ for some $p \in R$. We have $xR \subset pR$, hence $x = pq$ for some $q \in R$. Since p is not a unit (otherwise $\mathfrak{p} = R$) and x is irreducible, the element q has to be a unit. Therefore $xR = pR$, proving that xR is prime. $\square$

Proposition 10.3.5. *A factorial ring is normal.*

Proof. Let R be a factorial ring, and $\mathfrak{p} \in \operatorname{Spec}(R)$. If $\operatorname{depth} R_{\mathfrak{p}} = 0$, the reduced ring $R_{\mathfrak{p}}$ must be a field by Lemma 7.1.1. If $\operatorname{depth} R_{\mathfrak{p}} = 1$, then $\operatorname{height} \mathfrak{p} = \dim R_{\mathfrak{p}} \geq 1$, hence we can find a prime $\mathfrak{q}$ of height one such that $\mathfrak{q} \subset \mathfrak{p}$. Since R is factorial, there is $x \in R$ such that $\mathfrak{q} = xR$. The image of x in $\mathfrak{p}R_{\mathfrak{p}}$ is a nonzero element of the integral domain $R_{\mathfrak{p}}$, and is thus a nonzerodivisor in $R_{\mathfrak{p}}$. Therefore $\operatorname{depth} R_{\mathfrak{p}}/xR_{\mathfrak{p}} = \operatorname{depth} R_{\mathfrak{p}} - 1 = 0$ by Proposition 5.2.2. Since the ideal $xR \subset R$ is prime and contained in $\mathfrak{p}$, the ideal $xR_{\mathfrak{p}} \subset R_{\mathfrak{p}}$ is prime. Thus the ring $R_{\mathfrak{p}}/xR_{\mathfrak{p}}$ is an integral domain, and being of depth zero, it is a field by Lemma 7.1.1. Thus $R_{\mathfrak{p}}$ is an integral domain whose maximal ideal $xR_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$ is principal, hence a discrete valuation ring. We conclude using Serre's criterion Theorem 7.3.4. $\square$

Remark 10.3.6. A factorial ring is also called a Unique Factorisation Domain (UFD). One may prove that a ring is factorial if and only if the decomposition of every element into a product of irreducible elements is unique (up to order and multiplication by units). Then using this characterisation, the classical proof that $\mathbb{Z}$ is an integrally closed domain can be used to give another proof of Proposition 10.3.5.

Lemma 10.3.7 (Nagata). *Let R be an integral domain, and $x \in R - \{0\}$ be such that xR is a prime ideal of R. If $R[x^{-1}]$ is factorial, then so is R.*

Proof. By Lemma 10.3.4, it will suffice to take a prime $\mathfrak{p}$ of height one in R, and prove that the ideal $\mathfrak{p}$ is principal. This is true if $\mathfrak{p} = xR$. Otherwise, since $\mathfrak{p}$ has height one, we must have $x \notin \mathfrak{p}$, and therefore $x^n \notin \mathfrak{p}$ for every n. It follows that $\mathfrak{p}R[x^{-1}]$ is a prime of height one in $R[x^{-1}]$. By assumption, we can find $y \in \mathfrak{p}R[x^{-1}]$ such that $\mathfrak{p}R[x^{-1}] = yR[x^{-1}]$. Multiplying with a power of x, we may assume that $y \in \mathfrak{p}$. Let E be the set of elements $y \in \mathfrak{p}$ such that $\mathfrak{p}R[x^{-1}] = yR[x^{-1}]$. We have just seen that $E \neq \varnothing$. Now the set of ideals $\{yR | y \in E\}$ of R admits a maximal element yR with $y \in E$ since R is noetherian.

We claim that $y \notin xR$. Indeed if $y = ax$ with $a \in R$, then $a \in E$ and $yR \subset aR$. By maximality $yR = aR$, hence we can find $b \in R$ such that $a = by$. Thus $y = bxy$, hence since R is an integral domain and $y \neq 0$ (because the prime $\mathfrak{p}R[x^{-1}]$ is not zero, being of height one), it follows that $bx = 1$, hence $xR = R$, a contradiction with assumption that xR is prime, proving the claim.

We now prove that $\mathfrak{p} = yR$. Since $y \in \mathfrak{p}$ by construction, it will suffice to prove that $\mathfrak{p} \subset yR$. Let $r \in \mathfrak{p}$. Since $yR[x^{-1}] = \mathfrak{p}R[x^{-1}]$, we have $x^n r = yc$ for some $c \in R$ and $n \in \mathbb{N}$. We prove that $r \in yR$ by induction on n. This is true if $n = 0$. Assume that $n > 0$. Then $yc \in xR$, and since $y \notin xR$ and xR is prime, we have $c \in xR$. Thus $x^{n-1}r = yc$, and by induction $r \in yR$. $\square$

Theorem 10.3.8 (Auslander-Buchsbaum). *A regular local ring is factorial.*

Proof. Let A be a regular local ring, with maximal ideal $\mathfrak{m}$. We proceed by induction on $\dim A$. If $\dim A = 0$, then A is a field, hence is factorial. Assume that $\dim A > 0$. Then we can find $x \in \mathfrak{m} - \mathfrak{m}^2$.

Let $\mathfrak{q}$ be a prime of height one in $A[x^{-1}]$. We have $\dim A[x^{-1}] < \dim A$, since any chain of primes in $A[x^{-1}]$ gives rise to chain in $\operatorname{Spec}(A) - \{\mathfrak{m}\}$, which can always be strictly enlarged by adding $\mathfrak{m}$. Let $\mathfrak{p} \in \operatorname{Spec}(A[x^{-1}])$. Then the ring $B = (A[x^{-1}])_{\mathfrak{p}}$ coincides with the localisation of the ring A at the prime $\mathfrak{p} \cap A$, hence is a regular local ring by Corollary 9.2.2. Since $\dim B \leq \dim A[x^{-1}] < \dim A$, we know that B is factorial by induction. The ideal $\mathfrak{q}B$ of B is either the unit ideal (if $\mathfrak{q} \not\subset \mathfrak{p}$) or a prime of height one (if $\mathfrak{q} \subset \mathfrak{p}$). In any case, this ideal is principal, and by Lemma 10.1.1 it follows that $\mathfrak{q}$ is a locally free $A[x^{-1}]$-module of rank one.

There is an ideal $\mathfrak{q}'$ of A such that $\mathfrak{q} = \mathfrak{q}'A[x^{-1}]$. By Theorem 9.2.1, we can find a finite resolution by finitely generated free modules of the A-module $\mathfrak{q}'$. Tensoring with $A[x^{-1}]$, we obtain finite resolution by finitely generated free modules of the $A[x^{-1}]$-module $\mathfrak{q}' \otimes_A A[x^{-1}] = \mathfrak{q}$. Since the $A[x^{-1}]$-module $\mathfrak{q}$ is projective Proposition 10.1.4, it is stably free by Lemma 10.1.6, and thus free of rank one by Proposition 10.2.6. In other words, the ideal $\mathfrak{q}$ of $A[x^{-1}]$ is principal. It follows from Lemma 10.3.4 that the ring $A[x^{-1}]$ is factorial. The ring A/xA is regular by Lemma 3.2.4, hence an integral domain by Proposition 3.2.6. It follows xA is a prime ideal of A, and we conclude that A is factorial using Lemma 10.3.7. $\square$

Bibliography

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[Bou98] Nicolas Bourbaki. *Commutative algebra. Chapters 1–7*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.

[Bou06] Nicolas Bourbaki. *Éléments de mathématique. Algèbre commutative, Chapitres 8 et 9*. Springer-Verlag, Berlin, 2006. Reprint of the 1983 original.

[Bou07] Nicolas Bourbaki. *Éléments de mathématique. Algèbre commutative. Chapitre 10*. Springer-Verlag, Berlin, 2007. Reprint of the 1998 original.

[Mat89] Hideyuki Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1989. Translated from the Japanese by M. Reid.

[Ser00] Jean-Pierre Serre. *Local algebra*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000. Translated from the French by CheeWhye Chin and revised by the author.