Introduction to commutative algebra
Lecture notes for Math 614, Fall 2022

Mircea Mustaţă

Department of Mathematics, University of Michigan, 530 Church Street, Ann Arbor, MI 48109, USA
Email address: mmustata@umich.edu

Contents

CHAPTER 1

Preface

Our goal in this course is to give an introduction to commutative algebra. We will not follow any textbook, but you can find the material that we will discuss (and quite a bit more) in either of the following two sources: [**Eis95**] and [**Mat89**].

We will assume familiarity with the definition of topological spaces and continuous maps. We will also assume familiarity with some basic algebraic notions and constructions, at the level of a first-year graduate course in algebra (prime and maximal ideals, localization, field extensions, modules, the isomorphism theorems for rings and modules, tensor products). We will review briefly some of these notions, but without going into details.

All rings that we will consider will have a unit and all ring homomorphisms we will consider will preserve the unit. Furthermore, unless explicitly mentioned otherwise, all rings that will appear will be assumed to be commutative.

CHAPTER 2

Prime ideals and localization

Let R be a ring (as usual, we assume that R is commutative).

2.1. Review of prime and maximal ideals

We begin by recalling the definition of prime and maximal ideals.

DEFINITION 2.1. An ideal $\mathfrak{p}$ in R is *prime* if $\mathfrak{p} \neq R$ and for every $a, b \in R$, if $ab \in \mathfrak{p}$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

REMARK 2.2. It follows directly from the definition that $\mathfrak{p}$ is a prime ideal in R if and only if $R/\mathfrak{p}$ is a domain.

DEFINITION 2.3. An ideal $\mathfrak{m}$ in R is *maximal* if $\mathfrak{m} \neq R$ and there is no ideal I, with $\mathfrak{m} \subsetneq I \subsetneq R$.

REMARK 2.4. Since the ideals in $R/\mathfrak{m}$ are in inclusion-preserving bijection with the ideals in R that contain $\mathfrak{m}$, it follows that $\mathfrak{m}$ is a maximal ideal if and only if $R/\mathfrak{m}$ is not the zero ring and it doesn't have any nontrivial ideals; in other words, $R/\mathfrak{m}$ is a field.

REMARK 2.5. Since every field is an integral domain, it follows that every maximal ideal is prime.

REMARK 2.6. A useful fact (proved using Zorn's lemma) is that if $I \subsetneq R$ is a proper ideal, then there is a maximal ideal $\mathfrak{m}$ in R with $I \subseteq \mathfrak{m}$.

2.2. The prime spectrum

Associated to every ring R, we have a topological space, the *prime spectrum* $\operatorname{Spec}(R)$, defined as follows. The underlying set of $\operatorname{Spec}(R)$ is the set of all prime ideals in R. It is convenient to describe the topology on this set in terms of closed sets (instead of open sets). For every ideal I in R, we put

$$V(I) = \big\{\mathfrak{p} \in \operatorname{Spec}(R) \mid I \subseteq \mathfrak{p}\big\}.$$

It is clear from the definition that for two ideals I and J, we have

$$V(I) \subseteq V(J) \quad \text{if} \quad J \subseteq I. \tag{2.1}$$

If $I = (a_1, \ldots, a_n)$, then we write $V(a_1, \ldots, a_n)$ for $V(I)$.

PROPOSITION 2.7. The sets $V(I)$, when I varies over the ideals in R, form the closed sets of a topology on $\operatorname{Spec}(R)$.

This topology is called the *Zariski topology* on $\operatorname{Spec}(R)$.

PROOF OF PROPOSITION 2.7. Recall that a family $\mathcal{F}$ of subsets of a set X form the closed sets of a topology if and only if it contains $\emptyset$ and X and it is closed under arbitrary intersections and finite unions. Let's check these properties in our setting.

Note first that $\emptyset = V(R)$ and $\mathrm{Spec}(R) = V(0)$. Suppose now that we have a family if ideals I_α of R. For an ideal $\mathfrak{p}$ in R, we have $I_\alpha \subseteq \mathfrak{p}$ for all α if and only if $\sum_\alpha I_\alpha \subseteq \mathfrak{p}$. Therefore we have

$$\bigcap_\alpha V(I_\alpha) = V\left(\sum_\alpha I_\alpha\right), \tag{2.2}$$

which implies that our family is closed under arbitrary intersections.

Suppose now that I and J are two ideals in R. We will show that

$$V(I) \cup V(J) = V(I \cap J) = V(I \cdot J), \tag{2.3}$$

which implies that our family is closed under finite unions. Since $I \cdot J \subseteq I \cap J$, the inclusions

$$V(I) \cup V(J) \subseteq V(I \cap J) \subseteq V(I \cdot J)$$

follows from (2.1). In order to complete the proof of (2.3) it is thus enough to show that $V(I \cdot J) \subseteq V(I) \cup V(J)$. Arguing by contradiction, suppose that we have a prime ideal $\mathfrak{p}$, such that $I \cdot J \subseteq \mathfrak{p}$, but $I \nsubseteq \mathfrak{p}$ and $J \nsubseteq \mathfrak{p}$. We can find $a \in I \smallsetminus \mathfrak{p}$ and $b \in J \smallsetminus \mathfrak{p}$. Therefore we have $ab \in I \cdot J \subseteq \mathfrak{p}$, but this contradicts the fact that $\mathfrak{p}$ is a prime ideal. This completes the proof of the proposition. □

REMARK 2.8. For every $a \in R$, let

$$D(a) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid a \notin \mathfrak{p}\} = \mathrm{Spec}(R) \smallsetminus V(a),$$

so this is an open subset of $\mathrm{Spec}(R)$. In fact, these open sets form a basis for the topology on $\mathrm{Spec}(R)$. Indeed, given an open subset U of $\mathrm{Spec}(R)$, there is an ideal I such that $U = \mathrm{Spec}(R) \smallsetminus V(I)$. If $I = (a_\lambda \mid \lambda \in \Lambda)$, then $U = \bigcup_{\lambda \in \Lambda} D(a_\lambda)$.

EXAMPLE 2.9. We have $\mathrm{Spec}(R) = \emptyset$ if and only if $R = 0$.

EXAMPLE 2.10. If k is a field, then $\mathrm{Spec}(k)$ consists of one point, namely (0).

EXAMPLE 2.11. If k is a field and $R = k[x]/(x^2)$, then again $\mathrm{Spec}(R)$ consists of only one point, namely $(x)/(x^2)$.

EXAMPLE 2.12. If $R = \mathrm{Spec}(\mathbf{Z})$, then $\mathrm{Spec}(\mathbf{Z})$ consists of the points $\eta = (0)$ and $p\mathbf{Z}$, where p is a positive prime integer. We note that each point $p\mathbf{Z}$ is a closed point of $\mathrm{Spec}(R)$, while $\overline{\{\eta\}} = \mathrm{Spec}(R)$ (since $\eta \in V(I)$ implies $I = (0)$).

EXAMPLE 2.13. Similarly, if k is a field and $R = k[x]$, then $\mathrm{Spec}(R)$ consists of $\eta = (0)$ and of the primes (f), where f runs over the monic irreducible polynomials in R. We use here the fact that every ideal in R is principal and a nonzero ideal (f) is prime if and only if f is an irreducible polynomial.

We next discuss the functoriality of the prime spectrum. Recall first that if M is an R-module and I is an ideal in M, then IM is the submodule of M generated by $\{ax \mid a \in I, x \in M\}$, that is,

$$IM = \left\{\sum_{i=1}^r a_i x_i \mid r \geq 0, a_i \in I, x_i \in M\right\}.$$

In particular, if $f\colon R \to S$ is a ring homomorphism and I is an ideal in R, we may consider IS. This is not just an R-submodule of S, but an ideal of S (in fact, it is the ideal generated by $f(I)$).

PROPOSITION 2.14. If $f\colon R \to S$ is a ring homomorphism, then for every prime ideal $\mathfrak{p}$ in S, the ideal $f^{-1}(\mathfrak{p}) \subseteq R$ is prime. Moreover the induced map

$$\operatorname{Spec}(f)\colon \operatorname{Spec}(S) \to \operatorname{Spec}(R),\ \mathfrak{p} \to f^{-1}(\mathfrak{p})$$

is continuous.

PROOF. The first assertion follows immediately from the definitions: if $a, b \in R$ are such that $ab \in f^{-1}(\mathfrak{p})$, then $f(a)f(b) = f(ab) \in \mathfrak{p}$. Since $\mathfrak{p}$ is a prime ideal, we have $f(a) \in \mathfrak{p}$ (in which case $a \in f^{-1}(\mathfrak{p})$) or $f(b) \in \mathfrak{p}$ (in which case $b \in f^{-1}(\mathfrak{p})$.

Note that $\operatorname{Spec}(f)$ is continuous if and only if the inverse image of any closed set is closed. If I is an ideal in R and $\mathfrak{p}$ is a prime ideal in S, then $I \subseteq f^{-1}(\mathfrak{p})$ if and only if $f(I) \subseteq \mathfrak{p}$, which is equivalent to $IS \subseteq \mathfrak{p}$. We thus have

$$\operatorname{Spec}(f)^{-1}\big(V(I)\big) = V(IS),$$

which implies that $\operatorname{Spec}(f)$ is a continuous map. □

REMARK 2.15. In this way we get a contravariant functor from the category of all commutative rings to the category of topological spaces. For this, it is enough to check that if $f\colon R \to S$ and $g\colon S \to T$ are ring homomorphisms, then $\operatorname{Spec}(g \circ f) = \operatorname{Spec}(f) \circ \operatorname{Spec}(g)$, which is clear.

DEFINITION 2.16. The *maximal spectrum* of a ring R is the topological space $\operatorname{Max}(R) \subseteq \operatorname{Spec}(R)$ (with the induced topology) consisting of all maximal ideals in R. We will see later that this subspace is important when R is a finitely generated algebra over a field, in which case $\operatorname{Max}(R)$ recovers all information about $\operatorname{Spec}(R)$.

2.3. Localization

In this section we review briefly, without checking the details, the localization construction for rings and modules. Let R be a ring. Recall that a subset $S \subseteq R$ is a *multiplicative system* if $1 \in S$ and whenever $s_1, s_2 \in S$, we have $s_1 s_2 \in S$. Given such a multiplicative system, the *ring of fractions* $S^{-1}R$ is defined as the set of all symbols $\frac{a}{s}$, where $a \in R$ and $s \in S$, modulo the equivalence relation $\frac{a_1}{s_1} \sim \frac{a_2}{s_2}$ if there is $s \in S$ such that $s(s_2 a_1 - s_1 a_2) = 0$ (note that if R is a domain and $S \subseteq R \setminus \{0\}$, then this condition is equivalent to $s_2 a_1 = s_1 a_2$). One can check that $S^{-1}R$ becomes a commutative ring with the operations given by

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{s_2 a_1 + s_1 a_2}{s_1 s_2} \quad \text{and} \quad \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}.$$

Moreover, we have a ring homomorphism $\varphi\colon R \to S^{-1}R$ given by $\varphi(a) = \frac{a}{1}$. This satisfies the following universal property: for every $s \in S$, the image $\varphi(s) \in S^{-1}R$ is invertible; moreover, φ is universal with this property (in other words, for every ring homomorphism $\varphi_T\colon R \to T$ such that $\varphi_T(s) \in T$ is invertible for all $s \in S$, there is a unique ring homomorphism $f\colon S^{-1}R \to T$ such that $f \circ \varphi = \varphi_T$).

Suppose now that $S \subseteq R$ is a multiplicative system and M is an R-module. We can similarly define $S^{-1}M$ as the set of all symbols $\frac{u}{s}$, where $u \in M$ and $s \in S$, modulo the equivalence relation $\frac{u_1}{s_1} \sim \frac{u_2}{s_2}$ if there is $s \in S$ such that we have

$s(s_2u_1 - s_1u_2) = 0$. One can check that $S^{-1}M$ becomes an $S^{-1}R$-module with respect to the operations

$$\frac{u_1}{s_1} + \frac{u_2}{s_2} = \frac{s_2u_1 + s_1u_2}{s_1s_2} \quad \text{and} \quad \frac{a}{s} \cdot \frac{u}{t} = \frac{au}{st}.$$

Moreover, we have a functor from the category of all R-modules to the category of all $S^{-1}R$-modules that takes M to $S^{-1}M$. We have a morphism of R-modules $\psi\colon M \to S^{-1}M$ (where we view $S^{-1}M$ as an R-module via φ) given by $\psi(u) = \frac{u}{1}$.

REMARK 2.17. Suppose that $f\colon R \to R'$ is a ring homomorphism and $S \subseteq R$ and $S' \subseteq R'$ are multiplicative systems such that $f(S) \subseteq S'$. In this case, it follows from the universal property of $S^{-1}R$ that we have a unique ring homomorphism $g\colon S^{-1}R \to S'^{-1}R'$ such that the diagram

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ {\scriptstyle \varphi_R}\downarrow & & \downarrow{\scriptstyle \varphi_{R'}} \\ S^{-1}R & \xrightarrow{g} & S'^{-1}R' \end{array}$$

is commutative. We also note that if $S' = f(S)$, then we have a canonical isomorphism of $S^{-1}R$-modules

$$S^{-1}R' \simeq S'^{-1}R',$$

where on the left-hand side we view R' as a left R-module via f.

EXAMPLE 2.18. If R is a ring and $a \in R$, then $S = \{a^n \mid n \geq 0\}$ is a multiplicative system in R. In this case we denote $S^{-1}R$ by R_a and if M is an R-module, we denote $S^{-1}M$ by M_a.

EXAMPLE 2.19. If $\mathfrak{p}$ is a prime ideal in a ring R, then $S = R \setminus \mathfrak{p}$ is a multiplicative system. In this case we write $R_\mathfrak{p}$ for $S^{-1}R$ and if M is an R-module, we write $M_\mathfrak{p}$ for $S^{-1}M$. A special case of this is when R is a domain and $\mathfrak{p} = (0)$: in this case $R_\mathfrak{p}$ is a field, the *field of fractions* of R, denoted $\mathrm{Frac}(R)$.

REMARK 2.20. It is useful to think of M_a as "describing the behavior of M on $D(a)$" and of $M_\mathfrak{p}$ as describing the behavior of M at the point $\mathfrak{p}$ of $\mathrm{Spec}(R)$. This can be made precise involving the notion of sheaf, but we will not go in that direction.

Passing from R to $R_\mathfrak{p}$ is useful because the ring $R_\mathfrak{p}$ satisfies the following property:

DEFINITION 2.21. A ring R is *local* if it has a unique maximal ideal $\mathfrak{m}$ (in this case we also say that $(R, \mathfrak{m})$ is a local ring). The *residue field* of the local ring is $R/\mathfrak{m}$.

REMARK 2.22. Since every proper ideal of R is contained in a maximal ideal, R is local if and only if there is a proper ideal $\mathfrak{m}$ of R that contains every proper ideal of R.

LEMMA 2.23. *If $\mathfrak{m}$ is an ideal in the ring R, then $(R, \mathfrak{m})$ is a local ring if and only if $\mathfrak{m} \neq R$ and every element of $R \setminus \mathfrak{m}$ is invertible.*

PROOF. The fact that all elements in $R \setminus \mathfrak{m}$ are invertible is equivalent to the fact that every proper ideal of R is contained in $\mathfrak{m}$. This gives the assertion in the lemma by Remark 2.22. □

REMARK 2.24. A fact that we will often use is that if $(R, \mathfrak{m})$ is a local ring, $u \in R$ is invertible, and $x \in \mathfrak{m}$, then $u + x$ is invertible. Indeed, we have $u + x \notin \mathfrak{m}$ (since otherwise we would get $u = (u + x) - x \in \mathfrak{m}$), hence it is invertible by the above lemma.

PROPOSITION 2.25. If $\mathfrak{p}$ is a prime ideal in a ring R, then $R_{\mathfrak{p}}$ is a local ring, with maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$.

PROOF. Note first that if $\frac{a}{s} = \frac{b}{t}$ and $a \in \mathfrak{p}$, then $b \in \mathfrak{p}$. Indeed, the equality of the two fractions means that there is $u \notin \mathfrak{p}$, such that $ubs = uat \in \mathfrak{p}$. Since $u, b \notin \mathfrak{p}$ and $\mathfrak{p}$ is a prime ideal, we have $b \in \mathfrak{p}$.

It is then easy to see that

$$\mathfrak{p}R_{\mathfrak{p}} = \left\{ \tfrac{a}{s} \mid a \in \mathfrak{p}, s \notin \mathfrak{p} \right\}$$

(we leave the proof of this assertion as an exercise). The fact that $\mathfrak{p}R_{\mathfrak{p}}$ is a proper ideal of $R_{\mathfrak{p}}$ is now clear, since $1 = \frac{1}{1} \notin \mathfrak{p}R_{\mathfrak{p}}$. On the other hand, if $\frac{a}{s} \notin \mathfrak{p}R_{\mathfrak{p}}$, then $a \notin \mathfrak{p}$, and thus $\frac{a}{s}$ is invertible in $R_{\mathfrak{p}}$, with inverse $\frac{s}{a}$. The assertion in the proposition then follows from Lemma 2.23. □

2.4. Nakayama's lemma

Many of the good properties of local rings can be traced back to the following

PROPOSITION 2.26 (Nakayama's Lemma). If $(R, \mathfrak{m})$ is a local ring and M is a finitely generated R-module such that $M = \mathfrak{m}M$, then $M = 0$.

PROOF. We use the so-called determinant trick. Let $u_1, \dots, u_n$ be generators of M. By assumption, we have $u_i \in \mathfrak{m}M$ for all i, hence we can write

$$u_i = \sum_{j=1}^{m_i} a_{i,j} v_{i,j} \quad \text{with} \quad a_{i,j} \in \mathfrak{m}, v_{i,j} \in M.$$

Since $u_1, \dots, u_n$ generate M, we can also write

$$v_{i,j} = \sum_{k=1}^{n} b_{i,j,k} u_k, \quad \text{with} \quad b_{i,j,k} \in R,$$

hence

$$u_i = \sum_{k=1}^{n} c_{i,k} u_k, \quad \text{where} \quad c_{i,k} = \sum_{j=1}^{m_i} a_{i,j} b_{i,j,k} \in \mathfrak{m}.$$

If C is the $n \times n$ matrix $(c_{i,k})$, then the above relations can be written as

$$(I_n - C) \cdot \begin{pmatrix} u_1 \\ \dots \\ u_n \end{pmatrix} = 0.$$

Multiplying this with the classical adjoint of $I_n - C$ we see that $\det(I_n - C)u_i = 0$ for all i. Since $u_1, \dots, u_n$ generate M, it follows that

$$\det(I_n - C) \cdot M = 0. \tag{2.4}$$

On the other hand, since $c_{i,k} \in \mathfrak{m}$ for all i and k, by expanding the determinant we see that $\det(I_n - C) = 1 + u$, where $u \in \mathfrak{m}$. Since R is local, with maximal ideal $\mathfrak{m}$, we conclude that $1 + u$ is invertible. Therefore (2.4) gives $M = 0$. □

We will often use Nakayama's lemma through the following

COROLLARY 2.27. If $(R, \mathfrak{m})$ is a local ring, M is a finitely generated R-module, and $N \subseteq M$ is a submodule such that $M = N + \mathfrak{m}M$, then $N = M$.

PROOF. The R-module $\overline{M} = M/N$ is finitely generated and the hypothesis implies $\mathfrak{m}\overline{M} = (N + \mathfrak{m}M)/N = \overline{M}$. Applying Nakayama's lemma gives $\overline{M} = 0$. □

REMARK 2.28. It follows from Corollary 2.27 that if $(R, \mathfrak{m})$ is a local ring and M is a finitely generated module, then $u_1, \ldots, u_n \in M$ generate M if and only if their images $\overline{u}_1, \ldots, \overline{u}_n \in M/\mathfrak{m}M$ generate $M/\mathfrak{m}M$ over the residue field $k = R/\mathfrak{m}$. Hence a minimal system of generators of M corresponds to a basis of $M/\mathfrak{m}M$ over k.

2.5. Exercises

Recall that a ring R is *reduced* if for every $a \in R$ such that $a^n = 0$ for some $n \geq 1$, we have $a = 0$. An ideal I in R is a *radical ideal* if the quotient ring R/I is reduced (equivalently, for every $a \in R$ such that $a^n \in I$ for some $n \geq 1$, we have $a \in I$).

EXERCISE 2.29. Let I be an ideal in a ring R. Show that

$$\operatorname{rad}(I) := \{a \in R \mid a^n \in I \text{ for some } n \geq 1\}$$

is the smallest radical ideal that contains I (it is called *the radical of* I).

EXERCISE 2.30. Show that if M' is a submodule of an R-module M and S is a multiplicative system in R, then the induced map $S^{-1}M' \to S^{-1}M$ is injective and its image is the kernel of the map $S^{-1}M \to S^{-1}(M/M')$ (induced by the canonical map $M \to M/M'$), which is surjective.

EXERCISE 2.31. Let R be a ring, $S \subseteq R$ a multiplicative system, and $\varphi\colon R \to T = S^{-1}R$ the canonical homomorphism. An ideal $\mathfrak{a}$ in R is *S-saturated* if whenever $a, b \in R$, with $a \in S$ and $ab \in \mathfrak{a}$, we have $b \in \mathfrak{a}$.

i) Show that if $\mathfrak{b}$ is an ideal in T, then there is a unique S-saturated ideal $\mathfrak{a}$ in R such that $S^{-1}\mathfrak{a} = \mathfrak{b}$, namely $\mathfrak{a} = \varphi^{-1}(\mathfrak{b})$. Moreover, if $\mathfrak{a}'$ is any ideal in R such that $S^{-1}\mathfrak{a}' = \mathfrak{b}$, then $\mathfrak{a}' \subseteq \mathfrak{a}$.

ii) Show that the induced map $\widetilde{\varphi}\colon \operatorname{Spec}(T) \to \operatorname{Spec}(R)$ induces a homeomorphism onto its image (with the induced topology), which consists of the prime ideals $\mathfrak{p}$ in R such that $S \cap \mathfrak{p} = \emptyset$.

EXERCISE 2.32. Let I be an ideal in the ring R. Recall that every ideal in the quotient ring R/I is of the form J/I, for a unique ideal J in R containing I. Show that J/I is a prime (maximal) ideal in R/I if and only if J has the same property.

EXERCISE 2.33. Show that if I is an ideal in the ring R and $\pi\colon R \to R/I$ is the canonical surjective homomorphism, then $\operatorname{Spec}(\pi)\colon \operatorname{Spec}(R/I) \to \operatorname{Spec}(R)$ is a homeomorphism onto a closed subset (with the induced topology).

EXERCISE 2.34. Show that if $R_1, \ldots, R_n$ are commutative rings and we take $R = R_1 \times \ldots \times R_n$, then we have a homeomorphism

$$\operatorname{Spec}(R) \xrightarrow{\simeq} \bigsqcup_{i=1}^{n} \operatorname{Spec}(R_i),$$

where on the right-hand side we have the disjoint union of the $\mathrm{Spec}(R_i)$, with the topology given by the condition that U is open if and only if $U \cap \mathrm{Spec}(R_i)$ is open for all i.

EXERCISE 2.35. Let I be an ideal in a ring R. Show that I is a radical ideal if and only if it is the intersection of a (possibly infinite) family of prime ideals in R.

EXERCISE 2.36. Let R be a ring. If $Z \subseteq \mathrm{Spec}(R)$ is a subset, we put

$$I(Z) := \bigcap_{\mathfrak{p} \in Z} \mathfrak{p}.$$

i) Show that for every subset $Z \subseteq \mathrm{Spec}(R)$, we have $V\big(I(Z)\big) = \overline{Z}$.
ii) Show that for every ideal $\mathfrak{a}$ in R, we have $I\big(V(\mathfrak{a})\big) = \mathrm{rad}(\mathfrak{a})$.
iii) Deduce that the maps $I(-)$ and $V(-)$ give order-reversing inverse bijections between the set of closed subsets of $\mathrm{Spec}(R)$ and the set of radical ideals in R.

EXERCISE 2.37. Show that if M is an R-module and $N \subseteq M$ is a submodule, then the following are equivalent:

i) $N = M$.
ii) $N_{\mathfrak{p}} = M_{\mathfrak{p}}$ for every prime ideal $\mathfrak{p}$ in R.
iii) $N_{\mathfrak{m}} = M_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$ in R.

EXERCISE 2.38. Prove the following variant of Nakayama's lemma: if R is a domain, $I \subsetneq R$ is an ideal, and M is a finitely generated module with no torsion (that is, if $a \in R$ and $x \in M$ are such that $ax = 0$, then $a = 0$ or $x = 0$) such that $IM = M$, then $M = 0$.

CHAPTER 3

Finite and integral homomorphisms

In this chapter we study in the context of rings two notions generalizing those of finite/algebraic field extensions. We first discuss some general properties of these notions and then study the induced map between the prime spectra.

3.1. Basic properties of finite and integral homomorphisms

Let $f\colon R \to S$ be a ring homomorphism (so S is an R-algebra).

DEFINITION 3.1.
1) We say that f is *of finite type* (or that S is a finite type R-algebra) if S is a finitely generated R-algebra (that is, there are $b_1, \ldots, b_n \in S$, for some positive integer n, such that $S = R[b_1, \ldots, b_n]$).
2) We say that f is *finite* (or that S is a finite R-algebra) if S is a finitely generated R-module.
3) We say that f is *integral* (or that S is an integral R-algebra) if every element $u \in S$ is integral over R: this means that there is a positive integer n and $a_1, \ldots, a_n \in R$ such that

$$u^n + a_1 u^{n-1} + \ldots + a_n = 0.$$

REMARK 3.2. Let $f\colon R \to T$ be a ring homomorphism. If I is an ideal in R and J is an ideal in T such that $I \subseteq f^{-1}(J)$, then we have an induced homomorphism $\overline{f}\colon R/I \to T/J$. If f is of finite type (or finite or integral), then $\overline{f}$ has the same property. Similarly, if S is a multiplicative system in R, then we get an induced homomorphism $g\colon S^{-1}R \to S^{-1}T$. If f is of finite type (or finite or integral), then g has the same property. Both assertions follow directly from definitions.

REMARK 3.3. It is clear that if f is finite, then it is also of finite type: if $b_1, \ldots, b_n$ generate S as an R-module, then they also generate S as an R-algebra. The converse is false: for example, the polynomial ring $R[x]$ is a finite type R-algebra, but it is not finite (prove this!).

REMARK 3.4. If f of finite type and also integral, then f is finite. More precisely, if $b_1, \ldots, b_n \in S$ generate S as an R-algebra and each b_i satisfies an equation

$$b_i^{d_i} + a_{i,1} b_i^{n_i - 1} + \ldots + a_{i,d_i} = 0,$$

for some $a_{i,1}, \ldots, a_{i,d_i} \in R$, then S is generated as an R-module by the monomials $b_1^{j_1} \ldots b_n^{j_n}$, with $0 \leq j_i \leq d_i - 1$ for all i.

In fact, the converse of the assertion in the last remark also holds, because we have

PROPOSITION 3.5. If S is a finite R-algebra, then S is an integral R-algebra.

PROOF. This is another application of the determinant trick: suppose that S is generated as an R-module by $b_1, \ldots, b_n$. Given any $y \in S$, for every $i \leq n$, we can write

$$yb_i = \sum_{j=1}^{n} a_{i,j} b_j \quad \text{for some} \quad a_{i,j} \in R.$$

If A is the $n \times n$ matrix $\big(f(a_{i,j})\big) \in M_n(S)$, then we have

$$(yI_n - A) \cdot \begin{pmatrix} u_1 \\ \ldots \\ u_n \end{pmatrix} = 0.$$

This implies $\det(yI_n - A) \cdot u_i = 0$ for $1 \leq i \leq n$. Since 1 is a linear combination of $u_1, \ldots, u_n$, we conclude that $\det(yI_n - A) = 0$. Expanding the determinant, we obtain

$$y^n + c_1 y^{n-1} + \ldots + c_n = 0 \quad \text{for some} \quad c_1, \ldots, c_n \in R.$$

Therefore y is integral over R. □

PROPOSITION 3.6. If $f\colon R \to S$ and $g\colon S \to T$ are ring homomorphisms and f and g are both finite (respectively of finite type or integral), then $g \circ f$ has the same property.

PROOF. If T is generated as an S-module by $u_1, \ldots, u_n$, and S is generated as an R-module by $v_1, \ldots, v_m$, then T is generated as an R-module by $f(v_i)u_j$, for $1 \leq i \leq m$ and $1 \leq j \leq n$. Indeed, given any $w \in T$, we can write $w = \sum_{i=1}^{n} a_i u_i$, with $a_1, \ldots, a_n \in S$, and for every i, we can write $a_i = \sum_{j=1}^{m} b_{i,j} v_j$, for some $b_{i,j} \in R$. We then have

$$w = \sum_{i=1}^{n} \sum_{j=1}^{n} b_{i,j} f(v_j) u_i.$$

If $T = S[u_1, \ldots, u_n]$ and $S = R[v_1, \ldots, v_m]$, then

$$T = R\big[u_1, \ldots, u_n, f(v_1), \ldots, f(v_m)\big],$$

hence T is a finitely generated R-algebra.

Finally, suppose that both f and g are integral homomorphisms. Given $u \in T$, there is a positive integer n and $a_1, \ldots, a_n \in S$ such that

$$u^n + a_1 u^{n-1} + \ldots + a_n = 0.$$

Since $a_1, \ldots, a_n$ are integral over R, the R-algebra $R' = R[a_1, \ldots, a_n]$ is finite by Remark 3.4. Similarly, since u is integral over R', the R'-algebra $R'[u]$ is finite, and thus $R'[u]$ is a finite R-algebra, by what we have already proved. Proposition 3.5 then implies that u is integral over R. □

PROPOSITION 3.7. If S is an R-algebra, then the subset $R' \subseteq S$ consisting of all elements of S that are integral over R is an R-subalgebra of S.

PROOF. If $u, v \in R'$, then $R[u, v]$ is a finite R-algebra by Remark 3.4. Therefore $u - v$ and uv are integral over R by Proposition 3.5, hence they belong to R'. □

DEFINITION 3.8. In the setting of the above proposition, R' is called the *integral closure* of R in S.

DEFINITION 3.9. If R is a domain, then the *integral closure* of R is its integral closure in $\mathrm{Frac}(R)$. We say that R is *integrally closed* if this integral closure is equal to R.

The following proposition will be useful when studying the behavior of prime ideals in integral extensions.

PROPOSITION 3.10. If $i\colon R \hookrightarrow S$ is an injective integral homomorphism, with both R and S domains, then R is a field if and only if S is a field.

PROOF. Since i is injective, in order to simplify notation, we may and will assume that R is a subring of S. Note first that since R and S are domains, we know that $R \neq 0$ and $S \neq 0$.

Suppose first that R is a field and let $u \in S \smallsetminus \{0\}$. Since u is integral over R, it follows that we can write

$$u^n + a_1 u^{n-1} + \ldots + a_n = 0$$

for some positive integer n, and some $a_1, \ldots, a_n \in R$. We may assume that n is chosen to be minimal; in this case, since $u \neq 0$, we have $a_n \neq 0$. We see that we have $uv = 1$, where

$$v = (-a_n)^{-1} \cdot (u^{n-1} + \ldots + a_{n-2}u + a_{n-1}),$$

hence u is invertible. Since this holds for every nonzero u, it follows that S is a field.

Conversely, suppose that S is a field and let $a \in R \smallsetminus \{0\}$. Let $b = \frac{1}{a} \in S$. Since b is integral over R, we can write

$$b^r + \alpha_1 b^{r-1} + \ldots + \alpha_r = 0$$

for some positive integer r and some $\alpha_1, \ldots, \alpha_r \in R$, hence

$$1 + \alpha_1 a + \ldots + \alpha_n a^n = 0.$$

Therefore

$$\frac{1}{a} = -\alpha_1 - \alpha_2 a - \ldots - \alpha_r a^{r-1} \in R,$$

we conclude that a in invertible in R. Since this holds for every nonzero $a \in R$, it follows that R is a field. □

COROLLARY 3.11. If $f\colon R \to S$ is an integral homomorphism, $\mathfrak{q} \in \mathrm{Spec}(S)$, and $\mathfrak{p} = f^{-1}(\mathfrak{q})$, then $\mathfrak{p}$ is a maximal ideal in R if and only if $\mathfrak{q}$ is a maximal ideal in R.

PROOF. The assertion follows by applying the proposition to the induced homomorphism $R/\mathfrak{p} \to S/\mathfrak{q}$ (it is clear that this is injective and integral). □

3.2. Behavior of prime ideals in integral homomorphisms

We now give the main results concerning $\mathrm{Spec}(f)$, when f is an integral homomorphism.

THEOREM 3.12. *If $f\colon R \to S$ is an injective integral homomorphism, then for every $\mathfrak{p} \in \mathrm{Spec}(R)$ there is $\mathfrak{q} \in \mathrm{Spec}(S)$ such that $\mathfrak{p} = f^{-1}(\mathfrak{q})$.*

PROOF. Consider the induced homomorphism $f_{\mathfrak{p}}\colon R_{\mathfrak{p}} \to S_{\mathfrak{p}}$, which is clearly injective and integral. If we have a prime ideal I in $S_{\mathfrak{p}}$ such that $f_{\mathfrak{p}}^{-1}(I) = \mathfrak{p}R_{\mathfrak{p}}$, then we can write $I = \mathfrak{q}R_{\mathfrak{p}}$, for a prime ideal $\mathfrak{q}$ in S and $\mathfrak{p} = f^{-1}(\mathfrak{q})$. Therefore we may and will assume that $\mathfrak{p}$ is a maximal ideal of R.

In this case it is enough to show that $\mathfrak{p}S \neq S$: every maximal ideal $\mathfrak{q}$ of S that contains $\mathfrak{p}S$ will have the property that $f^{-1}(\mathfrak{q}) = \mathfrak{p}$. Let us assume that $\mathfrak{p}S = S$, so we can write

$$1 = \sum_{i=1}^{n} a_i b_i, \quad \text{for some} \quad a_i \in \mathfrak{p}, b_i \in S.$$

In this case $R' = R[b_1, \ldots, b_n]$ is a finite R-algebra by Remark 3.4 and $\mathfrak{p}R' = R'$: indeed, for every $u \in R'$, we can write $u = \sum_{i=1}^{n} a_i(b_i u) \in \mathfrak{p}R'$. Nakayama's lemma implies $R' = 0$, a contradiction with the fact that f is injective. This completes the proof. □

Recall that a map $f\colon X_1 \to X_2$ is *closed* if $f(F)$ is closed in X_2 for every closed subset $F \subseteq X_1$.

COROLLARY 3.13. If $f\colon R \to S$ is an injective integral homomorphism, then $\varphi = \operatorname{Spec}(f)\colon \operatorname{Spec}(S) \to \operatorname{Spec}(R)$ is a surjective closed map (this implies that a subset $Z \subseteq \operatorname{Spec}(R)$ is closed if and only if $\varphi^{-1}(Z)$ is closed).

PROOF. Surjectivity follows directly from the theorem. In order to prove that φ is closed, it is enough to show that for every ideal I in S, we have

$$\varphi\big(V(I)\big) = V\big(f^{-1}(I)\big).$$

The inclusion "$\subseteq$" is a general fact: it follows from the fact that if $I \subseteq \mathfrak{q}$, then $f^{-1}(I) \subseteq f^{-1}(\mathfrak{q})$. The reverse inclusion follows by applying the theorem for the injective integral homomorphism $R/f^{-1}(I) \to S/I$. □

THEOREM 3.14 (Going-up). *If $f\colon R \to S$ is an integral homomorphism and $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ are prime ideals in R and $\mathfrak{q}_1$ is a prime ideal in S such that $f^{-1}(\mathfrak{q}_1) = \mathfrak{p}_1$, then there is a prime ideal $\mathfrak{q}_2$ in S with $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ and $f^{-1}(\mathfrak{q}_2) = \mathfrak{p}_2$.*

PROOF. Consider the induced homomorphism $g\colon R/\mathfrak{p}_1 \to S/\mathfrak{q}_1$, which is injective and integral. Applying Theorem 3.12 for the prime ideal $\mathfrak{p}_2/\mathfrak{p}_1$ in $R/\mathfrak{p}_1$, we conclude that there is a prime ideal $\mathfrak{q}_2/\mathfrak{q}_1$ in $S/\mathfrak{q}_1$ such that $g^{-1}(\mathfrak{q}_2/\mathfrak{q}_1) = \mathfrak{p}_2/\mathfrak{p}_1$. It is then clear that $\mathfrak{q}_2$ satisfies the conclusion of the theorem. □

THEOREM 3.15. *If $f\colon R \to S$ is an integral homomorphism and $\mathfrak{q}_1 \subsetneq \mathfrak{q}_2$ are prime ideals in S, then $f^{-1}(\mathfrak{q}_1) \neq f^{-1}(\mathfrak{q}_2)$.*

PROOF. Arguing by contradiction, suppose that $\mathfrak{p} = f^{-1}(\mathfrak{q}_1) = f^{-1}(\mathfrak{q}_2)$. Consider the induced homomorphism $g\colon R_{\mathfrak{p}} \to S_{\mathfrak{p}}$, which is again integral. Note that $\mathfrak{q}_1 S_{\mathfrak{p}} \subseteq \mathfrak{q}_2 S_{\mathfrak{p}}$ are distinct prime ideals in $S_{\mathfrak{p}}$. In particular, $\mathfrak{q}_1 S_{\mathfrak{p}}$ is not a maximal ideal. However, $g^{-1}(\mathfrak{q}_1 S_{\mathfrak{p}})$ is the maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$, contradicting Corollary 3.11. □

CHAPTER 4

Noetherian rings and modules

In this chapter we discuss the definition and some basic properties of Noetherian rings and modules. We then prove the main result on this topic, Hilbert's Basis Theorem and give some applications, to the Artin-Rees theorem and the Krull Intersection Theorem.

4.1. Definition and first properties

In this section we do not assume that the rings are commutative since the notions we discuss are useful also in the non-commutative context. Let R be a ring and M a left (or right) R-module.

DEFINITION 4.1. M is a *Noetherian* module if it satisfies the *Ascending Chain Condition* (ACC, for short), that is, there is no strictly increasing infinite sequence of submodules

$$M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq \ldots \subsetneq M. \tag{4.1}$$

We say that the ring R is left (respectively, right) Noetherian if it is Noetherian as a left (respectively, right) R-module.

In order to fix ideas, we will work with left R-modules, but of course all results have analogous ones for right R-modules.

PROPOSITION 4.2. Given a ring R and a left R-module M, the following are equivalent:

i) Every submodule N of M is finitely generated.
ii) M is a Noetherian R-module.
iii) Every nonempty family of submodules of M contains a maximal element.

PROOF. Suppose first that i) holds. If there is an infinite strictly increasing sequence of submodules of M as in (4.1), consider $N := \bigcup_{i\geq 1} M_i$. This is a submodule of M, hence it is finitely generated by i). If $u_1, \ldots, u_r$ generate N, then we can find m such that $u_i \in M_m$ for all i. In this case we have $N = M_j$ for all $j \geq m$, contradicting the fact that the sequence is strictly increasing.

The implication ii)⇒iii) is clear: if a nonempty family $\mathcal{F}$ has no maximal element, let us choose $N_1 \in \mathcal{F}$. Since this is not maximal, there is $N_2 \in \mathcal{F}$ such that $N_1 \subsetneq N_2$, and we continue in this way to construct an infinite strictly increasing sequence of submodules of M.

In order to prove the implication iii)⇒i), let N be a submodule of M and consider the family $\mathcal{F}$ of all finitely generated submodules of N. This is nonempty, since it contains the zero submodule. By iii), $\mathcal{F}$ has a maximal element N'. If $N' \neq N$, then there is $u \in N \setminus N'$ and the submodule $N' + Ru$ is a finitely generated

submodule of N strictly containing N', a contradiction with the maximality of N'. Therefore $N' = N$ and thus N is finitely generated. □

PROPOSITION 4.3. If M' is a submodule of a left R-module M, then M is Noetherian if and only if both M' and M/M' are Noetherian.

PROOF. We will use the characterization of the Noetherian property in Proposition 4.2i). Suppose first that M is Noetherian. Since every submodule of M' is a submodule of M, hence finitely generated, it follows that M' is Noetherian. Since every submodule of M/M' is isomorphic to N/M', for a submodule N of M that contains M', and since N being finitely generated implies that N/M' is finitely generated, we conclude that M/M' is Noetherian.

Conversely, suppose that both M' and M/M' are Noetherian, and let N be a submodule of M. Since $N \cap M'$ is a submodule of M', it is finitely generated, and since $N/(N \cap M')$ is isomorphic to a submodule of M/M', we have that $N/(N \cap M')$ is finitely generated. Finally, since both $N \cap M'$ and $N/(N \cap M')$ are finitely generated, it follows that N is finitely generated: if $N \cap M'$ is generated by $u_1, \ldots, u_r$ and $N/(N \cap M')$ is generated by $\overline{v_1}, \ldots, \overline{v_s}$, then N is generated by $u_1, \ldots, u_r, v_1, \ldots, v_s$. □

COROLLARY 4.4. If R is a Noetherian ring, then an R-module M is Noetherian if and only if it is finitely generated.

PROOF. We only need to show that if M is finitely generated, then it is Noetherian, since the converse follows from Proposition 4.2. Since M is finitely generated, we have a surjective morphism $R^{\oplus n} \to M$, and it follows from Proposition 4.3 that it is enough to show that $R^{\oplus n}$ is Noetherian. This follows again from the proposition by induction on n. □

REMARK 4.5. If R is a commutative Noetherian ring and I is an ideal in R, then R/I is a Noetherian ring. Indeed, every left ideal in R/I is of the form J/I, for some left ideal J in R containing I. Since J is finitely generated, it follows that J/I is finitely generated.

REMARK 4.6. If R is a Noetherian commutative ring and $S \subseteq R$ is a multiplicative system, then $S^{-1}R$ is a Noetherian ring. Indeed, every ideal in $S^{-1}R$ is of the form $S^{-1}J$, for some ideal J in R. If J is generated by $a_1, \ldots, a_r$, then $S^{-1}J$ is generated by $\frac{a_1}{1}, \ldots, \frac{a_r}{1}$.

EXAMPLE 4.7. If R is any commutative ring, the polynomial ring in countably many variables $R[x_i \mid i \geq 1]$ is not Noetherian. Indeed, we have the following strictly increasing chain of ideals:

$$(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \ldots .$$

EXERCISE 4.8. Let R be a commutative ring and $I_1, \ldots, I_k$ be ideals in R such that $I_1 \cap \ldots \cap I_k = (0)$. Show that if R/I_j is a Noetherian ring for $1 \leq j \leq k$, then R is a Noetherian ring.

A topological space X is Noetherian if there is no infinite strictly decreasing sequence

$$F_1 \supsetneq F_2 \supsetneq F_3 \supsetneq \cdots$$

of closed subsets of X.

EXERCISE 4.9. Show that if R is a Noetherian ring, then $\mathrm{Spec}(R)$ is a Noetherian topological space.

Given a closed subset Z of a topological space X, we say that Z is *irreducible* if it is nonempty and it can't be written as $Z = Z_1 \cup Z_2$, where $Z_1, Z_2 \subseteq X$ are closed subsets with $Z_1 \neq Z$ and $Z_2 \neq Z$.

EXERCISE 4.10. Show that if Z, $Z_1, \ldots, Z_r$ are closed subsets of a topological space X, with $Z \subseteq Z_1 \cup \ldots \cup Z_r$, and if Z is irreducible, then there is i such that $Z \subseteq Z_i$.

EXERCISE 4.11. Show that if R is a ring, then a closed subset $Z \subseteq \mathrm{Spec}(R)$ is irreducible if and only if $Z = V(\mathfrak{p})$ for some prime ideal $\mathfrak{p}$ of R.

EXERCISE 4.12. Show that a nonempty topological space is irreducible if and only if every nonempty open subset of X is dense in X.

EXERCISE 4.13. Show that if X is a Noetherian topological space, then every nonempty closed subset Z of X can be written as a finite union $Z = Z_1 \cup \ldots \cup Z_r$, with $Z_1, \ldots, Z_r$ irreducible closed subsets of X. Furthermore, if we assume that $Z_i \not\subseteq Z_j$ for any $i \neq j$ (which we can always do), then $Z_1, \ldots, Z_r$ are unique up to reordering (they are the *irreducible components* of Z).

EXERCISE 4.14. Show that if $I \subsetneq R$ is a proper ideal in a Noetherian ring R, then the irreducible components of $V(I)$ correspond to the minimal prime ideals containing I. Deduce that there are finitely many such prime ideals.

4.2. Hilbert's Basis Theorem

From now on we assume again that all rings are commutative. The following result was one of the most influential in the development of commutative algebra.

THEOREM 4.15 (Hilbert's Basis Theorem). *If R is a Noetherian ring, then the polynomial ring $R[x]$ is Noetherian.*

PROOF. Let I be an ideal in $R[x]$. We consider the following recursive construction. If $I \neq 0$, let $f_1 \in I$ be a polynomial of minimal degree. If $I \neq (f_1)$, then let $f_2 \in I \setminus (f_1)$ be a polynomial of minimal degree. Suppose now that $f_1, \ldots, f_n$ have been chosen. If $I \neq (f_1, \ldots, f_n)$, let $f_{n+1} \in I \setminus (f_1, \ldots, f_n)$ be a polynomial of minimal degree.

If this process stops, then I is finitely generated. Let us assume that this is not the case, aiming for a contradiction. We write

$$f_i = a_i x^{d_i} + \text{lower degree terms}, \quad \text{with} \quad a_i \neq 0.$$

By our minimality assumption, we have

$$d_1 \leq d_2 \leq \ldots.$$

Let J be the ideal of R generated by the a_i, with $i \geq 1$. Since R is Noetherian, J is a finitely generated ideal, hence there is m such that J is generated by $a_1, \ldots, a_m$. In particular, we can find $u_1, \ldots, u_m \in R$ such that

$$a_{m+1} = \sum_{i=1}^{m} u_i a_i.$$

In this case, we have

$$h := f_{m+1} - \sum_{i=1}^{m} u_i x^{d_{m+1}-d_i} f_i \in I \smallsetminus (f_1, \ldots, f_m)$$

and $\deg(h) < d_{m+1}$, a contradiction. This completes the proof of the theorem. □

COROLLARY 4.16. If R is a Noetherian ring, then every R-algebra of finite type is Noetherian.

PROOF. Since every R-algebra of finite type is a quotient of a polynomial algebra $R[x_1, \ldots, x_n]$, it follows from Remark 4.5 that it is enough to show that $R[x_1, \ldots, x_n]$ is Noetherian. This follows from the theorem by induction on n. □

EXAMPLE 4.17. Since a field is clearly Noetherian, it follows from Corollary 4.16 that every k-algebra of finite type is Noetherian.

EXAMPLE 4.18. If R is a PID (for example, $R = \mathbf{Z}$), then every ideal in R is principal, hence finitely generated. Therefore R is Noetherian and it follows from Corollary 4.16 that every R-algebra of finite type is Noetherian.

4.3. The Artin-Rees theorem and Krull's Intersection Theorem

We begin by discussing the Artin-Rees Theorem. This concerns the interplay between multiplying with (powers of) a given ideal and intersection with a submodule.

THEOREM 4.19 (Artin-Rees). *Let A be a Noetherian ring, M a finitely generated A-module, and $N \subseteq M$ a submodule. For every ideal $I \subseteq A$, there is a nonnegative integer a such that*

$$I^n M \cap N \subseteq I^{n-a} N \quad \textit{for all} \quad n \geq a.$$

The proof of the theorem makes use of the *Rees construction*, which is of independent interest. The Rees algebra of the ring A with respect to an ideal I is the A-algebra

$$R(I, A) = \bigoplus_{n \geq 0} I^n t^n \subseteq \bigoplus_{n \geq 0} A t^n = A[t].$$

Note that $R(I, A)$ is indeed an A-subalgebra of $A[t]$ since $I^m \cdot I^n = I^{m+n}$ for every $m, n \geq 0$.

REMARK 4.20. If A is a Noetherian ring, then $R(I, A)$ is a finitely generated A-algebra. Indeed, if $I = (f_1, \ldots, f_n)$, then $R(I, A) = A[f_1 t, \ldots, f_n t]$. In particular, $R(I, A)$ is a Noetherian ring by Corollary 4.16.

Suppose now that M is an A-module. We put

$$R(I, M) = \bigoplus_{n \geq 0} (I^n M) t^n,$$

which is naturally an $R(I, A)$-module, using the fact that $I^m \cdot I^n M = I^{m+n} M$ for all $m, n \geq 0$.

REMARK 4.21. If M is generated over A by $u_1, \ldots, u_d$, then $R(I, M)$ is generated over $R(I, A)$ by $u_1 t, \ldots, u_d t$. In particular, it is a finitely generated $R(I, A)$-module. Using also Remark 4.20, we thus see that if A is a Noetherian ring and M is a finitely generated A-module, then $R(I, M)$ is a Noetherian $R(I, A)$-module.

PROOF OF THEOREM 4.19. Consider the following $R(I,A)$-submodule of $R(I,M)$:

$$T = \bigoplus_{n\geq 0}(I^nM \cap N)t^n \hookrightarrow R(I,M).$$

Since $R(I,M)$ is a Noetherian $R(I,A)$-module by Remark 4.21, it follows that T is a finitely generated $R(I,A)$-module. We may choose a system of generators $u_1t^{i_1},\ldots,u_Nt^{i_N}$. If we take $a = \max\{i_1,\ldots,i_N\}$, then we see that for every $n \geq a$ and every $u \in I^nM \cap N$, we can write

$$ut^n = \sum_{j=1}^{N}(f_jt^{n-i_j})u_jt^{i_j} \quad \text{for some} \quad f_j \in I^{n-i_j},$$

hence $u \in I^{n-a}N$. □

As a consequence, we obtain the following

COROLLARY 4.22 (Krull's Intersection Theorem). If R is a Noetherian ring, M is a finitely generated R-module, and $I \subseteq R$ is an ideal, and if $N = \bigcap_{n\geq 1} I^nM$, then $N = IN$. In particular, if in addition $(R,\mathfrak{m})$ is local and $I \subseteq \mathfrak{m}$, then $\bigcap_{n\geq 1} I^nM = 0$.

PROOF. The second assertion follows from the first one and Nakayama's lemma, hence it is enough to prove the first assertion. Of course, we only need to prove $N \subseteq IN$. By the Artin-Rees theorem, there is a nonnegative integer a such that $I^nM \cap N \subseteq I^{n-a}N$ for all $n \geq a$. Since $N \subseteq I^{a+1}M$ by definition, we obtain $N \subseteq I^{a+1}M \cap N \subseteq IN$. □

CHAPTER 5

Associated primes and primary decomposition

In the first section we prove a basic general result about prime ideals: the Prime Avoidance lemma. In the second section we discuss associated primes and zero-divisors. Finally, in the last section we discuss primary decomposition in Noetherian rings.

5.1. The prime avoidance lemma

The following result, known as the Prime Avoidance lemma, is often useful.

LEMMA 5.1. *Let R be a commutative ring, r a positive integer, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ ideals in R such that $\mathfrak{p}_i$ is prime for all $i \geq 3$. If I is an ideal in R such that $I \subseteq \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_r$, then $I \subseteq \mathfrak{p}_i$ for some $i \geq 1$.*

PROOF. The assertion is trivial for $r = 1$. We prove it by induction on $r \geq 2$. If $r = 2$ and $I \not\subseteq \mathfrak{p}_1$ and $I \not\subseteq \mathfrak{p}_2$, then we may choose $a \in I \smallsetminus \mathfrak{p}_1$ and $b \in I \smallsetminus \mathfrak{p}_2$. Note that since $I \subseteq \mathfrak{p}_1 \cup \mathfrak{p}_2$, we have $a \in \mathfrak{p}_2$ and $b \in \mathfrak{p}_1$. Since $a + b \in I$, we have $a + b \in \mathfrak{p}_1$ or $a + b \in \mathfrak{p}_2$. In the first case, we see that $a = (a + b) - b \in \mathfrak{p}_1$, a contradiction and in the second case, we see that $b = (a+b) - a \in \mathfrak{p}_2$, leading again to a contradiction. This settles the case $r = 2$.

Suppose now that $r \geq 3$ and that we know the assertion for $r - 1$ ideals. If $I \not\subseteq \mathfrak{p}_i$ for every i, it follows from the induction hypothesis that given any i, we have $I \not\subseteq \bigcup_{j \neq i} \mathfrak{p}_j$. Let us choose

$$a_i \in I \smallsetminus \bigcup_{j \neq i} \mathfrak{p}_j.$$

By hypothesis, we must have $a_i \in \mathfrak{p}_i$ for all i.

Since $\mathfrak{p}_r$ is a prime ideal and $a_i \notin \mathfrak{p}_r$ for $i \neq r$, it follows that $\prod_{1 \leq j \leq r-1} a_j \notin \mathfrak{p}_r$. Consider now the element

$$u = a_r + \prod_{1 \leq j \leq r-1} a_j \in I.$$

By assumption, we have $u \in \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_r$. If $u \in \mathfrak{p}_r$, since $a_r \in \mathfrak{p}_r$, we deduce that $\prod_{1 \leq j \leq r-1} a_j \in \mathfrak{p}_r$, a contradiction. On the other hand, if $u \in \mathfrak{p}_i$ for some $i \leq r - 1$, since $\prod_{1 \leq j \leq r-1} a_j \in \mathfrak{p}_i$, we conclude that $a_r \in \mathfrak{p}_i$, a contradiction. We thus conclude that $I \subseteq \mathfrak{p}_i$ for some i, completing the proof of the induction step. □

5.2. Associated primes and zero-divisors

The associated primes provide a way to handle the zero-divisors in a ring or with respect to a module.

DEFINITION 5.2. If R is a ring and M is an R-module, a *zero-divisor* on M is an element $a \in R$ such that $au = 0$ for some nonzero $u \in M$. If a does not satisfy this condition, then it is a *non-zero-divisor*. By taking $M = R$, we have the notion of zero-divisor and non-zero-divisor in R.

Since we often deal with rings that are not domains, it is important to find a description of all zero-divisors in the ring. Even if one is only interested in the ring itself, it turns out that it is more convenient to treat the more general case of R-modules.

DEFINITION 5.3. If M is an R-module, an *associated prime* of M is a prime ideal $\mathfrak{p}$ in R such that

$$\mathfrak{p} = \mathrm{Ann}_R(u) := \{a \in R \mid au = 0\} \quad \text{for some} \quad u \in M, u \neq 0.$$

The set of associated primes of M is denoted $\mathrm{Ass}(M)$ (we write $\mathrm{Ass}_R(M)$ if the ring is not understood from the context).

EXAMPLE 5.4. If $\mathfrak{p}$ is a prime ideal in R, then $\mathrm{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$. Indeed, for every $u \in R \smallsetminus \mathfrak{p}$, we have $\mathrm{Ann}_R(\overline{u}) = \mathfrak{p}$.

The following is the main result concerning associated primes. The assertion in iii) is the reason why associated primes are important.

THEOREM 5.5. *If R is a Noetherian ring and M is a finitely generated R-module, then the following hold:*

i) *The set* $\mathrm{Ass}(M)$ *is finite.*
ii) *If* $M \neq 0$*, then* $\mathrm{Ass}(M)$ *is non-empty.*
iii) *The set of zero-divisors of M is equal to*

$$\bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}.$$

We begin with the following easy lemma:

LEMMA 5.6. *If M' is a submodule of M, then we have the following inclusions:*

$$\mathrm{Ass}(M') \subseteq \mathrm{Ass}(M) \subseteq \mathrm{Ass}(M') \cup \mathrm{Ass}(M/M').$$

PROOF. The first inclusion is obvious, hence we only prove the second one. Suppose that $\mathfrak{p} \in \mathrm{Ass}(M)$, and let us write $\mathfrak{p} = \mathrm{Ann}_R(u)$, for some nonzero $u \in M$. If $u \in M'$, then clearly $\mathfrak{p} \in \mathrm{Ass}(M')$. Otherwise, the image $\overline{u}$ of u in M'' is nonzero and it is clear that $\mathfrak{p} \subseteq \mathrm{Ann}_R(\overline{u})$. If this is an equality, then $\mathfrak{p} \in \mathrm{Ass}(M'')$, hence let us assume that there is $a \in \mathrm{Ann}_R(\overline{u}) \smallsetminus \mathfrak{p}$. In this case $au \in M' \smallsetminus \{0\}$, and the fact that $\mathfrak{p}$ is prime implies that the obvious inclusion $\mathrm{Ann}_R(u) \subseteq \mathrm{Ann}_R(au)$ is an equality. Therefore $\mathfrak{p} \in \mathrm{Ass}(M')$. □

COROLLARY 5.7. If $M_1, \ldots, M_r$ are R-modules, then

$$\mathrm{Ass}(M_1 \oplus \ldots \oplus M_r) = \bigcup_{i=1}^{r} \mathrm{Ass}(M_i).$$

PROOF. Arguing by induction on r, we see that it is enough to prove the assertion for $r = 2$. In this case, we have an embedding of M_1 and M_2 in $M_1 \oplus M_2$, such that the quotients are isomorphic to M_2, respectively M_1. The equality in the corollary then follows from the lemma. □

PROOF OF THEOREM 5.5. We may assume that M is nonzero, as otherwise all assertions are trivial. Consider the set $\mathcal{P}$ consisting of the ideals of R of the form $\mathrm{Ann}_R(u)$, for some $u \in M \smallsetminus \{0\}$. Since R is Noetherian, there is a maximal element $\mathfrak{p} \in \mathcal{P}$. We show that in this case $\mathfrak{p}$ is a prime ideal, so that $\mathfrak{p} \in \mathrm{Ass}(M)$.

By assumption, we can write $\mathfrak{p} = \mathrm{Ann}_R(u)$, for some $u \in M \smallsetminus \{0\}$. Since $u \neq 0$, we have $\mathfrak{p} \neq R$. If $b \in R \smallsetminus \mathfrak{p}$, then $bu \neq 0$ and we clearly have

$$\mathrm{Ann}_R(u) \subseteq \mathrm{Ann}_R(bu).$$

By the maximality of $\mathfrak{p}$, we conclude that this is an equality, hence for every $a \in R$ such that $ab \in \mathfrak{p}$, we have $a \in \mathfrak{p}$; we thus conclude that $\mathfrak{p}$ is a prime ideal.

In particular, this proves ii). We thus know that if M is non-zero, then we can find $u \in M \smallsetminus \{0\}$ such that $\mathrm{Ann}_R(u) = \mathfrak{p}_1$ is a prime ideal. If $M_1 = Ru$, then the map $R \to M$ that maps a to au gives an isomorphism $R/\mathfrak{p}_1 \simeq M_1$. Since $\mathfrak{p}_1$ is a prime ideal, it follows from Example 5.4 that $\mathrm{Ass}(R/\mathfrak{p}_1) = \{\mathfrak{p}_1\}$, and the lemma implies

$$\mathrm{Ass}(M) \subseteq \mathrm{Ass}(M/M_1) \cup \{\mathfrak{p}_1\}.$$

Therefore in order to prove that $\mathrm{Ass}(M)$ is finite it is enough to show that $\mathrm{Ass}(M/M_1)$ is finite. If $M/M_1 \neq 0$, we can repeat this argument and find $M_1 \subseteq M_2$ such that $M_2/M_1 \simeq R/\mathfrak{p}_2$, for some prime ideal $\mathfrak{p}_2$ in R. Since M is a Noetherian module, this process must terminate, hence after finitely many steps we conclude that $\mathrm{Ass}_R(M)$ is finite.

We now prove the assertion in iii). It is clear from definition that for every $\mathfrak{p} \in \mathrm{Ass}(M)$, the ideal $\mathfrak{p}$ is contained in the set of zero-divisors of M. On the other hand, if $a \in R$ is a zero-divisor, then $a \in I$, for some $I \in \mathcal{P}$. If we choose a maximal $\mathfrak{p}$ in $\mathcal{P}$ that contains I, then we have seen that $\mathfrak{p} \in \mathrm{Ass}_R(M)$, hence a lies in the union of the associated primes of M. This completes the proof of the theorem. □

We record in the next corollary a useful assertion that we obtained in the above proof.

COROLLARY 5.8. If R is a Noetherian ring and M is a finitely generated R-module, then there is a sequence of submodules

$$0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_r = M$$

such that $M_i/M_{i-1} \simeq R/\mathfrak{p}_i$ for $1 \leq i \leq r$, where each $\mathfrak{p}_i$ is a prime ideal in R.

REMARK 5.9. The results in Theorem 5.5 are often applied as follows: if an ideal I in R contains no non-zero-divisors on M, then it is contained in the union of the associated primes. Since there are finitely such prime ideals, the Prime Avoidance lemma implies that I is contained in one of them. Therefore there is a nonzero $u \in M$ such that $I \cdot u = 0$.

REMARK 5.10. Let M be a an R-module and $I \subseteq \mathrm{Ann}_R(M)$ an ideal, where

$$\mathrm{Ann}_R(M) = \{a \in R \mid au = 0 \text{ for all } u \in M\}$$

is the *annihilator* of M (it is easy to see that this is an ideal of R). Note that M can be viewed as an R/I-module. It is clear from definition that if $\mathfrak{p} \in \mathrm{Ass}(M)$, then $I \subseteq \mathfrak{p}$. Moreover, we have

$$\mathrm{Ass}_{R/I}(M) = \{\mathfrak{p}/I \mid \mathfrak{p} \in \mathrm{Ass}_R(M)\}.$$

EXERCISE 5.11. Show that if M is a module over a Noetherian ring R and S is a multiplicative system in R, then

$$\mathrm{Ass}_{S^{-1}R}(S^{-1}M) = \{S^{-1}\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Ass}(M), S \cap \mathfrak{p} = \emptyset\}.$$

EXERCISE 5.12. Show that if M' is a submodule of M, then

$$\mathrm{Supp}(M) = \mathrm{Supp}(M') \cup \mathrm{Supp}(M/M').$$

DEFINITION 5.13. If M is an R-module, then the *support* of M is

$$\mathrm{Supp}(M) = \big\{\mathfrak{p} \in \mathrm{Spec}(R) \mid M_{\mathfrak{p}} \neq 0\big\}.$$

PROPOSITION 5.14. If M is a finitely generated R-module, then

$$\mathrm{Supp}(M) = V\big(\mathrm{Ann}_R(M)\big).$$

In particular, the support of M is a closed subset of $\mathrm{Spec}(R)$.

PROOF. The fact that every $\mathfrak{p} \in \mathrm{Supp}(M)$ contains $\mathrm{Ann}_R(M)$ holds for every R-module M: by assumption, there is a nonzero element $\frac{u}{s} \in M_{\mathfrak{p}}$. In this case we have $\mathrm{Ann}_R(M) \subseteq \mathrm{Ann}_R(u) \subseteq \mathfrak{p}$.

For the reverse inclusion we need the fact that M is finitely generated: suppose that $\mathrm{Ann}_R(M) \subseteq \mathfrak{p}$. Arguing by contradiction, suppose that $M_{\mathfrak{p}} = 0$. If $u_1, \ldots, u_n$ generate M, since $\frac{u_i}{1} = 0$ in $M_{\mathfrak{p}}$, we conclude that there is $s_i \notin \mathfrak{p}$ such that $s_i u_i = 0$. In this case $s = \prod_i s_i \notin \mathfrak{p}$ and $su_i = 0$ for all i, hence $s \in \mathrm{Ann}_R(M)$. This contradicts our assumption. □

REMARK 5.15. Note that for every R-module M and every $\mathfrak{p} \in \mathrm{Ass}(M)$, we have $\mathrm{Ann}_R(M) \subseteq \mathfrak{p}$ (we have already mentioned this in Remark 5.10).

PROPOSITION 5.16. If M is a nonzero finitely generated module over the Noetherian ring R, then every minimal prime $\mathfrak{p}$ in $\mathrm{Supp}(M)$ is in $\mathrm{Ass}(M)$.

PROOF. By assumption, the $R_{\mathfrak{p}}$-module $M_{\mathfrak{p}}$ is nonzero, hence $\mathrm{Ass}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}})$ is non-empty by Theorem 5.5. However, note that $\mathrm{Ann}_R(M)_{\mathfrak{p}} \subseteq \mathrm{Ann}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}})$ and our assumption implies that the only prime ideal in $R_{\mathfrak{p}}$ containing $\mathrm{Ann}_R(M)_{\mathfrak{p}}$ is $\mathfrak{p}R_{\mathfrak{p}}$. Therefore $\mathfrak{p}R_{\mathfrak{p}} \in \mathrm{Ass}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}})$ and using Exercise 5.11 we see that $\mathfrak{p} \in \mathrm{Ass}_R(M)$. □

A prime in $\mathrm{Ass}(M)$ which is not minimal in $\mathrm{Supp}(M)$ is an *embedded associated prime* of M.

REMARK 5.17. If $I \subsetneq R$ is a proper ideal in a Noetherian ring, since $\mathrm{Ass}_R(R/I)$ is finite by Theorem 5.5, it follows from Proposition 5.16 that there are finitely minimal primes containing I. Recall that we have also seen this, with a different proof, in Exercise 4.14.

REMARK 5.18. If I is an ideal in a ring R, then every prime ideal $\mathfrak{p}$ containing I contains a minimal prime ideal containing I. Note first that by replacing R by R/I, we may assume that $I = 0$. We prove the assertion by considering the (nonempty) family $\mathcal{P}$ of prime ideals of R contained in $\mathfrak{p}$ and using Zorn's lemma. It is enough to show that given a set of elements $(\mathfrak{p}_i)_{i \in J}$ of $\mathcal{P}$, any two of them comparable via inclusion, the intersection $\mathfrak{q} = \bigcap_{i \in J} \mathfrak{p}_i$ is in $\mathcal{P}$. If $x, y \in R$ are such that $x, y \notin \mathfrak{q}$, then there are $i, j \in J$ such that $x \notin \mathfrak{p}_i$ and $y \notin \mathfrak{p}_j$. We have either $\mathfrak{p}_i \subseteq \mathfrak{p}_j$ or $\mathfrak{p}_j \subseteq \mathfrak{p}_i$. Without any loss of generality we may assume we are in the former case, so $x, y \notin \mathfrak{p}_i$, hence $xy \notin \mathfrak{p}_i$, and thus $xy \notin \mathfrak{q}$.

REMARK 5.19. Let I be a proper radical ideal in the Noetherian ring R. We have seen in Exercise 2.35 that I is an intersection of prime ideals. Since there are finitely many minimal primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ containing I and since we have seen in the previous remark that every prime ideal containing I contains a minimal such prime ideal, it follows that we can write

$$I = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r.$$

Note that every $a \in R \setminus \bigcup_i \mathfrak{p}_i$ is a non-zero-divizor on R/I: indeed, if $b \in R$ is such that $ab \in I$, we have $b \in \mathfrak{p}_i$ for all i, hence $b \in I$. We thus conclude that in this case R/I has no embedded associated primes.

5.3. Primary decomposition

In this section we discuss primary decomposition and its connection to associated primes. For simplicity, and since we will only need this case in what follows, we stick to the case of ideals (as opposed to submodules of a module). Actually, while associated primes will play an important role, primary decomposition will not feature much in the later chapters.

Let R be a Noetherian ring. Recall that every proper radical ideal I in R can be written as a finite intersection

$$I = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r,$$

where the $\mathfrak{p}_i$ are prime ideals. Our goal is to get a similar description for arbitrary ideals in R.

DEFINITION 5.20. A proper ideal $\mathfrak{q}$ in R is *primary* if whenever $a, b \in R$ are such that $ab \in \mathfrak{q}$ and $a \notin \mathfrak{q}$, we have $b \in \mathrm{rad}(\mathfrak{q})$.

REMARK 5.21. Of course, every prime ideal is a primary ideal. However, we will see that there are a lot more primary ideals than prime ideals.

REMARK 5.22. Note that if $\mathfrak{q}$ is a primary ideal, then $\mathfrak{p} := \mathrm{rad}(\mathfrak{q})$ is a prime ideal (it is common to say that $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal). First, since $\mathfrak{q} \neq R$, we have $\mathfrak{p} \neq R$. Suppose now that $a, b \in R$ are such that $ab \in \mathfrak{p}$ and $a \notin \mathfrak{p}$. Let $n \geq 1$ be such that $(ab)^n \in \mathfrak{q}$. Using repeatedly the fact that $\mathfrak{q}$ is a primary ideal and $a \notin \mathfrak{p}$, we conclude that $b^n \in \mathfrak{q}$, hence $b \in \mathfrak{p}$.

DEFINITION 5.23. A *primary decomposition* of a proper ideal I is an expression

$$I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n,$$

where all $\mathfrak{q}_i$ are primary ideals.

REMARK 5.24. It follows from definition that if $I \subseteq \mathfrak{q}$ are ideals in R, then $\mathfrak{q}/I$ is a primary ideal in R/I if and only if $\mathfrak{q}$ is a primary ideal in R.

PROPOSITION 5.25. If $\mathfrak{q}$ is an ideal in R, then $\mathfrak{q}$ is a primary ideal if and only if $\mathrm{Ass}_R(R/\mathfrak{q})$ has only one element. Moreover, in this case the only associated prime of $R/\mathfrak{q}$ is $\mathrm{rad}(\mathfrak{q})$.

PROOF. Suppose first that $\mathfrak{q}$ is $\mathfrak{p}$-primary. Note that $\mathfrak{p}$ is a minimal prime ideal containing $\mathfrak{q}$ (in fact, it is the unique such prime ideal), hence $\mathfrak{p} \in \mathrm{Ass}(R/\mathfrak{q})$ by Proposition 5.16. On the other hand, since $\mathfrak{q}$ is $\mathfrak{p}$-primary, it follows that every zero-divisor of $R/\mathfrak{q}$ lies in $\mathfrak{p}$. Since the set of zero-divisors of $R/\mathfrak{q}$ is the union of

the associated primes of $R/\mathfrak{q}$ by Theorem 5.5, and each of these associated primes contains $\mathrm{Ann}_R(R/\mathfrak{q}) = \mathfrak{q}$, we conclude that $\mathfrak{p}$ is the only element of $\mathrm{Ass}_R(R/\mathfrak{q})$.

Conversely, suppose that $\mathrm{Ass}_R(R/\mathfrak{q})$ has only one element $\mathfrak{p}$. In this case, it follows from Proposition 5.16 that $\mathfrak{p}$ is the unique minimal prime containing $\mathfrak{q}$, hence $\mathfrak{p} = \mathrm{rad}(\mathfrak{q})$. Moreover, it follows from Theorem 5.5 that the set of non-zero-divisors of $R/\mathfrak{q}$ is equal to $\mathfrak{p}$, which implies, by definition, that $\mathfrak{q}$ is a primary ideal. □

EXAMPLE 5.26. If $\mathfrak{q}$ is an ideal such that $\mathfrak{p} := \mathrm{rad}(\mathfrak{q})$ is a maximal ideal, then $\mathfrak{q}$ is a primary ideal. Indeed, in this case the only prime ideal containing $\mathfrak{q}$ is $\mathfrak{m}$. In particular, $\mathrm{Ass}_R(R/I)$ has only one associated prime and the assertion follows from Proposition 5.25.

THEOREM 5.27 (Lasker-Noether). *Every proper ideal I in R has a primary decomposition.*

PROOF. After replacing R by R/I, we may assume that $I = 0$ (see Remark 5.24). We claim that for every $\mathfrak{p} \in \mathrm{Ass}(R)$, there is a primary ideal $\mathfrak{q}$ in R (in fact, a $\mathfrak{p}$-primary ideal) such that $\mathfrak{p} \notin \mathrm{Ass}(\mathfrak{q})$. Indeed, consider the ideals J in R such that $\mathfrak{p} \notin \mathrm{Ass}(J)$ (the set is non-empty since it contains 0) and since R is Noetherian, we may choose an ideal $\mathfrak{q}$ which is maximal with this property. Note that since $\mathfrak{p} \in \mathrm{Ass}(R)$, we have $\mathfrak{q} \neq R$, hence $\mathrm{Ass}(R/\mathfrak{q})$ is non-empty. By Proposition 5.25, in order to show that $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal, it is enough to show that for every prime ideal $\mathfrak{p}' \neq \mathfrak{p}$, we have $\mathfrak{p}' \notin \mathrm{Ass}(R/\mathfrak{q})$. If $\mathfrak{p}' \in \mathrm{Ass}(R/\mathfrak{q})$, then we obtain an ideal $\mathfrak{q}' \supseteq \mathfrak{q}$ such that $\mathfrak{q}'/\mathfrak{q} \simeq R/\mathfrak{p}'$. We assumed $\mathfrak{p}' \neq \mathfrak{p}$, while Lemma 5.6 implies

$$\mathrm{Ass}(\mathfrak{q}') \subseteq \mathrm{Ass}(\mathfrak{q}) \cup \mathrm{Ass}(\mathfrak{q}'/\mathfrak{q}) = \mathrm{Ass}(\mathfrak{q}) \cup \{\mathfrak{p}'\},$$

hence $\mathfrak{p} \notin \mathrm{Ass}(\mathfrak{q}')$, contradicting the maximality of $\mathfrak{q}$.

We thus conclude that if $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are the associated primes of R, we can find primary ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ such that $\mathfrak{p}_i \notin \mathrm{Ass}(\mathfrak{q}_i)$ for all i. If $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$, then $\mathrm{Ass}(\mathfrak{a}) \subseteq \mathrm{Ass}(R)$ and at the same time $\mathrm{Ass}(\mathfrak{a}) \subseteq \mathrm{Ass}(\mathfrak{q}_i)$ for all i, hence $\mathfrak{p}_i \notin \mathrm{Ass}(\mathfrak{a})$. This implies that $\mathfrak{a}$ has no associated primes, hence $\mathfrak{a} = 0$. □

REMARK 5.28. Note that if $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ are $\mathfrak{p}$-primary ideals, then $\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ is a $\mathfrak{p}$-primary ideal. It is thus straightforward to see that given any ideal I and any primary decomposition $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$, we can obtain a *minimal* such decomposition, in the sense that the following conditions are satisfied:

i) We have $\mathrm{rad}(\mathfrak{q}_i) \neq \mathrm{rad}(\mathfrak{q}_j)$ for all i and j, and
ii) For every i, with $1 \leq i \leq r$, we have $\bigcap_{j \neq i} \mathfrak{q}_j \neq I$.

Given such a minimal primary decomposition, if $\mathfrak{p}_i = \mathrm{rad}(\mathfrak{q}_i)$, then $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are the distinct associated primes of R/I. Indeed, the injective morphism

$$R/I \hookrightarrow \bigoplus_{i=1}^{r} R/\mathfrak{q}_i,$$

together with Corollary 5.7 and Proposition 5.25 give that $\mathrm{Ass}(R/I) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. On the other hand, for every i, there is $u \in \bigcap_{j \neq i} \mathfrak{q}_j$ such that $u \notin \mathfrak{q}_i$. Moreover, after multiplying u by a suitable element in $\mathfrak{p}_i^m$, for some non-negative integer m, we may assume that $u \cdot \mathfrak{p}_i \subseteq \mathfrak{q}_i$. In this case, $\mathfrak{p}_i$ is the annihilator of the image of u in R/I, hence $\mathfrak{p}_i \in \mathrm{Ass}(R/I)$.

REMARK 5.29. In general, the primary ideals in a minimal primary decomposition of I are not unique. However, if $\mathfrak{p}$ is a minimal prime containing I, then the corresponding $\mathfrak{p}$-primary ideal $\mathfrak{q}$ in a minimal primary decomposition of I is unique. Indeed, it is easy to check that $I \cdot R_{\mathfrak{p}} = \mathfrak{q} \cdot R_{\mathfrak{p}}$ and deduce, using that $\mathfrak{q}$ is $\mathfrak{p}$-primary, that $\mathfrak{q} = \varphi^{-1}(I \cdot R_{\mathfrak{p}})$, where $\varphi\colon R \to R_{\mathfrak{p}}$ is the canonical homomorphism.

EXERCISE 5.30. Show that if $n \in \mathbf{Z}$ is a nonzero integer and $n = \pm p_1^{k_1} \cdots p_r^{k_r}$ is the prime factorization, then

$$(n) = (p_1)^{k_1} \cap \ldots \cap (p_r)^{k_r}$$

is the unique primary decomposition of (n).

EXERCISE 5.31. Let k be a field and consider the ideal $(x^2, xy) \subset k[x, y]$.

i) Give two distinct minimal primary decompositions of I.
ii) Show that $k[x, y]/(x^2, xy)$ has one minimal prime and one embedded associated prime.

EXERCISE 5.32. Let k be a field and let $R = k[x, y, z]/(xy - z^2)$. Show that the ideal $\mathfrak{p} = (\overline{x}, \overline{z}) \subset R$ is prime, $\operatorname{rad}(\mathfrak{p}^2) = \mathfrak{p}$, but $\mathfrak{p}^2$ is not a primary ideal.

EXERCISE 5.33. Let R be a ring, S a multiplicative system in R, and $\varphi\colon R \to S^{-1}R$ the canonical homomorphism.

i) Show that if $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal in R and $S \cap \mathfrak{q} \neq \emptyset$, then $\mathfrak{q}S^{-1}R$ is a $\mathfrak{p}S^{-1}R$-primary ideal in $S^{-1}R$. Moreover, we have $\mathfrak{q} = \varphi^{-1}(\mathfrak{q}S^{-1}R)$.
ii) Conversely, show that if $\mathfrak{a}$ is a $\mathfrak{b}$-primary ideal in $S^{-1}R$, then $\varphi^{-1}(\mathfrak{a})$ is a $\varphi^{-1}(\mathfrak{b})$-primary ideal in R, with $S \cap \varphi^{-1}(\mathfrak{a}) = \emptyset$.
iii) Show that if I is a proper ideal in R with a primary decomposition $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$, then $IS^{-1}R$ is a proper ideal in $S^{-1}R$ if and only if there is i, with $1 \leq i \leq r$, such that $S \cap \mathfrak{q}_i = \emptyset$. In this case

$$IS^{-1}R = \bigcap_{i, \mathfrak{q}_i \cap S = \emptyset} \mathfrak{q}_i S^{-1}R$$

is a primary decomposition of $IS^{-1}R$.

EXERCISE 5.34. Let $\mathfrak{p}$ be a prime ideal in a Noetherian ring R and let $\varphi\colon R \to R_{\mathfrak{p}}$ be the canonical homomorphism.

i) Show that for every positive integer n, the ideal $\mathfrak{p}^{(n)} := \varphi^{-1}(\mathfrak{p}^n R_{\mathfrak{p}})$ is $\mathfrak{p}$-primary (it is called the n^{th} symbolic power of $\mathfrak{p}$).
ii) Show that we always have $\mathfrak{p}^n \subseteq \mathfrak{p}^{(n)}$ and give an example where this inclusion is strict.

EXERCISE 5.35. Let A be a reduced Noetherian ring and B the total ring of fractions of A (that is, $B = S^{-1}A$, where S is the set of all non-zero-divisors in A). Show that B is a direct product of fields.

EXERCISE 5.36. Let I and J be ideals in the Noetherian ring A. Show that if $I_{\mathfrak{p}} \subseteq J_{\mathfrak{p}}$ for every $\mathfrak{p} \in \operatorname{Ass}_A(A/J)$, then $I \subseteq J$.

EXERCISE 5.37. Let $f\colon R \to S$ be a homomorphism of Noetherian rings and let M be a finitely generated S-module. Show that if $\varphi = \operatorname{Spec}(f)\colon \operatorname{Spec}(S) \to \operatorname{Spec}(R)$, then

$$\varphi\big(\operatorname{Ass}_S(M)\big) = \operatorname{Ass}_R(M).$$

Note that this implies that $\mathrm{Ass}_R(M)$ is finite, in spite of the fact that M might not be finitely generated over R.

CHAPTER 6

Noether normalization, Nullstellensatz, and the maximal spectrum

Our goal in this chapter is to give an introduction to affine algebraic geometry, explaining the correspondence between algebraic subsets of the affine space and radical ideals in the polynomial ring over an algebraically closed field. This is based on Hilbert's Nullstellensatz, which in turn is a consequence of Noether normalization. In the last section we discuss briefly the situation over general fields.

6.1. Noether normalization

The following result allows, in certain instances, reducing the study of arbitrary domains of finite type over a field k to that of polynomial rings. We will make use of it in this chapter to prove Hilbert's Nullstellensatz, but we will see later in the course that it has other useful applications.

THEOREM 6.1 (Noether normalization). *Let k be a field and A a finitely generated k-algebra which is a domain, with fraction field K. If $\operatorname{trdeg}(K/k) = n$, then there is a k-subalgebra B of A, such that*

1) *B is isomorphic as a k-algebra to the polynomial algebra $k[x_1, \dots, x_n]$, and*
2) *The inclusion $B \hookrightarrow A$ is finite.*

We first give the following

LEMMA 6.2. *If $A \hookrightarrow B$ is an injective, finite homomorphism between two domains, and $K = \operatorname{Frac}(A)$ and $L = \operatorname{Frac}(B)$, then the induced field extension $K \hookrightarrow L$ is finite.*

PROOF. Let $S = A \setminus \{0\}$ and consider the induced injective homomorphisms

$$K = S^{-1}A \xhookrightarrow{i} S^{-1}B \hookrightarrow L.$$

If B is generated as an A-module by $b_1, \dots, b_m$, then $S^{-1}B$ is generated over $S^{-1}A$ by $\frac{b_1}{1}, \dots, \frac{b_r}{1}$. In particular, i is a finite homomorphism. Since K is a field and $S^{-1}B$ is a domain, it follows from Proposition 3.10 that $S^{-1}B$ is a field as well. Therefore we have $S^{-1}B = L$ (this follows, for example, from the universal property of $\operatorname{Frac}(B)$). In particular, we see that $[L : K] < \infty$. □

PROOF OF THEOREM 6.1. We give the proof following [**Mum99**, p. 2]. Let $y_1, \dots, y_m \in A$ be generators of A as a k-algebra. In particular, we have $K = k(y_1, \dots, y_m)$, hence $m \geq n$. We argue by induction on m. Note that if $m = n$, then $y_1, \dots, y_m$ are algebraically independent over k and we are done. Suppose now that $m > n$ and note that it is enough to show that we can find a k-subalgebra

$A' \subseteq A$ that is generated over k by $m-1$ elements and such that A is a finite A'-algebra. Indeed, in this case it follows by the induction hypothesis that there is a k-subalgebra $B \subseteq A'$ that is isomorphic to $k[x_1, \ldots, x_n]$ (note that $K' = \mathrm{Frac}(A')$ and K au the same transcendence degree over k since the extension K/K' is algebraic by Lemma 6.2). Moreover, A is a finite B-algebra by Proposition 3.6, hence we are done.

Since $m > n$, it follows that $y_1, \ldots, y_m$ are algebraically dependent over k. Therefore there is a nonzero polynomial $f \in k[x_1, \ldots, x_m]$ such that $f(y_1, \ldots, y_m) = 0$. For positive integers $r_2, \ldots, r_m$, we define $z_2, \ldots, z_m$ by

$$z_2 = y_2 - y_1^{r_2},\ z_3 = y_3 - y_1^{r_3}, \ldots, z_m = y_m - y_1^{r_m}.$$

It is then clear that $A = k[y_1, z_2, \ldots, z_m]$. If we show that we can choose $r_2, \ldots, r_m$ such that y_1 is integral over $B = k[z_2, \ldots, z_m]$, then A is a finite B-algebra (see Remark 3.4) and we are done.

Let us write $f = \sum_{\alpha \in \Lambda} c_\alpha x^\alpha$ for a finite set $\Lambda \subseteq \mathbf{Z}^m_{\geq 0}$, where all c_α are nonzero and where for $\alpha = (\alpha_1, \ldots, \alpha_m)$ we write x^α for $x_1^{\alpha_1} \cdots x_m^{\alpha_m}$. We know that

$$f(y_1, z_2 + y_1^{r_2}, \ldots, z_m + y_1^{r_m}) = 0.$$

Note that for every $\alpha = (\alpha_1, \ldots, \alpha_m) \in \Lambda$, in the expansion of

$$c_\alpha y_1^{\alpha_1}(z_2 + y_1^{r_2})^{\alpha_2} \cdots (z_m + y_m^{r_m})^{\alpha_m}$$

the unique monomial of top degree with respect to y_1 is

$$y_1^{\alpha_1 + \alpha_2 r_2 + \ldots + \alpha_m r_m}. \tag{6.1}$$

The point is that if we choose $r_2, \ldots, r_m$ such that $0 \ll r_2 \ll r_3 \ll \ldots \ll r_m$, then all the exponents in (6.1), when α runs over the elements of Λ, are distinct. More precisely, we construct $r_2, \ldots, r_m$ inductively such that if $1 \leq k \leq m$ and $\alpha, \beta \in \Lambda$ are such that $(\alpha_1, \ldots, \alpha_k) \neq (\beta_1, \ldots, \beta_k)$, then $\alpha_1 + \alpha_2 r_2 + \ldots + \alpha_k r_k \neq \beta_1 + \beta_2 r_2 + \ldots + \beta_k r_k$. Indeed, there is nothing to do for $k = 1$. If $k \geq 2$ and $r_1, \ldots, r_{k-1}$ have been constructed, we only need to choose r_k such that for α, β as above, we have

$$(\alpha_k - \beta_k) r_k \neq (\beta_1 - \alpha_1) + \ldots + (\alpha_{k-1} - \beta_{k-1}) r_{k-1}.$$

If $\alpha_k - \beta_k = 0$, then this is satisfied by the inductive hypothesis, while if $\alpha_k - \beta_k \neq 0$, then this is clearly achieved for $r_k \gg 0$ (we only need to avoid finitely many values). This completes the proof of the theorem. □

Exercise 6.3. Let $f\colon R \to S$ be an injective homomorphism of finite type and consider the corresponding continuous map $\varphi\colon \mathrm{Spec}(S) \to \mathrm{Spec}(R)$. Show that if R and S are domains, then the following hold:

i) There is a nonzero $f \in R$ such that the inclusion $R_f \hookrightarrow S_f$ factors as

$$R_f \overset{i}{\hookrightarrow} R_f[x_1, \ldots, x_n] \overset{j}{\hookrightarrow} S_f,$$

where $x_1, \ldots, x_n$ are algebraically independent over $\mathrm{Frac}(R)$ and j is finite.

ii) Deduce that there is a nonempty open subset U of $\mathrm{Spec}(R)$ that's contained in $\mathrm{Im}(\varphi)$; in particular, $\mathrm{Im}(\varphi)$ is dense in $\mathrm{Spec}(R)$.

6.2. Hilbert's Nullstellensatz

In this section we deduce some easy consequences of Noether normalization.

COROLLARY 6.4. If k is a field, A is a finitely generated k-algebra, and $K = A/\mathfrak{m}$, where $\mathfrak{m}$ is a maximal ideal in A, then K is a finite extension of k.

PROOF. Note that K is a field which is finitely generated as a k-algebra. It follows from Theorem 6.1 that if $n = \operatorname{trdeg}(K/k)$, then there is a finite injective homomorphism

$$k[x_1, \dots, x_n] \hookrightarrow K.$$

Since K is a field, it follows from Proposition 3.10 that $k[x_1, \dots, x_n]$ is a field, hence $n = 0$. Therefore K/k is finite. □

COROLLARY 6.5. If k is a field and $f\colon A \to B$ is a homomorphism of finitely generated k-algebras, then for every maximal ideal $\mathfrak{m}$ in B, the ideal $f^{-1}(\mathfrak{m}) \subseteq A$ is maximal.

PROOF. If $\mathfrak{p} = f^{-1}(\mathfrak{m})$, then we have an injective k-algebra homomorphism $i\colon A/\mathfrak{p} \hookrightarrow K = B/\mathfrak{m}$. By assumption, K is a field, and Corollary 6.4 implies that K/k is a finite extension. In particular, i is an integral homomorphism, hence Proposition 3.10 implies that $A/\mathfrak{p}$ is a field, hence $\mathfrak{p}$ is a maximal ideal. □

REMARK 6.6. It follows from Corollary 6.5 that if $f\colon A \to B$ is a homomorphism of finitely generated k-algebras, then $\operatorname{Spec}(f)$ induces a (continuous) map $\operatorname{Max}(B) \to \operatorname{Max}(A)$. Our goal in the remaining part of this chapter is to show that for finitely generated algebras over a field, the maximal spectrum recovers, in fact, all the topological information contained in the prime spectrum. We will do this first when the field k is algebraically closed, by making use of the following result.

COROLLARY 6.7 (Hilbert's Nullstellensatz, weak version). If k is an algebraically closed field, then every maximal ideal $\mathfrak{m}$ in $R = k[x_1, \dots, x_n]$ is of the form $(x_1 - a_1, \dots, x_n - a_n)$, for some $a_1, \dots, a_n \in k$.

PROOF. It follows from Corollary 6.4 that if $K = R/\mathfrak{m}$, then the field extension K/k is finite. Since k is algebraically closed, the canonical homomorphism $k \to K$ is an isomorphism. In particular, for every i there is $a_i \in R$ such that $x_i - a_i \in \mathfrak{m}$. Therefore we have $(x_1 - a_1, \dots, x_n - a_n) \subseteq \mathfrak{m}$ and since both ideals are maximal, they must be equal. □

We will prove a stronger version of Nullstellensatz in the next section, after discussing the correspondence between ideals in $k[x_1, \dots, x_n]$ and subsets of k^n.

6.3. Introduction to classical affine algebraic geometry

Let $R_n = k[x_1, \dots, x_n]$, where k is an algebraically closed field and n is a positive integer. Recall that $\operatorname{Spec}(R_n)$ contains as a subspace the *maximal spectrum* $\operatorname{Max}(R_n)$, consisting of the maximal ideals in R_n, with the induced topology. Note that by Corollary 6.7 we have a canonical bijection between $\operatorname{Max}(R_n)$ and the set k^n (also written as $\mathbf{A}^n_k$ and called the *n-dimensional affine space* over k), that maps the maximal ideal $(x_1 - a_1, \dots, x_n - a_n)$ to the point $(a_1, \dots, a_n)$. We get a topology on $\mathbf{A}^n_k$ (the *Zariski topology*) that makes this bijection a homeomorphism. The closed subsets of $\mathbf{A}^n_k$ are also called *algebraic subsets*.

By definition, a closed subset of $\mathrm{Max}(R_n)$ is of the form $V(I) \cap \mathrm{Max}(R_n)$, for some ideal $I \subseteq R_n$. We will denote the corresponding algebraic subset of $\mathbf{A}_k^n$ by $Z(I)$ (though this is sometimes denoted by $V(I)$ as well). Note that for every $a = (a_1, \ldots, , a_n) \in k^n$, the kernel of the evaluation homomorphism

$$k[x_1, \ldots, x_n] \to k, \quad f \to f(a)$$

is the maximal ideal $(x_1 - a_1, \ldots, x_n - a_n)$. We thus see that for an ideal I in R_n, we have $I \subseteq (x_1 - a_1, \ldots, x_n - a_n)$ if and only if $f(a) = 0$ for all $f \in I$. Since $V(I) \cap \mathrm{Max}(R_n)$ consists of all maximal ideals containing I, it follows that

$$Z(I) = \big\{(a_1, \ldots, a_n) \in \mathbf{A}_k^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\big\}.$$

Remark 6.8. Of course, in this context one is interested in studying the algebraic subsets of the affine space and the Zariski topology on $\mathbf{A}_k^n$ provides a convenient framework for doing so. Moreover, this motivates the definition of the topology on $\mathrm{Spec}(R)$ for an arbitrary ring R.

Recall that for any ring R, we have seen in Exercise 2.36 we have order reversing inverse bijections between the closed subsets of $\mathrm{Spec}(R)$ and the radical ideals in R. The same result holds for $\mathrm{Max}(R_n)$, though here the result is less formal: it relies on a strong version of Nullstellensatz. As in Exercise 2.36, if V is a closed subset of $\mathrm{Max}(R_n)$, we put $I(V) := \bigcap_{\mathfrak{m} \in V} \mathfrak{m} \subseteq R_n$. Note that if $Z \subseteq \mathbf{A}_k^n$ is the closed subset corresponding to V, then $I(V)$ (which we also write as $I(Z)$) is given by

$$I(V) = \{f \in k[x_1, \ldots, x_n] \mid f(a) = 0 \text{ for all } a \in Z\}.$$

In the next proposition we collect some easy properties of the maps $I(-)$ and $Z(-)$.

Proposition 6.9. Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals in R_n and A, B be closed subsets of $\mathbf{A}_k^n$.

i) If $\mathfrak{a} \subseteq \mathfrak{b}$, then $Z(\mathfrak{b}) \subseteq Z(\mathfrak{a})$.
ii) If $A \subseteq B$, then $I(B) \subseteq I(A)$.
iii) We have $Z\big(I(A)\big) = A$.
iv) We have $\mathrm{rad}(\mathfrak{a}) \subseteq I\big(Z(\mathfrak{a})\big)$.

Proof. The assertions in i) and ii) are straightforward to check. Furthermore, it follows directly from the definitions that we have the inclusions $A \subseteq Z\big(I(A)\big)$ and $\mathfrak{a} \subseteq I\big(Z(\mathfrak{a})\big)$. For every $Z \subseteq \mathbf{A}_k^n$, the ideal $I(Z)$ is radical (being an intersection of maximal ideals), hence $\mathrm{rad}(\mathfrak{a}) \subseteq I\big(Z(\mathfrak{a})\big)$.

In order to complete the proof of the proposition, we are left with proving the inclusion $Z\big(I(A)\big) \subseteq A$ in iii). Since A is closed, we can write $A = Z(J)$ for some ideal J in R_n. In this case, the inclusion $J \subseteq I\big(Z(J)\big)$ implies by i) that we have

$$A = Z(J) \supseteq Z\big(I(Z(J))\big) = Z\big(I(A)\big).$$

This completes the proof of the proposition. □

We next show that, in fact, we have equality in iv) above:

Theorem 6.10 (Hilbert's Nullstellensatz, strong version). *If $\mathfrak{a}$ is an ideal in R_n, then $I\big(Z(\mathfrak{a})\big) = \mathrm{rad}(\mathfrak{a})$.*

PROOF. It follows from Corollary 6.7 that given any ideal $\mathfrak{b}$ of R_n, different from R_n, the zero-locus $Z(\mathfrak{b})$ of $\mathfrak{b}$ is nonempty. Indeed, since $\mathfrak{b} \neq R_n$, there is a maximal ideal $\mathfrak{m}$ containing $\mathfrak{b}$. By Corollary 6.7, we have

$$\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n) \quad \text{for some} \quad a_1, \dots, a_n \in k.$$

In particular, we see that $a = (a_1, \dots, a_n) \in Z(\mathfrak{m}) \subseteq Z(\mathfrak{b})$. We will use this fact in the polynomial ring $R_{n+1} = k[x_1, \dots, x_n, y]$; this is *Rabinovich's trick*.

We only need to prove the inclusion $I\big(Z(\mathfrak{a})\big) \subseteq \operatorname{rad}(\mathfrak{a})$. Suppose that $f \in I\big(Z(\mathfrak{a})\big)$. Consider now the ideal $\mathfrak{b}$ in R_{n+1} generated by $\mathfrak{a}$ and by $1 - fy$. If $\mathfrak{b} \neq R_{n+1}$, we have seen that there is $(a_1, \dots, a_n, b) \in Z(\mathfrak{b})$. By definition of $\mathfrak{b}$, this means that $g(a_1, \dots, a_n) = 0$ for all $g \in \mathfrak{a}$ (that is, $(a_1, \dots, a_n) \in Z(\mathfrak{a})$) and $1 = f(a_1, \dots, a_n)g(b)$. In particular, we have $f(a_1, \dots, a_n) \neq 0$, contradicting the fact that $f \in I\big(Z(\mathfrak{a})\big)$.

We thus conclude that $\mathfrak{b} = R$. Therefore we can find $f_1, \dots, f_r \in \mathfrak{a}$ and $g_1, \dots, g_{r+1} \in R_{n+1} = R_n[y]$ such that

$$\sum_{i=1}^{r} f_i(x)g_i(x, y) + \big(1 - f(x)y\big)g_{r+1}(x, y) = 1. \tag{6.2}$$

We now consider the R_n-algebra homomorphism $\varphi\colon R_n[y] \to (R_n)_f$ given by $\varphi(y) = \frac{1}{f}$. The relation (6.2) gives

$$\sum_{i=1}^{r} f_i(x)g_i\big(x, 1/f(x)\big) = 1$$

and after clearing the denominators (recall that R_n is a domain), we see that there is a positive integer N such that $f^N \in (f_1, \dots, f_r)$, hence $f \in \operatorname{rad}(\mathfrak{a})$. This completes the proof of the theorem. □

COROLLARY 6.11. If R is a k-algebra of finite type, where k is an algebraically closed field, then for every closed subset Z of $\operatorname{Spec}(R)$, $Z \cap \operatorname{Max}(R)$ is dense in Z.

PROOF. Let's consider a surjective k-algebra homomorphism

$$p\colon S = k[x_1, \dots, x_n] \to R.$$

In this case, $\operatorname{Spec}(p)$ gives a homeomorphism of $\operatorname{Spec}(R)$ onto a closed subset of $\operatorname{Spec}(S)$. Without any loss of generality, we may thus assume that $R = k[x_1, \dots, x_n]$. Let $I \subseteq R$ be an ideal such that $Z = V(I)$ and suppose that $U \subseteq V(I)$ is nonempty. By Remark 2.8, we may assume that $U = Z \cap D(a)$, for some $a \in R$. The fact that U is nonempty is equivalent to $V(I) \not\subseteq V(a)$, which by Exercise 2.36 is equivalent to $a \notin \operatorname{rad}(I)$. In this case, it follows from Theorem 6.10 that there is $\mathfrak{m} \in \operatorname{Max}(R)$ with $\mathfrak{m} \supseteq I$ and such that $a \notin \mathfrak{m}$. Therefore $Z \cap D(a) \cap \operatorname{Max}(R)$ is nonempty. □

We end this chapter by briefly describing the category of affine algebraic varieties over k.

DEFINITION 6.12. An *affine algebraic variety* (over k) is an algebraic subset X of some affine space $\mathbf{A}_k^n$, for some $n \geq 0$. Given such X, the *coordinate ring* of X is the quotient $\mathcal{O}(X) := k[x_1, \dots, x_n]/I(X)$. Note that this is a reduced k-algebra of finite type and every such k-algebra is isomorphic to the coordinate ring of an algebraic variety.

REMARK 6.13. Note that we have a canonical homomorphism

$$\mathcal{O}(X) \to \{f\colon X \to k\}$$

that maps the class $\overline{g}$ of $g \in k[x_1, \ldots, x_n]$ to the map $a \to g(a)$ (note that this is indeed well-defined and the resulting homomorphism is injective by definition of $I(X)$). The image of $\mathcal{O}(X)$ are the *regular functions* on X.

DEFINITION 6.14. Let $X \subseteq \mathbf{A}_k^m$ and $Y \subseteq \mathbf{A}_k^n$. A *morphism of affine algebraic varieties* $f\colon X \to Y$ is a map such that the composition $X \xrightarrow{f} Y \hookrightarrow \mathbf{A}_k^n$ is given by $(f_1, \ldots, f_n)$, where each $f_i\colon X \to k$ is a regular function on X.

EXERCISE 6.15. Show that if $f\colon X \to Y$ and $g\colon Y \to Z$ are morphisms of affine algebraic varieties, then their composition $g \circ f$ is a morphism of affine algebraic varieties. We thus see that we have the *category of affine algebraic varieties over* k.

REMARK 6.16. Let X and Y be as in Definition 6.14. Given $f_1, \ldots, f_n \in k[x_1, \ldots, x_m]$, we have a unique morphism of k-algebras

$$\varphi\colon k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_m],\ \varphi(x_i) = f_i \quad \text{for} \quad 1 \leq i \leq n.$$

Note that the map $f = (f_1, \ldots, f_n)\colon X \to \mathbf{A}_k^n$ is uniquely determined by the classes of $f_1, \ldots, f_n$ in $\mathcal{O}(X)$. Moreover, the image of f is contained in Y (so it corresponds to a morphism $X \to Y$) if and only if for every $g \in I(Y)$, we have $\varphi(g) \in I(X)$. This is the case if and only if φ induces a k-algebra homomorphism $\mathcal{O}(Y) \to \mathcal{O}(X)$. We thus have a canonical bijection between the morphisms of affine algebraic varieties $X \to Y$ and $\mathrm{Hom}_{k-\mathrm{alg}}\big(\mathcal{O}(Y), \mathcal{O}(X)\big)$. It is easy to check that this identification is compatible with composition. Since every reduced k-algebra of finite type is isomorphic to $\mathcal{O}(X)$ for some affine algebraic variety X over k, a general result of category theory implies that the functor that maps every affine variety X to the k-algebra $\mathcal{O}(X)$ and every morphism $X \to Y$ to the corresponding k-algebra homomorphism $\mathcal{O}(Y) \to \mathcal{O}(X)$, gives an equivalence of categories between the category of affine algebraic varieties over k and the dual of the category of reduced finitely generated k-algebras.

EXAMPLE 6.17. The projection $p\colon \mathbf{A}_k^n \to \mathbf{A}_k^{n-1}$ given by $p(a_1, \ldots, a_n) = (a_1, \ldots, a_{n-1})$ is a morphism of affine algebraic varieties. The corresponding k-algebra homomorphism is the inclusion $k[x_1, \ldots, x_{n-1}] \hookrightarrow k[x_1, \ldots, x_n]$.

EXAMPLE 6.18. The map $f\colon \mathbf{A}_k^2 \to \mathbf{A}_k^2$ given by $f(a_1, a_2) = (a_1, a_1a_2)$ is a morphism of affine algebraic varieties. The corresponding k-algebra homomorphism $\varphi\colon k[x_1, x_2] \to k[x_1, x_2]$ is given by $\varphi(x_1) = x_1$ and $\varphi(x_2) = x_1x_2$.Note that image of f consists of $\big((\mathbf{A}^1 \smallsetminus \{0\}) \times \mathbf{A}^1\big) \cup \big\{(0,0)\big\}$.

DEFINITION 6.19. A map $f\colon X \to Y$ between affine algebraic varieties over k is an *isomorphism* if it is bijective and both f and f^{-1} are morphisms. It follows easily from the above remark that a morphism $f\colon X \to Y$ is an isomorphism if and only if the corresponding k-algebra homomorphism $\mathcal{O}(Y) \to \mathcal{O}(X)$ is an isomorphism.

EXAMPLE 6.20. Let $X = Z(x_1^2 - x_2^3) \subseteq \mathbf{A}_k^2$ and consider the map $f\colon \mathbf{A}^1 \to X$ given by $f(a) = (a^3, a^2)$. This is a morphism of affine algebraic varieties corresponding the the k-algebra homomorphism $\varphi\colon k[x_1, x_2]/(x_1^2 - x_2^3) \to k[y]$ given by $\varphi(\overline{x_1}) = y^3$ and $\varphi(\overline{x_2}) = y^2$. Note that f is a bijective morphism, but it is not an isomorphism.

EXAMPLE 6.21. Suppose now that $\mathrm{char}(k) = p > 0$ and consider the map $f\colon \mathbf{A}_k^n \to \mathbf{A}_k^n$ given by $f(a_1, \ldots, a_n) = (a_1^p, \ldots, a_n^p)$. This is a morphism that is bijective, but it is not an isomorphism.

EXERCISE 6.22. Show that if $X \subseteq \mathbf{A}_k^m$ and $Y \subseteq \mathbf{A}_k^n$ are two affine algebraic varieties and $f\colon X \to Y$ is a morphism, then f is continuous.

EXERCISE 6.23.
i) Show that if X and Y are topological spaces, with X irreducible, and $f\colon X \to Y$ is a continuous map, then $\overline{f(X)}$ is irreducible.
ii) Show that the subset
$$M_{m,n}^r(k) = \{A \in M_{m,n}(k) \mid \mathrm{rank}(A) \leq r\}$$
of $\mathbf{A}_k^{mn}$ is closed and irreducible.

EXERCISE 6.24. Let $n \geq 2$ be an integer.
i) Show that the set
$$B_n = \left\{(a_0, a_1, \ldots, a_n) \in \mathbf{A}_k^{n+1} \mid \mathrm{rank} \begin{pmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ a_1 & a_2 & \ldots & a_n \end{pmatrix} \leq 1\right\}$$
is a closed subset of $\mathbf{A}_k^{n+1}$.
ii) Show that
$$B_n = \{(s^n, s^{n-1}t, \ldots, t^n) \mid s, t \in k\}.$$
Deduce that B_n is irreducible.

6.4. The case of arbitrary fields

Our goal is to prove the following version of Corollary 6.11 over arbitrary fields.

PROPOSITION 6.25. If R is an algebra of finite type over a field, then for every closed subset Z of $\mathrm{Spec}(R)$, $Z \cap \mathrm{Max}(R)$ is dense in Z.

The proof of Proposition 6.25 follows verbatim the proof of Corollary 6.11, once we show the following

THEOREM 6.26. *If $\mathfrak{a}$ is an ideal in a finitely generated algebra R over a field k, then $\mathrm{rad}(\mathfrak{a}) = \bigcap_{\mathfrak{m} \supseteq \mathfrak{a}} \mathfrak{m}$, where $\mathfrak{m}$ varies over the maximal ideals containing $\mathfrak{a}$.*

PROOF. Since we know that $\mathrm{rad}(\mathfrak{a}) = \bigcap_{\mathfrak{p} \supseteq \mathfrak{a}} \mathfrak{p}$, where $\mathfrak{p}$ varies over the prime ideals containing $\mathfrak{a}$ (see Exercise 2.35), it follows that it is enough to prove the assertion in the theorem when $\mathfrak{a}$ is a prime ideal, hence from now on we make this assumption. Of course, the inclusion $\mathfrak{a} \subseteq \bigcap_{\mathfrak{m} \supseteq \mathfrak{a}} \mathfrak{m}$ is trivial, hence we only need to prove the opposite inclusion.

Note that we can find an isomorphism $R \simeq k[x_1, \ldots, x_n]/I$ and the ideal $\mathfrak{a}$ corresponds to $\mathfrak{b}/I$, for some prime ideal $\mathfrak{b}$ in $k[x_1, \ldots, x_n]$. After replacing R by $k[x_1, \ldots, x_n]$ and $\mathfrak{a}$ by $\mathfrak{b}$, we see that we may assume that $R = k[x_1, \ldots, x_n]$.

Consider an algebraic closure $\overline{k}$ of k and consider the inclusion homomorphism
$$i\colon R = k[x_1, \ldots, x_n] \hookrightarrow R' = \overline{k}[x_1, \ldots, x_n].$$
This is an integral homomorphism: every element of $\overline{k}$ is integral over k, hence over R, and each x_i is clearly integral over R; therefore the assertion follows from

Proposition 3.7. We apply Theorem 3.12 for the prime ideal $\mathfrak{a} \subseteq R$: we get a prime ideal $\mathfrak{a}' \subseteq R'$ such that $\mathfrak{a}' \cap R = \mathfrak{a}$. Applying Theorem 6.10, we obtain

$$\mathfrak{a}' = \bigcap_{\mathfrak{m}' \supseteq \mathfrak{a}'} \mathfrak{m}',$$

where the intersection is over the maximal ideals in $\mathfrak{m}' \subseteq R'$ that contain $\mathfrak{a}'$. Note that for every such ideal $\mathfrak{m}'$, the intersection $\mathfrak{m}' \cap R$ is a maximal ideal in R by Corollary 3.11. The conclusion of the proposition thus follows from the inclusion

$$\bigcap_{\mathfrak{m} \supseteq \mathfrak{a}} \mathfrak{m} \subseteq R \cap \bigcap_{\mathfrak{m}' \supseteq \mathfrak{a}'} \mathfrak{m}' = R \cap \mathfrak{a}' = \mathfrak{a}.$$

□

CHAPTER 7

Dimension theory

Our goal in this chapter is to discuss the main results concerning the dimension theory of Noetherian rings.

7.1. The dimension of a ring

The notion of (Krull) dimension makes sense for an arbitrary topological space, as follows.

DEFINITION 7.1. If X is a nonempty topological space, then the *dimension* of X (also called *Krull dimension*), denoted $\dim(X)$, is the supremum over the nonnegative integers n, with the property that there is a sequence

$$X_0 \subsetneq X_1 \subsetneq \ldots \subsetneq X_n,$$

where $X_0, \ldots, X_n$ are irreducible closed subsets of X (we will refer to this as a *chain of irreducible closed subsets* of X). By convention, we put $\dim(X) = -1$ if $X = \emptyset$.

DEFINITION 7.2. If R is a commutative ring, then the *dimension* of R, denoted $\dim(R)$, is the dimension of $\mathrm{Spec}(R)$.

REMARK 7.3. Note that by Exercise 4.11, the irreducible subsets of $\mathrm{Spec}(R)$ are those of the form $V(\mathfrak{p})$, where $\mathfrak{p}$ is a prime ideal of R. Moreover, it follows from Exercise 2.36 that if $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime ideals in R, we have $V(\mathfrak{p}_1) \subseteq V(\mathfrak{p}_2)$ if and only if $\mathfrak{p}_2 \subseteq \mathfrak{p}_1$. Therefore if $R \neq 0$, then the dimension of R is the supremum of the nonnegative integers n, such that there is a sequence

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$$

of prime ideals in R (we will refer to this as a *chain of prime ideals* in R).

EXAMPLE 7.4. It is clear that if k is a field, then $\dim(k) = 0$. In general, for a ring R we have $\dim(R) = 0$ if and only if every prime ideal is maximal.

EXAMPLE 7.5. Let k be a field. For every positive integer n, we have the following sequence of prime ideals in $k[x_1, \ldots, x_n]$:

$$(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \ldots \subsetneq (x_1, \ldots, x_n).$$

This implies that $\dim\big(k[x_1, \ldots, x_n]\big) \geq n$. We will see later that this is, in fact, an equality.

EXAMPLE 7.6. Since the prime ideals in $\mathbf{Z}$ are (0) and (p), where p is a prime integer, it follows that $\dim(\mathbf{Z}) = 1$. The same argument shows that if R is a PID and it is not a field, then $\dim(R) = 1$.

EXAMPLE 7.7. For every ideal I in R, we have $\dim(R/I) \leq \dim(R)$. Similarly, for every multiplicative system S in R, we have $\dim(S^{-1}R) \leq \dim(R)$. The assertions follow from the description of the prime ideals in R/I and $S^{-1}R$ in terms of the prime ideals in R.

DEFINITION 7.8. If M is a finitely generated module over a ring R, then the *dimension* of M is

$$\dim(M) := \dim\big(\mathrm{Supp}(M)\big).$$

REMARK 7.9. Note that by Proposition 5.14, we have

$$\dim(M) = \dim\big(R/\mathrm{Ann}_R(M)\big).$$

DEFINITION 7.10. If X is a topological space and Z is an irreducible closed subset of X, then the *codimension* of Z, denoted $\mathrm{codim}(Z)$ or $\mathrm{codim}_X(Z)$, is the supremum of the nonnegative integers n, with the property that there is a sequence

$$Z = Z_0 \subsetneq Z_1 \subsetneq \ldots \subsetneq Z_n \subseteq X,$$

with each Z_i a closed and irreducible subset of X. If X is a Noetherian topological space and Z is *any* nonempty closed subset, then the codimension of Z is defined by

$$\mathrm{codim}(Z) = \min_{W \subseteq Z} \mathrm{codim}(W),$$

where W is a maximal irreducible closed subset of Z.

DEFINITION 7.11. For every ring R, if $\mathfrak{p}$ is a prime ideal in R, the *codimension* $\mathrm{codim}(\mathfrak{p})$ (sometimes also called *height* and denoted $\mathrm{ht}(\mathfrak{p})$) is the codimension of the corresponding closed irreducible subset $V(\mathfrak{p})$ of $\mathrm{Spec}(R)$. Explicitly, this is the supremum over the nonnegative integers n such that there is a sequence

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n = \mathfrak{p}$$

of prime ideals in R.

If I is a proper ideal in R, the *codimension* $\mathrm{codim}(I)$ is the codimension of $V(I)$ in $\mathrm{Spec}(R)$. If $(\mathfrak{p}_i)_{i\in I}$ are the minimal prime ideals containing I, then

$$\mathrm{codim}(I) = \min_{i\in I} \mathrm{codim}(\mathfrak{p}_i).$$

In the next proposition we collect a few properties of Krull dimension and codimension that follow directly from the definition.

PROPOSITION 7.12. Let $\mathfrak{a}$ and $\mathfrak{p}$ be ideals in R, with $\mathfrak{p}$ prime and $\mathfrak{a} \neq R$.

i) If $(\mathfrak{q}_i)_{i\in I}$ are the minimal prime ideals in R, then $\dim(R) = \sup_i \dim(R/\mathfrak{q}_i)$.
ii) If $(\mathfrak{p}_j)_{j\in J}$ are the minimal primes of R contained in $\mathfrak{p}$, then $\mathrm{codim}(\mathfrak{p}) = \sup_j \mathrm{codim}(\mathfrak{p}/\mathfrak{p}_j)$.
iii) We have $\mathrm{codim}(\mathfrak{p}) = \dim(R_\mathfrak{p})$.
iv) We have $\dim(R) \geq \dim(R/\mathfrak{a}) + \mathrm{codim}(\mathfrak{a})$.

PROOF. The assertions in i) and ii) follow from the definition and the fact that every prime ideal contains a minimal prime ideal (see Remark 5.18). The equality in iii) follows from the description of prime ideals in localizations (see Exercise 2.31). Finally, in order to prove iv), note that if $(\mathfrak{p}_j)_{j\in J}$ are the minimal prime ideals containing I, then it follows from i) that

$$\dim(R/I) = \sup_{j\in J} \dim(R/\mathfrak{p}_j).$$

Note now that since we can concatenate a chain of prime ideals contained in $\mathfrak{p}_j$ with a sequence of prime ideals containing $\mathfrak{p}_j$, we have

$$\dim(R) \geq \dim(R/\mathfrak{p}_j) + \operatorname{codim}(\mathfrak{p}_j) \quad \text{for all} \quad j \in J.$$

By definition of $\operatorname{codim}(I)$, we thus have

$$\operatorname{codim}(I) \leq \operatorname{codim}(\mathfrak{p}_j) \leq \dim(R) - \dim(R/\mathfrak{p}_j) \quad \text{for all} \quad j \in J.$$

By taking the infimum over $j \in J$, we obtain the inequality in iv). □

As a consequence of our results on the behavior of prime ideals in integral ring extensions, we obtain the following:

THEOREM 7.13. *If $R \hookrightarrow S$ is an injective integral homomorphism, then* $\dim(R) = \dim(S)$.

PROOF. We prove separately the two inequalities. Suppose first that we have a chain of prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$$

in R. First, it follows from Theorem 3.12 that there is a prime ideal $\mathfrak{q}_0$ in S such that $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$. Next, by successively applying Theorem **??**, we obtain prime ideals $\mathfrak{q}_i$ in S, for $1 \leq i \leq n$, such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ and $\mathfrak{q}_{i-1} \subseteq \mathfrak{q}_i$ for $1 \leq i \leq n$. Note that $\mathfrak{q}_{i-1} \neq \mathfrak{q}_i$ since $\mathfrak{q}_{i-1} \cap R \neq \mathfrak{q}_i \cap R$. We thus see that $\dim(S) \geq n$, hence $\dim(S) \geq \dim(R)$.

In order to prove the reverse inequality, suppose that we have a chain of prime ideals

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_m$$

in S. If $\mathfrak{p}_i = \mathfrak{q}_i \cap R$, then we have a sequence of prime ideals in R

$$\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \ldots \subseteq \mathfrak{p}_m.$$

Moreover, all inclusions are strict by Theorem 3.15. Therefore $\dim(R) \geq m$ and we obtain $\dim(R) \geq \dim(S)$. □

EXERCISE 7.14. Prove that for any rings $R_1, \ldots, R_n$, we have

$$\dim(R_1 \times \ldots \times R_n) = \max_{i=1}^{n} \dim(R_i).$$

7.2. Modules of finite length

Before proving the main results in dimension theory, we discuss Artinian rings and, more generally, modules of finite length. To begin with, let R be an arbitrary (commutative) ring.

DEFINITION 7.15. An R-module M is *simple* if $M \neq 0$ and for every submodule M' of M, we have either $M' = 0$ or $M' = M$.

REMARK 7.16. An R-module M is simple if and only if it is isomorphic to $R/\mathfrak{m}$, for some maximal ideal $\mathfrak{m}$ of R. Indeed, suppose that M is simple and let $u \in M \smallsetminus \{0\}$. Since M is simple, it follows that $Ru = M$. If $\mathfrak{m} = \operatorname{Ann}_R(u)$, then $M = Ru \simeq R/\mathfrak{m}$ and the fact that M is simple implies that $\mathfrak{m}$ is a maximal ideal in R. The converse is clear.

DEFINITION 7.17. An R-module M is of *finite length* if it has a *composition series*, that is, a sequence of submodules

$$0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_r = M$$

such that M_i/M_{i-1} is a simple module for $1 \leq i \leq r$. We denote by $\ell(M)$ (or $\ell_R(M)$ if the ring is not clear from the context) the smallest r such that we have a composition series of length r, as above (we will see shortly that, in fact, all composition series have the same length).

DEFINITION 7.18. An R-module M is *Artinian* if it satisfies the *Descending Chain Condition* (DCC, for short), that is, there is no infinite strictly decreasing sequence

$$M_1 \supsetneq M_2 \supsetneq \ldots$$

of submodules of M. The ring R is *Artinian* if it is Artinian when viewed as an R-module.

We begin with some easy properties regarding finite length modules.

PROPOSITION 7.19. If M' is a submodule of the R-module M, then the module M has finite length if and only if both M' and M/M' have finite length, Moreover, if $M' \neq M$, then $\ell(M') < \ell(M)$.

PROOF. It is clear that if M' and M'' have finite length, then we obtain a composition series for M by concatenating the composition series for M' and M''. Suppose now that M has finite length and consider a composition series

$$0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_n = M.$$

Note that for $1 \leq i \leq n$, the quotient $(M_i \cap M')/(M_{i-1} \cap M')$ is isomorphic to a submodule of M_i/M_{i-1}, hence it is either 0 or a simple module. It follows that after removing the repeated terms in the sequence

$$0 = M_0 \cap M' \subseteq M_1 \cap M' \subseteq \ldots \subseteq M_n \cap M' = M',$$

we obtain a composition series for M'.

This implies $\ell(M') \leq \ell(M)$. Furthermore, we see that if we have equality, then there are no terms to remove, that is

$$(M_i \cap M')/(M_{i-1} \cap M') = M_i/M_{i-1} \quad \text{for} \quad 1 \leq i \leq n.$$

This implies $M_i \subseteq M_{i-1} + M'$ for $1 \leq i \leq n$, and we see by induction on i that $M_i \subseteq M'$ for all i, hence $M = M'$.

In order to show that M/M' has finite length, consider the image $\overline{M}_i$ of M_i in M/M'. In this case $\overline{M}_i/\overline{M}_{i-1}$ is a quotient of M_i/M_{i-1}, hence it is either 0 or a simple module. It follows that after removing the repeated terms in the sequence

$$0 = \overline{M}_0 \subseteq \overline{M}_1 \subseteq \ldots \subseteq \overline{M}_n = M/M',$$

we obtain a composition series for M/M'. □

PROPOSITION 7.20. An R-module M has finite length if and only if it is both Noetherian and Artinian.

PROOF. Suppose first that M is both Noetherian and Artinian. Since M is Noetherian, it follows from Proposition 4.2 that if $M \neq 0$, then the family $\mathcal{P}_1$ consisting of all proper submodules of M (this is nonempty, since it contains 0) has a maximal element M_1. It is then clear that M/M_1 is simple. If $M_1 \neq 0$, then we

apply again Proposition 4.2 to conclude that the family $\mathcal{P}_2$ consisting of all proper submodules of M_1 has a maximal element M_2, so M_1/M_2 is simple. Repeating this argument, we construct a sequence of submodules

$$M \supsetneq M_1 \supsetneq M_2 \supsetneq \dots;$$

since M is Artinian, this sequence stabilizes, that is, then is n such that $M_n = 0$. We thus obtain a composition series for M.

Suppose now that M has finite length. If there is a strictly increasing infinite sequence of submodules

$$M_1 \subsetneq M_2 \subsetneq \dots \subseteq M,$$

ihen it follows from Proposition 7.19 that all M_n have finite length and

$$\ell(M_1) < \ell(M_2) < \dots \leq \ell(M),$$

a contradiction, since all $\ell(M_i)$ are integers.

Similarly, if there is a strictly decreasing infinite sequence of submodules

$$M \supseteq M_1 \supsetneq M_2 \supsetneq \dots,$$

then all M_n have finite length and

$$\ell(M_1) > \ell(M_2) > \dots,$$

a contradiction, since all $\ell(M_n)$ are nonnegative integers. □

PROPOSITION 7.21 (Jordan-Hölder). If M is an R-module of finite length, then any two composition series of M have the same length, and moreover, the successive quotients are pairwise isomorphic after relabeling.

PROOF. We say that two composition series are *equivalent* if the successive quotients are pairwise isomorphic, after relabeling. We argue by contradiction. Recall first that all submodules of M have finite length by Proposition 7.19. Assuming that the conclusion fails for M, we replace M by a *minimal* element of the family consisting of the submodules of M for which the conclusion fails (note that such a minimal element exists since M is Artinian by Proposition 7.20). Therefore we may and will assume that the theorem holds for all proper submodules of M.

Consider two composition series

$$M_\bullet : \ 0 = M_r \subsetneq M_{r-1} \subsetneq \dots \subsetneq M_0 = M \quad \text{and}$$

$$N_\bullet : \ 0 = N_s \subsetneq N_{s-1} \subsetneq \dots \subsetneq N_0 = M$$

that are not equivalent. If $M_1 = N_1$, then the corresponding composition series of this submodule are equivalent, and we get a contradiction. Suppose now that $M_1 \neq N_1$, in which case, using the fact that M/M_1 is simple, we conclude that $M_1 + N_1 = M$. Therefore we have

$$M_1/(M_1 \cap N_1) \simeq M/N_1 \quad \text{and} \quad N_1/(M_1 \cap N_1) \simeq M/M_1. \tag{7.1}$$

After choosing any composition series for $M_1 \cap N_1$, we obtain the following composition series for M:

$$M'_\bullet : \quad 0 = K_t \subsetneq K_{t-1} \subsetneq \dots \subsetneq K_0 = M_1 \cap N_1 \subsetneq M_1 \subsetneq M \quad \text{and}$$

$$N'_\bullet : \quad 0 = K_t \subsetneq K_{t-1} \subsetneq \dots \subsetneq K_0 = M_1 \cap N_1 \subsetneq N_1 \subsetneq M.$$

Since M_1 satisfies the proposition, it follows that $M_\bullet$ and $M'_\bullet$ are equivalent, and since N_1 satisfies the theorem, it follows that $N_\bullet$ and $N'_\bullet$ are equivalent. Since

$M'_\bullet$ and $N'_\bullet$ are equivalent by (7.1), it follows that $M_\bullet$ and $N_\bullet$ are equivalent, a contradiction. □

COROLLARY 7.22. If M' is a submodule of an R-module of finite length M, then

$$\ell(M) = \ell(M') + \ell(M'').$$

PROOF. It follows from Proposition 7.19 that both M' and M'' have finite length. Moreover, as pointed out in the proof of the same proposition, we obtain a composition series of M by concatenating composition series for M' and M/M'. Since we now know that all composition series have the same length, we obtain the equality in the statement. □

PROPOSITION 7.23. If R is a Noetherian ring, then an R-module M has finite length if and only if M is finitely generated and $\dim\big(R/\mathrm{Ann}_R(M)\big) = 0$.

REMARK 7.24. Note that if a Noetherian ring has dimension 0, then it has finitely many prime ideals. Indeed, in this case every prime ideal is a minimal prime and we know that there are only finitely many such prime ideals by Remark 5.17.

PROOF OF PROPOSITION 7.23. Suppose first that M has a composition series

$$0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_r = M,$$

with $M_i/M_{i-1} \simeq R/\mathfrak{m}_i$ for $1 \leq i \leq r$, where each $\mathfrak{m}_i$ is a maximal ideal of R. Since each M_i/M_{i-1} is finitely generated, we conclude that M is finitely generated (alternatively, we could use the fact that M is Noetherian by Proposition 7.20, and thus finitely generated). Moreover, we have $\prod_{i=1}^r \mathfrak{m}_i \subseteq \mathrm{Ann}_R(M)$, hence if a prime $\mathfrak{p}$ contains $\mathrm{Ann}_R(M)$, then it must contain some $\mathfrak{m}_i$, hence $\mathfrak{p} = \mathfrak{m}_i$. This implies that $\dim\big(R/\mathrm{Ann}_R(M)\big) = 0$.

Conversely, if M is finitely generated over R, then it follows from Corollary 5.8 that we have submodules

$$0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_r = M,$$

such that $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$ for $1 \leq i \leq r$, where each $\mathfrak{p}_i$ is a prime ideal in R. If we have $\dim\big(R/\mathrm{Ann}_R(M)\big) = 0$, then every prime ideal in $R/\mathrm{Ann}_R(M)$ is a maximal ideal. Since we clearly have $\mathrm{Ann}_R(M) \subseteq \mathfrak{p}_i$ for all i, we conclude that each quotient M_i/M_{i-1} is a simple module, hence M has finite length. □

COROLLARY 7.25. If R is a Noetherian ring, then R is Artinian if and only if $\dim(R) = 0$.

PROOF. If $\dim(R) = 0$, then it follows from Proposition 7.23 that R has finite length as a module over itself, and thus it is Artinian by Proposition 7.20. Conversely, suppose that R is Artinian. Since we know that R is Noetherian, it follows from Proposition 7.20 that R has finite length as a module over itself, in which case $\dim(R) = 0$ by Proposition 7.23. □

REMARK 7.26. If $(R, \mathfrak{m})$ is a Noetherian local ring, then $\dim(R) = 0$ if and only if $\mathfrak{m}^N = 0$ for some N. Indeed, suppose first that $\dim(R) = 0$. In this case it follows from Corollary 7.25 that R is Artinian. By considering the sequence of ideals

$$\ldots \supseteq \mathfrak{m}^N \supseteq \mathfrak{m}^{N+1} \supseteq \ldots,$$

we see that there is N such that $\mathfrak{m}^N = \mathfrak{m}^{N+1}$. In this case Nakayama's Lemma implies $\mathfrak{m}^N = 0$.

Conversely, if we know that $\mathfrak{m}^N = 0$, then for every prime ideal $\mathfrak{p}$ in R, we have $\mathfrak{m}^N \subseteq \mathfrak{p}$, hence $\mathfrak{m} \subseteq \mathfrak{p}$, and thus $\mathfrak{p} = \mathfrak{m}$. Therefore R has a unique prime ideal and it is clear that $\dim(R) = 0$.

Note that if M is a finitely generated module, then by applying the above assertion for $R/\mathrm{Ann}_R(M)$ and using Proposition 7.23, we conclude that M has finite length if and only if there is N such that $\mathfrak{m}^N \cdot M = 0$.

REMARK 7.27. It is in fact a result due to Akizuki that if R is Artinian, it is also Noetherian. For a proof, see [**Mat89**, Theorem 3.2]. We do not discuss the proof since we will not need this result.

REMARK 7.28. We note that if R is a Noetherian ring, with $\dim(R) = 0$, then R is the product of finitely many local rings. Indeed, given a minimal primary decomposition

$$(0) = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r,$$

by the Chinese Remainder theorem we have

$$R \simeq \prod_{i=1}^{r} R/\mathfrak{q}_i$$

(note that the ideals $\mathrm{rad}(\mathfrak{q}_i)$ are mutually distinct maximal ideals, hence $\mathfrak{q}_i + \mathfrak{q}_j = R$ whenever $i \neq j$). Note that each $R/\mathfrak{q}_i$ is a local ring, with maximal ideal $\mathrm{rad}(\mathfrak{q}_i)/\mathfrak{q}_i$.

PROPOSITION 7.29. If R is an algebra of finite type over a field k and M is an R-module, then M has finite length if and only if $\dim_k(M) < \infty$. In particular, R is Artinian if and only if $\dim_k(R) < \infty$.

PROOF. Note that since R is an algebra of finite type over a field, then it is Noetherian (see Example 4.17), hence Proposition 7.20 implies that R is Artinian if and only if it has finite length as an R-module. Therefore the second assertion in the proposition follows from the first one.

Suppose first that M has finite length. Consider a composition series

$$0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_r = M.$$

Note that for $1 \leq i \leq r$, we have $M_i/M_{i-1} \simeq R/\mathfrak{m}_i$ for a maximal ideal $\mathfrak{m}_i$ of R. By Corollary 6.4, we have $\dim_k(M_i/M_{i-1}) < \infty$. In this case we have

$$\dim_k(M) = \sum_{i=1}^{r} \dim_k(M_i/M_{i-1}) < \infty.$$

Conversely, suppose that $\dim_k(M) < \infty$. This clearly implies that M has finite length as a k-vector space, hence it is both Noetherian and Artinian as a k-vector space by Proposition 7.20. Since every R-submodule of M is also a k-vector subspace, it follows that M is both Noetherian and Artinian as an R-module, and thus has finite length by Proposition 7.20. □

EXERCISE 7.30. Let R be a Noetherian ring with $\dim(R) = 0$ and let $f\colon R \to R$ be an R-linear map. Show that if f is injective, then it is also surjective.

EXERCISE 7.31. Prove that if R is a Noetherian ring with $\dim(R) = 0$, and if $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are the prime ideals of R, then the canonical homomorphism

$$\varphi\colon R \to R_{\mathfrak{p}_1} \times \ldots \times R_{\mathfrak{p}_n},\ \varphi(x) = \left(\tfrac{x}{1}, \ldots, \tfrac{x}{1}\right)$$

is a ring isomorphism.

EXERCISE 7.32. Suppose now that R is a Noetherian ring, M is an R-module of finite length, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are the prime ideals in $\mathrm{Supp}(M)$.

i) Show that every module $M_{\mathfrak{p}_i}$ is of finite length (over R) and

$$\ell_R(M) = \sum_{i=1}^{n} \ell(M_{\mathfrak{p}_i}).$$

ii) Show that the canonical R-linear map

$$\varphi\colon M \to \bigoplus_{i=1}^{r} M_{\mathfrak{p}_i}$$

is injective.

iii) Deduce that φ is an isomorphism.

EXERCISE 7.33. Let k a field.

i) Show that if A is an Artinian algebra of finite type over k and k is algebraically closed, then $\ell_A(A) = \dim_k(A)$.

ii) Show that if $R = k[x_1, \ldots, x_n]$, $\mathfrak{m} = (x_1, \ldots, x_n)$, then for every $d \geq 1$, the R-module $R/\mathfrak{m}^d$ has finite length and this is equal to $\binom{n+d-1}{d-1}$.

7.3. The Principal Ideal theorem

The starting point in dimension theory is the following result, known as Krull's Principal Ideal theorem.

THEOREM 7.34. *If R is a Noetherian ring and $\mathfrak{p}$ is a minimal prime ideal containing a principal ideal (x), then* $\mathrm{codim}(\mathfrak{p}) \leq 1$.

PROOF. After replacing R by $R_{\mathfrak{p}}$, we may assume that R is a local ring and $\mathfrak{p}$ is the maximal ideal. It is enough to show that for every prime ideal $\mathfrak{q} \subsetneq \mathfrak{p}$ in R, we have $\mathrm{codim}(\mathfrak{q}) = 0$.

The ring $R/(x)$ is Noetherian and by hypothesis, has only one prime ideal, namely $\mathfrak{p}/(x)$. It follows from Corollary 7.25 that $R/(x)$ is Artinian. Note that if we put $\mathfrak{q}^{(n)} := \mathfrak{q}^n R_{\mathfrak{q}} \cap R$ for $n \geq 1$, then we have the non-increasing chain of ideals in $R/(x)$:

$$\left(\mathfrak{q}^{(1)} + (x)\right)/(x) \supseteq \left(\mathfrak{q}^{(2)} + (x)\right)/(x) \supseteq \ldots \supseteq \left(\mathfrak{q}^{(n)} + (x)\right)/(x) \supseteq \ldots,$$

which thus must stabilize. We deduce that we have $n \geq 1$ such that $\mathfrak{q}^{(n)} + (x) = \mathfrak{q}^{(n+1)} + (x)$. This implies that for every $u \in \mathfrak{q}^{(n)}$, there are $a \in R$ and $v \in \mathfrak{q}^{(n+1)}$ such that $u = v + ax$. Since $ax \in \mathfrak{q}^{(n)}$ and $x \notin \mathfrak{q}$, we have $a \in \mathfrak{q}^{(n)}$ (recall that $\mathfrak{q}^{(n)}$ is $\mathfrak{q}$-primary by Exercise 5.34). We thus conclude that $\mathfrak{q}^{(n)} = x \cdot \mathfrak{q}^{(n)} + \mathfrak{q}^{(n+1)}$. Since x lies in the unique maximal ideal in R, it follows from Nakayama's lemma (see Corollary 2.27) that $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$. This implies that $\mathfrak{q}^n R_{\mathfrak{q}} = \mathfrak{q}^{n+1} R_{\mathfrak{q}}$, and using Nakayama's lemma in $R_{\mathfrak{q}}$, we conclude that $\mathfrak{q}^n R_{\mathfrak{q}} = 0$. This implies that $\mathrm{codim}(\mathfrak{q}) = \dim(R_{\mathfrak{q}}) = 0$ (see Remark 7.26) and thus completes the proof of the theorem. □

The above theorem is usually applied in the following more general form.

COROLLARY 7.35. If R is a Noetherian ring and $\mathfrak{p}$ is a minimal prime ideal containing $(x_1, \ldots, x_n)$, then $\operatorname{codim}(\mathfrak{p}) \leq n$.

PROOF. We argue by induction on n. The assertion is trivial if $n = 0$ (in this case $\mathfrak{p}$ is a minimal prime, hence $\operatorname{codim}(\mathfrak{p}) = 0$) and if $n = 1$, then it follows from the theorem. Suppose now that $n \geq 2$ and we know the assertion for $n - 1$.

Suppose that we have a sequence of prime ideals

$$\mathfrak{p}_m \subsetneq \ldots \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_0 = \mathfrak{p}$$

in R. We need to prove that $m \leq n$. Note first that we may assume that there is no prime ideal $\mathfrak{q}$ with $\mathfrak{p}_1 \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$. Indeed, it is enough to replace $\mathfrak{p}_1$ by a maximal element of $\{\mathfrak{q} \in \operatorname{Spec}(R) \mid \mathfrak{p}_1 \subseteq \mathfrak{q} \subsetneq \mathfrak{p}\}$ (note that such a maximal element exists since R in Noetherian, see Proposition 4.2).

Since $\mathfrak{p}$ is minimal over $(x_1, \ldots, x_n)$, it follows that there is i, with $1 \leq i \leq n$, such that $x_i \notin \mathfrak{p}_1$. After relabeling the x_j, we may assume that $i = 1$. Since there is no prime ideal strictly between $\mathfrak{p}_1$ and $\mathfrak{p}$, it follows that $\mathfrak{p}$ is a minimal prime containing $\mathfrak{p}_1 + (x_1)$. Suppose that the other minimal prime ideals containing $\mathfrak{p}_1 + (x_1)$ are $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$. Let $f \in (\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_s) \smallsetminus \mathfrak{p}$ (since $\mathfrak{q}_i \not\subseteq \mathfrak{p}$, we can choose $f_i \in \mathfrak{q}_i \smallsetminus \mathfrak{p}$ for all i, and then take $f = \prod_{i=1}^{s} f_i$). Note that we may replace R by R_f: since $f \notin \mathfrak{p}$, then we have the sequence of prime ideals in R_f:

$$\mathfrak{p}_m R_f \subsetneq \ldots \subsetneq \mathfrak{p}_1 R_f \subsetneq \mathfrak{p} R_f$$

and $\mathfrak{p}R_f$ is clearly a minimal prime ideal containing $\left(\frac{x_1}{1}, \ldots, \frac{x_n}{1}\right)$. Therefore, after possibly replacing R by R_f, we may and will assume that $\mathfrak{p}$ is the unique minimal prime ideal containing $\mathfrak{p}_1 + (x_1)$, hence $\mathfrak{p}$ is the radical of $\mathfrak{p}_1 + (x_1)$. In this case, for every j, with $2 \leq j \leq n$, we can write

$$x_j^{m_j} - y_j \in (x_1), \quad \text{where} \quad m_j \in \mathbf{Z}_{>0},\ y_j \in \mathfrak{p}_1.$$

Note that we have $(y_2, \ldots, y_n) \subseteq \mathfrak{p}_1$. In order to complete the proof, it is enough to show that $\mathfrak{p}_1$ is a minimal prime ideal containing $(y_2, \ldots, y_n)$: indeed, the inductive hypothesis then gives $m - 1 \leq n - 1$. Suppose that there is a prime ideal $\mathfrak{q}$, with $(y_2, \ldots, y_n) \subseteq \mathfrak{q} \subsetneq \mathfrak{p}_1$. Note that in the quotient ring $R/(y_2, \ldots, y_n)$, the ideal $\overline{\mathfrak{p}} = \mathfrak{p}/(y_2, \ldots, y_n)$ is a minimal prime ideal containing (x_1): this follows from the fact that $\mathfrak{p}$ is a minimal prime ideal containing $(x_1, \ldots, x_n)$ and the fact that in this quotient ring we have $\overline{x_j} \in \operatorname{rad}(x_1)$ for $2 \leq j \leq n$. We thus deduce from the theorem that $\operatorname{codim}(\overline{\mathfrak{p}}) \leq 1$ and thus there is no prime ideal $\mathfrak{q}$, with $(y_2, \ldots, y_r) \subseteq \mathfrak{q} \subsetneq \mathfrak{p}_1$. This completes the proof of the corollary. □

COROLLARY 7.36. If $\mathfrak{p}$ is a prime ideal in a Noetherian ring R, then $\operatorname{codim}(\mathfrak{p}) < \infty$.

PROOF. If $\mathfrak{p} = (a_1, \ldots, a_n)$, then it follows from Corollary 7.35 that $\operatorname{codim}(\mathfrak{p}) \leq n$. □

REMARK 7.37. We note that it is *not* true that if R is a Noetherian ring, then $\dim(R) < \infty$. A famous counterexample was given by Nagata.

We also have the following partial converse to Corollary 7.35:

PROPOSITION 7.38. If $\mathfrak{p}$ is a prime ideal in a Noetherian ring R and $\operatorname{codim}(\mathfrak{p}) = n$, then there are $x_1, \ldots, x_n \in \mathfrak{p}$ such that $\mathfrak{p}$ is a minimal prime containing $(x_1, \ldots, x_n)$.

PROOF. We construct inductively $x_1, \ldots, x_n \in \mathfrak{p}$ such that for every r, with $1 \leq r \leq n$, every ideal containing $x_1, \ldots, x_r$ has codimension $\geq r$. This satisfies the conclusion of the corollary: if $(x_1, \ldots, x_n) \subseteq \mathfrak{q} \subsetneq \mathfrak{p}$, with $\mathfrak{q}$ prime, then $\operatorname{codim}(\mathfrak{q}) \geq n$, hence $\operatorname{codim}(\mathfrak{p}) \geq n+1$, a contradiction.

Let's begin by constructing x_1, assuming $n \geq 1$. Note that if $\mathfrak{p}_1, \ldots, \mathfrak{p}_d$ are the minimal primes of R, then $\mathfrak{p} \not\subseteq (\mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_d)$: otherwise the Prime Avoidance lemma implies $\mathfrak{p} \subseteq \mathfrak{p}_i$ for some i, which implies $\mathfrak{p} = \mathfrak{p}_i$ has codimension 0. We may thus choose $x_1 \in \mathfrak{p} \smallsetminus (\mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_d)$. By construction, every prime ideal containing x_1 has codimension ≥ 1.

Suppose now that $x_1, \ldots, x_r \in \mathfrak{p}$ have been constructed such that every prime ideal containing $x_1, \ldots, x_r$ has codimension $\geq r$. If $r = n$, then we are done. On the other hand, if $r < n$, then $\mathfrak{p}$ is not a minimal prime containing $(x_1, \ldots, x_r)$: by construction and Corollary 7.35, those have codimension r. Arguing as before, we may choose $x_{r+1} \in \mathfrak{p} \smallsetminus (\mathfrak{q}_1 \cup \ldots \cup \mathfrak{q}_s)$, where $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ are the minimal primes containing $(x_1, \ldots, x_r)$. If $\mathfrak{q}$ is a prime ideal containing $(x_1, \ldots, x_{r+1})$, then there is j such that $\mathfrak{q}_j \subsetneq \mathfrak{q}$, hence

$$\operatorname{codim}(\mathfrak{q}) \geq \operatorname{codim}(\mathfrak{q}_j) + 1 \geq r + 1.$$

This completes the proof of the inductive step. □

The following result will allow us to give the first nontrivial examples of dimension computation:

THEOREM 7.39. *If R is a Noetherian ring, then* $\dim\big(R[x]\big) = \dim(R) + 1$.

PROOF. Note first that if I is any ideal in R, we get an ideal $I[x]$ in $R[x]$ consisting of all polynomials with coefficients in I. It is clear that we have an isomorphism $R[x]/I[x] \simeq (R/I)[x]$. Since a polynomial ring over a domain is again a domain, it follows that if $\mathfrak{p}$ is a prime ideal in R, then $\mathfrak{p}[x]$ is a prime ideal in $R[x]$. Moreover, we note that $I[x]$ is never a maximal ideal, since x is not invertible in $(R/I)[x]$ when $I \neq R$.

Given a chain of prime ideals in R

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n,$$

we obtain a chain of prime ideals in $R[x]$

$$\mathfrak{p}_0[x] \subsetneq \mathfrak{p}_1[x] \subsetneq \ldots \subsetneq \mathfrak{p}_n[x].$$

Since $\mathfrak{p}_n[x]$ is not a maximal ideal, it follows that $\dim\big(R[x]\big) \geq n+1$. Since this holds for every chain of prime ideals in R, we have $\dim\big(R[x]\big) \geq \dim(R) + 1$.

In order to prove the opposite inequality, it is enough to show that for every prime ideal $\mathfrak{q}$ in $R[x]$, if $\mathfrak{p} = \mathfrak{q} \cap R$, then

$$\operatorname{codim}(\mathfrak{q}) \leq \operatorname{codim}(\mathfrak{p}) + 1. \tag{7.2}$$

Note that we have $\mathfrak{p}[x] \subseteq \mathfrak{q}$. In order to prove (7.2), we may replace R by $R_{\mathfrak{p}}$ and $R[x]$ by $R_{\mathfrak{p}}[x] \simeq R[x]_{\mathfrak{p}}$, so we may assume that $\mathfrak{p}$ is a maximal ideal. Therefore $R[x]/\mathfrak{p}[x] \simeq k[x]$, where $k = R/\mathfrak{p}$ is a field. Therefore $\mathfrak{q}/\mathfrak{p}[x]$ is a principal ideal, hence there is $f \in \mathfrak{q}$ such that $\mathfrak{q} = \mathfrak{p}[x] + (f)$. Note now that by Proposition 7.38, if $\operatorname{codim}(\mathfrak{p}) = r$, then there are $x_1, \ldots, x_r \in \mathfrak{p}$ such that $\mathfrak{p}$ is a minimal prime ideal containing $(x_1, \ldots, x_r)$. In this case $\mathfrak{q}$ is a minimal ideal containing $(x_1, \ldots, x_r, f)$: indeed, if $(x_1, \ldots, x_r, f) \subseteq \mathfrak{q}' \subsetneq \mathfrak{q}$, with $\mathfrak{q}'$ a prime ideal, then $(x_1, \ldots, x_r) \subseteq \mathfrak{q}' \cap R \subseteq$

$\mathfrak{p}$, hence $\mathfrak{q}' \cap R = \mathfrak{p}$; we thus have $\mathfrak{q} = \mathfrak{p}[x] + (f) \subseteq \mathfrak{q}'$, hence $\mathfrak{q}' = \mathfrak{q}$. We conclude that $\operatorname{codim}(\mathfrak{q}) \leq r + 1$ by Corollary 7.35. This completes the proof of the theorem. □

EXAMPLE 7.40. It follows from the theorem, by induction on n, that if k is a field, then $\dim\big(k[x_1, \ldots, x_n]\big) = n$. Similarly, we have $\dim\big(\mathbf{Z}[x_1, \ldots, x_n]\big) = n + 1$.

THEOREM 7.41. *If R is a finitely generated k-algebra which is a domain and $K = \operatorname{Frac}(R)$, then $\dim(R) = \operatorname{trdeg}(K/k)$.*

PROOF. It follows from Theorem 6.1 that if $n = \operatorname{trdeg}(K/k)$, then we have an injective finite homomorphism $k[x_1, \ldots, x_n] \hookrightarrow R$. In this case we have

$$\dim(R) = \dim\big(k[x_1, \ldots, x_n]\big) = n,$$

where the first equality follows from Theorem 7.13 and the second equality follows from Example 7.40. □

DEFINITION 7.42. A *saturated chain* of prime ideals in a ring R is a sequence of prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_r$$

such that for every i, with $1 \leq i \leq r$, there is no prime ideal strictly between $\mathfrak{p}_{i-1}$ and $\mathfrak{p}_i$ (in other words, $\operatorname{codim}(\mathfrak{p}_i/\mathfrak{p}_{i-1}) = 1$).

REMARK 7.43. Note that if R is a Noetherian ring, then between any two prime ideals $\mathfrak{p} \subseteq \mathfrak{q}$ in R there is a saturated chain of prime ideals: this is due to the fact that every chain has length $\leq \operatorname{codim}(\mathfrak{q}/\mathfrak{p})$.

DEFINITION 7.44. A ring R is *catenary* if between any two prime ideals $\mathfrak{p} \subseteq \mathfrak{q}$ there is a saturated chain of prime ideals and any two such chains have the same length.

Proving that algebras of finite type over a field are catenary is a bit painful (for a geometric proof of the Principal Ideal theorem that also allows showing the catenarity of such algebras, see [**Mum99**, Chapter I.7]). We will deduce this fact from a more general result later in the course (we will then return and give some further results concerning dimension theory of algebras of finite type over a field). In fact, essentially all rings one encounters are catenary. The first example of a non-catenary ring was due to Nagata.

EXERCISE 7.45. Show that if R is a Noetherian ring with finitely many prime ideals, then $\dim(R) \leq 1$.

EXERCISE 7.46. Let k be a field and $R = k[x_1, \ldots, x_n]/(f)$, for some $n \geq 1$ and some $f \notin k$. Show that $\dim(R) = n - 1$. Hint: you can use the proof of Noether's Normalization theorem.

EXERCISE 7.47. Show that if $(R, \mathfrak{m})$ is a Noetherian local ring, M is a finitely generated nonzero R-module, and $x \in \mathfrak{m}$ is a non-zero-divisor on M, then

$$\dim(M/xM) = \dim(M) - 1.$$

EXERCISE 7.48. Let k be a field and consider the ideal $I \subseteq S = k[a, b, c, d]$ generated by the 2×2 minors of the matrix

$$\begin{pmatrix} a & b & c \\ b & c & d \end{pmatrix}$$

and let $R = S/I$.

i) Show that $R_a \simeq k[x,y] \simeq R_d$. Deduce that $\dim(R) \geq 2$.
ii) Show that if $\mathfrak{p}$ is an ideal in R containing $\overline{a}$, then $(\overline{a}, \overline{b}, \overline{c}) \subseteq \mathfrak{p}$. Deduce that $\dim\big(R/(\overline{a})\big) = 1$.
iii) Show that $\dim(R) = 2$.

7.4. Dimension of fibers

DEFINITION 7.49. If $f\colon R \to S$ is a ring homomorphism and $\mathfrak{p} \in \operatorname{Spec}(R)$, then the *fiber* of f at $\mathfrak{p}$ is the ring $S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}}$.

REMARK 7.50. If $g\colon S \to S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}}$ is the canonical homomorphism, then the induced continuous map gives a homeomorphism of $\operatorname{Spec}(S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}})$ onto $\varphi^{-1}(\mathfrak{p})$, where $\varphi = \operatorname{Spec}(f)$ (this justifies the name of $S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}}$). Indeed, this follows from Exercises 2.31 and 2.33 and the fact that the prime ideals $\mathfrak{q}$ in S such that $\mathfrak{p} \subseteq f^{-1}(\mathfrak{q})$ are precisely those such that $\mathfrak{p}S \subseteq \mathfrak{q}$, while those such that $f^{-1}(\mathfrak{q}) \subseteq \mathfrak{p}$ are those such that $f(R \smallsetminus \mathfrak{p}) \cap \mathfrak{q} = \emptyset$.

REMARK 7.51. Note that $S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}}$ is naturally a $k(\mathfrak{p})$-algebra, where $k(\mathfrak{p}) = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ is the residue field of $R_{\mathfrak{p}}$ (also called the *residue field of* R at $\mathfrak{p}$).

THEOREM 7.52. *Let $f\colon R \to S$ be an injective ring homomorphism, of finite type, with both R and S domains. If $\operatorname{Frac}(R) = K$ and $\operatorname{Frac}(S) = L$ and $\operatorname{trdeg}(L/K) = d$, then there is a nonempty open subset U of $\operatorname{Spec}(R)$ such that for every $y \in U$, the fiber of $\operatorname{Spec}(f)$ over y has dimension d (in particular, it is nonempty).*

We first give a slight variation on the result in Proposition 7.13.

LEMMA 7.53. *If $f\colon A \to B$ is a finite ring homomorphism, with A a domain, such that the induced map $\operatorname{Spec}(f)$ is surjective, then $\dim(A) = \dim(B)$.*

PROOF. Let $I = \ker(f)$. For every $\mathfrak{q} \in \operatorname{Spec}(B)$, we have $I \subseteq f^{-1}(\mathfrak{q})$. Since $(0) \in \operatorname{Im}\big(\operatorname{Spec}(f)\big)$, it follows that $I = (0)$, hence f is injective. In this case the assertion in the lemma follows from Proposition 7.13. □

PROOF OF THEOREM 7.52. Note that L/K is a finitely generated field extension, so indeed $d = \operatorname{trdeg}(L/K) < \infty$. Let $\mathfrak{p} = (0) \subseteq R$ and consider the injective ring homomorphism $K = R_{\mathfrak{p}} \hookrightarrow S_{\mathfrak{p}}$, which is again of finite type. Note that $S_{\mathfrak{p}}$ is a subring of L, with field of fractions L. By Theorem 6.1, we can find $x_1, \ldots, x_d \in S_{\mathfrak{p}}$ that are algebraically independent over K and such that $K[x_1, \ldots, x_n] \hookrightarrow S_{\mathfrak{p}}$ is finite, hence integral. We claim that there is $f \in R$ nonzero such that the injective homomorphism $B = R_f[x_1, \ldots, x_n] \hookrightarrow S_f$ is finite.

Indeed, for every $u \in S$, there is an equation

$$u^N + a_1 u^{N-1} + \ldots + a_N = 0,$$

with $a_1, \ldots, a_N \in R_{\mathfrak{p}}[x_1, \ldots, x_n]$. By taking the product of the denominators of all nonzero coefficients of $a_1, \ldots, a_N$, we find $f_u \in R$ nonzero such that u is integral over $R_{f_u}[x_1, \ldots, x_d]$. If $S = R[u_1, \ldots, u_r]$, it follows that if $f = \prod_i f_{u_i}$, then the injective homomorphism $R_f[x_1, \ldots, x_d] \hookrightarrow S_f$ is finite by Remark 3.4.

We now show that $U = D(f) \subseteq \operatorname{Spec}(R)$ has the desired property. We will use the factorization of $R_f \hookrightarrow S_f$ as

$$R_f \hookrightarrow B = R_f[x_1, \ldots, x_d] \hookrightarrow S_f.$$

Note that B is a polynomial algebra over R_f in $x_1, \dots, x_d$, hence for every $\mathfrak{q} \in U$, we have

$$B_{\mathfrak{q}}/\mathfrak{q}B_{\mathfrak{q}} \simeq k(\mathfrak{q})[x_1, \dots, x_d].$$

In particular, this is a domain. On the other hand, since $i\colon B \hookrightarrow S_f$ is finite and injective, it follows that $\operatorname{Spec}(i)$ is surjective, and thus

$$g\colon B_{\mathfrak{q}}/\mathfrak{q}B_{\mathfrak{q}} \to (S_f)_{\mathfrak{q}}/\mathfrak{q}(S_f)_{\mathfrak{q}} = S_{\mathfrak{q}}/\mathfrak{q}S_{\mathfrak{q}}$$

has the property that $\operatorname{Spec}(g)$ is surjective. We thus conclude using the lemma that

$$\dim(S_{\mathfrak{q}}/\mathfrak{q}S_{\mathfrak{q}}) = \dim(B_{\mathfrak{q}}/\mathfrak{q}B_{\mathfrak{q}}) = d,$$

where the last equality follows from Example 7.40. □

Remark 7.54. Note that under the assumptions in Theorem 7.52, if R is a finitely generated k-algebra, where k is a field, then

$$\operatorname{trdeg}(L/K) = \operatorname{trdeg}(L/k) - \operatorname{trdeg}(K/k) = \dim(S) - \dim(R),$$

where the second equality follows from Theorem 7.41.

We end this chapter with a general result giving a lower bound for the dimension of the fiber. We begin by introducing a notion that comes up often in commutative algebra.

Definition 7.55. If $(A, \mathfrak{m})$ and $(B, \mathfrak{n})$ are local rings, then a ring homomorphism $f\colon A \to B$ is a *local homomorphism* if $f(\mathfrak{m}) \subseteq \mathfrak{n}$.

Remark 7.56. The condition in the above definition can be rewritten as $\mathfrak{m} \subseteq f^{-1}(\mathfrak{n})$. Note that this automatically implies $\mathfrak{m} = f^{-1}(\mathfrak{n})$: this follows from the fact that every $u \in A \smallsetminus \mathfrak{m}$ is invertible in A, hence $f(u)$ is invertible in B.

Remark 7.57. Given any ring homomorphism $f\colon R \to S$, if $\mathfrak{q}$ is a prime ideal in S and $\mathfrak{p} = f^{-1}(\mathfrak{q})$, then we get an induced homomorphism $g\colon R_{\mathfrak{p}} \to S_{\mathfrak{q}}$ by the universal property of localization. In fact, this is a *local homomorphism*. In the same way that $S_{\mathfrak{q}}$ records the properties of S at $\mathfrak{q}$, the homomorphism g records the properties of f at $\mathfrak{q}$.

Theorem 7.58. *If $f\colon (A, \mathfrak{m}) \to (B, \mathfrak{n})$ is a local homomorphism of Noetherian local rings, then*

$$\dim(B) \leq \dim(B/\mathfrak{m}B) + \dim(A).$$

Proof. Note that the dimension of a local ring is the same as the codimension of the maximal ideal. We deduce from Proposition 7.38 that if $\dim(B/\mathfrak{m}B) = s$ and $\dim(A) = r$, then there are $x_1, \dots, x_r \in \mathfrak{m}$ and $y_1, \dots, y_s \in \mathfrak{n}$ such that $\mathfrak{m}$ is a minimal prime containing $(x_1, \dots, x_r)$ and $\mathfrak{n}/\mathfrak{m}B$ is a minimal prime containing $(\overline{y_1}, \dots, \overline{y_s})$. In this case $\mathfrak{n}$ is a minimal prime ideal containing

$$I = \big(f(x_1), \dots, f(x_r), y_1, \dots, y_s\big).$$

Indeed, if $\mathfrak{q}$ is a prime ideal in B containing I, then $(x_1, \dots, x_n) \subseteq f^{-1}(\mathfrak{q})$, hence $f^{-1}(\mathfrak{q}) = \mathfrak{m}$. In this case we have $\mathfrak{m}B + (y_1, \dots, y_s) \subseteq \mathfrak{q}$, hence $\mathfrak{q} = \mathfrak{n}$. The fact that $\operatorname{codim}(\mathfrak{n}) \leq r + s$ now follows from Corollary 7.35. □

CHAPTER 8

Special classes of rings

In this chapter we discuss various important classes of rings and the connections between them. We begin with valuation rings and especially DVRs, and then turn to UFDs, normal rings, and Dedekind domains.

8.1. Valuation rings and DVRs

Let K be a field. Consider a *totally ordered Abelian group* $(\Gamma, +, \leq)$. Recall that this means that $(\Gamma, +)$ is an Abelian group and we have a total order $\leq$, such that if $a \leq b$, then for every c, we have $a + c \leq b + c$. We also consider $\Gamma \cup \{\infty\}$, where $a \leq \infty$ for all $a \in \Gamma$ and $a + \infty = \infty$ for all $a \in \Gamma$ and $\infty + \infty = \infty$.

DEFINITION 8.1. A *valuation* on K with values in Γ is a map $v\colon K \to \Gamma \cup \{\infty\}$ that satisfies the following properties:

i) $v(a) = \infty$ if and only if $a = 0$.
ii) $v(a + b) \geq \min\{v(a), v(b)\}$ for all $a, b \in K$.
iii) $v(ab) = v(a) + v(b)$ for all $a, b \in K$.

A *discrete valuation* on K is a valuation with $\Gamma = \mathbf{Z}$, and with v is surjective.

REMARK 8.2. With v and K as in the above definition, note that i) plus iii) imply $v(1) = 0$. Moreover, by letting $a = b = -1$ in iii), we get[1] $v(-1) = 0$. We now see using iii) that $v(a) = v(-a)$ for all $a \in K$.

PROPOSITION 8.3. If v is a valuation on K with values in Γ, then

$$R := \{a \in K \mid v(a) \geq 0\}$$

is a subring of K that has the property that for every $a \in K \smallsetminus \{0\}$, we have $a \in R$ or $a^{-1} \in R$ (in particular, we have $\mathrm{Frac}(R) = K$).

PROOF. Property i) implies $0 \in R$ and we have already seen in Remark 8.2 that $1 \in R$ and if $a \in R$, then $-a \in R$. We now deduce from ii) that R is a subgroup of K with respect to addition and iii) implies that it is closed under multiplication. The last assertion in the proposition follows from the fact that if $a \neq 0$, then $v(a^{-1}) = -v(a)$ by iii). □

DEFINITION 8.4. We say that a domain R, with fraction field K, is a *valuation ring* if for every element $a \in K \smallsetminus \{0\}$, we have $a \in R$ or $a^{-1} \in R$.

REMARK 8.5. If R is a valuation ring, then

$$\mathfrak{m} = \{x \in R \mid x^{-1} \notin R\}$$

[1]Note that if $a \in \Gamma$ is such that $a + a = 0$, then $a = 0$. Indeed, we have either $a \geq 0$ or $a \leq 0$. In the former case, $0 = a + a \geq a \geq 0$, hence $a = 0$; the case $a \leq 0$ is similar.

is an ideal in R. Indeed, note first that if $a \in R$ and $x \in \mathfrak{m}$, since $x^{-1} = a(ax)^{-1}$, it follows that $ax \in \mathfrak{m}$. Suppose now that $x, y \in \mathfrak{m}$, with both x and y nonzero, and let's show that $x+y \in \mathfrak{m}$. Since R is a valuation ring, we have $\frac{x}{y} \in R$ or $\frac{y}{x} \in R$. By symmetry, we may assume that we are in the former case, hence $x = by$ for some $b \in R$. In this case $x + y = (1 + b)y$, and this lies in $\mathfrak{m}$, by what we have already mentioned.

Since every element in $R \smallsetminus \mathfrak{m}$ is invertible, it follows that R is a local ring, with maximal ideal $\mathfrak{m}$. Note that if we are in the setting in Proposition 8.3, then $\mathfrak{m} = \{x \in R \mid v(x) > 0\}$.

Our next result gives a converse to Proposition 8.3.

PROPOSITION 8.6. If R is a valuation ring, with fraction field K, then there is a valuation $v\colon K \to \Gamma \cup \{\infty\}$ such that

$$R = \{x \in K \mid v(x) \geq 0\}.$$

PROOF. Let $R^\times = R \smallsetminus \mathfrak{m}$ be the multiplicative group of invertible elements in R. This is a subgroup of $K^\times = K \smallsetminus \{0\}$, and we put $\Gamma = K^\times/R^\times$. We define an order on Γ by putting $\overline{x} \leq \overline{y}$ if $\frac{y}{x} \in R$. It is straightforward to see that this is well-defined. It is an order:

a) We have $\overline{x} \leq \overline{x}$ for every $\overline{x} \in \Gamma$.
b) If $\overline{x} \leq \overline{y}$ and $\overline{y} \leq \overline{x}$, then $\frac{x}{y} \in R^\times$, hence $\overline{x} = \overline{y}$.
c) If $\overline{x} \leq \overline{y}$ and $\overline{y} \leq \overline{z}$, then $\frac{z}{x} = \frac{z}{y} \cdot \frac{y}{x} \in R$, hence $\overline{x} \leq \overline{z}$.

The fact that this is a total order follows from the fact that R is a valuation ring. Finally, if $\overline{x} \leq \overline{y}$, then $\overline{xz} \leq \overline{yz}$ for every $z \in K^\times$: this is clear. Therefore Γ is an ordered Abelian group.

If we define $v\colon K \to \Gamma \cup \{\infty\}$ by $v(0) = \infty$ and $v(x) = \overline{x}$ for $x \in K^\times$, then v is a valuation:

i) $v(a) = \infty$ if and only if $a = 0$: this follows from definition.
ii) $v(a + b) \geq \min\{v(a), v(b)\}$ for all $a, b \in K$. Of course, we may assume that a, b, and $a + b$ are nonzero. In this case, if $v(a) \geq v(b)$, then $\frac{a}{b} \in R$, and $\frac{a+b}{b} = 1 + \frac{a}{b} \in R$, hence $v(a + b) \geq v(b)$.
iii) $v(ab) = v(a) \cdot v(b)$ for all $a, b \in K$ (recall that the operation in Γ is denoted multiplicatively). Again, we may assume that a and b are nonzero. In this case, the formula follows from the definition.

Finally, it is clear from the definition that

$$R = \{a \in K \mid v(a) \geq \overline{1}\}$$

(recall that the identity in Γ is $\overline{1}$). This completes the proof. □

We next consider in more detail the case of discrete valuations. Recall that a principal ideal domain (or PID, for short) is a domain with the property that every ideal is a principal ideal.

PROPOSITION 8.7. Given an domain R, with fraction field K, the following are equivalent:

i) There is a discrete valuation v on K such that $R = \{a \in K \mid v(a) \geq 0\}$.
ii) R is a local PID, which is not a field.
iii) R is local, Noetherian, and the maximal ideal is principal and non-zero.

DEFINITION 8.8. A ring that satisfies the above equivalent properties is a *discrete valuation ring* (or *DVR*, for short).

PROOF OF PROPOSITION 8.7. Let us show first that i)⇒ii). We have already seen that in this case R is a local ring, with maximal ideal

$$\mathfrak{m} = \{a \in K \mid v(a) > 0\}$$

(see Remark 8.5).

Given any non-zero ideal I in R, consider $a \in I$ such that $v(a)$ is minimal. Given any other $b \in I$, we have $v(b) \geq v(a)$, hence $v(ba^{-1}) \geq 0$, and therefore $b \in (a)$. This shows that $I = (a)$ and therefore R is a PID. Note that R is not a field, since an element $a \in K$ with $v(a) = 1$ is a non-invertible element of R.

Since the implication ii)⇒iii) is trivial, in order to complete the proof, it is enough to prove iii)⇒i). Suppose that $(R, \mathfrak{m})$ is a Noetherian local domain and $\mathfrak{m} = (\pi)$, for some $\pi \neq 0$. Given any non-zero element α, it follows from Krull's Intersection theorem (see Corollary 4.22) that there is $j \geq 0$ such that $\alpha \in \mathfrak{m}^j \smallsetminus \mathfrak{m}^{j+1}$. Therefore we can write $\alpha = u\pi^j$, with u invertible. Since K is the fraction ring of R, it follows that every non-zero element β in K can be written as $\beta = u\pi^j$ for a unique $j \in \mathbf{Z}$ and $u \in R \smallsetminus \mathfrak{m}$. If we put $v(\beta) = j$ (and $v(0) = \infty$), then we see as in the proof of Proposition 8.6 that v is a (discrete) valuation and we have $R = \{a \in K \mid v(a) \geq 0\}$. □

REMARK 8.9. Note that if $(R, \mathfrak{m})$ is a DVR, then it follows from the above proof that every nonzero ideal of R is equal to $\mathfrak{m}^i$, for some $i \in \mathbf{Z}_{\geq 0}$. In particular, we see that the only prime ideals of R are (0) and $\mathfrak{m}$, hence $\dim(R) = 1$.

EXAMPLE 8.10. If R is a PID which is not a field and $\mathfrak{p}$ is a nonzero prime ideal in R, then it follows from Proposition 8.7 that the localization $R_{\mathfrak{p}}$ is a DVR. For example, the localization $\mathbf{Z}_{p\mathbf{Z}}$, where $p \in \mathbf{Z}$ is a prime integer, is a DVR. The corresponding valuation is given by $v(a) = m$ if for $a \in \mathbf{Q}$ nonzero we write $a = p^m \frac{r}{s}$, where $r, s \neq 0$ are integers relatively prime to p.

Similarly, if k is a field, then the localization $k[x]_{(x)}$ is a DVR. The corresponding valuation on $k(x)$ is given by $v(f) = m$ if for $f \in k(x)$ nonzero we write $f = x^m \frac{g}{h}$, with $g(0) \neq 0 \neq h(0)$.

EXAMPLE 8.11. Let k be a field and $v\colon k(x, y) \to \mathbf{Z} \cup \{0\}$ be defined as follows. Given $u \in k(x, y)$ nonzero, we write $u = x^m \frac{g}{h}$, for some $g, h \in k[x, y]$, none of them divisible by x. It is straightforward to check that v is a discrete valuation, with corresponding DVR given by $k[x, y]_{(x)}$.

EXAMPLE 8.12. Let us consider an example of a non-discrete valuation. Let $v\colon k(x, y) \to \mathbf{R} \cup \{0\}$ be the unique valuation with the property that $v(x) = 1$ and $v(y) = \sqrt{2}$. Explicitly, if $f = \sum_{i,j} a_{i,j} x^i y^j \in k[x, y]$ is nonzero, then

$$v(f) = \min\{i + j\sqrt{2} \mid a_{i,j} \neq 0\}.$$

This extends uniquely to a valuation on K such that $v(f/g) = v(f) - v(g)$ for every nonzero $f, g \in k[x, y]$. Describing the corresponding valuation ring R is more complicated. We clearly have $k[x, y] \subseteq R$, but we also have the monomials $x^i y^j \in R$, where $i, j \in \mathbf{Z}$, with $i + j\sqrt{2} \geq 0$.

We end this section with a result that identifies the Noetherian valuation rings.

PROPOSITION 8.13. If R is a valuation ring, then R is Noetherian if and only if R is a DVR or a field.

PROOF. By Proposition 8.7, it is enough to show that if R is a Noetherian valuation ring which is not a field (hence its maximal ideal $\mathfrak{m}$ is nonzero), then $\mathfrak{m}$ is principal. Since R is Noetherian, we may choose an ideal (x) which is maximal among all principal ideals contained in $\mathfrak{m}$. Note that since $\mathfrak{m}$ is nonzero, it follows that $x \neq 0$. If there is $y \in \mathfrak{m} \smallsetminus (x)$, then $\frac{y}{x} \notin R$, hence R being a valuation ring, we have $\frac{x}{y} \in R$. We thus see that $(x) \subsetneq (y) \subseteq \mathfrak{m}$, a contradiction with our choice of x. Therefore $\mathfrak{m} = (x)$. □

EXERCISE 8.14. Let K be a field and $v\colon K \to \Gamma \cup \{\infty\}$ a valuation on K Show that if $R = \{x \in K \mid v(x) \geq 0\}$ is the corresponding valuation ring, and if $w\colon K \to K^\times/R^\times \cup \{\infty\}$ is the valuation we defined in the proof of Proposition 8.6, then there is an injective group homomorphism $\varphi\colon K^\times/R^\times \to \Gamma$, which preserves the order, and such that $v(x) = \varphi\big(w(x)\big)$ for every $x \in K \smallsetminus \{0\}$.

EXERCISE 8.15. Let K be a field. We consider local subrings $(A, \mathfrak{m})$ of K. We say that $(B, \mathfrak{n})$ *dominates* $(A, \mathfrak{m})$ is $A \subseteq B$ and the inclusion $A \hookrightarrow B$ is a local homomorphism (that is, we have $\mathfrak{m} = \mathfrak{n} \cap A$).

i) Show that any local subring $(A, \mathfrak{m})$ of K is contained in a maximal such subring (with respect to the relation of dominance).
ii) Show that a local subring $(A, \mathfrak{m})$ of K is maximal with respect to the relation of dominance if and only if A is a valuation ring, with $\mathrm{Frac}(A) = K$.

EXERCISE 8.16. Let R be a domain.

i) Show that R is a valuation ring if and only if for every two ideals $\mathfrak{a}$ and $\mathfrak{b}$ in R, we have $\mathfrak{a} \subseteq \mathfrak{b}$ or $\mathfrak{b} \subseteq \mathfrak{a}$.
ii) Deduce that if R is a valuation ring and $\mathfrak{p}$ is a prime ideal in R, then $R_\mathfrak{p}$ and $R/\mathfrak{p}$ are valuation rings.

EXERCISE 8.17. Let R be a valuation ring, with fraction field K. Show that for every ring S, with $R \subseteq S \subseteq K$, there is a unique prime ideal $\mathfrak{p}$ in R such that $S = R_\mathfrak{p}$. Deduce that the set of such rings S is totally ordered with respect to inclusion.

8.2. Unique Factorization Domains

In this section we review some notions regarding Unique Factorization Domains, that we assume are more or less familiar, and only discuss in detail the interplay of this notion with that of Noetherian ring.

DEFINITION 8.18. Let R be a domain and let $a \in R$ be nonzero and noninvertible. We say that a is a *prime* element if the ideal (a) is a prime ideal. We say that a is an irreducible element if whenever $a = bc$, with $b, c \in R$, either b or c is a unit.

REMARK 8.19. It is clear from the definition that if $u \in R$ is invertible and $a \in R$ is arbitrary, then au is irreducible or prime if and only if a has this property.

EXERCISE 8.20. Show that every prime element is irreducible.

DEFINITION 8.21. A domain R is a Unique Factorization Domain (UFD, for short) if the following conditions hold:

i) For every nonzero, noninvertible $a \in R$, we can write

$$a = \pi_1 \cdots \pi_r,$$

for some $r \geq 1$ and irreducible elements $\pi_1, \ldots, \pi_r$.

ii) Such an expression is essentially unique, in the sense that if

$$a = \pi_1' \cdots \pi_s'$$

is another such expression, then $r = s$ and after relabeling that π_i', we have $(\pi_i) = (\pi_i')$ for all i.

PROPOSITION 8.22. A domain R is a UFD if and only if condition i) in Definition 8.21 holds and every irreducible element is prime.

PROOF. Suppose first that R is a UFD and let us show that if $a \in R$ is irreducible, then it is prime. Suppose that $b, c \in R$ are such that $bc \in (a)$, hence we can write $bc = ad$ for some $d \in R$. After writing each of of b, c, and d as products of irreducible elements and using assertion ii) in Definition 8.21 and the fact that a is irreducible, we see that $b \in (a)$ or $c \in (a)$.

Conversely, suppose that i) in Definition 8.21 holds and that every irreducible element in R is prime. It follows that in order to prove that ii) in Definition 8.21 holds it is enough to prove the same uniqueness result for factorizations in *prime elements*. Suppose that

$$a = \pi_1 \cdots \pi_r = \pi_1' \cdots \pi_s',$$

with π_i and π_j' prime elements. Arguing by induction on $\min\{r, s\}$, we may assume that $(\pi_i) \neq (\pi_j')$ for every i and j. If $r \geq 1$, since $\pi_1' \cdots \pi_s' \in (\pi_1)$, which is a prime ideal, it follows that $s \geq 1$ and there is j such that $\pi_j' \in (\pi_1)$. Since π_j' is prime, hence irreducible, it follows that $(\pi_1) = (\pi_j')$, a contradiction. The argument in the case $s \geq 1$ is similar. □

PROPOSITION 8.23. If R is a Noetherian domain, then every nonzero, noninvertible element $a \in R$ can be written as $a = \pi_1 \cdots \pi_r$, for some $r \geq 1$ and irreducible elements $\pi_1, \ldots, \pi_r$.

PROOF. Arguing by contradiction, let us assume that there is a that does not satisfy the conclusion and let us choose one such that the ideal (a) is maximal among all such ideals (we can do this since R is Noetherian). In particular, a is not irreducible, hence we can write $a = a_1 a_2$, with a_1 and a_2 noninvertible. In this case we have $(a) \subsetneq (a_1)$ and $(a) \subsetneq (a_2)$, hence by maximality of (a), it follows that we can write $a_1 = b_1 \cdots b_r$ and $a_2 = c_1 \cdots c_s$, with $b_1, \ldots, b_r, c_1, \ldots, c_s$ irreducible. Since $a = b_1 \cdots b_r c_1 \cdots c_s$, we have a contradiction. □

By combining Propositions 8.22 and 8.23, we obtain the following

COROLLARY 8.24. If R is a Noetherian domain, then R is a UFD if and only if every irreducible element is prime.

The following characterization of the UFD property in Noetherian rings makes a connection with dimension theory:

PROPOSITION 8.25. If R is a Noetherian domain, then R is a UFD if and only if every prime ideal $\mathfrak{p}$ in R, with $\operatorname{codim}(\mathfrak{p}) = 1$, is principal.

PROOF. Suppose first that R is a UFD. If $\mathfrak{p}$ is a prime ideal of codimension 1, let us choose a non-zero $a \in \mathfrak{p}$. If we write $a = a_1 \cdots a_r$, with all a_i irreducible elements, since $\mathfrak{p}$ is prime, it follows that $a_i \in \mathfrak{p}$ for some i. Since R is a UFD, the ideal (a_i) is a prime ideal (see Proposition 8.22), and since $\operatorname{codim}(\mathfrak{p}) = 1$, it follows that $\mathfrak{p} = (a_i)$.

Conversely, suppose that every codimension 1 prime ideal in R is principal. By Corollary 8.24, we see that in order to show that R is a UFD, it is enough to show that if π is an irreducible element in R, then (π) is a prime ideal. Let $\mathfrak{p}$ be a minimal prime ideal containing (π). If follows from the Principal Ideal theorem that $\operatorname{codim}(\mathfrak{p}) = 1$; note that we can't have $\operatorname{codim}(\mathfrak{p}) = 0$ since the only prime ideal of codimension 0 is the ideal (0). By assumption, $\mathfrak{p}$ is a principal ideal. If we write $\mathfrak{p} = (b)$, the inclusion $(\pi) \subseteq (b)$ implies that $\pi = bc$, for some $c \in R$. Since π is irreducible, it follows that c is invertible, hence $(\pi) = (b)$ is a prime ideal. □

REMARK 8.26. If R is a Noetherian UFD and S is a multiplicative system in R, then $S^{-1}R$ is a UFD. Indeed, this follows from Proposition 8.25: a prime ideal in $S^{-1}R$ is of the form $\mathfrak{q} = \mathfrak{p} \cdot S^{-1}R$ for some prime ideal $\mathfrak{p}$ in R, with $S \cap \mathfrak{p} \neq \emptyset$ and $\operatorname{codim}(\mathfrak{q}) = \operatorname{codim}(\mathfrak{p})$; moreover, if $\mathfrak{p}$ is principal, then so is $\mathfrak{q}$. However, one can remove the condition that R is Noetherian and prove the assertion starting from the definition: we leave this as an exercise.

We end this section by discussing some examples.

EXAMPLE 8.27. Every PID is a UFD. Indeed, since a PID is Noetherian, the assertion trivially follows from Proposition 8.25.

EXAMPLE 8.28. If R is a domain, then R is a UFD if and only if the polynomial ring $R[x]$ is a UFD (for a proof, see for example [**DF04**, Chapter 8,Theorem 7]). In particular, since any field k is trivially a UFD, it follows by induction on n that any polynomial ring $k[x_1, \ldots, x_n]$ is a UFD. Note that for $n \neq 2$, we get examples of UFDs that are not PIDs.

Similarly, since $\mathbf{Z}$ is a UFD by Example 8.27, it follows by induction on n that every polynomial ring $\mathbf{Z}[x_1, \ldots, x_n]$ is a UFD.

EXAMPLE 8.29. Let k be a field and $f = x_1x_2 - x_3x_4 \in S = k[x_1, x_2, x_3, x_4]$. It is easy to see that f is irreducible (if it factors as a product $f = gh$, with both g and h noninvertible, it follows that both g and h have total degree 1 and we get a contradiction by inspecting the coefficients). Since S is a UFD, it follows that (f) is a prime ideal, so $R = S/(f)$ is a domain. Note that R is not a UFD: this follows from the fact that $\overline{x_1} \cdot \overline{x_2} = \overline{x_3} \cdot \overline{x_4}$ are two distinct irreducible decompositions (check this!).

EXERCISE 8.30. Let $d \in \mathbf{Z}$ be an integer that is not a square and consider the subring

$$\mathbf{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbf{Z}\}$$

of $\mathbf{C}$. For every $u = a + b\sqrt{d}$, we put

$$N(u) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 \in \mathbf{Z}.$$

i) Show that if $N(u)$ is a prime integer, then u is irreducible.
ii) Use this to show that $\mathbf{Z}[\sqrt{-5}]$ is not a UFD, by considering the following factorizations:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

8.3. Normal rings

Recall that a domain R with fraction field K is *integrally closed* if every element of K that is integral over R lies in R.

EXAMPLE 8.31. If R is a UFD, then R is normal. Indeed, suppose that $a, b \in R \setminus \{0\}$ are such that $u = \frac{a}{b}$ is integral over R, but $\frac{a}{b} \notin R$. Since R is a UFD, the latter condition implies that there is a prime element $\pi \in R$ such that $b \in (\pi)$, but $a \notin (\pi)$. Since u is integral over R, we can find $c_1, \ldots, c_n \in R$ such that

$$u^n + c_1 u^{n-1} + \ldots + c_n = 0.$$

Clearing the denominators, we obtain

$$a^n = -c_1 a^{n-1} b - \ldots - c_n b^n \in (\pi).$$

Since (π) is a prime ideal, we obtain $a \in (\pi)$, a contradiction.

EXAMPLE 8.32. Let $S = k[x, y, z]$, where k is a field, and $R = S/(x^2 - yz^2)$. It is easy to see that $x^2 - yz^2$ is irreducible (check this!), hence prime, since S is a UFD. Therefore R is a domain. Note that R is not integrally closed, since $u = \frac{\overline{x}}{\overline{z}} \in \mathrm{Frac}(R) \setminus R$, and it is integral over R, since $u^2 - \overline{y} = 0$ (check the details!).

Our next goal is to give a definition of integral closure that does not require R to be a domain. We begin with a proposition that treats the behavior of integral closure with respect to localization.

LEMMA 8.33. *Let R be a domain, with fraction field K, and R' the integral closure of R in K.*

i) *If S is a multiplicative system in R, then the integral closure of $S^{-1}R$ in K is $S^{-1}R'$.*
ii) *In particular, R is integrally closed in K if and only if $R_{\mathfrak{p}}$ is integrally closed in K for every prime (maximal) ideal $\mathfrak{p}$ in R.*

PROOF. We first prove i). If $u \in R'$, then we can find a positive integer n and $a_1, \ldots, a_n \in R$ such that

$$u^n + \sum_{i=1}^{n} a_i u^{n-i} = 0.$$

In this case, for every $s \in S$, we have

$$\Big(\frac{u}{s}\Big)^n + \sum_{i=1}^{n} \frac{a_i}{s^i} \cdot \Big(\frac{u}{s}\Big)^{n-i} = 0,$$

hence $\frac{u}{s}$ lies in the integral closure of $S^{-1}R$.

Conversely, suppose that $v \in K$ lies in the integral closure of $S^{-1}R$. We can thus find a positive integer n and $b_i \in S^{-1}R$ such that

$$v^n + \sum_{i=1}^{n} b_i v^{n-i} = 0.$$

We can find $s \in S$ such that $sv \in R$ and $sb_i \in R$ for all i, in which case we see that

$$(sv)^n + \sum_{i=1}^{n} (s^i b_i)(sv)^{n-i} = 0,$$

hence $sv \in R'$ and thus $v \in S^{-1}R'$. This completes the proof of i).

The assertion in ii) follows immediately from the fact that $R = R'$ if and only if $R_{\mathfrak{p}} = R'_{\mathfrak{p}}$ for all prime (maximal) ideals $\mathfrak{p}$ in R (see Exercise 2.37). □

DEFINITION 8.34. A ring R is *normal* if $R_{\mathfrak{p}}$ is an integrally closed domain for every prime ideal $\mathfrak{p}$ in R.

REMARK 8.35. In the above definition, it is enough to put the condition for maximal ideals. Indeed, every prime ideal $\mathfrak{p}$ is contained in a maximal ideal $\mathfrak{m}$, and if $R_{\mathfrak{m}}$ is an integrally closed domain, then so is its localization $R_{\mathfrak{p}} = (R_{\mathfrak{m}})_{\mathfrak{p}R_{\mathfrak{m}}}$ by Lemma 8.33.

REMARK 8.36. If R is a domain, then R is normal if and only if it is integrally closed. This follows from Lemma 8.33.

PROPOSITION 8.37. If a ring R has the property that $R_{\mathfrak{m}}$ is reduced for every maximal ideal $\mathfrak{m}$ in R, then R is reduced. In particular, every normal ring is reduced.

PROOF. If R is normal, then for every prime ideal $\mathfrak{p}$, the localization $R_{\mathfrak{p}}$ is a domain, hence it is reduced. Therefore it is enough to prove the first assertion in the proposition.

If $a \in R$ is such that $a^n = 0$ for some positive integer n, then $\frac{a}{1} = 0$ in $R_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$ in R. This implies that the ideal $I = \{b \in R \mid ba = 0\}$ is not contained in any maximal ideal, hence $I = R$, and thus $a = 0$. Therefore R is reduced. □

PROPOSITION 8.38. Let R be a ring.

i) If $R = R_1 \times \ldots \times R_n$, then R is normal if and only if R_i is normal for every i.
ii) If R is a normal Noetherian ring, then $R \simeq R_1 \times \ldots \times R_n$, for some integrally closed domains $R_1, \ldots, R_n$.

PROOF. Indeed, every prime ideal $\mathfrak{p}$ in R is of the form $\pi_i^{-1}(\mathfrak{p}_i)$, for some i and some prime ideal $\mathfrak{p}_i$ in R_i, where $\pi_i \colon R_1 \times \ldots \times R_n \to R_i$ is the projection. Moreover, in this case the canonical morphism $R_{\mathfrak{p}} \to (R_i)_{\mathfrak{p}_i}$ is an isomorphism (check this!). Therefore the assertion in i) follows from the definition.

Suppose now that R is Noetherian and normal. In this case R is reduced by Proposition 8.37, hence if $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are the minimal primes of R, we have $(0) = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n$ (see Remark 5.19), hence the canonical morphism

$$R \to R/\mathfrak{p}_1 \times \ldots \times R/\mathfrak{p}_n$$

is injective. It is also surjective by the Chinese Remainder theorem, since $\mathfrak{p}_i + \mathfrak{p}_j = R$ for $i \neq j$ (this is due to the fact that no maximal prime ideal $\mathfrak{m}$ contains both $\mathfrak{p}_i$ and $\mathfrak{p}_j$, since $R_{\mathfrak{m}}$ has a unique minimal prime, namely (0)). The fact that each $R/\mathfrak{p}_i$ is normal (hence integrally closed) now follows from i). □

We can use normality to give another characterization of DVRs.

PROPOSITION 8.39. A ring R is a DVR if and only if it is a local Noetherian normal domain, of dimension 1.

We begin with the following

LEMMA 8.40. *If R is a Noetherian domain ring, then for every nonzero $a \in R$ and every $\mathfrak{p} \in \operatorname{Ass}\big(R/(a)\big)$, the localization $R_{\mathfrak{p}}$ is a DVR.*

PROOF. The hypothesis implies that $\mathfrak{p}R_{\mathfrak{p}} \in \mathrm{Ass}\big(R_{\mathfrak{p}}/aR_{\mathfrak{p}}\big)$ (see Exercise 5.11). We may thus replace R by $R_{\mathfrak{p}}$ in order to assume that $(R, \mathfrak{p})$ is a local ring By assumption, there is $b \in R$ such that

$$\mathfrak{p} = \{h \in R \mid hb \in (a)\}. \tag{8.1}$$

In particular, we have $\frac{b}{a} \notin R$ and $\mathfrak{p} \cdot \frac{b}{a} \subseteq R$. If $\mathfrak{p} \cdot \frac{b}{a} \subseteq \mathfrak{p}$, then the determinantal trick (see, for example, the proof of Proposition 3.5) implies that $\frac{b}{a}$ is integral over R; since R is integrally closed, we get $\frac{b}{a} \in R$, a contradiction. Therefore $\mathfrak{p} \cdot \frac{b}{a} = R$, that is, $\frac{a}{b} \in \mathfrak{p}$. Moreover, if $u \in \mathfrak{p}$, then it follows from (8.1) that $u \in \big(\frac{a}{b}\big)$. Therefore $\mathfrak{p} = \big(\frac{a}{b}\big)$, hence R is a DVR by Proposition 8.7. □

PROOF OF PROPOSITION 8.39. It follows from Proposition 8.7 that if R is a DVR, then it is a local PID. In particular, it is a local Noetherian domain, and it is a UFD, hence it is normal (see Example 8.31). Moreover, it follows from Remark 8.9 that $\dim(R) = 1$.

We now prove the converse. Since $\dim(R) = 1$, it follows that $\mathfrak{m} \neq (0)$. Let $a \in \mathfrak{m} \smallsetminus \{0\}$. By Theorem 5.5ii), we have $\mathrm{Ass}_R\big(R/(a)\big) \neq \emptyset$, and since (0) and $\mathfrak{m}$ are the only prime ideals in R, it follows that $\mathfrak{m} \in \mathrm{Ass}_R\big(R/(a)\big)$. Lemma 8.40 implies that R is a DVR. □

We end this section with the following characterization of normal domains, which is a variant of a criterion due to Serre.

PROPOSITION 8.41. A Noetherian domain R is normal if and only if the following two conditions hold:

i) For every prime ideal $\mathfrak{p}$ in R, with $\mathrm{codim}(\mathfrak{p}) = 1$, the ring $R_{\mathfrak{p}}$ is a DVR.
ii) We have $R = \bigcap_{\mathrm{codim}(\mathfrak{p})=1} R_{\mathfrak{p}}$, where the intersection is over all prime ideals $\mathfrak{p}$ in R, of codimension 1.

Moreover, in general condition ii) is equivalent to the following variant:

ii') For every $a \in R$ nonzero, and every $\mathfrak{p} \in \mathrm{Ass}_R\big(R/(a)\big)$, we have $\mathrm{codim}(\mathfrak{p}) = 1$.

PROOF. Let K be the fraction field of R. We first prove the equivalence of ii) and ii'). Suppose first that ii') holds and consider $0 \neq \frac{b}{a} \in K$ that lies in $R_{\mathfrak{p}}$ for all prime ideals $\mathfrak{p}$ in R of codimension 1. We consider a minimal primary decomposition

$$(a) = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r.$$

It follows from Remark 5.28 that if $\mathfrak{p}_j = \mathrm{rad}(\mathfrak{q}_j)$, then $\mathfrak{p}_j \in \mathrm{Ass}_R\big(R/(a)\big)$, hence $\mathrm{codim}(\mathfrak{p}_j) = 1$ for all j by ii'). By hypothesis, we have $\frac{b}{a} \in R_{\mathfrak{p}_j}$ for all j, hence there is $s_j \in R \smallsetminus \mathfrak{p}_j$ such that $s_j b \in (a) \subseteq \mathfrak{q}_j$. Since $\mathfrak{q}_j$ is a primary ideal, we conclude that $b \in \mathfrak{q}_j$ for all j, hence $\frac{b}{a} \in R$.

Conversely, suppose that ii) holds and consider $0 \neq a \in R$ and $\mathfrak{p} \in \mathrm{Ass}_R\big(R/(a)\big)$. It follows that there is $b \in R$ such that $\mathfrak{p} = \{u \in R \mid ub \in (a)\}$. In particular, we have $b \notin (a)$, and thus by assumption, we can find a prime ideal $\mathfrak{q}$ with $\mathrm{codim}(\mathfrak{q}) = 1$, such that $\frac{b}{a} \notin R_{\mathfrak{q}}$. This implies that

$$\mathfrak{p} = \{u \in R \mid ub \in (a)\} \subseteq \mathfrak{q}.$$

Since $\mathfrak{p} \neq (0)$ (note that $a \in \mathfrak{p}$) and $\mathfrak{q}$ has codimension 1, we conclude that $\mathfrak{p} = \mathfrak{q}$, and thus $\mathrm{codim}(\mathfrak{p}) = 1$.

Suppose now that conditions i) and ii) hold. It follows from i) that if $\mathfrak{p}$ is a codimension 1 prime ideal in R, then $R_{\mathfrak{p}}$ is integrally closed. We then deduce from ii) that R is integrally closed: if $u \in K$ is integral over R, then it is clearly integral over $R_{\mathfrak{p}}$, for every prime ideal $\mathfrak{p}$ in R of codimension 1, and thus $u \in \bigcap_{\mathrm{codim}(\mathfrak{p})=1} R_{\mathfrak{p}} = R$.

On the other hand, if R is normal, then it follows from Proposition 8.39 that condition i) holds and it follows from Lemma 8.40 that condition ii') holds. This completes the proof. □

8.4. Finiteness of integral closure

If A is a domain, with fraction field K, then we get a normal domain associated to A by taking the integral closure B of A in K. In general, even if A is Noetherian, it does not follow that B is Noetherian. However, this holds for most examples of interest, since one can show that B is a finite A-algebra. In this section we prove that this is the case for algebras of finite type over a field. More generally, we prove the following

THEOREM 8.42. *Let A be an algebra of finite type over a field k, with A an integral domain. If K is the fraction field of A and L is a finite field extension of K, then the integral closure B of A in L is finite over A.*

PROOF. We give the proof following [**Eis95**]. Note that since A is Noetherian, it is enough to show that B is a submodule of a finitely generated A-module. In particular, we may replace at any point L by a finite extension L': if the integral closure of A in L' is finite over A, then so is B.

The first step in the proof is to show that we may assume that A is normal and the field extension L/K is a separable extension. We apply Noether Normalization to find a subring R of A that is isomorphic to a polynomial ring $k[x_1, \ldots, x_n]$ and such that A is finite over R. In this case, B is also the integral closure of R in L, hence after replacing A by R, we may assume that $A = k[x_1, \ldots, x_n]$. In particular, A is normal, and $K = k(x_1, \ldots, x_n)$.

After possibly replacing L by a suitable finite extension, we may assume that the extension L/K is normal. Let us show that we may assume that the extension is also separable. If this is not separable, then let $p = \mathrm{char}(k) > 0$, $G = G(L/K)$, and K' the subfield of L fixed by G. In this case the extension L/K' is separable and K'/K is purely inseparable. If we show that the integral closure A' of A in K' is finite over A, then we only need to show that the integral closure of A' in L is finite over A'; since A' is normal, this would complete the proof of the reduction step. Since K'/K is purely inseparable, we can find $e > 0$ such that for every $f \in K'$, we have $f^{p^e} \in K = k(x_1, \ldots, x_n)$. We can thus find a finite extension k' of k such that $K' \subseteq K'' = k'(x_1^{1/p^e}, \ldots, x_n^{1/p^e})$. Note that the integral closure of A in K'' is $k'[x_1^{1/p^e}, \ldots, x_n^{1/p^e}]$ (indeed, this is a finite extension of $k[x_1, \ldots, x_n]$ and it is a normal ring); this is clearly finite over A and since it contains A', it follows that A' is finite over A.

We conclude that in order to complete the proof it is enough to treat the case when A is normal and the extension L/K is separable. We note that from now on we don't use anymore the fact that A is a finite type algebra over a field (only the fact that it is Noetherian). After possibly enlarging L, we may assume that L/K is a Galois extension, with group G. Let $\sigma_1, \ldots, \sigma_r$ be the elements of G

and let $u_1, \ldots, u_r \in L$ be a basis of L over K. After multiplying each u_i by a suitable element of A, we may assume that $u_i \in B$ for every i (if $S = A \smallsetminus \{0\}$, then $S^{-1}A = K \hookrightarrow S^{-1}B$ is an integral, injective homomorphism, hence $S^{-1}B$ is a field by Proposition 3.10, and thus $S^{-1}B = L$). In this case we have $\sigma_i(u_j) \in B$ for all i, j (note that $\sigma_i(B) \subseteq B$, as follows by applying σ_i to a monic equation that witnesses the fact that an element in B is integral over A). Let us consider the matrix $M = \big(\sigma_i(u_j)\big) \in M_r(B)$, with $D = \det(M)$.

Note first that $D \neq 0$. Indeed, if $D = 0$, then there are $\lambda_1, \ldots, \lambda_r \in L$, not all 0, such that $\left(\sum_{i=1}^r \lambda_i \sigma_i\right)(u_j) = 0$ for all j. Hence $\sum_{i=1}^r \lambda_i \sigma_i = 0$. This can't happen since distinct field automorphisms of L are linearly independent over L. We recall the argument: after relabeling the σ_i, we may assume that $\sum_{i=1}^s \lambda_i \sigma_i = 0$, with all $\lambda_i \neq 0$, and that s is minimal with the property that we have such a relation. Note that $s \geq 2$. For every $a, b \in L$, we have

$$0 = \sum_{i=1}^s \lambda_i \sigma_i(ab) = \left(\sum_{i=1}^s \lambda_i \sigma_i(a) \sigma_i\right)(b),$$

hence

$$\sum_{i=1}^r \lambda_i \sigma_i(a) \sigma_i = 0.$$

Choose a such that $\sigma_1(a) \neq \sigma_2(a)$ and note that we have

$$\sum_{i=2}^s \big(\sigma_1(a) - \sigma_i(a)\big) \lambda_i \sigma_i = 0.$$

Since the coefficient of σ_2 is non-zero, this contradicts the minimality of s.

We thus have $D \neq 0$. Note that for every i, $\sigma_i(D)$ is the determinant of a matrix obtained by permuting the rows of M, hence $\sigma_i(D) = \pm D$. This implies that $\sigma_i(D^2) = D^2$ for all i, hence $D^2 \in K$.

We will show that $B \subseteq \frac{1}{D^2} \cdot \sum_{i=1}^r A \cdot u_i$, which is a finitely generated A-module. This would imply that B is finite over A, completing the proof. Given any $u \in B$, we can write $u = \sum_{j=1}^r \alpha_j u_j$, with $\alpha_j \in K$. In order to obtain our assertion, we need to show that $D^2 \alpha_j \in A$ for all j. Note that since $u \in B$, we have $\sigma_i(u) \in B$ for all i, hence

$$\sigma_i(u) = \sum_{j=1}^r \sigma_i(u_j) \alpha_j \in B.$$

Since the matrix $M \cdot (\alpha_1, \ldots, \alpha_r)^\intercal$ has entries in B, after multiplying with the classical adjoint of M, we deduce that $D \cdot \alpha_j \in B$ for all j. Since we have $D \in B$ and $D^2 \in K$, it follows that

$$D^2 \alpha_j \in B \cap K = A \quad \text{for all} \quad j,$$

where the equality follows from the fact that A is integrally closed in K. This completes the proof of the theorem. □

For future reference, we state explicitly the result that we proved as part of the above proof.

THEOREM 8.43. *If A is a Noetherian normal domain, with fraction field K, and L/K is a finite, separable field extension, then the integral closure of A in L is a finite A-algebra.*

8.5. Dedekind domains

DEFINITION 8.44. A *Dedekind domain* is a Noetherian domain R such that $R_{\mathfrak{m}}$ is a DVR for every maximal ideal $\mathfrak{m}$.

EXAMPLE 8.45. Every PID R which is not a field is a Dedekind domain. Indeed, this follows from the characterization of DVRs in Proposition 8.7ii).

PROPOSITION 8.46. A ring R is a Dedekind domain if and only if it is a normal, Noetherian domain, with $\dim(R) = 1$.

PROOF. The assertion follows from the definition of Dedekind domains and the characterization of DVRs in Proposition 8.39, using the fact that R is normal if and only if $R_{\mathfrak{m}}$ is normal for all maximal ideals $\mathfrak{m}$ of R (see Lemma 8.33). □

The following result can be used to provide many examples of Dedekind domains.

THEOREM 8.47. *If R is a Dedekind domain with fraction field K and L/K is a finite separable field extension, then the integral closure S of R in L is a Dedekind domain.*

PROOF. It follows from Theorem 8.43 that the inclusion $R \hookrightarrow S$ is finite. In particular, since R is Noetherian, so is S. We also have $\dim(S) = \dim(R) = 1$ by Proposition 7.13. Since S is normal by construction, it follows that S is Dedekind domain by Proposition 8.46. □

REMARK 8.48. The condition that the field extension is separable in the above theorem can be removed. In fact, there is a much more general result due to Krull and Akizuki, which says that if R is a Noetherian domain with $\dim(R) = 1$, and L is a finite field extension of $\mathrm{Frac}(R)$, then every ring S with $R \subseteq S \subseteq L$ is a Noetherian ring, with $\dim(S) \leq 1$. For a proof, see [**Mat89**, Theorem 11.7].

EXAMPLE 8.49. Recall that a *number field* is a finite field extension K of $\mathbf{Q}$. In this case, the *ring of integers* of K is the integral closure O_K of $\mathbf{Z}$ in K. Since $\mathbf{Z}$ is a Dedekind domain by Example 8.45, it follows from Theorem 8.47 that O_K is a Dedekind domain. Note that O_K is a finitely generated free $\mathbf{Z}$-module (it is finitely generated by Theorem 8.43, and it is free, having no torsion, by the structure theorem for finitely generated $\mathbf{Z}$-modules).

The following result gives an analogue of unique factorization in arbitrary Dedekind domains.

THEOREM 8.50. *Every proper nonzero ideal $\mathfrak{a}$ in a Dedekind domain R can be written as a product*

$$\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r},$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are pairwise distinct maximal ideals in R and $a_1, \ldots, a_r$ are positive integers. Moreover, the pairs $(\mathfrak{p}_1, a_1), \ldots, (\mathfrak{p}_r, a_r)$ are uniquely determined, up to reordering.

PROOF. Since $\dim(R) = 1$ and $\mathfrak{a}$ is a proper, nonzero ideal, it follows that $R/\mathfrak{a}$ is a nonzero Noetherian ring, of dimension 0. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the prime (maximal) ideals in R that contain $\mathfrak{a}$. Since R is a Dedekind domain, it follows that each $R_{\mathfrak{p}_i}$

is a DVR. In particular, it is principal, hence there is a positive integer a_i such that $\mathfrak{a}R_{\mathfrak{p}_i} = \mathfrak{p}_i^{a_i} R_{\mathfrak{p}_i}$ (see Remark 8.9). We claim that

$$\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}.$$

In order to check this equality, it is enough to check that equality holds in each $R_{\mathfrak{m}}$, where $\mathfrak{m}$ is a maximal ideal in R. This is clear. Uniqueness follows similarly by localizing at each maximal ideal of R. □

We end this section by discussing the characterization of Dedekind domains in terms of fractional ideals and the class group of a Dedekind domain.

DEFINITION 8.51. Let R be a domain, with fraction field K. A *fractional ideal* $\mathfrak{a}$ of R is an R-submodule of K contained in $\frac{1}{a}R$ for some $a \in R$ nonzero.

REMARK 8.52. If R is a Noetherian domain, since every ideal in R is finitely generated and since for every finitely many elements $u_1, \ldots, u_n \in K$ there is a nonzero $s \in R$ such that $su_i \in R$ for all i, we see that the fractional ideals of R are precisely the R-submodules of K that are finitely generated as R-modules.

DEFINITION 8.53. With the above notation, if $\mathfrak{a} \subseteq K$ is a fractional ideal of R, then

$$\mathfrak{a}^{-1} := \{u \in K \mid u \cdot \mathfrak{a} \subseteq R\}.$$

LEMMA 8.54. *If R is a domain, with fraction field K, and $\mathfrak{a} \subseteq K$ is a nonzero fractional ideal of R, then $\mathfrak{a}^{-1}$ is a nonzero fractional ideal, as well.*

PROOF. It is straightforward to see that $\mathfrak{a}^{-1}$ is an R-submodule of K. If $\frac{a}{b} \in \mathfrak{a}$ is nonzero, then it follows from the definition that $\mathfrak{a}^{-1} \subseteq \frac{b}{a} \cdot R$, hence $\mathfrak{a}^{-1}$ is a fractional ideal. In order to see that $\mathfrak{a}^{-1}$ is nonzero, note that by assumption, we have $\mathfrak{a} \subseteq \frac{1}{s}R$, for some nonzero $s \in R$. In this case, it is clear that $s \in \mathfrak{a}^{-1}$. □

LEMMA 8.55. *If R is a Noetherian integral domain, with fraction field K, and $\mathfrak{a} \subseteq K$ is a fractional ideal of R, then for every multiplicative system $S \subseteq R \setminus \{0\}$, we have that $S^{-1}\mathfrak{a}$ is a fractional ideal of $S^{-1}R$ and $(S^{-1}\mathfrak{a})^{-1} = S^{-1}(\mathfrak{a}^{-1})$.*

PROOF. If $\mathfrak{a} \subseteq \frac{1}{b}R$, then we have $S^{-1}\mathfrak{a} \subseteq \frac{1}{b}S^{-1}R$, hence $S^{-1}\mathfrak{a}$ is a fractional ideal. The inclusion $S^{-1}(\mathfrak{a}^{-1}) \subseteq (S^{-1}\mathfrak{a})^{-1}$ follows immediately from definition. For the reverse inclusion, suppose that $\frac{b}{s} \in (S^{-1}\mathfrak{a})^{-1}$, and let $u_1, \ldots, u_r \in \mathfrak{a}$ be a system of generators as an R-module (note that $\mathfrak{a}$ is a finitely generated R-module, see Remark 8.52). For every i, with $1 \leq i \leq r$, we can find $t_i \in S$ such that $\frac{t_i b}{s} u_i \in R$. In this case, if $t = \prod_i t_i$, then $\frac{tb}{s} \in \mathfrak{a}^{-1}$ and we have $\frac{b}{s} = \frac{1}{t} \cdot \frac{tb}{s} \in S^{-1}(\mathfrak{a}^{-1})$. □

DEFINITION 8.56. Let R be a domain, with fraction field K, and let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional ideals of R. In this case we denote by $\mathfrak{a} \cdot \mathfrak{b}$ the R-submodule of K generated by all ab, with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. We say that a nonzero fractional ideal $\mathfrak{a}$ is *invertible* if $\mathfrak{a} \cdot \mathfrak{a}^{-1} = R$ (note that the inclusion "$\subseteq$" follows from the definition of $\mathfrak{a}^{-1}$).

REMARK 8.57. With the notation is the above definition, note that $\mathfrak{a} \cdot \mathfrak{b}$ is a fractional ideal of R: if $\mathfrak{a} \subseteq \frac{1}{s}R$ and $\mathfrak{b} \subseteq \frac{1}{t}R$, for nonzero $s, t \in R$, then $\mathfrak{a} \cdot \mathfrak{b} \subseteq \frac{1}{st}R$.

EXAMPLE 8.58. If $\mathfrak{a}$ is a principal fractional ideal (that is, it is generated by one element), then $\mathfrak{a}$ is clearly invertible: indeed, if $\mathfrak{a} = R \cdot \frac{a}{b}$, then $\frac{b}{a} \in \mathfrak{a}^{-1}$, hence $\mathfrak{a} \cdot \mathfrak{a}^{-1} = R$.

LEMMA 8.59. *If R is a domain and $\mathfrak{a}$ is an invertible fractional ideal of R, then $\mathfrak{a}$ is finitely generated.*

PROOF. It follows from the definition that there are $u_1, \dots, u_n \in \mathfrak{a}$ and $v_1, \dots, v_n \in \mathfrak{a}^{-1}$ such that $\sum_{i=1}^n u_i v_i = 1$. In this case $\mathfrak{a} = (u_1, \dots, u_n)$: indeed, for every $w \in \mathfrak{a}$, we have

$$w = \sum_{i=1}^{n} u_i (v_i w)$$

and $v_i w \in R$ for all i. □

If R is local, we can be more precise:

LEMMA 8.60. *If R is a local domain and $\mathfrak{a}$ is an invertible fractional ideal of R, then $\mathfrak{a}$ is a principal ideal.*

PROOF. With the notation in the proof of the previous lemma, note that since R is local, it follows that there is i such that $u_i v_i$ is invertible. In this case $\mathfrak{a} = (u_i)$: if $w \in \mathfrak{a}$, then $w = u_i(u_i v_i)^{-1}(v_i w) \in (u_i)$, since $v_i w \in R$. □

THEOREM 8.61. *A Noetherian domain R is a Dedekind domain if and only if it is not a field and every nonzero fractional ideal is invertible.*

PROOF. Suppose first that R is a Dedekind domain and let $\mathfrak{a}$ be a nonzero fractional ideal of R. Since R is Noetherian, it follows from Lemma 8.55 that for every maximal ideal $\mathfrak{p}$, we have $(\mathfrak{a}^{-1})_{\mathfrak{p}} = (\mathfrak{a}_{\mathfrak{p}})^{-1}$. Since $R_{\mathfrak{p}}$ is a DVR, it follows that $\mathfrak{a}_{\mathfrak{p}}$ is a principal fractional ideal: indeed, it is of the form $\frac{1}{s}\mathfrak{b}$, for some ideal $\mathfrak{b}$ in $R_{\mathfrak{p}}$, and every such ideal is principal. We thus conclude that $\mathfrak{a}_{\mathfrak{p}}$ is invertible by Example 8.58. Since localization clearly commutes with taking the product of fractional ideals, we thus conclude that

$$(\mathfrak{a} \cdot \mathfrak{a}^{-1})_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}} \cdot (\mathfrak{a}_{\mathfrak{p}})^{-1} = R_{\mathfrak{p}}.$$

Since this holds for every maximal ideal $\mathfrak{p}$, we conclude that $\mathfrak{a} \cdot \mathfrak{a}^{-1} = R$ (see Exercise 2.37). Therefore $\mathfrak{a}$ is invertible.

Conversely, suppose that R is not a field and every nonzero ideal of R is invertible. First, we conclude that R is Noetherian using Lemma 8.59. In order to show that R is Dedekind, it is enough to show that for every maximal ideal $\mathfrak{p}$ of R, the ideal $\mathfrak{p}R_{\mathfrak{p}}$ is principal (note that it is nonzero R is not a field). Since $\mathfrak{p}$ is invertible, it follows that $\mathfrak{p}R_{\mathfrak{p}}$ is invertible using Lemma 8.55. Therefore it is principal by Lemma 8.60. □

Let R be a Dedekind domain. Note that the nonzero fractional ideals of R form an Abelian group under multiplication, with identity R: the only nontrivial thing to check is the existence of inverses, and this follows from the fact that every fractional ideal is invertible by Theorem 8.61. This contains the subgroup of principal fractional ideals. The quotient is the *class group* $\mathrm{Cl}(R)$.

REMARK 8.62. Let R be a Dedekind domain, with fraction field K. For every maximal ideal $\mathfrak{p}$ of R, the ring $R_{\mathfrak{p}}$ is a DVR. Let $v_{\mathfrak{p}} \colon K \to \mathbf{Z} \cup \{\infty\}$ be the discrete valuation such that $R_{\mathfrak{p}} = \{x \in K \mid v_{\mathfrak{p}}(x) \geq 0\}$. If Λ is the set of maximal ideals in R, then it follows from Theorem 8.50 that for every $a \in K$ nonzero, we can write

$$(a) = \prod_{\mathfrak{p} \in \Lambda} \mathfrak{p}^{n_{\mathfrak{p}}},$$

where only finitely many $n_{\mathfrak{p}}$ are nonzero. Localizing at $\mathfrak{p}$, we see that $n_{\mathfrak{p}} = v_{\mathfrak{p}}(a)$.

We deduce from the definition of $\mathrm{Cl}(R)$ that if $\mathrm{Div}(R)$ is the free Abelian group on the set of maximal ideals of R, then $\mathrm{Cl}(R)$ is canonically isomorphic to the cokernel of the group homomorphism

$$K^\times \xrightarrow{\mathrm{div}} \mathrm{Div}(R),$$

given by $\mathrm{div}(\varphi) = \sum_{\mathfrak{p}} v_{\mathfrak{p}}[\mathfrak{p}]$. Note that the kernel of this homomorphism is $R^\times$: indeed, if $a = \frac{a_1}{a_2}$ is such that $v_{\mathfrak{p}}(a_1) = v_{\mathfrak{p}}(a_2)$ for all $\mathfrak{p} \in \Lambda$, then $(a_1) = (a_2)$ by Exercise 2.37, hence $a \in R^\times$.

PROPOSITION 8.63. If R is a Dedekind domain, then the following are equivalent:

i) $\mathrm{Cl}(R) = 0$.
ii) R is a PID.
iii) R is a UFD.

PROOF. If $\mathrm{Cl}(R) = 0$, then it follows from the definition that every (fractional) ideal of R is principal, hence R is a PID. Since the implication ii)⇒iii) is a general fact, we only need to prove iii)⇒i). If R is a UFD, since it is a Noetherian domain of dimension 1, it follows from Proposition 8.25 that every maximal ideal in R is principal. Theorem 8.50 thus implies that every fractional ideal in R is principal, hence $\mathrm{Cl}(R) = 0$. □

EXERCISE 8.64. Prove that the converse of the assertion in Theorem 8.50 holds: if R is a domain such that every proper nonzero ideal is a product of prime ideals, then R is a Dedekind domain.

CHAPTER 9

Tor and Ext

9.1. Categories and functors

9.1.1. Abelian categories. We begin with a brief overview of some notions of category theory. These will not play an important role in what follows since we will only deal with categories of R-modules.

DEFINITION 9.1. A *category* $\mathcal{C}$ consists of a class of objects $\mathrm{Ob}(\mathcal{C})$ and for every A, $B \in \mathrm{Ob}(\mathcal{C})$ of a set of *morphisms* (or *arrows*) $\mathrm{Hom}_{\mathcal{C}}(A, B)$, such that for every $A \in \mathrm{Ob}(\mathcal{C})$ we have an element $1_A \in \mathrm{Hom}_{\mathcal{C}}(A)$ and for every $A, B, C \in \mathrm{Ob}(\mathcal{C})$ we have a *composition map*

$$\mathrm{Hom}_{\mathcal{C}}(A, B) \times \mathrm{Hom}_{\mathcal{C}}(B, C) \to \mathrm{Hom}_{\mathcal{C}}(A, C),\ (f, g) \mapsto g \circ f,$$

that satisfy the following two conditions:

i) For every $u \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, we have $u \circ 1_A = u$ and $1_B \circ u = u$.
iii) For every $u \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, $v \in \mathrm{Hom}_{\mathcal{C}}(B, C)$, and $w \in \mathrm{Hom}_{\mathcal{C}}(C, D)$, we have

$$w \circ (v \circ u) = (w \circ v) \circ u.$$

REMARK 9.2. It is common to write $u\colon A \to B$ or $A \xrightarrow{u} B$ instead of $u \in \mathrm{Hom}_{\mathcal{C}}(A, B)$.

EXAMPLE 9.3. The category $\mathcal{S}ets$ has objects all the sets and the morphisms are the maps between the corresponding sets, with the usual composition and identity elements.

EXAMPLE 9.4. If R is a commutative[1] ring, then $\mathcal{M}od(R)$ is the category in which the objects are left R-modules, the morphisms are usual R-linear maps, and with the usual composition and identity morphisms. If $R = \mathbf{Z}$, then we have the category $\mathcal{A}b$ of Abelian groups.

EXAMPLE 9.5. If $\mathcal{C}$ is any category, then the *dual* category $\mathcal{C}^\circ$ has $\mathrm{Ob}(\mathcal{C}^\circ) = \mathrm{Ob}(\mathcal{C})$ and $\mathrm{Hom}_{\mathcal{C}^\circ}(A, B) = \mathrm{Hom}_{\mathcal{C}}(B, A)$ and such that if $u \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ and $v \in \mathrm{Hom}_{\mathcal{C}}(B, C)$, then the composition $u \circ v$ in $\mathcal{C}^\circ$ is equal to $v \circ u$ in $\mathcal{C}$. Note that we have $(\mathcal{C}^\circ)^\circ = \mathcal{C}$.

REMARK 9.6. The dual category provides a convenient tool for treating dual notions. They will not play an important role in what follows since we will typically prove our results for categories of R-modules (as opposed to arbitrary categories).

[1] If R is not necessarily commutative, then we have two distinct categories, that of left R-modules and that of right R-modules.

DEFINITION 9.7. A morphism $u \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ is an *isomorphism* if there is a morphism $v \in \mathrm{Hom}_{\mathcal{C}}(B, A)$ such that $v \circ u = 1_A$ and $u \circ v = 1_B$ (it is an easy exercise to see that such a morphism is unique if it exists). We say that $A, B \in \mathrm{Ob}(\mathcal{C})$ are *isomorphic* if there is an isomorphism in $\mathrm{Hom}_{\mathcal{C}}(A, B)$ (it is straightforward to check that this is an equivalence relation).

REMARK 9.8. It is typical that when working in a categorical setting we are only interested in objects up to isomorphism.

DEFINITION 9.9. The categories that we will consider have more structure: they are *additive categories*, in the following sense:

i) For every $A, B \in \mathrm{Ob}(\mathcal{C})$, the set $\mathrm{Hom}_{\mathcal{C}}(A, B)$ is endowed with an Abelian group structure such that the compositions are bilinear maps.
ii) We have a *zero-object* $0 = 0_{\mathcal{C}} \in \mathrm{Ob}(\mathcal{C})$ such that $\mathrm{Hom}_{\mathcal{C}}(A, 0) = 0 = \mathrm{Hom}_{\mathcal{C}}(0, A)$ for every $A \in \mathrm{Ob}(\mathcal{C})$.
ii) For every two objects $A, B \in \mathrm{Ob}(\mathcal{C})$, a *direct sum* $A \oplus B$ exists in $\mathcal{C}$ (this is an object $A \oplus B$ with morphisms $i\colon A \to A \oplus B$ and $j\colon B \to A \oplus B$ such that for every $M \in \mathrm{Ob}(\mathcal{C})$ and every morphisms $u\colon A \to M$ and $v\colon B \to M$, there is a unique morphism $\varphi\colon A \oplus B \to M$ such that $\varphi \circ i = u$ and $\varphi \circ j = v$.

REMARK 9.10. Note that for a ring R, the category $\mathcal{M}od(R)$ is an additive category.

REMARK 9.11. Note that if $\mathcal{C}$ is an additive category and 0 and $0'$ are zero objects in $\mathcal{C}$, then the unique morphism $0 \to 0'$ is an isomorphism. Similarly, if we have two objects in $\mathcal{C}$ that satisfy the definition of $A \oplus B$, then there is a unique isomorphism between them that commutes with the morphisms $A \to A \oplus B$ and $B \to A \oplus B$.

PROPOSITION 9.12. If $\mathcal{C}$ is a category that satisfies conditions i) and ii) in Definition 9.9, then for every A, B, and M in $\mathcal{C}$, the following are equivalent:

i) We have morphisms $i\colon A \to M$ and $j\colon B \to M$ that make M a direct sum of A and B in $\mathcal{C}$.
ii) We have morphisms $p\colon M \to A$ and $q\colon M \to B$ that make M a direct sum of A and B in $\mathcal{C}^\circ$ (one says that M is a *direct product* of A and B).
iii) We have morphisms $i\colon A \to M$, $j\colon B \to M$, $p\colon M \to A$, and $q\colon M \to B$ such that

$$p \circ i = 1_A,\ p \circ j = 0,\ q \circ i = 0,\ q \circ j = 1_B, \quad \text{and} \quad i \circ p + j \circ q = 1_M.$$

PROOF. We only prove the equivalence of i) and iii), the proof of ii) and iii) follows similarly (or by applying the equivalence we prove for $\mathcal{C}^\circ$). Suppose first that i) holds. It follows from the definition of the direct sum that we have unique $p\colon M \to A$ and $q\colon M \to B$ such that

$$p \circ i = 1_A,\ p \circ j = 0,\ q \circ i = 0,\ q \circ j = 1_B.$$

Furthermore, in order to show that $i \circ p + j \circ q = 1_M$, it is enough to show that we get the same morphism when we compose each side with i and j. This is straightforward to check. We thus obtain iii).

Conversely, suppose that iii) holds. Given $P \in \mathrm{Ob}(\mathcal{C})$ and two morphisms $u\colon A \to P$ and $v\colon B \to P$, we need to show that there is a unique morphism

$w\colon M \to P$ such that $w \circ i = u$ and $w \circ j = v$. Note first that if w satisfies these conditions, then

$$w = w \circ (i \circ p + j \circ q) = u \circ p + v \circ q,$$

hence we have uniqueness. The existence follows from the fact that if $w = u \circ p + v \circ q$, then

$$w \circ i = u \circ (p \circ i) + v \circ (q \circ ji = u \circ 1_A + v \circ 0 = u$$

and similarly $w \circ j = q$. □

COROLLARY 9.13. If $\mathcal{C}$ is an additive category, then $\mathcal{C}^\circ$ is an additive category, too.

PROOF. Indeed, the fact that $\mathcal{C}^\circ$ satisfies conditions i) and ii) in Definition 9.9 is clear, and the fact that it satisfies condition iii) follows from the proposition. □

DEFINITION 9.14. Let $\mathcal{C}$ be an additive category and $u\colon A \to B$ a morphism. A *kernel* of u is a morphism $i\colon \ker(u) \to A$ such that $u \circ i = 0$ and it is universal with this property (that is, for every morphism $v\colon M \to A$ such that $u \circ v = 0$, there is a unique morphism $v'\colon M \to \ker(u)$ such that $v = i \circ v'$). A *cokernel* of u is a morphism $p\colon B \to \operatorname{coker}(u)$ such that $p \circ u = 0$ and it is universal with this property.

REMARK 9.15. It is straightforward to see that given two kernels of $u\colon A \to B$, there is a unique isomorphism between them that commutes with the morphisms to A; the same holds for cokernels.

REMARK 9.16. Note that the kernel (cokernel) of $u\colon A \to B$ in $\mathcal{C}$ is the same as the cokernel (respectively, kernel) of u in $\mathcal{C}^\circ$.

EXAMPLE 9.17. Of course, if $\mathcal{C} = \mathcal{M}od(R)$, then these notions corresponds to the familiar notions of kernel and cokernel for R-linear maps. In particular, we see that kernels and cokernels exist in $\mathcal{M}od(R)$.

DEFINITION 9.18. Let $u\colon A \to B$ be a morphism in an additive category $\mathcal{C}$ that has kernels and cokernels. In this case, by definition of kernels and cokernels, we have a unique morphism $\overline{u}\colon \overline{A} = \operatorname{coker}\big(\ker(u) \to A\big) \to \overline{B} = \ker\big(B \to \operatorname{coker}(u)\big)$ such that the following diagram is commutative:

$$\begin{array}{ccc} A & \xrightarrow{u} & B \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ \overline{A} & \xrightarrow[\overline{u}]{} & \overline{B}, \end{array}$$

where p and i are the maps that come with the definition of a cokernel and kernel, respectively. The category $\mathcal{C}$ is *Abelian* if every morphism has a kernel and cokernel and for every u as above, $\overline{u}$ is an isomorphism.

REMARK 9.19. For a ring R, the fact that $\mathcal{M}od(R)$ is an Abelian category is a consequence of the First Isomorphism theorem.

REMARK 9.20. With the notation in Definition 9.18, it is easy to see that if we consider $u \in \operatorname{Hom}_{\mathcal{C}^\circ}(B, A)$, then the associated morphism is $\overline{u} \in \operatorname{Hom}_{\mathcal{C}^\circ}(\overline{B}, \overline{A})$. This implies that $\mathcal{C}$ is an Abelian category if and only if $\mathcal{C}^\circ$ is an Abelian category.

9.1.2. Functors. We will only consider categories of modules, so we will not really need general notions and results concerning Abelian categories. On the other hand, the language of functors will be very important.

DEFINITION 9.21. Given categories $\mathcal{C}$ and $\mathcal{D}$, a *functor* $F\colon \mathcal{C} \to \mathcal{D}$ is given by associating to every object $A \in \mathrm{Ob}(\mathcal{C})$ an object $F(A) \in \mathrm{Ob}(\mathcal{D})$ and to every morphism $u\colon A \to B$ in $\mathcal{C}$ a morphism $F(u)\colon F(A) \to F(B)$ in $\mathcal{D}$ such that the following two conditions are satisfied:

i) For every $A \in \mathrm{Ob}(\mathcal{C})$, we have $F(1_A) = 1_{F(A)}$.
ii) For every morphisms $A \xrightarrow{u} B \xrightarrow{v} C$ in $\mathcal{C}$, we have

$$F(v \circ u) = F(v) \circ F(u).$$

DEFINITION 9.22. A *contravariant functor* $F\colon \mathcal{C} \to \mathcal{D}$ is a functor $\mathcal{C}^\circ \to \mathcal{D}$. Explicitly, this means that F associates to every object $A \in \mathrm{Ob}(\mathcal{C})$ an object $F(A) \in \mathrm{Ob}(\mathcal{D})$ and to every morphism $u\colon A \to B$ in $\mathcal{C}$ a morphism $F(u)\colon F(B) \to F(A)$ in $\mathcal{D}$ such that the following two conditions are satisfied:

i) For every $A \in \mathrm{Ob}(\mathcal{C})$, we have $F(1_A) = 1_{F(A)}$.
ii) For every morphisms $A \xrightarrow{u} B \xrightarrow{v} C$ in $\mathcal{C}$, we have

$$F(v \circ u) = F(u) \circ F(v).$$

REMARK 9.23. It follows easily from the definition that if $F\colon \mathcal{C} \to \mathcal{D}$ is a (possibly contravariant) functor and $f\colon A \to B$ is an isomorphism in $\mathcal{C}$, then $F(f)\colon F(A) \to F(B)$ is an isomorphism.

DEFINITION 9.24. If $\mathcal{C}$ and $\mathcal{D}$ are additive categories, then an *additive* functor $F\colon \mathcal{C} \to \mathcal{D}$ is a functor such that for every $A, B \in \mathrm{Ob}(\mathcal{C})$, the map $\mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}\big(F(A), F(B)\big)$ induced by F is a group homomorphism. We can similarly define *additive contravariant functors*.

From now on we assume that R is a commutative ring.

EXAMPLE 9.25. We have a *forgetful functor* $\mathcal{M}od(R) \to \mathcal{A}b$ that associates to an R-module the underlying Abelian group and to an R-map, the same map, viewed as a group homomorphism.

EXAMPLE 9.26. For every ring R and every R-module M, we have an additive covariant functor

$$\mathrm{Hom}_R(M, -)\colon \mathcal{M}od(R) \to \mathcal{M}od(R)$$

that associates to an R-module N the R-module[2] $\mathrm{Hom}_R(M, N)$ and to an R-linear map $\varphi\colon N \to N'$ the R-linear map

$$\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N'),\ f \mapsto \varphi \circ f.$$

Similarly, we have an additive contravariant functor $\mathrm{Hom}_R(-, M)\colon \mathcal{M}od(R) \to \mathcal{M}od(R)$ that associates to an R-module P the R-module $\mathrm{Hom}_R(P, M)$ and to an R-linear map $\varphi\colon P' \to P$ the R-linear map

$$\mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P', M),\ f \mapsto f \circ \varphi.$$

[2]The R-module structure on $\mathrm{Hom}_R(M, N)$ is given by $(a\varphi)(u) = a\varphi(u) = \varphi(au)$ for $\varphi \in \mathrm{Hom}_R(M, N)$, $a \in R$, and $u \in M$; the fact that this is, indeed, an R-linear map, makes use of the fact that R is commutative.

PROPOSITION 9.27. If $F\colon \mathcal{C} \to \mathcal{D}$ is an additive functor between additive categories, then F commutes with finite direct sums.

PROOF. Note that if $A_1, \dots, A_n \in \mathrm{Ob}(\mathcal{C})$, then the canonical morphisms $A_i \to A_1 \oplus \dots \oplus A_n$ induce morphisms $F(A_i) \to F(A_1 \oplus \dots \oplus A_n)$, and by the definition of the direct sum, we get a morphism

$$F(A_1) \oplus \dots \oplus F(A_n) \to F(A_1 \oplus \dots \oplus A_n).$$

The assertion in the proposition is that this is an isomorphism. Arguing by induction on n, it is enough to treat the case $n = 2$. In this case the assertion follows from the characterization of the direct sum in Proposition 9.12iii). □

DEFINITION 9.28. Let $F, G\colon \mathcal{C} \to \mathcal{D}$ be two functors. A *natural transformation* $u\colon F \to G$ associates to every $A \in \mathrm{Ob}(\mathcal{C})$ an element $u_A \in \mathrm{Hom}_{\mathcal{D}}\big(F(A), G(A)\big)$ such that for every $\varphi \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, the diagram

$$\begin{array}{ccc} F(A) & \xrightarrow{F(\varphi)} & F(B) \\ {\scriptstyle u_A}\downarrow & & \downarrow{\scriptstyle u_B} \\ G(A) & \xrightarrow[G(\varphi)]{} & G(B), \end{array}$$

is commutative. A *natural transformation* of contravariant functors is simply a natural transformation of functors $\mathcal{C}^\circ \to \mathcal{D}$.

It is clear that we can define a composition of natural transformations, which is associative and has identity elements 1_F for every functor $F\colon \mathcal{C} \to \mathcal{C}$.

DEFINITION 9.29. An *isomorphism* between two functors $F, G\colon \mathcal{C} \to \mathcal{D}$ is a natural transformation $u\colon F \to G$ such that u_A is an isomorphism for every $A \in \mathrm{Ob}(\mathcal{C})$; equivalently, there is another natural transformation $v\colon G \to F$ such that $v \circ u = 1_F$ and $u \circ v = 1_G$. In this case we also say that we have a functorial isomorphism $F(A) \simeq G(A)$ for all $A \in \mathrm{Ob}(\mathcal{C})$.

The following definition is important because it applies to many interesting pairs of functors and it leads to useful properties of those functors.

DEFINITION 9.30. Let $\mathcal{C}$ and $\mathcal{D}$ be two additive categories and $F\colon \mathcal{C} \to \mathcal{D}$ and $G\colon \mathcal{D} \to \mathcal{C}$ be two additive functors. We say that (F, G) is an adjoint pair (or that F is the *left adjoint* of G, or that G is the right adjoint of F) if for every $A \in \mathrm{Ob}(\mathcal{C})$ and $B \in \mathrm{Ob}(\mathcal{D})$, we have a group isomorphism

$$\eta_{A,B}\colon \mathrm{Hom}_{\mathcal{D}}\big(F(A), B\big) \xrightarrow{\simeq} \mathrm{Hom}_{\mathcal{C}}\big(A, G(B)\big)$$

which is functorial with respect to both A and B, that is, for every morphisms $u\colon A' \to A$ in $\mathcal{C}$ and $v\colon B \to B'$ in $\mathcal{D}$, the following diagram is commutative:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{D}}\big(F(A), B\big) & \xrightarrow{\eta_{A,B}} & \mathrm{Hom}_{\mathcal{C}}\big(A, G(B)\big) \\ {\scriptstyle \varphi}\downarrow & & \downarrow{\scriptstyle \psi} \\ \mathrm{Hom}_{\mathcal{D}}\big(F(A'), B'\big) & \xrightarrow[\eta_{A',B'}]{} & \mathrm{Hom}_{\mathcal{C}}\big(A', G(B')\big), \end{array}$$

where $\varphi(f) = v \circ f \circ F(u)$ and $\psi(g) = G(v) \circ g \circ u$.

REMARK 9.31. One can show that if (F, G) and (F, G') are adjoint pairs, then G and G' are isomorphic, and a similar assertion holds with respect to the first component. However, we will not need this fact.

EXERCISE 9.32. Let $\mathcal{C}$ be a category. If $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, show that the following are equivalent:

i) f is an isomorphism.
ii) $\mathrm{Hom}(X, f)$ is an isomorphism for all $X \in \mathrm{Ob}(\mathcal{C})$.
iii) $\mathrm{Hom}(f, X)$ is an isomorphism for all $X \in \mathrm{Ob}(\mathcal{C})$.

9.1.3. The tensor product. We briefly review the definition and basic properties of the tensor product of R-modules. Let R be a not-necessarily commutative ring.

DEFINITION 9.33. Recall that if M is a right R-module and N is a left R-module and P is an Abelian group, then an *R-balanced map* $\varphi\colon M \times N \to P$ is a map that is additive in each variable and such that $\varphi(ua, v) = \varphi(u, av)$ for all $u \in M$, $v \in N$, and $a \in R$. The *tensor product* $M \otimes_R N$ is an Abelian group, together with an R-balanced map $- \otimes -\colon M \times N \to M \otimes_R N$ which is universal, that is, such that for every Abelian group P and every R-balanced map $\varphi\colon M \times N \to P$, there is a unique group homomorphism $\psi\colon M \otimes_R N \to P$ such that $\psi(a \otimes_R b) = \varphi(a, b)$ for every $a \in M$ and $b \in N$.

REMARK 9.34. With the above notation, it is clear that the tensor product is unique up to a unique group isomorphism that commutes with the R-balanced map $M \times N \to M \otimes N$.

REMARK 9.35. The existence of $M \otimes_R N$ is easy to prove, by taking the free $\mathbf{Z}$-module with basis $\{e_{(x,y)} \mid (x, y) \in M \times N\}$, modulo the relations that guarantee that a map is R-balanced, namely:

i) $e_{(x_1+x_2,y)} - e_{(x_1,y)} - e_{(x_2,y)}$, for $x_1, x_2 \in M$ and $y \in N$;
ii) $e_{(x,y_1+y_2)} - e_{(x,y_1)} - e_{(x,y_2)}$, for $x \in M$ and $y_1, y_2 \in N$;
iii) $e_{(xa,y)} - e_{(x,ay)}$, for $x \in M$, $y \in N$, and $a \in R$,

and by taking $a \otimes b$, for $a \in M$ and $b \in N$ to be the image of the basis element $e_{(a,b)}$. A consequence of this description is that $M \otimes_R N$ is generated as a group by $\{a \otimes b \mid a \in M, b \in N\} \subseteq M \otimes_R N$.

REMARK 9.36. For every R-module M, we get a functor

$$M \otimes_R -\colon \mathcal{M}od^{\ell}(R) \to \mathcal{A}b,$$

where $\mathcal{M}od^{\ell}(R)$ is the category of left R-modules, that takes an R-module N to $M \otimes_R N$ and an R-linear map $f\colon N \to N'$ to the unique group homomorphism $g = M \otimes_R f\colon M \otimes_R N \to M \otimes_R N'$ such that $g(a \otimes b) = a \otimes f(b)$ for all $a \in M$ and $b \in N$. We similarly get a functor

$$- \otimes_R M\colon \mathcal{M}od^{\mathrm{r}}(R) \to \mathcal{A}b,$$

from the category of right R-modules to the category of Abelian groups.

From now on, we assume that R is commutative. In particular, there is no distinction between left and right R-modules.

REMARK 9.37. In this case $M \otimes_R N$ has a canonical structure of R-module, in which multiplication by an element $a \in R$ is given by $M \otimes_R \beta_a = \alpha_a \otimes_R N$, where α_a and β_a are the multiplication maps by a on M and N, respectively (note that these are R-linear maps since R is commutative). If P is an R-module, then for every R-bilinear map $\varphi\colon M \times N \to P$, the unique group homomorphism $\psi\colon M \otimes_R N \to P$ such that $\psi(u \otimes v) = \varphi(u, v)$ for all $u \in M$, $v \in N$ is a morphism of R-modules. As in Remark 9.36, we see that we get a functor

$$M \otimes_R -\colon \mathcal{M}od(R) \to \mathcal{M}od(R).$$

Similarly, we have a functor $- \otimes_R M\colon \mathcal{M}od(R) \to \mathcal{M}od(R)$ and it is clear that the two functors are isomorphic (this follows from the universal property in the definition of $M \otimes_R N$ and the fact that giving an R-bilinear map $M \times N \to P$ is equivalent to giving an R-bilinear map $N \times M \to P$).

REMARK 9.38. If the R-module M is generated by $\{x_i \mid i \in I\}$ and the R-module N is generated by $\{y_j \mid j \in J\}$, then the R-module $M \otimes_R N$ is generated by $\{x_i \otimes y_j \mid i \in I, j \in J\}$. This follows from the fact that $M \otimes_R N$ is generated as an Abelian group by $\{x \otimes y \mid x \in M, y \in N\}$. In particular, we see that if both M and N are finitely generated R-modules, then so is $M \otimes_R N$.

REMARK 9.39. If R is a ring and M is an R-module, then $\big(-\otimes_R M, \mathrm{Hom}_R(M, -)\big)$ form an adjoint pair of functors. Indeed, for every R-modules N and P, we have an isomorphism of Abelian groups (in fact, of R-modules)

$$\mathrm{Hom}_R\big(N \otimes_R M, P\big) \simeq \mathrm{Hom}_R\big(N, \mathrm{Hom}_R(M, P)\big),$$

which is functorial with respect to both N and P. Indeed, this follows from the universal property in Remark 9.37, by noting that giving an R-linear map $N \to \mathrm{Hom}_R(M, P)$ is equivalent to giving an R-bilinear map $M \times N \to P$.

EXERCISE 9.40. Show that if M, N, and P are R-modules, then we have a functorial isomorphism of R-modules (in each of the 3 entries)

$$(M \otimes_R N) \otimes_R P \simeq M \otimes_R (N \otimes_R P), \quad (x \otimes y) \otimes z \mapsto x \otimes (y \otimes z).$$

REMARK 9.41. Suppose that R and S are commutative rings, N is an R-module, and M is an R-S-bimodule (this means that M has a structure of R-module and a structure of S-module that are compatible in the sense that $\lambda(\mu x) = \mu(\lambda x)$ for all $\lambda \in R$, $\mu \in S$, and $x \in M$). In this case $N \otimes_R M$ is an R-S-bimodule too, where $\mu(a \otimes b) = a \otimes \mu b$ for every $a \in N$, $b \in M$, and $\mu \in S$. Indeed, for every $\mu \in S$, we have the R-linear map $f_\mu\colon M \to M$ given by $f_\mu(x) = \mu x$ for all $x \in M$. We thus have an induced R-linear map $N \otimes_R f_\mu$, which gives the multiplication by μ on $N \otimes_R M$. Checking that this makes $N \otimes_R M$ an R-S-bimodule is straightforward. It is easy to see also that we get in this way functors $N \otimes_R -$ and $- \otimes_R M$ from the category of R-S-bimodules (respectively R-modules) to the category of R-S-bimodules.

EXERCISE 9.42. Suppose that M is an R-S bimodule. Note that in this case, for every S-module P, the Abelian group $\mathrm{Hom}_S(M, P)$ has a structure of R-module induced by the R-module structure on M. Show that in this case the functor $- \otimes_R M\colon \mathcal{M}od(R) \to \mathcal{M}od(S)$ is the left adjoint of the functor $\mathrm{Hom}_S(M, -)\colon \mathcal{M}od(S) \to \mathcal{M}od(R)$, that is, we have a functorial isomorphism of Abelian groups (in fact, of R-S-bimodules)

$$\mathrm{Hom}_S\big(N \otimes_R M, P\big) \simeq \mathrm{Hom}_R\big(N, \mathrm{Hom}_S(M, P)\big).$$

We now come to one of the main reasons why the tensor product is important: as we have already discussed, in order to study properties of rings, it is important to also study properties of modules over those rings In the presence of a ring homomorphism, the tensor product provides one of the two functors allowing us to relate the two categories of modules, as follows.

REMARK 9.43. Let $f\colon R \to S$ be a ring homomorphism. In this case we have a *restriction of scalars* functor $G\colon \mathcal{M}od(S) \to \mathcal{M}od(R)$ that associates to an S-module M, the R-module with underlying Abelian group M, and scalar multiplication given by $au = f(a)u$ for all $a \in R$ and $u \in M$; similarly, it associates to an S-map the same map, which is clearly R-linear.

We also have an *extension of scalars* functor

$$F\colon -\otimes_R S\colon \mathcal{M}od(R) \to \mathcal{M}od(S),$$

using the fact that S is an R-S-bimodule. Note that G is isomorphic to the functor $\mathrm{Hom}_S(S,-)$, for which we use the R-S-bimodule structure of S, hence we deduce from Exercise 9.42 that (F,G) is an adjoint pair of functors. Explicitly, this says that for every R-module M and every S-module N, we have a functorial isomorphism (of S-modules):

$$\mathrm{Hom}_S(M \otimes_R S, N) \simeq \mathrm{Hom}_R(M,N)$$

given by the composition with $M \to M \otimes_R S$, $x \mapsto x \otimes 1$.

EXERCISE 9.44. Suppose that R is a commutative ring and $f\colon R \to S = T^{-1}R$ is the canonical homomorphism, where $T \subseteq R$ is a multiplicative system. Show that for every R-module M, we have a functorial isomorphism

$$M \otimes_R S \simeq T^{-1}M.$$

PROPOSITION 9.45. Given a family $(M_i)_{i\in I}$ of R-modules and an R-module N, if $\alpha_j\colon M_j \to \bigoplus_{i\in I} M_i$ are the canonical homomorphisms, then the induced homomorphisms $\alpha_j \otimes_R N$ give an isomorphism of R-modules

$$\alpha\colon \bigoplus_{i\in I}(M_i \otimes N) \to \left(\bigoplus_{i\in I} M_i\right) \otimes_R N.$$

PROOF. Indeed, by the universal property of direct sums, we get a unique homomorphism α whose restriction to each $M_i \otimes N$ is $\alpha_i \otimes_R N$. On the other hand, we have an R-bilinear map

$$\left(\bigoplus_{i\in I} M_i\right) \times N \to \bigoplus_{i\in I}(M_i \otimes_R N),\ \big((x_i)_{i\in I}, y\big) \mapsto (x_i \otimes y)_{i\in I}$$

that corresponds by the universal property of the tensor product to a unique homomorphism

$$\beta\colon \left(\bigoplus_{i\in I} M_i\right) \otimes_R N \to \bigoplus_{i\in I}(M_i \otimes_R N).$$

It is then straightforward to see that α and β are mutual inverses. □

EXERCISE 9.46. Show that, more generally, if $(M_i, f_{i,j})_{i\in I}$ is a direct system of R-modules, then for every R-module N, we have a functorial isomorphism

$$\big(\varinjlim_{i\in I} M_i\big) \otimes_R N \simeq \varinjlim_{i\in I}(M_i \otimes_R N).$$

REMARK 9.47. It is a general fact that if (F, G) is an adjoint pair, then F commutes with arbitrary direct limits and G commutes with arbitrary inverse limits.

REMARK 9.48. For every R-module M, an R-bilinear map $\varphi\colon R \times M \to P$ is uniquely determined by the induced map $\varphi(1, -)\colon M \to P$, which is R-linear. We thus deduce from the universal property of the tensor product that the R-linear map $f\colon M \to R \otimes_R M$, given by $f(x) = 1 \otimes x$, is an isomorphism. Its inverse map $R \otimes_R M \to M$ maps $a \otimes x$ to ax.

Using Proposition 9.45, we conclude that if N is a free module, with a basis of cardinality I, then we have a functorial isomorphism $N \otimes_R M \simeq M^{(I)}$ for all R-modules M.

9.1.4. Exact sequences and exact functors. In this chapter we introduce the first concepts of homological algebra. Let us fix a commutative ring R.

DEFINITION 9.49. A *complex* of R-modules is given by a sequence

$$M^\bullet : \quad \ldots \to M^n \xrightarrow{d^n} M^{n+1} \xrightarrow{d^{n+1}} \ldots,$$

where each M^n is an R-module, each $d^n\colon M^n \to M^{n+1}$ is an R-linear map, and $d^{n+1} \circ d^n = 0$ for all $n \in \mathbf{Z}$. The maps d^n are the *differentials* of the complex. We sometimes write such a complex as

$$\ldots \to M_p \to M_{p-1} \to \ldots$$

and we follow the convention that $M_p = M^{-p}$ (and the maps are suitably identified). It is also common to not write the terms that are 0.

Note that if $M^\bullet$ is a complex as above and

$$B^n = B^n(M^\bullet) := \mathrm{Im}(d^{n-1}) \quad \text{and} \quad Z^n = Z^n(M^\bullet) := \ker(d^n),$$

then $B^n \subseteq Z^n$ for all $n \in \mathbf{Z}$.

DEFINITION 9.50. The n^{th} *cohomology module* of $M^\bullet$ is

$$H^n(M^\bullet) := Z^n/B^n.$$

We say that the complex $M^\bullet$ is *exact at* M^i if $\mathcal{H}^i(M^\bullet) = 0$ and we say that $M^\bullet$ is *exact* if it is exact everywhere.

DEFINITION 9.51. If $M^\bullet$ and $N^\bullet$ are complexes of R-modules, then a *morphism of complexes* $f\colon M^\bullet \to N^\bullet$ is given by a family $(f^n\colon M^n \to N^n)_{n\in\mathbf{Z}}$ of R-linear maps such that all squares in the diagram

$$\begin{array}{ccccccc}
\ldots & \longrightarrow & M^n & \xrightarrow{d^n} & M^{n+1} & \xrightarrow{d^{n+1}} & \ldots \\
 & & \downarrow{\scriptstyle f^n} & & \downarrow{\scriptstyle f^{n+1}} & & \\
\ldots & \longrightarrow & N^n & \xrightarrow{d^n} & N^{n+1} & \xrightarrow{d^{n+1}} & \ldots
\end{array}$$

are commutative. It is clear that we can compose morphisms of complexes of R-modules component-wise. In this way we get the *category* $\mathcal{C}om\big(\mathcal{M}od(R)\big)$ of complexes of R-modules. This is an additive category (in fact, an Abelian category), in which the definition of sum of morphisms is done component-wise and kernels, cokernels, and direct sums can be constructed component-wise.

REMARK 9.52. It follows from the commutativity of the diagram in the above definition that if $f\colon M^\bullet \to N^\bullet$ is a morphism of complexes, then each f^n induces a R-linear map $B^n(M^\bullet) \to B^n(N^\bullet)$ and $Z^n(M^\bullet) \to Z^n(N^\bullet)$. We thus get an induced map

$$H^n(f)\colon H^n(M^\bullet) \to H^n(N^\bullet).$$

It is straightforward to see that $H^n(-)$ gives an (additive) functor $\mathcal{C}om\big(\mathcal{M}od(R)\big) \to \mathcal{M}od(R)$.

The following notion is very important for showing that two morphisms of complexes induce the same map in cohomology. It will play an important role in the construction of derived functors.

DEFINITION 9.53. Two morphisms of complexes $f, g\colon M^\bullet \to N^\bullet$ are *homotopic* if we have a sequence of R-linear maps $\theta^n\colon M^n \to N^{n-1}$ for $n \in \mathbf{Z}$ such that

$$f^n - g^n = d_N^{n-1} \circ \theta^n + \theta^{n+1} \circ d_M^n \quad \text{for all} \quad n \in \mathbf{Z}.$$

REMARK 9.54. With the notation in the above definition, note that if $x \in Z^n(M^\bullet)$, then $f^n(x) - g^n(x) = d_N^{n-1}\big(\theta^n(x)\big)$, hence f and g induce the same map $H^n(M^\bullet) \to H^n(N^\bullet)$.

DEFINITION 9.55. Given a sequence of morphisms

$$A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} \dots \xrightarrow{f_{n-1}} A_n,$$

we say that this is *exact* if $\mathrm{Im}(f_i) = \ker(f_{i+1})$ for $1 \le i \le n-2$.

EXAMPLE 9.56. An important example is that of a *short exact sequence*: this is an exact sequence of the form

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0.$$

Note that exactness at M' is equivalent to i being injective, exactness at M is equivalent to $i(M') = \mathrm{Ker}(p)$, and exactness at M'' is equivalent to p being surjective (hence $M'' = \mathrm{coker}(i)$). Therefore every short exact sequence is isomorphic (in the obvious sense) to a short exact sequence of the form

$$0 \to M' \xhookrightarrow{i} M \xrightarrow{p} M/M' \to 0,$$

where i is the inclusion map of a submodule and p is the quotient map.

EXERCISE 9.57. Show that for a short exact sequence

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0,$$

the following are equivalent:

i) There is an R-linear map $q\colon M \to M'$ such that $q \circ i = 1_{M'}$.
ii) There is an R-linear map $j\colon M'' \to M$ such that $p \circ j = 1_{M''}$.
iii) There is an R-submodule N of M such that $M = i(M') \oplus N$ (in which case p induces an isomorphism $N \simeq M''$).

In this case we say that the short exact sequence is *split*.

EXERCISE 9.58. Show that a sequence of R-modules

$$A_1 \to A_2 \to \ldots \to A_n$$

is exact if and only if for all maximal (or prime) ideals $\mathfrak{m}$ of R, the sequence

$$(A_1)_{\mathfrak{m}} \to (A_2)_{\mathfrak{m}} \to \ldots \to (A_n)_{\mathfrak{m}}$$

is exact.

We next discuss two useful results, both of which are proved via "diagram chasing". The first one is known as the 5-lemma.

PROPOSITION 9.59. Consider the following commutative diagram in $\mathcal{M}od(R)$:

$$\begin{array}{ccccccccc} A_1 & \xrightarrow{u_1} & A_2 & \xrightarrow{u_2} & A_3 & \xrightarrow{u_3} & A_4 & \xrightarrow{u_4} & A_5 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_4} & & \downarrow{\scriptstyle f_5} \\ B_1 & \xrightarrow[v_1]{} & B_2 & \xrightarrow[v_2]{} & B_3 & \xrightarrow[v_3]{} & B_4 & \xrightarrow[v_4]{} & B_5, \end{array}$$

with exact rows.

i) If f_2 and f_4 are surjective and f_5 is injective, then f_3 is surjective.
ii) If f_2 and f_4 are injective and f_1 is surjective, then f_3 is injective.
iii) If f_1, f_2, f_4, and f_5 are isomorphisms, then so is f_3.

PROOF. The assertion in iii) is a consequence of i) and ii). We only prove i), the proof of ii) is similar. Suppose that $y \in B_3$. The idea is to apply, at each step, the map we can apply, using the exactness hypothesis and the other hypotheses on the given maps. We begin by considering $v_3(y)$. Since f_4 is surjective, there is $a \in A_4$ such that $f_4(a) = v_3(y)$. Since

$$f_5\big(u_4(a)\big) = v_4\big(f_4(a)\big) = v_4\big(v_3(y)\big) = 0$$

and f_5 is injective, it follows that $u_4(a) = 0$. Since $\ker(u_4) = \mathrm{Im}(u_3)$, it follows that we can write $a = u_3(a')$, hence $v_3(y) = f_4\big(u_3(a')\big) = v_3\big(f_3(a')\big)$. Therefore $y - f_3(a') \in \ker(v_3) = \mathrm{Im}(v_2)$, hence we can write $y - f_3(a') = v_2(b)$. Since f_2 is surjective, we can write $b = f_2(a'')$. We thus conclude that

$$y = f_3(a') + v_2\big(f_2(a'')\big) = f_3\big(a' + u_2(a'')\big).$$

Therefore f_3 is surjective. □

PROPOSITION 9.60. Let us consider a short exact sequence of complexes[3] of R-modules

$$0 \to A^\bullet \xrightarrow{f} B^\bullet \xrightarrow{g} C^\bullet \to 0.$$

In this case, for every n we have an R-linear map $\delta\colon H^n(C^\bullet) \to H^{n+1}(A^\bullet)$ (the *connecting homomorphism*) such that we have an exact complex (the *long exact sequence in cohomology*)

$$\ldots \to H^n(A^\bullet) \xrightarrow{H^n(f)} H^n(B^\bullet) \xrightarrow{H^n(g)} H^n(C^\bullet) \xrightarrow{\delta} H^{n+1}(A^\bullet) \to \ldots.$$

[3]This means that for every n, we have a short exact sequence $0 \to A^n \to B^n \to C^n \to 0$.

Moreover, the connecting homomorphism is functorial with respect to morphisms of short exact sequences: given a morphism of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^\bullet & \xrightarrow{f} & B^\bullet & \xrightarrow{g} & C^\bullet & \longrightarrow & 0\,, \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & A'^\bullet & \xrightarrow{f'} & B'^\bullet & \xrightarrow{g'} & C'^\bullet & \longrightarrow & 0 \end{array}$$

for every $n \in \mathbf{Z}$, the diagram

$$\begin{array}{ccc} H^n(C^\bullet) & \xrightarrow{\delta} & N^{n+1}(A^\bullet) \\ {\scriptstyle H^n(\gamma)}\downarrow & & \downarrow{\scriptstyle H^{n+1}(\alpha)} \\ H^n(C'^\bullet) & \xrightarrow{\delta'} & H^{n+1}(A'^\bullet) \end{array}$$

is commutative.

Proof. Let us begin by defining $\delta\colon H^n(C^\bullet) \to H^{n+1}(A^\bullet)$. In order to simplify the notation, we write d for all the differential in all the 3 complexes. Let $\overline{c} \in H^n(C^\bullet)$, where $c \in C^n$ is such that $d(c) = 0$. Since g^n is surjective, there is $b \in B^n$ such that $g^n(b) = c$. We have

$$g^{n+1}\big(d(b)\big) = d\big(g^n(b)\big) = 0,$$

hence by the exactness of the sequence of complexes, there is a unique $a \in A^{n+1}$ such that $d(b) = f^{n+1}(a)$. Moreover, we have

$$f^{n+2}\big(d(a)\big) = d\big(f^{n+1}(a)\big) = d\big(d(b)\big) = 0,$$

hence using the injectivity of f^{n+2}, we conclude that $a \in Z^{n+1}(A^\bullet)$. We put $\delta(\overline{c}) = \overline{a} \in H^{n+1}(A^\bullet)$.

We first need to show that $\delta(\overline{c})$ does not depend of any choices. Suppose that $c' = c + d(w)$, for some $w \in C^{n-1}$, let $b' \in B^n$ be such that $g^n(b') = c'$, and let $a' \in A^{n+1}$ be such that $f^{n+1}(a') = d(b')$. We may write $w = g^{n-1}(v)$, for some $v \in B^{n-1}$, in which case we have

$$g^n(b' - b) = d\big(g^{n-1}(v)\big) = g^{n-1}\big(d(v)\big),$$

hence $b' - b - d(v) = f^n(u)$, for some $u \in A^n$. We thus have

$$f^{n+1}(a' - a) = d(b' - b) = d\big(d(v) + f^n(u)\big) = d\big(f^n(u)\big) = f^{n+1}\big(d(u)\big),$$

and the injectivity of f^{n+1} implies that $a' = a + d(u)$ has the same class as a in $\mathcal{H}^{n+1}(A^\bullet)$. Therefore δ is well-defined and it is straightforward to check that it is R-linear and that it is functorial with respect to morphisms of short exact sequences of complexes.

Let us prove that the following sequence is exact:

$$H^n(B^\bullet) \xrightarrow{H^n(g)} H^n(C^\bullet) \xrightarrow{\delta} H^{n+1}(A^\bullet). \tag{9.1}$$

Let's show first that $\delta \circ H^n(g) = 0$. Indeed, if $b \in Z^n(B^\bullet)$ and $c = g^n(b)$, then in the definition of $\delta(\overline{c})$, we can use this b. Since $d(b) = 0$, it follows that $\delta(\overline{c}) = 0$.

Let's show now that $\ker(\delta) \subseteq \mathrm{Im}\big(H^n(g)\big)$. If $\delta(\overline{c}) = 0$ and $b \in B^n$ is such that $g^n(b) = c$, then we know that $d(b) = f^{n+1}\big(d(a')\big)$ for some $a' \in A^n$. Therefore $d(b) = d\big(f^n(a')\big)$, hence $b' := b - f^n(a') \in Z^n(B^\bullet)$ and thus $\overline{c} = H^n(g)(\overline{b'})$. This

completes the proof of the exactness of (9.1). We leave the proof of the other two exactness statements as an exercise. □

EXERCISE 9.61. Consider the following diagram of R-modules

$$\begin{array}{ccccccccc} & & M_1 & \xrightarrow{i} & M_2 & \xrightarrow{p} & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & N_1 & \xrightarrow{j} & N_2 & \xrightarrow{q} & N_3 & & \end{array}$$

in which the squares are commutative and the rows are exact. Show that there is a morphism $\delta\colon \ker(h) \to \operatorname{coker}(f)$ such that we have an exact sequence

$$\ker(f) \to \ker(g) \to \ker(h) \xrightarrow{\delta} \operatorname{coker}(f) \to \operatorname{coker}(g) \to \operatorname{coker}(h).$$

We end this section with the key definition of exact functors and by discussing the main examples of interest for us.

DEFINITION 9.62. Let $F\colon \mathcal{M}od(R) \to \mathcal{M}od(S)$ be an additive functor.

i) The functor F is *exact* if for every short exact sequence of R-modules
$$0 \to M' \to M \to M'' \to 0,$$
the sequence
$$0 \to F(M') \to F(M) \to F(M'') \to 0$$
is exact.

ii) The functor F is *left exact* if for every exact sequence
$$0 \to M' \to M \to M''$$
in $\mathcal{M}od(R)$, the sequence
$$0 \to F(M') \to F(M) \to F(M'')$$
is exact.

iii) We say that F is *right exact* if for every exact sequence
$$M' \to M \to M'' \to 0$$
in $\mathcal{M}od(R)$, the sequence
$$F(M') \to F(M) \to F(M'') \to 0$$
is exact.

iv) If $G\colon \mathcal{M}od(R) \to \mathcal{M}od(S)$ is a contravariant functor, then G is a *left exact functor* if it is left exact as a functor $\mathcal{M}od(R)^\circ \to \mathcal{M}od(S)$. Explicitly, for every exact sequence
$$M' \to M \to M'' \to 0$$
in $\mathcal{M}od(R)$, the sequence
$$0 \to G(M'') \to G(M) \to G(M')$$
is exact.

EXAMPLE 9.63. If S is a multiplicative system in R, then the functor $\mathcal{M}od(R) \to \mathcal{M}od(S^{-1}R)$ that takes M to $S^{-1}M$ is exact. Indeed, this follows from Exercise 2.30.

REMARK 9.64. For every additive functor $F\colon \mathcal{M}od(R) \to \mathcal{M}od(S)$, if

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

is a split short exact sequence of R-modules, the corresponding sequence

$$0 \to F(M') \to F(M) \to F(M'') \to 0$$

is split exact. This follows from the fact that F commutes with finite direct sums (see Proposition 9.27).

REMARK 9.65. If $F\colon \mathcal{M}od(R) \to \mathcal{M}od(S)$ is an exact functor and

$$A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} \dots \xrightarrow{f_{n-1}} A_n \tag{9.2}$$

is an exact sequence of R-modules, then the corresponding sequence of S-modules

$$F(A_1) \xrightarrow{F(f_1)} F(A_2) \xrightarrow{F(f_2)} \dots \xrightarrow{F(f_{n-1})} F(A_n)$$

is exact. Indeed, by the exactness of (9.2), we have submodules $B_i \subseteq A_i$ for $1 \leq i \leq n$ such that

$$B_i = \ker(f_i) \text{ for } 1 \leq i \leq n-1 \text{ and } B_i = \mathrm{Im}(f_{i-1}) \text{ for } 2 \leq i \leq n.$$

The short exact sequence

$$0 \to B_i \to A_i \to B_{i+1} \to 0$$

for $1 \leq i \leq n-1$ implies, by the exactness of F, a short exact sequence

$$0 \to F(B_i) \to F(A_i) \to F(B_{i+1}) \to 0.$$

This implies that for $1 \leq i \leq n-1$, the morphism of S-modules $F(f_i)$ factors as a composition

$$F(A_i) \to F(B_{i+1}) \to F(A_{i+1}),$$

with the second map being injective and the first one surjective, with kernal the image of $F(B_i) \to F(A_i)$. We thus have

$$\mathrm{Im}\big(F(f_i)\big) = \ker\big(F(f_{i+1})\big) \quad \text{for} \quad 1 \leq i \leq n-1,$$

giving our assertion.

The following proposition contains the examples of interest for us:

PROPOSITION 9.66. The following properties hold:

i) The sequence

$$0 \to M' \xrightarrow{u} M \xrightarrow{v} M'' \tag{9.3}$$

is exact if and only if for every R-module N, the sequence

$$0 \to \mathrm{Hom}_R(N, M') \to \mathrm{Hom}_R(N, M) \to \mathrm{Hom}_R(N, M'') \tag{9.4}$$

is exact. In particular, the functor $\mathrm{Hom}_R(N, -)$ is left exact for every R-module N.

ii) The sequence

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

is exact if and only if the sequence

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

is exact for all R-modules N. In particular, the contravariant functor $\mathrm{Hom}_R(-, N)$ is left exact for all R-modules N.

iii) The functor $M \otimes_R -$ is right exact for all R-modules M.

PROOF. Note that the sequence (9.3) is exact if and only if $M' \xrightarrow{u} M$ is the kernel of $M \xrightarrow{v} M''$. If this is the case, then (9.4) is exact for every N by the universal property of the kernel. Conversely, if (9.4) is exact for all N, then by taking $N = M'$ and by considering the effect of the composition of the two maps on $1_{M'}$, we see that $v \circ u = 0$. The exactness of (9.4) implies that u satisfies the universal property of the kernel, so (9.3) is exact.

The argument for ii) is similar, using the definition of the cokernel. Let us prove iii). Given an exact sequence

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

we need to show that the induced sequence

$$M \otimes_R N' \to M \otimes_R N \to M \otimes_R N'' \to 0$$

is exact. By ii), this is the case if and only if for every P, the induced sequence

$$0 \to \mathrm{Hom}_R\big(M \otimes_R N'', P\big) \to \mathrm{Hom}_R(M \otimes_R N, P) \to \mathrm{Hom}_R(M \otimes_R N', P)$$

is exact. However, by adjointness (see Remark 9.39) this is isomorphic to the sequence

$$0 \to \mathrm{Hom}_R\big(N'', \mathrm{Hom}_R(M, P)\big) \to \mathrm{Hom}_R\big(N, \mathrm{Hom}_R(M, P)\big) \to \mathrm{Hom}_R\big(N', \mathrm{Hom}_R(M, P)\big),$$

and this is exact by ii). This completes the proof of iii). □

COROLLARY 9.67. If R is a Noetherian ring and M and N are finitely generated R-modules, then $\mathrm{Hom}_R(M, N)$ is a finitely generated R-module.

PROOF. Since M is finitely generated, there is a surjective morphism of R-modules $p\colon R^{\oplus n} \to M$. The left exactness of $\mathrm{Hom}_R(-, N)$ implies that we get an injective morphism of R-modules

$$\mathrm{Hom}_R(M, N) \hookrightarrow \mathrm{Hom}_R(R^{\oplus n}, N) \simeq N^{\oplus n}.$$

Since N is finitely generated, so is $N^{\oplus n}$, and since R is Noetherian, so is $\mathrm{Hom}_R(M, N)$. □

EXAMPLE 9.68. Given an ideal I in R and an R-module M, if we tensor the exact sequence

$$0 \to I \to R \to R/I \to 0$$

by M, it follows from Proposition 9.66 that we have an exact sequence

$$I \otimes_R M \to M \to R/I \otimes_R M \to 0,$$

where we use the isomorphism $M \simeq R \otimes_R M$ (see Remark 9.48). Since the image of $I \otimes_R M \to M$ is IM, we conclude that we have an isomorphism

$$R/I \otimes_R M \simeq M/IM.$$

The functors $\mathrm{Hom}_R(M, -)$, $\mathrm{Hom}_R(-, M)$, and $M \otimes_R -$ are not, in general, exact. This is what motivates the construction of derived functors. In the next section we will discuss for which R-modules M the functors $\mathrm{Hom}_R(M, -)$, $\mathrm{Hom}_R(-, M)$ are exact. The following chapter will be devoted to those R-modules M such that $M \otimes_R -$ is an exact functor.

9.2. Projective and injective modules

Let R be a commutative ring.

DEFINITION 9.69. An R-module P is *projective* if $\mathrm{Hom}_R(P,-)$ is an exact functor. Dually, an R-module I is *injective* if $\mathrm{Hom}_R(-,I)$ is an exact functor.

REMARK 9.70. It follows from Proposition 9.66i) that the functor $\mathrm{Hom}_R(P,-)$ is always left exact, hence P is a projective R-module if and only if it takes surjective maps to surjective maps, that is, for every surjective R-linear map $p\colon U \to V$ and every morphism $f\colon P \to V$, there is a morphism $g\colon P \to U$ such that $f = p \circ g$.

Similarly, since the contravariant functor $\mathrm{Hom}_R(-,I)$ is always left exact by Proposition 9.66ii), it follows that I is an injective module if and only if it takes injective maps to surjective maps, that is, for every injective R-linear map $i\colon A \to B$ and every R-linear map $f\colon A \to I$, there is an R-linear map $g\colon B \to I$ such that $g \circ i = f$.

PROPOSITION 9.71. Given a short exact sequence of R-modules

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0,$$

if A is an injective module or if C is a projective module, then the sequence is split.

PROOF. If A is injective, then applying the description of injective morphisms in Remark 9.70, we see that there is a morphism $g\colon B \to A$ such that $g \circ i = 1_A$, hence the sequence is split. The case when C is a projective module is similar. □

The following proposition gives a very useful description of projective modules:

PROPOSITION 9.72. The R-module P is projective if and only if there are R-modules F and Q, with F free, such that $F \simeq P \oplus Q$.

PROOF. Let's show first that if F is a free R-module, then F is projective. Let $(e_i)_{i\in\Lambda}$ be a basis of F. Given a surjective R-linear map $p\colon U \to V$ and a morphism $f\colon F \to V$, for every $i \in \Lambda$, there is $u_i \in U$ such that $p(u_i) = f(e_i)$. Let $g\colon F \to U$ be the unique R-linear map $g\colon F \to U$ such that $g(e_i) = u_i$ for all $i \in \Lambda$. We thus have $f = p \circ g$ since the two R-linear maps take the same values on each e_i.

Suppose now that $F \simeq P \oplus Q$. Since

$$\mathrm{Hom}_R(F,M) \simeq \mathrm{Hom}_R(P,M) \oplus \mathrm{Hom}_R(Q,M)$$

for every R-module M, it is clear that the exactness of $\mathrm{Hom}_R(F,-)$ implies the exactness of $\mathrm{Hom}_R(P,-)$.

Conversely, suppose that P is a projective module. Let us consider a surjective morphism $\varphi\colon A \to P$, where A is a free R-module (for example, we may choose a system of generators $(x_i)_{i\in I}$ of P, let A be a free R-module with basis $(e_i)_{i\in I}$, and let φ be the unique R-linear map such that $\varphi(e_i) = x_i$ for all $i \in I$). We thus have a short exact sequence

$$0 \longrightarrow \ker(\varphi) \longrightarrow A \xrightarrow{\varphi} P \longrightarrow 0.$$

Since P is projective, this is split by Proposition 9.71, hence $A \simeq P \oplus \ker(\varphi)$. □

REMARK 9.73. One consequence of the above proposition is that the category $\mathcal{M}od(R)$ *has enough projectives*: this means that for every R-module M, there is a surjective R-linear map $f\colon P \to M$, where P is a projective R-module. Indeed, we can find such a morphism with P free.

The following result gives an important characterization of projective finitely generated modules over Noetherian rings.

THEOREM 9.74. *Let P be a finitely generated module over a Noetherian ring R. Then P is projective if and only if $P_{\mathfrak{m}}$ is a free $R_{\mathfrak{m}}$-module for every maximal (or prime) ideal $\mathfrak{m}$ of R.*

Before giving the proof of the theorem, we need a result about the behavior of Hom modules under localization, which is useful also in other situations. Its proof in turn will make use of the following notion:

DEFINITION 9.75. Given an R-module M, a *finite free presentation* of M is an exact sequence of the form

$$F_1 \to F_0 \to M \to 0,$$

where F_1 and F_0 are finitely generated modules.

REMARK 9.76. Such a presentation always exists if M is finitely generated and R is Noetherian: indeed, after choosing finitely many generators $u_1, \dots, u_n$ of M, we get a surjective morphism $p\colon R^{\oplus n} \to M$ that maps e_i to u_i for $1 \leq i \leq n$. Since R is Noetherian, the R-module $\ker(p)$ is finitely generated, and thus proceeding as above, we get a surjective morphism $R^{\oplus m} \to \ker(p)$. We thus obtain a finite free presentation

$$R^{\oplus m} \to R^{\oplus n} \to M \to 0.$$

LEMMA 9.77. *If S is a multiplicative system in a Noetherian ring R, then for every R-modules M and N, with M finitely generated, we have a functorial isomorphism of $S^{-1}R$-modules*

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

PROOF. The argument we give below applies in many other instances: once we construct a functorial transformation, in the presence of a suitable exactness property, we can reduce to the case $M = A$, which is straightforward. Note that we have a morphism of R-modules

$$\mathrm{Hom}_R(M,N) \to \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N), \quad \varphi \mapsto S^{-1}\varphi.$$

Since the right-hand side is an $S^{-1}R$-module, we get an induced morphism of $S^{-1}R$-modules

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

(see Remark 9.43). It is straightforward to see that this is functorial with respect to M (and also with N). Let us choose a finite free presentation

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

It follows from Proposition 9.66 and Example 9.63 that in the commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & S^{-1}\mathrm{Hom}_R(M,N) & \longrightarrow & S^{-1}\mathrm{Hom}_R(F_0,N) & \longrightarrow & S^{-1}\mathrm{Hom}_R(F_1,N) \\
 & & \downarrow{\scriptstyle \tau_{M,N}} & & \downarrow{\scriptstyle \tau_{F_0,N}} & & \downarrow{\scriptstyle \tau_{F_1,N}} \\
0 & \longrightarrow & \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) & \longrightarrow & \mathrm{Hom}_{S^{-1}R}(S^{-1}F_0, S^{-1}N) & \longrightarrow & \mathrm{Hom}_{S^{-1}R}(S^{-1}F_1, S^{-1}N)
\end{array}$$

the rows are exact. We then deduce from the 5-lemma (see Proposition 9.59) that it is enough to show that $\tau_{F_0,N}$ and $\tau_{F_1,N}$ are isomorphisms. Since we deal with

additive functors and since it is clear that $\tau_{M_1 \oplus M_2, N} = \tau_{M_1,N} \oplus \tau_{M_2,N}$ for every R-modules M_1 and M_2, we see that it is enough to show that $\tau_{R,N}$ is an isomorphism, but this is clear, using the canonical isomorphisms

$$\mathrm{Hom}_R(R, N) \simeq N \quad \text{and} \quad \mathrm{Hom}_{S^{-1}R}(S^{-1}R, S^{-1}N) \simeq S^{-1}N.$$

This completes the proof of the lemma. □

We can now prove the characterization of finitely generated projective modules.

Proof of Theorem 9.74. We first show that P is projective if and only if $P_\mathfrak{m}$ is projective for every maximal (or prime) ideal of R. Indeed, note first that if P is projective, then it follows from Proposition 9.72 that there are R-modules F and Q, with F free, such that $F \simeq P \oplus Q$. If $\mathfrak{m}$ is a prime ideal of R, then we get an isomorphism $F_\mathfrak{m} \simeq P_\mathfrak{m} \oplus Q_\mathfrak{m}$. Since $F_\mathfrak{m}$ is a free $R_\mathfrak{m}$-module, it follows that $P_\mathfrak{m}$ is a projective $R_\mathfrak{m}$-module by Proposition 9.72.

Conversely, suppose that $R_\mathfrak{m}$ is a projective R-module for all maximal ideals $\mathfrak{m}$ of R. Given a surjective morphism of R-modules $p\colon A \to B$, we need to show that the induced morphism

$$\mathrm{Hom}_R(M, A) \to \mathrm{Hom}_R(M, B) \tag{9.5}$$

is surjective. By Exercise 9.58, it is enough to show that for every maximal ideal $\mathfrak{m}$ of R, the induced map

$$\mathrm{Hom}_R(M, A)_\mathfrak{m} \to \mathrm{Hom}_R(M, B)_\mathfrak{m}$$

is surjective. Since M is a finitely generated module over a Noetherian ring, Lemma 9.77 implies that it is enough to show that the map

$$\mathrm{Hom}_{R_\mathfrak{m}}(M_\mathfrak{m}, A_\mathfrak{m}) \to \mathrm{Hom}_{R_\mathfrak{m}}(M_\mathfrak{m}, B_\mathfrak{m})$$

is surjective. This follows from the fact that $M_\mathfrak{m}$ is projective and $A_\mathfrak{m} \to B_\mathfrak{m}$ is surjective.

In order to complete the proof of the theorem it is thus enough to show that if $(R, \mathfrak{m})$ is a local Noetherian ring and M is a finitely generated R-module, then M is projective if and only if M is free. The "if" part follows from Proposition 9.72. Suppose now that M is projective. Let $u_1, \dots, u_n \in M$ be such that $\overline{u_1}, \dots, \overline{u_n} \in M/\mathfrak{m}M$ give a basis over $R/\mathfrak{m}$. It follows from Nakayama's lemma that $u_1, \dots, u_n$ generate M, hence we have a surjective morphism $p\colon R^{\oplus n} \to M$ such that $p(e_i) = u_i$ for $1 \leq i \leq n$. If $K = \ker(p)$, then we have a short exact sequence

$$0 \longrightarrow K \longrightarrow R^{\oplus n} \xrightarrow{p} M \longrightarrow 0.$$

Since M is projective, this sequence is split by Proposition 9.71, hence tensoring with $R/\mathfrak{m}$, gives an exact sequence

$$0 \to K/\mathfrak{m}K \to (R/\mathfrak{m})^{\oplus n} \xrightarrow{\overline{p}} M/\mathfrak{m} \to 0.$$

By construction, $\overline{p}$ is an isomorphism, hence $K/\mathfrak{m}K = 0$. Since R is Noetherian, K is finitely generated, hence another application of Nakayama's lemma gives $K = 0$. Therefore $M \simeq R^{\oplus n}$ is free. This completes the proof of the theorem. □

Our next goal is to show that for every ring R, the category $\mathcal{M}od(R)$ has enough injectives:

Theorem 9.78. *For every R-module M, there is an injective morphism $M \hookrightarrow Q$, where Q is an injective R-module.*

The proof proceeds by first treating the case when $R = \mathbf{Z}$. In this case, the key fact is the characterization of injective $\mathbf{Z}$-modules as divisible groups. This in turn follows from the following criterion for a module to be injective:

PROPOSITION 9.79. (Baer) An R-module Q is injective if and only if for every left ideal I in R, the induced morphism of Abelian groups

$$Q = \mathrm{Hom}_R(R, Q) \to \mathrm{Hom}_R(I, Q)$$

is surjective.

PROOF. Of course, we only need to prove the "if" part. Suppose that M is an R-module and M' is a submodule. We need to show that for every morphism $\varphi' \colon M' \to Q$, there is a morphism $\varphi \colon M \to Q$ such that $\varphi|_{M'} = \varphi'$. We consider the set $\mathcal{M}$ of all pairs (M_1, φ_1), where M_1 is a submodule of M containing M' and $\varphi_1 \colon M_1 \to Q$ is a morphism such that $\varphi_1|_{M'} = \varphi'$. We order this set by putting $(M_1, \varphi_1) \leq (M_2, \varphi_2)$ if $M_1 \subseteq M_2$ and $\varphi_2|_{M_1} = \varphi_1$.

Since we have $(M', \varphi') \in \mathcal{M}$, we see that $\mathcal{M}$ is non-empty. Moreover, given a family $(M_i, \varphi_i)_{i \in I}$ of elements of $\mathcal{M}$, any two of them comparable, we can take $M'' = \bigcup_{i \in I} M_i$ and $\varphi'' \colon M'' \to Q$ such that $\varphi''|_{M_i} = \varphi_i$ for all i; in this case $(M'', \varphi'') \in \mathcal{M}$ is the supremum of the family $(M_i, \varphi_i)_{i \in I}$.

We can thus apply Zorn's lemma to choose a maximal element (M_0, φ_0) in $\mathcal{M}$. We claim that $M_0 = M$, which would complete the proof. Suppose that this is not the case and let $u \in M \smallsetminus M_0$. We will show that there is an extension of φ_0 to a morphism $\varphi_1 \colon M_0 + Ru \to Q$; this would contradict the maximality of (M_0, φ_0).

Let $I = \{a \in R \mid au \in M_0\}$. Note that I is an ideal of R and we can define a morphism $\psi \colon I \to Q$ by $\psi(a) = \varphi_0(au)$. By assumption, there is $w \in Q$ such that $\psi(a) = aw$ for every $a \in I$. We define $\varphi \colon M_0 + Ru \to Q$ by

$$\varphi_1(v + au) = \varphi_0(v) + aw \quad \text{for} \quad v \in M_0, a \in R.$$

Note that φ_1 is well-defined: if $v + au = v' + a'u$, then $(a - a')u = v' - v \in M_0$, hence $a - a' \in I$. We thus have

$$\varphi_0(v' - v) = \varphi_0\big((a - a')u\big) = (a - a')w,$$

hence $\varphi_0(v') + a'w = \varphi_0(v) + aw$. It is now straightforward to see that φ_1 is R-linear and $\varphi_1|_{M_0} = \varphi_0$. This completes the proof. □

Recall that an Abelian group A is *divisible* if for every positive integer n, the multiplication map $A \xrightarrow{\cdot n} A$ is surjective.

COROLLARY 9.80. A $\mathbf{Z}$-module Q is injective if and only if it is a divisible Abelian group.

PROOF. Since every ideal of $\mathbf{Z}$ is of the form $n\mathbf{Z}$, for some non-negative integer n, it follows from the proposition that Q is injective if and only if for every such n, the induced morphism of Abelian groups

$$Q \to \mathrm{Hom}_{\mathbf{Z}}(n\mathbf{Z}, Q)$$

is surjective. This is clearly the case if $n = 0$. If $n > 0$, then this morphism gets identified to the morphism $Q \to Q$ given by multiplication by n, and we obtain the assertion in the corollary. □

We can now prove the existence of embeddings in injective modules.

PROOF OF PROPOSITION 9.78. Suppose first that $R = \mathbf{Z}$. In this case, by the above corollary, we need to show that every Abelian group M can be embedded in a divisible Abelian group A. Write $M \simeq F/G$, where $F \simeq \mathbf{Z}^{(I)}$ is a free Abelian group. Since F is free, it has no torsion, and thus the canonical morphism $F \hookrightarrow F \otimes_{\mathbf{Z}} \mathbf{Q} \simeq \mathbf{Q}^{(I)}$ is injective. We thus have an injective morphism $M \hookrightarrow A := (F \otimes_{\mathbf{Z}} \mathbf{Q})/G$. It is clear that $F \otimes_{\mathbf{Z}} \mathbf{Q}$ is divisible, and thus its image A is divisible, too.

Consider now the general case. By considering on M the underlying structure of $\mathbf{Z}$-module and applying what we have already proved, we get an injective morphism of $\mathbf{Z}$-modules $j\colon M \hookrightarrow A$, where A is an injective $\mathbf{Z}$-module. We claim that if we consider on $\mathrm{Hom}_{\mathbf{Z}}(R, A)$ the R-module structure induced by the one on R (that is, we have

$$(\lambda \cdot \varphi)(r) = \varphi(r\lambda) \quad \text{for all} \quad \lambda, r \in R, \varphi \in \mathrm{Hom}_{\mathbf{Z}}(R, A)),$$

then $\mathrm{Hom}_{\mathbf{Z}}(R, A)$ is an injective R-module. In order to see this, it is enough to note that since $R \otimes_R -$ is the left adjoint of $\mathrm{Hom}_{\mathbf{Z}}(R, -)$ (see Remark 9.42), for every R-module N, we have a canonical isomorphism

$$\mathrm{Hom}_R\big(N, \mathrm{Hom}_{\mathbf{Z}}(R, A)\big) \simeq \mathrm{Hom}_{\mathbf{Z}}(N \otimes_R R, A) \simeq \mathrm{Hom}_{\mathbf{Z}}(N, A).$$

Since $\mathrm{Hom}_{\mathbf{Z}}(-A)$ is an exact functor, it follows that $\mathrm{Hom}_R\big(-, \mathrm{Hom}_{\mathbf{Z}}(R, A)\big)$ is an exact functor.

Finally, we note that we have an injective morphism of R-modules given by

$$M \to \mathrm{Hom}_{\mathbf{Z}}(R, A), \quad M \ni v \mapsto \varphi_v, \quad \text{where} \quad \varphi_v(r) = j(rv).$$

This completes the proof. □

REMARK 9.81. While projective and injective objects are dual categorical notions, we have seen that their behavior in the category $\mathcal{M}od(R)$ is quite different. Given an R-module M, it is easy to find a surjective R-linear map $P \to M$, with P a projective module, and this can be carried out efficiently in practice. On the other hand, while we will make use in the next section of the existence of an injective R-linear map $M \to I$, where I is an injective R-module, this is never done explicitly in practice (part of the reason is that even if M is finitely generated over a Noetherian ring R, the R-module I is almost never finitely generated).

9.3. Construction of derived functors

We begin by discussing the notions of injective and projective resolutions. Let us fix a (commutative) ring R.

DEFINITION 9.82. Given an R-module M, a *projective* resolution $F_\bullet \xrightarrow{\epsilon} M$ of M is a complex $F_\bullet$ (note the lower indexing) such that F_p is a projective R-module for all p and $F_p = 0$ for $p < 0$, together with a morphism $\epsilon\colon F_0 \to M$, such that the resulting complex

$$\ldots \to F_p \to \ldots \to F_1 \to F_0 \to M \to 0$$

is exact. If the F_p are free, then $F_\bullet \to M$ is a *free* resolution.

An *injective resolution* $M \xrightarrow{\epsilon} I^\bullet$ of M is a complex $I^\bullet$ such that I^p is an injective R-module for all p and $I^p = 0$ for $p < 0$, together with a morphism $M \to I^0$ such that the resulting complex

$$0 \to M \to I^0 \to I^1 \to \ldots \to I^p \to \ldots$$

is exact

Projective and injective resolutions are the main tools for constructing derived functors. The following two results give the main properties of these notions. We begin with injective resolutions.

PROPOSITION 9.83. Let M and N be R-modules.

i) There is an injective resolution $M \xrightarrow{\alpha} I^\bullet$ of M.

ii) Given a morphism of R-modules $f\colon M \to N$ and injective resolutions $M \xrightarrow{\alpha} I^\bullet$ and $N \xrightarrow{\beta} J^\bullet$, there is a morphism of complexes $u\colon I^\bullet \to J^\bullet$ such that also the diagram

$$\begin{array}{ccc} M & \xrightarrow{\alpha} & I^0 \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle u^0} \\ N & \xrightarrow{\beta} & J^0 \end{array}$$

is commutative.

iii) If u and v both satisfy the conclusion in ii), then they are homotopic.

PROOF. In order to prove i), we begin by using Proposition 9.78 to find an injective R-module I^0 and an injective morphism $M \hookrightarrow I^0$. If C is the cokernel of this map, we use the same proposition to find an injective R-module I^1 and an injective homomorphism $C \hookrightarrow I^1$. We thus have an exact sequence

$$0 \to M \to I^0 \to I^1.$$

Continuing in this way we obtain the injective resolution $I^\bullet$.

For ii), we construct the morphisms $u^i\colon I^i \to J^i$ recursively, as follows. Since the morphism $M \to I^0$ is injective and J^0 is an injective R-module, we can find $u^0\colon I^0 \to J^0$ such that the diagram

$$\begin{array}{ccc} M & \xrightarrow{\alpha} & I^0 \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle u^0} \\ N & \xrightarrow{\beta} & J^0 \end{array}$$

is commutative. Since $I^\bullet$ is a resolution, the induced morphism $\operatorname{coker}(\alpha) \to I^1$ is injective. On the other hand, u^0 induces a morphism $\overline{u_0}\colon \operatorname{coker}(\alpha) \to \operatorname{coker}(\beta)$, and since J^1 is injective, there is a morphism $u^1\colon I^1 \to J^1$ such that the right square in the diagram

$$\begin{array}{ccccc} I^0 & \longrightarrow & \operatorname{coker}(\alpha) & \longrightarrow & I^1 \\ {\scriptstyle u^0}\downarrow & & {\scriptstyle \overline{u_0}}\downarrow & & \downarrow{\scriptstyle u^1} \\ J^0 & \longrightarrow & \operatorname{coker}(\beta) & \longrightarrow & J^1 \end{array}$$

is commutative as well. Iterating this argument, we obtain the assertion in ii).

Finally, suppose that u and v both satisfy the condition in ii). We construct recursively morphisms $\theta^i\colon I^i \to J^{i-1}$ for $i \geq 1$ such that $u^i - v^i = d \circ \theta^i + \theta^{i+1} \circ d$ for all $i \geq 0$ (where $\theta^0 = 0$). The assumption implies that u^0 and v^0 agree on the image of $M \to I^0$, hence $u^0 - v^0$ induces a morphism $\operatorname{coker}(\alpha) \to J^0$. Using the fact that J^0 is an injective R-module and the morphism $\operatorname{coker}(\alpha) \hookrightarrow I^1$ is injective, we obtain a morphism $\theta^1\colon I^1 \to J^0$ such that $u^0 - v^0 = \theta^1 \circ d$. Note now that

$$(u^1 - v^1 - d \circ \theta^1) \circ d = d \circ (u^0 - v^0 - \theta^1 \circ d) = 0,$$

hence $u^1 - v^1 - d \circ \theta^1$ induces a morphism $\gamma\colon \operatorname{coker}(I^0 \to I^1) \to J^1$. Since $H^1(I^\bullet) = 0$, the induced morphism $\operatorname{coker}(I^0 \to I^1) \hookrightarrow I^2$ is injective, hence γ has an extension as a morphism $\theta^2\colon I^2 \to J^1$ by the injectivity of J^2. We thus have $\theta^2 \circ d + d \circ \theta^1 = u^1 - v^1$. Iterating this argument, we get that u and v are homotopic. □

The following result gives the corresponding assertions for projective resolutions.

PROPOSITION 9.84. Let M and N be R-modules.

i) There is a projective (in fact, free) resolution $P_\bullet \xrightarrow{\alpha} M$ of M.
ii) Given a morphism of R-modules $f\colon M \to N$ and projective resolutions $P_\bullet \xrightarrow{\alpha} M$ and $Q_\bullet \xrightarrow{\beta} N$, there is a morphism of complexes $u\colon P_\bullet \to Q_\bullet$ such that also the diagram

$$\begin{array}{ccc} P_0 & \xrightarrow{\alpha} & M \\ {\scriptstyle u_0}\downarrow & & \downarrow{\scriptstyle f} \\ Q_0 & \xrightarrow{\beta} & N \end{array}$$

is commutative.
iii) If u and v both satisfy the conclusion in ii), then they are homotopic.

PROOF. The argument is entirely analogous to that in the proof of Proposition 9.83, so we omit it. We only note that the construction of a projective (even free) resolution is due to the fact that every R-module M admits a surjective morphism $F \to M$, where F is a free (hence projective) R-module. □

We will also need the following lemma regarding the construction of resolutions for the modules in a short exact sequence. This will allow us to apply Proposition 9.60 to get the long exact sequence for derived functors.

LEMMA 9.85. *Given an exact sequence of R-modules*

$$0 \to M \to N \to P \to 0$$

and injective resolutions $M \to I^\bullet$ and $P \to J^\bullet$, we can find a commutative diagram of complexes[4]

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & N & \longrightarrow & P & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & I^\bullet & \xrightarrow{u} & Q^\bullet & \xrightarrow{v} & J^\bullet & \longrightarrow & 0, \end{array}$$

such that for every i, the sequence

$$0 \to I^i \to Q^i \to J^i \to 0$$

is (split) exact. In particular, the middle vertical arrow in the above commutative diagram gives an injective resolution of N.

[4]We think of the top row as an exact sequence of complexes, with the only nontrivial entries in degree 0.

PROOF. For every $i \geq 0$, we put $Q^i = I^i \oplus J^i$ and take the maps $u^i \colon I^i \to Q^i$ and $v^i \colon Q^i \to J^i$ to be the canonical injection and surjection, respectively. We will show that we can find morphisms $N \to Q^0$ and $Q^i \to Q^{i+1}$ for $i \geq 0$ such that we have a commutative diagram of complexes as in the lemma. We define $(\alpha, \beta) \colon N \to Q^0 = I^0 \oplus J^0$, where β is the composition $N \to P \to J^0$ and $\alpha \colon N \to I^0$ is an extension of the map $M \to I^0$ (we use here the fact that I^0 is injective). We thus obtain a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & N & \longrightarrow & P & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & I^0 & \longrightarrow & Q^0 & \longrightarrow & J^0 & \longrightarrow & 0, \end{array}$$

and it follows easily (one could also use Proposition 9.60) that we get a short exact sequence

$$0 \to \operatorname{coker}(M \to I^0) \to \operatorname{coker}(N \to Q^0) \to \operatorname{coker}(P \to J^0) \to 0.$$

We can now repeat the construction to obtain the commutative diagram of complexes in the statement.

Finally, it is clear, by construction, that Q^i is an injective R-module for every $i \geq 0$ (it is easy to see, using the definition, that the direct sum of two injective modules is injective). The fact that $N \to Q^\bullet$ is an injective resolution follows from Proposition 9.60. □

Of course, there is a similar statement for projective resolutions and we leave formulating and proving that as an exercise for the reader. We now turn to the definition of derived functors. We want to construct derived functors for 2 functors: a left exact functor, namely $\operatorname{Hom}_R(M, -)$ and a right exact functor, namely $M \otimes_R -$ (we also have a left exact contravariant functor, namely $\operatorname{Hom}_R(-, M)$, but it will turn out that this does not need separate treatment). In what follows, we explain in detail the case of $\operatorname{Hom}_R(M, -)$ and only state the corresponding statements for $M \otimes_R -$.

Suppose that $F \colon \mathcal{C} \to \mathcal{D}$ is a left exact additive functor, where $\mathcal{C} = \mathcal{M}od(R)$ and $\mathcal{D} = \mathcal{M}od(S)$, where R and S are fixed rings. In order to measure the failure of F to be exact, we will extend it to a sequence of functors, as follows.

DEFINITION 9.86. A *cohomological δ-functor* is a sequence of functors $(F^i)_{i \geq 0}$ from $\mathcal{C}$ to $\mathcal{D}$, together with the following data: for every short exact sequence in $\mathcal{C}$

$$0 \longrightarrow A' \xrightarrow{u} A \xrightarrow{v} A'' \longrightarrow 0, \tag{9.6}$$

we have "connecting morphisms" $\delta \colon F^i(A'') \to F^{i+1}(A')$ for $i \geq 0$, such that the complex

$$0 \to F^0(A') \xrightarrow{F^0(u)} F^0(A) \xrightarrow{F^0(v)} F^0(A'') \xrightarrow{\delta} F^1(A') \xrightarrow{F^1(u)} F^1(A) \to \dots$$

is exact (this is the *long exact sequence* associated to (9.6)). Moreover, the connecting morphisms are required to be functorial: given a morphism of short exact

sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & B' & \longrightarrow & B & \longrightarrow & B'' & \longrightarrow & 0, \end{array}$$

for every $i \geq 0$ we have a commutative diagram

$$\begin{array}{ccc} F^i(A'') & \xrightarrow{\delta} & F^{i+1}(A') \\ \downarrow & & \downarrow \\ F^i(B'') & \xrightarrow{\delta} & \mathcal{F}^{i+1}(B'). \end{array}$$

DEFINITION 9.87. Given two cohomological δ-functors $(F_i)_{i\geq 0}$ and $(G_i)_{i\geq 0}$ from $\mathcal{C}$ to $\mathcal{D}$, a *morphism of cohomological δ-functors* is given by natural transformations $(F_i \to G_i)_{i\geq 0}$ such that for every short exact sequence in $\mathcal{C}$

$$0 \to A' \to A \to A'' \to 0,$$

we have a commutative diagram

$$\begin{array}{ccc} F^i(A'') & \xrightarrow{\delta} & F^{i+1}(A') \\ \downarrow & & \downarrow \\ G^i(A'') & \xrightarrow{\delta} & G^{i+1}(A''). \end{array}$$

Note that in this case, by the functoriality of the transformations $F^i \to G^i$, we have a morphism of long exact sequences.

The following is the fundamental result in the construction of derived functors.

THEOREM 9.88. *If $F\colon \mathcal{C} \to \mathcal{D}$ is a left exact functor, then there is a cohomological δ-functor $(R^iF)_{i\geq 0}$ such that the following two conditions are satisfied:*

i) *We have a natural isomorphism $R^0F \simeq F$, and*
ii) *$R^iF(I) = 0$ for every injective object $I \in \mathcal{C}$ and every $i \geq 1$.*

Such a cohomological δ-functor is unique up to a unique isomorphism that corresponds to the identity on $R^0F \simeq F$. Moreover, if $(G^i)_{i\geq 0}$ is any cohomological δ-functor and we have a functorial transformation $F \to G^0$, then there is a unique extension of this to a morphism of cohomological δ-functors $(R^iF)_{i\geq 0} \to (G^i)_{i\geq 0}$.

PROOF. For every object A in $\mathcal{C}$, we choose an injective resolution $A \to I^\bullet$ and put

$$R^iF(A) := H^i\big(F(I^\bullet)\big).$$

Given a morphism $f\colon A \to B$, if $A \to I^\bullet$ and $B \to J^\bullet$ are the chosen injective resolutions, then it follows from Proposition 9.83 that there is a morphism $u\colon I^\bullet \to J^\bullet$ such that we have a commutative diagram

$$\begin{array}{ccc} A & \longrightarrow & I^\bullet \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle u} \\ B & \longrightarrow & J^\bullet. \end{array}$$

We put $R^iF(f) = H^i\big(F(u)\big)$. Note that u is not unique, but if v is another such morphism, then it follows from Proposition 9.83 that u and v are homotopic. In this case it follows from the definition (and the fact that F is additive) that $F(u)$ and $F(v)$ are homotopic, so they induce the same morphism in cohomology by Remark 9.54). Using this, it is straightforward to see that as defined R^iF is a functor. This also shows that if $A \to I'^{\bullet}$ is another injective resolution, then we have a canonical isomorphism $R^iF(A) \simeq H^i\big(F(I'^{\bullet})\big)$.

We now show that we can put on the sequence $(R^iF)_{i\geq 0}$ the structure of a δ-functor. Suppose that we have an exact sequence

$$0 \to A' \to A \to A'' \to 0$$

and that the chosen injective resolutions are $A' \to I^{\bullet}$, $A \to I^{\bullet}$, and $A'' \to I''^{\bullet}$. It follows from Lemma 9.85 that there is an injective resolution $A \to Q^{\bullet}$ such that we have a commutative diagram of complexes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & I'^{\bullet} & \longrightarrow & Q^{\bullet} & \longrightarrow & I''^{\bullet} & \longrightarrow & 0, \end{array}$$

such that for every i, the sequence

$$0 \to I'^m \to Q^m \to I''^m \to 0$$

is split exact. Since applying F preserves split exact sequences (see Remark 9.64), we obtain a short exact sequence of complexes

$$0 \to F(I'^{\bullet}) \to F(Q^{\bullet}) \to F(I''^{\bullet}) \to 0,$$

and Proposition 9.60 gives a long exact sequence

$$\ldots \longrightarrow R^iF(A') \longrightarrow H^i\big(F(Q^{\bullet})\big) \longrightarrow R^iF(A'') \xrightarrow{\delta} R^{i+1}F(A') \longrightarrow \ldots.$$

Since we have a canonical isomorphism $R^iF(A) \simeq H^i\big(F(Q^{\bullet})\big)$ and since the connecting homomorphisms that we constructed are functorial with respect to morphisms of short exact sequences, we see that $(R^iF)_{i\geq 0}$ form a δ-functor.

The fact that we have a functorial isomorphism $R^0F \simeq F$ follows from definition and the fact that F is a left exact functor. In order to see that if Q is an injective object in $\mathcal{C}$, then $R^iF(Q) = 0$ for $i \geq 1$, we may consider the injective resolution $I^{\bullet}$ of Q such that $Q \to I^0$ is the identity and $I^i = 0$ for $i \geq 1$. In this case, the assertion is clear.

Note now that the uniqueness of the sequence $(R^iF)_{i\geq 0}$ follows if we show that properties i) and ii) imply the last assertion in the theorem. Given an object A in $\mathcal{C}$, choose an exact sequence

$$0 \to A \to I \to B \to 0, \tag{9.7}$$

where I is injective. The long exact sequence for (9.7) gives a commutative diagram

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & F(A) & \longrightarrow & F(I) & \longrightarrow & F(B) & \longrightarrow & R^1F(A) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & & & \\ 0 & \longrightarrow & G^0(A) & \longrightarrow & G^0(I) & \longrightarrow & G^0(B) & \longrightarrow & G^1(A) & & \end{array}$$

and since the top row is exact (we use here that $R^1F(I) = 0$), we obtain an induced morphism $R^1F(A) \to G^1(A)$ that makes the square commutative. It is easy to see, arguing as before, that this is independent of the choice of I and gives a natural transformation of functors.

We construct the natural transformations $R^iF \to G^i$ by induction on $i \geq 1$. We have just treated the case $i = 1$. Suppose now that we have constructed this transformation for some $i \geq 1$. The long exact sequence for (9.7) also gives the horizontal maps in

$$\begin{array}{ccc} R^iF(B) & \longrightarrow & R^{i+1}F(A) \\ \downarrow & & \\ G^i(B) & \longrightarrow & G^{i+1}(A), \end{array}$$

in which the vertical map is given by the inductive assumption. Since the top horizontal map is an isomorphism (we use here the fact that $R^iF(I) = 0 = R^{i+1}F(I)$), it follows that we have a unique map $R^{i+1}F(A) \to G^{i+1}(A)$ that makes the square commutative. It is then not hard to see that the transformations $(R^iF \to G^i)_{i\geq 0}$ constructed in this way give a morphism of δ-functors and that this is the unique such morphism that extends $F \to G^0$. □

Definition 9.89. The functor R^iF in the above theorem is the ith *right derived functor* of F. If $F = \mathrm{Hom}_R(M, -)$, for an R-module M, then we write $\mathrm{Ext}^i_R(M, -)$ for its ith derived functor.

Remark 9.90. Given a morphism of R-modules $u\colon M \to M'$, we get a natural transformation of functors

$$\mathrm{Hom}_R(M', -) \to \mathrm{Hom}_R(M, -)$$

given by precomposing with u. Using the last assertion in Theorem 9.88, we see that we get a unique extension between the corresponding δ-functors given by natural transformations

$$\mathrm{Ext}^i_R(M', -) \to \mathrm{Ext}^i_R(M, -) \quad \text{for} \quad i \geq 0.$$

We proceed similarly to construct the derived functors of $M \otimes_R -$. We only briefly mention how things have to be modified in this case.

Definition 9.91. A *homological δ-functor* is a sequence of functors $(F_i)_{i\geq 0}$ from $\mathcal{C}$ to $\mathcal{D}$, together with the following data: for every short exact sequence in $\mathcal{C}$

$$0 \longrightarrow A' \xrightarrow{u} A \xrightarrow{v} A'' \longrightarrow 0,$$

we have "connecting morphisms" $\delta\colon F_i(A'') \to F_{i-1}(A')$ for $i \geq 1$, such that the complex

$$\ldots \to F_1(A) \xrightarrow{F_1(v)} F_1(A'') \xrightarrow{\delta} F_0(A') \xrightarrow{F_0(u)} F_0(A) \xrightarrow{F_0(v)} F_0(A'') \to 0$$

is exact. Moreover, the connecting morphisms are required to be functorial: given a morphism of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & B' & \longrightarrow & B & \longrightarrow & B'' & \longrightarrow & 0, \end{array}$$

for every $i \geq 1$ we have a commutative diagram

$$\begin{array}{ccc} F_i(A'') & \xrightarrow{\delta} & F_{i-1}(A') \\ \downarrow & & \downarrow \\ F_i(B'') & \xrightarrow{\delta} & F_{i-1}(B'). \end{array}$$

The notion of morphism of homological δ-functors is defined in the obvious way.

THEOREM 9.92. *If $F\colon \mathcal{C} \to \mathcal{D}$ is a right exact functor, then there is a homological δ-functor $(L_iF)_{i\geq 0}$ such that the following two conditions are satisfied:*

i) *We have a natural isomorphism $L_0F \simeq F$, and*
ii) *$L_iF(P) = 0$ for every projective object $P \in \mathcal{C}$ and every $i \geq 1$.*

Such a homological δ-functor is unique up to a unique isomorphism that corresponds to the identity on $L_0F \simeq F$. Moreover, if $(G_i)_{i\geq 0}$ is any homological δ-functor and we have a functorial transformation $G_0 \to F$, then there is a unique extension of this to a morphism of homological δ-functors $(G_i)_{i\geq 0} \to (L_iF)_{i\geq 0}$.

PROOF. The proof is entirely analogous to that of Theorem 9.88, so we only mention how L_iF is defined: for every R-module M, we choose a projective resolution $P_\bullet \to M$, and put $L_iF(M) := H_i\big(F(P_\bullet)\big)$. The proof then proceeds as before. □

DEFINITION 9.93. The functor L_iF in the above theorem is the ith *left derived functor* of F. If $F = M \otimes_R -$, for an R-module M, then we write $\operatorname{Tor}_i^R(M, -)$ for its ith left derived functor.

REMARK 9.94. Given a morphism of R-modules $u\colon M \to M'$, we have a natural transformation of functors

$$M \otimes_R - \to M' \otimes_R -.$$

Using the last assertion in Theorem 9.92, we see that we get a unique extension between the corresponding δ-functors given by natural transformations

$$\operatorname{Tor}_i^R(M, -) \to \operatorname{Tor}_i^R(M', -) \quad \text{for} \quad i \geq 0.$$

The following result shows, in particular, that the R-modules $\operatorname{Ext}_R^i(M, N)$ can also be computed using a projective resolution of M.

PROPOSITION 9.95. Given an R-module M and a projective resolution $P_\bullet \xrightarrow{\epsilon} M$, the sequence of functors

$$\big(H^i(\operatorname{Hom}_R(P_\bullet, -))\big)_{i\geq 0}$$

admits a structure of cohomological δ-functor that is isomorphic to $\big(\operatorname{Ext}_R^i(M, -)\big)_{i\geq 0}$.

PROOF. For every R-module N, the complex $C^\bullet(N) := \operatorname{Hom}_R(P_\bullet, N)$ is given by

$$0 \to \operatorname{Hom}_R(P_0, N) \to \operatorname{Hom}_R(P_1, N) \to \dots.$$

It is clear that we get a functor $\mathcal{M}od(R) \to \operatorname{Com}(\mathcal{M}od(R))$. By taking cohomology, we get a sequence of functors $G^i = H^i\big(C^\bullet(-)\big)$. Note that since $\operatorname{Hom}_R(-, N)$, is left exact, it follows that we have an isomorphism of functors $G^0 \simeq \operatorname{Hom}_R(M, -)$.

Suppose now that we have a short exact sequence

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

Since $\mathrm{Hom}_R(P_i, -)$ is an exact functor for every i, we have a short exact sequence of complexes

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

In this case, it follows from Proposition 9.60 that for every i, we have a morphism $\delta\colon G^i(N'') \to G^{i+1}(N')$ such that we have a long exact sequence

$$0 \to G^0(N') \to G^0(N) \to G^0(N'') \to G^1(N') \to G^1(N) \to \dots.$$

Moreover, it is easy to see that δ is functorial with respect to morphisms of exact sequences. Therefore $(G^i)_{i\geq 0}$ is a cohomological functor.

By the uniqueness assertion in Theorem 9.88, we see that the assertion in the proposition follows if we show that $G^i(N) = 0$ for all $i \geq 1$ if N is injective. This is clear, by definition of projective resolutions, since the functor $\mathrm{Hom}_R(-, N)$ is exact in this case. This completes the proof of the proposition. □

A similar argument shows the commutativity of Tor modules with respect to the two variables.

Proposition 9.96. Given an R-module M and a projective resolution $P_\bullet \xrightarrow{\epsilon} M$, the sequence of functors

$$\big(H^i(P_\bullet \otimes_R -)\big)_{i\geq 0}$$

admits a structure of homological δ-functor that is isomorphic to $\big(\mathrm{Tor}_R^i(M, -)\big)_{i\geq 0}$. In particular, we have functorial isomorphisms (with respect to both variables)

$$\mathrm{Tor}_i^R(M, N) \simeq \mathrm{Tor}_i^R(N, M) \quad \text{for all} \quad i \geq 0.$$

Proof. The argument is similar to the one for Proposition 9.95, so we leave it as an exercise. However, we need the exactness of the functor $P \otimes_R -$ when P is a projective R-module. This is the content of the next lemma. □

Lemma 9.97. *If P is a projective R-module, then the functor $P \otimes_R -$ is exact.*

Proof. Since P is projective, it follows from Proposition 9.72 that there are R-modules Q and F, with F free, such that $P \oplus Q \simeq F$. If $F \simeq R^{(I)}$ for some set I, then for every R-module N we have a functorial isomorphism

$$(P \otimes_R N) \oplus (Q \otimes_R N) \simeq N^{(I)}$$

(this follows from the fact that the tensor product commutes with arbitrary direct sums, see Proposition 9.45). Since it is clear that a direct sum of complexes is exact if and only if each complex is exact, we obtain the exactness of $P \otimes_R -$. □

Finally, we end this chapter with a result that shows that the Ext modules also have a long exact sequence with respect to the first variable.

Proposition 9.98. For every R-module N and every short exact sequence of R-modules

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

there is a long exact sequence

$$0 \to \mathrm{Hom}_R(M'', N) \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M', N) \to \mathrm{Ext}^1_R(M'', N) \to \mathrm{Ext}^1_R(M, N) \to \dots,$$

which is functorial with respect to both N and the short exact sequence.

PROOF. If $N \to I^\bullet$ is an injective resolution, since each $\operatorname{Hom}_R(-, I^p)$ is an exact functor, we get a short exact sequence of complexes

$$0 \to \operatorname{Hom}_R(M'', I^\bullet) \to \operatorname{Hom}_R(M, I^\bullet) \to \operatorname{Hom}_R(M', I^\bullet) \to 0.$$

The assertion in the proposition follows by taking the long exact sequence of cohomology (see Proposition 9.60). Functoriality is straightforward to check. □

EXERCISE 9.99. Let M and N be finitely generated modules over the Noetherian ring R.

i) Show that $\operatorname{Tor}_i^R(M, N)$ is a finitely generated R-module for every $i \geq 0$.
ii) Show that $\operatorname{Ext}^i_R(M, N)$ is a finitely generated R-module for every $i \geq 0$.

We will often use the assertions in the following exercise:

EXERCISE 9.100. Let M and N be R-modules. For a given $a \in R$, let $f_a \colon M \to M$ and $g_a \colon N \to N$ be the maps given by multiplication by a.

i) Show that for every $i \geq 0$, multiplication by a on $\operatorname{Ext}^i_R(M, N)$ is equal to both $\operatorname{Ext}^i_R(f_a, N)$ and $\operatorname{Ext}^i_R(M, g_a)$.
ii) Show that for every $i \geq 0$, multiplication by a on $\operatorname{Tor}_i^R(M, N)$ is equal to both $\operatorname{Tor}_i^R(f_a, N)$ and $\operatorname{Tor}_i^R(M, g_a)$.

In particular, if $aM = 0$ or $aN = 0$, then $a \cdot \operatorname{Ext}^i_R(M, N) = 0$ and $a \cdot \operatorname{Tor}_i^R(M, N) = 0$.

CHAPTER 10

Flatness

Let R be an arbitrary (commutative) ring.

DEFINITION 10.1. An R-module M is *flat* if the functor $M \otimes_R -$ is exact. We say that a ring homomorphism $R \to S$ is flat (or that S is a flat R-algebra) if S is flat as an R-module.

REMARK 10.2. We have seen in Proposition 9.66 that the functor $M \otimes_R -$ is always right exact, hence M is flat if and only if for every injective morphism of R-modules $N \to N'$, the induced morphism

$$M \otimes_R N \to M \otimes_R N'$$

is injective.

EXAMPLE 10.3. Since $R \otimes_R -$ is isomorphic to the identity functor, it is clear that R is a flat R-module. More generally, it follows Lemma 9.97 that every projective R-module is flat. We will see in Proposition 10.11 that the converse holds if R is Noetherian and M is finitely generated.

REMARK 10.4. If R is a domain and M is a flat R-module, then M has no torsion (that is, every nonzero element of R is a non-zero-divisor on M). Indeed, if $a \in R$ is nonzero, then multiplication by $a \in R$, gives an injective map $R \xrightarrow{\cdot a} R$. Tensoring with M gives the map $M \xrightarrow{\cdot a} M$, and this is injective since M is a flat R-module.

EXAMPLE 10.5. If S is a multiplicative system in R, then $S^{-1}R$ is a flat R-module by Example 9.63.

EXAMPLE 10.6. The polynomial R-algebra $R[x_1, \ldots, x_n]$ is flat since $R[x_1, \ldots, x_n]$ is a free R-module.

We begin with some general formal properties of flatness that follow directly from definition.

PROPOSITION 10.7. Let M be an R-module.

i) If M is flat, then for every ring homomorphism $R \to T$, the T-module $M \otimes_R T$ is flat.
ii) If $R_0 \to R$ is a flat ring homomorphism and M is flat as an R-module, then M is flat as an R_0-module.
iii) If $S \subseteq R$ is a multiplicative system and M is an $S^{-1}R$-module, then M is flat as an R-module if and only if it is flat as an $S^{-1}R$-module.
iv) M is a flat R-module if and only if for every maximal (or prime) ideal $\mathfrak{m}$ in R, the $R_{\mathfrak{m}}$-module $M_{\mathfrak{m}}$ is flat.

PROOF. The assertion in i) follows from the fact that for every T-module N, we have canonical isomorphisms

$$(M \otimes_R T) \otimes_T N \simeq M \otimes_R (T \otimes_T N) \simeq M \otimes_R N$$

(the first isomorphism is a version of the associativity property in Exercise 9.40).

Similarly, the assertion in ii) follows from the fact that for every R_0-module N, we have a canonical isomorphism

$$M \otimes_{R_0} N \simeq M \otimes_R (R \otimes_{R_0} N).$$

With the notation in iii), note that if M is a flat $S^{-1}R$-module, since $S^{-1}R$ is a flat R-algebra by Example 10.5, we conclude that M is flat over R by ii). The converse follows from the fact that if N is an $S^{-1}R$-module, then we have canonical isomorphisms

$$M \otimes_{S^{-1}R} N \simeq (M \otimes_R S^{-1}R) \otimes_{S^{-1}R} N \simeq M \otimes_R (S^{-1}R \otimes_R N) \simeq M \otimes_R N$$

(we use here the fact that if Q is an $S^{-1}R$-module, then the canonical morphism of $S^{-1}R$-modules $Q \otimes_R S^{-1}R \to Q$ is an isomorphism).

We now prove iv). If M is a flat R-module, then $M_{\mathfrak{m}} \simeq M \otimes_R R_{\mathfrak{m}}$ is a flat $R_{\mathfrak{m}}$-module by i) for every prime ideal $\mathfrak{m}$ in R. Conversely, suppose that $M_{\mathfrak{m}}$ is a flat $R_{\mathfrak{m}}$-module for all maximal ideals $\mathfrak{m}$ in R. Given an injective map of R-modules $N' \hookrightarrow N$, we see that for every maximal ideal $\mathfrak{m}$, the induced map of $R_{\mathfrak{m}}$-modules $N'_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective, and thus the induced homomorphism

$$(M \otimes_R N')_{\mathfrak{m}} \simeq M_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} N'_{\mathfrak{m}} \to M_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} N_{\mathfrak{m}} \simeq (M \otimes_R N)_{\mathfrak{m}}$$

is injective. This implies the injectivity of

$$M \otimes_R N' \to M \otimes_R N$$

by Exercise 9.58. □

We next give a characterization of flatness in terms of Tor vanishing.

PROPOSITION 10.8. Given an R-module M, the following are equivalent:

i) M is a flat R-module.
ii) We have $\operatorname{Tor}_i^R(M, N) = 0$ for all $i \geq 1$ and all R-modules N.
iii) We have $\operatorname{Tor}_1^R(M, N) = 0$ for all R-modules N.

PROOF. Suppose first that M is flat over R. Given an R-module N, if $F_\bullet$ is a projective resolution of N, then

$$\operatorname{Tor}_i^R(M, N) \simeq H_i(M \otimes_R F_\bullet) = 0 \quad \text{for all} \quad i \geq 1$$

by the flatness of M. We thus have i)⇒ii).

Since ii)⇒iii) is trivial, in order to finish the proof, it is enough to show iii)⇒i). Given a short exact sequence of R-modules,

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

the corresponding long exact sequence for Tor modules gives

$$\ldots \to 0 = \operatorname{Tor}_1^R(M, N'') \to M \otimes_R N' \to M \otimes_R N \to M \otimes_R N'' \to 0.$$

This implies that M is flat over R. □

We use the above characterization of flat modules to prove some basic properties of flat modules.

COROLLARY 10.9. Given a short exact sequence of R-modules

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

the following hold:

i) If M' and M'' are flat, then M is flat.
ii) If M and M'' are flat, then M' is flat.

PROOF. Given an R-module N, it follows from Proposition 9.96 that we have an exact complex

$$\operatorname{Tor}_2^R(M'', N) \to \operatorname{Tor}_1^R(M', N) \to \operatorname{Tor}_1^R(M, N) \to \operatorname{Tor}_1^R(M'', N).$$

The assertions in the proposition now follow from the characterization of flatness in Proposition 10.8. □

COROLLARY 10.10. Given a short exact sequence of R-modules

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

with M'' flat, for every R-module N, the sequence

$$0 \to M' \otimes_R N \to M \otimes_R N \to M'' \otimes_R N \to 0$$

is exact.

PROOF. It follows from it follows from Proposition 9.96 that we have an exact sequence

$$\operatorname{Tor}_1^R(M'', N) \to M' \otimes_R N \to M \otimes_R N \to M'' \otimes_R N \to 0.$$

Since M'' is flat, it follows from Proposition 10.8 that $\operatorname{Tor}_1^R(M'', N) = 0$, and we get the assertion in the corollary. □

PROPOSITION 10.11. If M is a finitely generated module over the Noetherian ring R, then M is flat if and only if it is projective.

PROOF. By Theorem 9.74, we know that M is projective if and only if $M_{\mathfrak{m}}$ is a free $R_{\mathfrak{m}}$-module for every maximal ideal $\mathfrak{m}$ of R. By Proposition 10.7, we know that M is flat if and only if $M_{\mathfrak{m}}$ is a flat $R_{\mathfrak{m}}$-module. Therefore it is enough to show that if $(R, \mathfrak{m})$ is a local Noetherian ring, then M is flat if and only if it is free. By Example 10.3, we only need to prove the "only if" part. The argument is entirely similar to the one in the proof of Theorem 9.74. After choosing a basis of $M/\mathfrak{m}M$ over $R/\mathfrak{m}$, we get a surjective R-map $p\colon F = R^{\oplus n} \to M$. If $K = \ker(p)$, then we have a short exact sequence

$$0 \to K \to F \to M \to 0.$$

Since M is a flat R-module, it follows from Corollary 10.10 that the induced sequence

$$0 \to K/\mathfrak{m}K \to (R/\mathfrak{m})^{\oplus n} \xrightarrow{\overline{p}} M/\mathfrak{m}M \to 0$$

is exact. By construction, $\overline{p}$ is an isomorphism, hence $K = \mathfrak{m}K$, and thus $K = 0$ by Nakayama's lemma. □

Our next goal is to show that flat ring homomorphisms satisfy the *Going-Down* property. We begin with a lemma which is of independent interest: it shows that for flat local homomorphisms of local rings, vanishing or exactness can be checked after applying extension of scalars.

LEMMA 10.12. *If $\varphi\colon (R,\mathfrak{m}) \to (S,\mathfrak{n})$ is a flat local homomorphism of local rings, then the following hold:*

i) *For every R-module M, we have $M = 0$ if and only if $M \otimes_R S = 0$.*
ii) *For every morphism of R-modules $u\colon M \to N$, we have $u = 0$ if and only if $u \otimes_R \mathrm{id}_R = 0$. In particular, φ is injective.*
iii) *Given two maps of R-modules*

$$M' \xrightarrow{u} M \xrightarrow{v} M'',$$

this is an exact sequence if and only if

$$M' \otimes_R S \xrightarrow{u\otimes \mathrm{id}_B} M \otimes_R S \xrightarrow{v\otimes \mathrm{id}_B} M'' \otimes_R S$$

is an exact sequence.

PROOF. In order to prove i), note that if $u \in M$ is nonzero and $I = \mathrm{Ann}_R(u)$, then $I \subseteq \mathfrak{m}$ and $Ru \simeq R/I$. We thus have an inclusion $R/I \hookrightarrow M$ and the flatness assumption implies that the induced morphism $S/IS \simeq R/I \otimes_R S \to M \otimes_R S$ is injective. Since $IS \subseteq \mathfrak{n}$, it follows that S/IS is nonzero, hence $M \otimes_R S$ is nonzero.

If $u\colon M \to N$ is a morphism of A-modules, since M is flat, we have

$$\mathrm{Im}(u \otimes_R S) \simeq \mathrm{Im}(u) \otimes_R S,$$

hence by i), $\mathrm{Im}(u \otimes_R S) = 0$ if and only if $\mathrm{Im}(u) = 0$. We thus obtain the first assertion in ii), and the second one follows by taking u to be the multiplication on R with an element $a \in R$.

The "only if" part in iv) follows directly from flatness. For the "if" part, note first that we get $v \circ u = 0$ by ii). The fact that $\ker(v) = \mathrm{Im}(u)$ follows from i) and the fact that by flatness, we have

$$\ker(v \otimes_R S)/\mathrm{Im}(u \otimes_R S) \simeq \big(\ker(v)/\mathrm{Im}(u)\big) \otimes_R S.$$

□

PROPOSITION 10.13 (Going-Down for flat homomorphisms). If $\varphi\colon R \to S$ is a flat ring homomorphism, then given prime ideals $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ in R and $\mathfrak{q}_2$ in S such that $\varphi^{-1}(\mathfrak{q}_2) = \mathfrak{p}_2$, there is a prime ideal $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ in S such that $\varphi^{-1}(\mathfrak{q}_1) = \mathfrak{p}_1$.

PROOF. Note that the induced local ring homomorphism $\psi\colon R_{\mathfrak{p}_2} \to S_{\mathfrak{q}_2}$ is flat. Indeed, this can be written as a composition

$$R_{\mathfrak{p}_2} \to S_{\mathfrak{p}_2} \to S_{\mathfrak{q}_2}.$$

The first homomorphism is flat since φ is flat, see Proposition 10.7i), and the second one is flat by Example 10.5. Therefore the composition is flat by Proposition 10.7ii).

It is enough to show that there is a prime ideal $\mathfrak{q}_1'$ in $S_{\mathfrak{q}_2}$ such that $\psi^{-1}(\mathfrak{q}_1') = \mathfrak{p}_1 R_{\mathfrak{p}_2}$. Indeed, in this case we have $\mathfrak{q}_1' = \mathfrak{q}_1 S_{\mathfrak{q}_2}$, for some prime ideal $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ and by taking the inverse image in R we see that $\varphi^{-1}(\mathfrak{q}_1) = \mathfrak{p}_1$. After replacing φ by ψ, we may thus assume that $(R,\mathfrak{p}_2)$ and $(S,\mathfrak{q}_2)$ are local rings and φ is a local homomorphism. In this case every prime ideal in S is contained in $\mathfrak{q}_2$. Since the prime ideals in S lying over $\mathfrak{p}_1$ are in bijection with the prime ideals in $S_{\mathfrak{p}_1}/\mathfrak{p}_1 S_{\mathfrak{p}_1} \simeq (R_{\mathfrak{p}_1}/\mathfrak{p}_1 R_{\mathfrak{p}_1}) \otimes_R S$, it is enough to show that this ring is not the zero ring. This is a consequence of Lemma 10.12i). □

PROPOSITION 10.14. If $\varphi\colon R \to S$ is a ring homomorphism that satisfies the Going-Down property in the previous proposition, then for every prime ideal $\mathfrak{q}$, if we put $\mathfrak{p} = \phi^{-1}(\mathfrak{q})$, then

$$\dim(S_\mathfrak{q}/\mathfrak{p}S_\mathfrak{q}) \leq \dim(S_\mathfrak{q}) - \dim(R_\mathfrak{p}).$$

PROOF. Let $r = \dim(S_\mathfrak{q}/\mathfrak{p}S_\mathfrak{q})$ and $s = \dim(R_\mathfrak{p})$. We can choose prime ideals $\mathfrak{p}_s \subsetneq \ldots \subsetneq \mathfrak{p}_0 = \mathfrak{p}$ in R and $\mathfrak{q}_r \subsetneq \ldots \subsetneq \mathfrak{q}_0 = \mathfrak{q}$ in S, with $\mathfrak{p}S \subseteq \mathfrak{q}_r$. Applying the Going-Down property successively, we obtain a sequence of prime ideals $\mathfrak{p}'_s \subseteq \ldots \subseteq \mathfrak{p}'_0 \subseteq \mathfrak{q}_r$ such that $\varphi^{-1}(\mathfrak{p}'_i) = \mathfrak{p}_i$ for $0 \leq i \leq s$. In particular, we have $\mathfrak{p}'_i \neq \mathfrak{p}'_{i+1}$ for $0 \leq i \leq s-1$ (however, we might have $\mathfrak{p}'_0 = \mathfrak{q}_s$). From the sequence of prime ideals in S

$$\mathfrak{p}'_s \subsetneq \ldots \subsetneq \mathfrak{p}'_1 \subsetneq \mathfrak{q}_r \subsetneq \ldots \subsetneq \mathfrak{q}_0 = \mathfrak{q},$$

we conclude that $\dim(S_\mathfrak{q}) \geq r + s$. □

The concept of flatness is particularly useful for ring homomorphisms $R \to S$, as it implies a certain uniform behavior of the fibers. The following result is an instance of this phenomenon.

COROLLARY 10.15. If $\varphi\colon R \to S$ is a flat homomorphism of Noetherian rings, then for every prime ideal $\mathfrak{q}$ in S, if we put $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$, then

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

PROOF. The inequality "$\geq$" follows from Propositions 10.13 and 10.14, while the opposite inequality follows from Theorem 7.58. □

EXERCISE 10.16. Let $(I, \leq)$ be a filtered ordered set (*filtered* means that for every $i, j \in I$, there is $k \in I$ such that $i \leq k$ and $j \leq k$). Given a ring R and a direct system (N_i, f_{ij}) of R-modules over R, show that for every R-module M and every $n \in \mathbf{Z}_{\geq 0}$, we have a functorial isomorphism

$$\varinjlim \operatorname{Tor}_n^R(M, N_i) \simeq \operatorname{Tor}_n^R(M, \varinjlim N_i).$$

EXERCISE 10.17. Let M be an R-module. Show that the following are equivalent:

i) M is a flat module.
ii) For every ideal I in R, we have $\operatorname{Tor}_1^R(M, R/I) = 0$.
iii) For every ideal I in R, the canonical morphism $I \otimes_R M \to M$ is injective.
ib) For every finitely generated ideal I in R, the canonical morphism $I \otimes_R M \to M$ is injective.

EXERCISE 10.18. Show that if R is a Dedekind ring and M is an R-module, then M is flat if and only if it has no torsion.

EXERCISE 10.19. Show that the following ring homomorphisms are not flat:

i) The inclusion $k[t^2, t^3] \hookrightarrow k[t]$.
ii) $f\colon k[x, y] \to k[x, y]$ given by $f(x) = x$ and $f(y) = xy$.
iii) The canonical surjection $R \to R/I$, where R is a local Noetherian ring and I is a nonzero ideal.

CHAPTER 11

Depth and Cohen-Macaulay rings and modules

In the first section we introduce the notion of regular sequences and depth of a module. After dimension, the depth is the most important numerical invariant of a module. In the second section we give an introduction to Cohen-Macaulay rings and modules, key concepts in commutative algebra. Finally, in the last section we discuss the Koszul complex and its connection with regular sequences and depth.

11.1. Regular sequences and depth

The following is a key notion for this chapter.

DEFINITION 11.1. Given a module M over the ring R, a sequence of elements $x_1, \dots, x_n \in R$ is an *M-regular sequence* (or a *regular sequence for M*) if the following conditions hold:

i) We have $(x_1, \dots, x_n)M \neq M$.
ii) For every i with $1 \leq i \leq n$, the element x_i is a non-zero-divisor on the R-module $M/(x_1, \dots, x_{i-1})M$.

If $M = R$, we simply say that $x_1, \dots, x_n$ form a *regular sequence*.

REMARK 11.2. If $x_1, \dots, x_n$ is an M-regular sequence and S is a multiplicative system in R such that $S^{-1}M/(x_1, \dots, x_n)S^{-1}M \neq 0$, then it is easy to see that $\frac{x_1}{1}, \dots, \frac{x_n}{1} \in S^{-1}R$ is an $S^{-1}M$-regular sequence (this follows from the fact that a non-zero-divisor on a module is also a non-zero-divisor on any localization of that module). As we will see later, regular sequences tend to behave better when we work in a local ring.

REMARK 11.3. The order of the elements in a regular sequence is important: for example, if $R = k[x, y, z]/\big((x-1)z\big)$, then $x, (x-1)y$ is a regular sequence, but $(x-1)y, x$ is not a regular sequence: for the first assertion, note that R is reduced, with minimal prime ideals $(x-1)$ and (z) and x is not in any of these, hence it is a non-zero-divisor. Furthermore, $R/(x) \simeq k[y, z]/(z) \simeq k[y]$ and the image of $(x-1)y$ corresponds to $y \in k[y]$, hence it is a non-zero-divisor. Note also that $R/\big(x, (x-1)y\big) \neq 0$, and thus $x, (x-1)y$ is a regular sequence. On the other hand, $(x-1)y, x$ is not a regular sequence since $(x-1)y$ is a zero divisor: we have $(x-1)yz = 0$, but $z \neq 0$ in R.

We now show that this issue does not arise if R is a local ring.

PROPOSITION 11.4. Let M be a finitely generated module over a local Noetherian ring $(R, \mathfrak{m})$. If $x_1, \dots, x_n$ is an M-regular sequence, then any permutation of this is a regular sequence.

PROOF. Since every permutation is a composition of transpositions of the form $(i, i+1)$, it is clear that it is enough to show that for every such module M,

if x, y is an M-regular sequence, then also y, x is an M-regular sequence. Since $(x, y)M \neq M$, we have $x, y \in \mathfrak{m}$.

The key point is showing that y is a non-zero-divisor on M. Suppose that $u \in M$ is such that $yu = 0$, but $u \neq 0$. By Krull's Intersection Theorem, there is $k \geq 0$ such that $u \in x^k M \smallsetminus x^{k+1}M$. If we write $u = x^k v$, since $yu = 0$ and x is a non-zero-divisor on M, it follows that $yv = 0$. Since y is a non-zero-divisor on M/xM, it follows that $v \in xM$, hence $u \in x^{k+1}M$, a contradiction.

Finally, we need to show that x is a non-zero-divisor on M/yM. This, in fact, does not need the fact that R is local: if $w_1 \in M$ is such that $x\overline{w_1} = 0$ in M/yM, then there is $w_2 \in M$ such that $xw_1 = yw_2$. Since y is a non-zero-divisor on M/xM, it follows that there is $w_3 \in M$ such that $w_2 = xw_3$, hence $x(w_1 - yw_3) = 0$. Since x is a non-zero-divisor on M, we conclude that $w_1 = yw_3$, hence $\overline{w_1} = 0$ in M/yM. This completes the proof. □

Remark 11.5. Suppose that M is a finitely generated module over a Noetherian ring R. If $x_1, \ldots, x_n$ is an M-regular sequence, then

$$(x_1)M \subsetneq (x_1, x_2)M \subsetneq \ldots \subsetneq (x_1, \ldots, x_n)M.$$

Indeed, if $1 \leq i \leq n$ is such that $x_i M \subseteq (x_1, \ldots, x_{i-1})M$, since x_i is a non-zero-divisor on $M/(x_1, \ldots, x_{i-1})M$, it follows that $(x_1, \ldots, x_{i-1})M = M$ contradicting condition i) in the definition of an M-regular sequence.

Since M is a Noetherian module, it follows that given any ideal I in M, every M-regular sequence of elements in I can be completed to a *maximal* such sequence. We note that if $IM \neq M$, an M-regular sequence $x_1, \ldots, x_n$ of elements in I is maximal among such sequences if and only if I is contained in the set of zero-divisors of $M/(x_1, \ldots, x_n)M$. By Remark 5.9, this is the case if and only if there is $u \in M \smallsetminus (x_1, \ldots, x_n)M$ such that $I \cdot u \subseteq (x_1, \ldots, x_n)M$.

Finally, we note that the condition $IM \neq M$ is satisfied in two important special cases: when $M = R$ and $I \neq R$ and when $(R, \mathfrak{m})$ is local, $I \subseteq \mathfrak{m}$, and $M \neq 0$.

Definition 11.6. Let M be a finitely generated module over a Noetherian ring R. If I is an ideal in R, we put

$$\operatorname{depth}(I, M) := \min\{i \geq 0 \mid \operatorname{Ext}^i_R(R/I, M) \neq 0\}.$$

Note that if the set on the right-hand side is empty, then we follow the convention that $\operatorname{depth}(I, M) = \infty$. If R is a local ring and $\mathfrak{m}$ is the maximal ideal, then we write $\operatorname{depth}(M)$ for $\operatorname{depth}(\mathfrak{m}, M)$ (we also write $\operatorname{depth}_R(M)$ if the ring is not clear from the context).

The following result makes the connection with regular sequences and motivates the above definition.

Theorem 11.7. *Let R be a Noetherian ring, M a finitely generated R-module, and I an ideal in R.*

i) *If $IM = M$, then $\operatorname{depth}(I, M) = \infty$.*
ii) *If $IM \neq M$, then $\operatorname{depth}(I, M)$ is equal to the length of every maximal M-regular sequence of elements of I.*

We first give a lemma concerning the behavior of Ext modules under localization.

LEMMA 11.8. *If R is a Noetherian ring and M and N are R-modules, with M finitely generated, then for every multiplicative system S in R, we have functorial isomorphisms*

$$S^{-1}\mathrm{Ext}^i_R(M,N) \simeq \mathrm{Ext}^i_{S^{-1}R}(S^{-1}M, S^{-1}N).$$

PROOF. Since M is a finitely generated module over a Noetherian ring, we can choose a projective resolution $F_\bullet \to M$ such that all F_i are finitely generated free R-modules. Note that in this case $S^{-1}F_\bullet \to S^{-1}M$ is a free resolution of the $S^{-1}R$-module $S^{-1}M$. The assertion in the lemma thus follows from the functorial isomorphisms

$$S^{-1}\mathrm{Ext}^i_R(M,N) \simeq S^{-1}H^i\big(\mathrm{Hom}_R(F_\bullet, N)\big) \simeq H^i\big(S^{-1}\mathrm{Hom}_R(F_\bullet, N)\big)$$

$$\simeq H^i\big(\mathrm{Hom}_{S^{-1}R}(S^{-1}F_\bullet, S^{-1}N)\big) \simeq \mathrm{Ext}^i_{S^{-1}R}(S^{-1}M, S^{-1}N).$$

Here the first and the last isomorphisms follow from Proposition 9.95, the second one follows from the exactness of the localization functor, and the third one follows from the fact that every F_i is isomorphic to some $R^{\oplus n_i}$ (see the proof of Lemma 9.77). □

PROOF OF THEOREM 11.7. Suppose first that $IM = M$. In order to show that $\mathrm{depth}(I,M) = \infty$ it is enough to show that for every prime ideal $\mathfrak{p}$ in R, we have $\mathrm{Ext}^i_R(R/I, M)_\mathfrak{p} = 0$ for all $i \geq 0$. Note that by Lemma 11.8, we have

$$\mathrm{Ext}^i_R(R/I, M)_\mathfrak{p} \simeq \mathrm{Ext}^i_{R_\mathfrak{p}}(R_\mathfrak{p}/IR_\mathfrak{p}, M_\mathfrak{p}).$$

If $I \subseteq \mathfrak{p}$, then the hypothesis together with Nakayama's lemma implies $M_\mathfrak{p} = 0$, hence $\mathrm{Ext}^i_{R_\mathfrak{p}}(R_\mathfrak{p}/IR_\mathfrak{p}, M_\mathfrak{p}) = 0$. On the other hand, if $I \not\subseteq \mathfrak{p}$, then $R_\mathfrak{p} = IR_\mathfrak{p}$, and again we have $\mathrm{Ext}^i_{R_\mathfrak{p}}(R_\mathfrak{p}/IR_\mathfrak{p}, M_\mathfrak{p}) = 0$. This completes the proof of i).

Suppose now that $IM \neq M$ and let $x_1, \ldots, x_n$ be a maximal M-regular sequence in I. We show that $\mathrm{depth}(I,M) = n$ arguing by induction on n. If $n = 0$, then there is no non-zero-divisor on M in I (we use here that $IM \neq M$). It follows that we have $u \in M \smallsetminus \{0\}$ such that $I \cdot u = 0$, and thus a non-zero morphism $R/I \to M$ that maps the image of 1 to u. This shows that $\mathrm{Hom}(R/I, M) \neq 0$, hence $\mathrm{depth}(I,M) = 0$.

Suppose now that we know the assertion when we have a maximal M-regular sequence of length $n-1$. Since x_1 is a non-zero-divisor on M, we have a short exact sequence

$$0 \to M \xrightarrow{\cdot x_1} M \to M/x_1M \to 0.$$

Note that multiplication by x_1 on each $\mathrm{Ext}^i_R(R/I, M)$ is 0 since $x_1 \in I$. The long exact sequence for Ext modules thus breaks into short exact sequences

$$0 \to \mathrm{Ext}^i_R(R/I, M) \to \mathrm{Ext}^i_R(R/I, M/x_1M) \to \mathrm{Ext}^{i+1}_R(R/I, M) \to 0.$$

This immediately implies that $\mathrm{depth}(I, M/x_1M) = \mathrm{depth}(I,M) - 1$. On the other hand, it is clear that $x_2, \ldots, x_n$ is a maximal M/x_1M-regular sequence in I. Since $I \cdot (M/x_1M) \neq M/x_1M$, we conclude using the induction hypothesis that $n - 1 = \mathrm{depth}(I,M) - 1$. This completes the proof of the induction step and thus the proof of the theorem. □

REMARK 11.9. It follows from the above proof that if $J = \mathrm{rad}(I)$, then

$$\mathrm{depth}(J,M) = \mathrm{depth}(I,M).$$

Note first that we have $IM = M$ if and only if $JM = M$. If this is not the case, then it is enough to show that $\operatorname{depth}(J, M)$ is equal to the length of any maximal M-regular sequence contained in I. The above proof carries through with one modification: we need to note that if there is a non-zero $u \in M$ such that $I \cdot u = 0$, then there is also a non-zero $v \in M$ with $J \cdot v = 0$ (indeed, if $J^m \subseteq I$, then there is $i \leq m-1$ such that $J^i u \neq 0$ and $J^{i+1}u = 0$, and we can take v to be a nonzero element in $J^i u$). Therefore we have $\operatorname{Hom}_R(R/J, M) \neq 0$.

REMARK 11.10. It follows from the theorem that if $\mathfrak{a}$ is an ideal in R such that $\mathfrak{a} \cdot M = 0$, then $\operatorname{depth}(I, M) = \operatorname{depth}\big((I+\mathfrak{a})/\mathfrak{a}, M\big)$, where in the second depth, we consider M as an $R/\mathfrak{a}$-module.

COROLLARY 11.11. If R, M, and I are as in the theorem, and $x_1, \ldots, x_r \in I$ is an M-regular sequence, then

$$\operatorname{depth}\big(I, M/(x_1, \ldots, x_r)M\big) = \operatorname{depth}(I, M) - r. \tag{11.1}$$

PROOF. Note first that $I \cdot M/(x_1, \ldots, x_r)M = M/(x_1, \ldots, x_r)M$ if and only if $IM = M$. We may assume that this is not the case. We have already shown the equality in the statement, in the case $r = 1$, in the proof of Theorem 11.7. The general case follows by induction on r. □

COROLLARY 11.12. If R, M, and I are as in the theorem and J is an ideal containing I, then

$$\operatorname{depth}(I, M) \leq \operatorname{depth}(J, M).$$

PROOF. The follows immediately from the description via regular sequences in the theorem. □

COROLLARY 11.13. If R, M, and I are as in the theorem, then

$$\operatorname{depth}(I, M) = \min\{\operatorname{depth}(M_{\mathfrak{p}}) \mid \mathfrak{p} \supseteq I\},$$

where the minimum is over the prime ideals $\mathfrak{p}$ containing I. In particular, if $\mathfrak{m}$ is a maximal ideal in R, then $\operatorname{depth}(\mathfrak{m}, M) = \operatorname{depth}(M_{\mathfrak{m}})$.

PROOF. For every prime ideal $\mathfrak{p}$ and every i, we have

$$\operatorname{Ext}^i_R(R/I, M)_{\mathfrak{p}} \simeq \operatorname{Ext}^i_{R_{\mathfrak{p}}}(R_{\mathfrak{p}}/IR_{\mathfrak{p}}, M_{\mathfrak{p}})$$

by Lemma 11.8. We thus obtain

$$\operatorname{depth}(I, M) \leq \operatorname{depth}(IR_{\mathfrak{p}}, M_{\mathfrak{p}}) \leq \operatorname{depth}(M_{\mathfrak{p}}),$$

where the second inequality follows from Corollary 11.12.

If $IM = M$, then we are done. Suppose now that $IM \neq M$ and let $x_1, \ldots, x_n$ be a maximal M-regular sequence contained in I. Since every element of I is a zero-divisor on $M/(x_1, \ldots, x_n)M$, it follows that there is $\mathfrak{p} \in \operatorname{Ass}_R\big(M/(x_1, \ldots, x_n)M\big)$ such that $I \subseteq \mathfrak{p}$ (see Remark 5.9). Since $\mathfrak{p}R_{\mathfrak{p}} \in \operatorname{Ass}_{R_{\mathfrak{p}}}\big(M_{\mathfrak{p}}/(x_1, \ldots, x_n)M_{\mathfrak{p}}\big)$, it follows that $\frac{x_1}{1}, \ldots, \frac{x_n}{1}$ is a maximal $M_{\mathfrak{p}}$-regular sequence in $\mathfrak{p}R_{\mathfrak{p}}$, and thus

$$\operatorname{depth}(I, M) = \operatorname{depth}(M_{\mathfrak{p}}).$$

□

PROPOSITION 11.14. Given a short exact sequence

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

of finitely generated modules over the Noetherian ring R, the following hold:

i) $\operatorname{depth}(I, M) \geq \min\{\operatorname{depth}(I, M'), \operatorname{depth}(I, M'')\}$.
ii) $\operatorname{depth}(I, M') \geq \min\{\operatorname{depth}(I, M), \operatorname{depth}(I, M'') + 1\}$.
iii) $\operatorname{depth}(I, M'') \geq \min\{\operatorname{depth}(I, M), \operatorname{depth}(I, M') - 1\}$.

PROOF. All assertions follows directly from definition and the long exact sequence for the Ext modules:

$$\ldots \to \operatorname{Ext}_R^{i-1}(R/I, M'') \to \operatorname{Ext}_R^i(R/I, M') \to \operatorname{Ext}_R^i(R/I, M)$$
$$\to \operatorname{Ext}_R^i(R/I, M'') \to \operatorname{Ext}_R^{i+1}(R/I, M') \to \ldots.$$

□

PROPOSITION 11.15. If M is a finitely generated module over a Noetherian local ring $(R, \mathfrak{m})$, then for every $\mathfrak{p} \in \operatorname{Ass}_R(M)$, we have

$$\operatorname{depth}(M) \leq \dim(R/\mathfrak{p}).$$

In particular, if $M \neq 0$, then $\operatorname{depth}(M) \leq \dim(M)$.

PROOF. Let $\mathfrak{p} \in \operatorname{Ass}_R(M)$. In particular, we see that $M \neq 0$, and thus $\mathfrak{m}M \neq M$ by Nakayama's lemma. We argue by induction on $n = \operatorname{depth}(M)$. If $n = 0$, then there is nothing to prove. Otherwise, let $x \in \mathfrak{m}$ be a non-zero-divisor on M. By Corollary 11.11, we have $\operatorname{depth}(M/xM) = n - 1$. On the other hand, by hypothesis, there is $u \in M$ such that $\mathfrak{p} = \operatorname{Ann}_R(u)$. By Krull's Intersection theorem (see Theorem 4.22), we have $\bigcap_{j\geq 0} x^j M = 0$, hence there is $\ell \geq 0$ such that $u = x^\ell v$ and $v \notin xM$. Since x is a non-zero-divisor on M, it follows that $\mathfrak{p} = \operatorname{Ann}_R(v)$ and thus $\mathfrak{p}$ annihilates the non-zero element $\overline{v} \in M/xM$. It follows from Remark 5.9 that there is $\mathfrak{q} \in \operatorname{Ass}_R(M/xM)$ such that $\mathfrak{p} \subseteq \mathfrak{q}$. Note that $x \in \operatorname{Ann}_R(M/xM) \subseteq \mathfrak{q}$, while $x \notin \mathfrak{p}$, since x is a non-zero-divisor on M. We thus have $\dim(R/\mathfrak{p}) \geq \dim(R/\mathfrak{q}) + 1$ and we conclude using the induction hypothesis.

The last assertion in the proposition follows from the fact that if $M \neq 0$, then $\dim(M)$ is the maximum of all $\dim(R/\mathfrak{p})$, where $\mathfrak{p}$ runs over the minimal primes in $V\big(\operatorname{Ann}_R(M)\big)$, which lie in $\operatorname{Ass}_R(M)$ by Proposition 5.16. □

REMARK 11.16. A related inequality says that if $\mathfrak{a} \subsetneq R$ is an ideal in a Noetherian ring R, then

$$\operatorname{depth}(\mathfrak{a}, R) \leq \operatorname{codim}(\mathfrak{a}).$$

Indeed, suppose that $\mathfrak{p} \supseteq \mathfrak{a}$ is a prime ideal such that $\operatorname{codim}(\mathfrak{p}) = \operatorname{codim}(\mathfrak{a})$. In this case we have

$$\operatorname{depth}(\mathfrak{a}, R) \leq \operatorname{depth}(\mathfrak{a}R_\mathfrak{p}, R_\mathfrak{p}) \leq \operatorname{depth}(R_\mathfrak{p}) \leq \dim(R_\mathfrak{p}) = \operatorname{codim}(\mathfrak{p}) = \operatorname{codim}(\mathfrak{a}),$$

where the first inequality follows from Remark 11.2, the second one from Corollary 11.12, and the third one from Proposition 11.15. This gives our assertion.

REMARK 11.17. It follows from the previous remark that if $x_1, \ldots, x_n$ is a regular sequence in a Noetherian ring R and $\mathfrak{a} = (x_1, \ldots, x_n)$, then $n \leq \operatorname{depth}(\mathfrak{a}, R) \leq \operatorname{codim}(\mathfrak{a})$. On the other hand, it follows from the general form of the Principal Ideal theorem (see Corollary 7.35) that every minimal prime ideal containing $\mathfrak{a}$ has codimension $\leq n$. We deduce that

$$\operatorname{codim}(\mathfrak{a}) = \operatorname{depth}(\mathfrak{a}, R) = n;$$

moreover, every minimal prime ideal containing $\mathfrak{a}$ has codimension n.

EXAMPLE 11.18. If A is a (nonzero) Noetherian ring, $R = A[x_1, \dots, x_n]$, and $I = (x_1, \dots, x_n)$, then $\operatorname{depth}(I, R) = n$. Indeed, $x_1, \dots, x_n$ is a regular sequence: for every i, with $1 \leq i \leq n$, x_i is a non-zero-divisor in $R/(x_1, \dots, x_{i-1}) \simeq A[x_i, \dots, x_n]$. It is also clear that this is a maximal regular sequence in I, since $I = (x_1, \dots, x_n)$.

EXAMPLE 11.19. Let k be a field, $R = k[x_1, \dots, x_n]/(x_1^2, x_1x_2, \dots, x_1x_n)$, and $I = (\overline{x_1}, \dots, \overline{x_n}) \subseteq R$. Note that $R_{\text{red}} = R/(\overline{x_1}) \simeq k[x_2, \dots, x_n]$, hence $\dim(R) = \dim(R_{\text{red}}) = n-1$. On the other hand, $I \cdot \overline{x_1} = 0$ and $\overline{x_1} \neq 0$, hence $\operatorname{depth}(I, R) = 0$.

EXAMPLE 11.20. Let k be a field, $R = k[x_1, \dots, x_n]/(x_1^2 + \dots + x_n^2)$, and $I = (\overline{x_1}, \dots, \overline{x_n})$. Note that $\overline{x_1}, \dots, \overline{x_{n-1}}$ form a regular sequence: this is due to the fact that

$$R/(\overline{x_1}, \dots, \overline{x_{i-1}}) \simeq k[x_i, \dots, x_n]/(x_i^2 + \dots + x_n^2)$$

and x_i is a non-zero-divisor on $k[x_i, \dots, x_n]/(x_i^2 + \dots + x_n^2)$ for $i \leq n-1$. In fact, it is a maximal regular sequence, since $I \cdot \overline{x_n} \subseteq (\overline{x_1}, \dots, \overline{x_{n-1}})$, while $\overline{x_n} \notin (\overline{x_1}, \dots, \overline{x_{n-1}})$. Therefore $\operatorname{depth}(I, R) = n - 1$.

EXERCISE 11.21. Let $(R, \mathfrak{m})$ be a Noetherian local ring and M a finitely generated R-module. Show that if $x_1, \dots, x_n$ is an M-regular sequence, then for every positive integers $a_1, \dots, a_n$, the sequence $x_1^{a_1}, \dots, x_n^{a_n}$ is M-regular.

EXERCISE 11.22. Let $f\colon (R, \mathfrak{m}) \to (S, \mathfrak{n})$ be a local homomorphism of Noetherian local rings and let M be a finitely generated S-module that is also finitely generated as an R module. Show that if $\mathfrak{m}S$ is $\mathfrak{n}$-primary, then

$$\operatorname{depth}_R(M) = \operatorname{depth}_S(M).$$

EXERCISE 11.23. Let R be a Noetherian ring, I and ideal in R, and M a finitely generated R-module. Recall that we have defined $\operatorname{depth}(I, M)$ as $\min\{i \mid \operatorname{Ext}^i_R(R/I, M) \neq 0\}$. Show that, more generally, if N is any finitely generated R-module with $\operatorname{Supp}(N) = V(I)$, then

$$\operatorname{depth}(I, M) = \min\{i \mid \operatorname{Ext}^i_R(N, M) \neq 0\}.$$

11.2. The Cohen-Macaulay condition

Using the notion of depth, we introduce Cohen-Macaulay rings and modules, give some examples, and discuss some basic properties.

DEFINITION 11.24. If R is a Noetherian local ring and M is a finitely generated, nonzero R-module, then M is a *Cohen-Macaulay module* if $\operatorname{depth}(M) = \dim(M)$. If R is an arbitrary Noetherian ring and M is a finitely generated R-module then M is a *Cohen-Macaulay module* if $M_{\mathfrak{p}}$ is a Cohen-Macaulay $R_{\mathfrak{p}}$-module for all maximal ideals $\mathfrak{p} \in \operatorname{Supp}(M)$ (thus, by convention, $M = 0$ is considered Cohen-Macaulay). If $M = R$, we say instead that R is a *Cohen-Macaulay* ring.

REMARK 11.25. It follows from Remark 11.10 that if M is a finitely generated module over a Noetherian ring R and $\mathfrak{a}$ is an ideal in R such that $\mathfrak{a} \cdot M = 0$, then M is a Cohen-Macaulay module over R if and only if it is a Cohen-Macaulay module over $R/\mathfrak{a}$.

In what follows we give some general properties of Cohen-Macaulay rings and modules.

PROPOSITION 11.26. Let M be a finitely generated module over a Noetherian ring R and $x_1, \ldots, x_n$ is an M-regular sequence. If M is Cohen-Macaulay, then $M/(x_1, \ldots, x_n)M$ is Cohen-Macaulay, and the converse holds if R is a local ring.

PROOF. Suppose first that R is a local ring. Arguing by induction on n, it is clear that it is enough to treat the case $n = 1$. In this case, since x_1 is a non-zero-divisor on M, it follows from Exercise 7.47 that

$$\dim(M/x_1M) = \dim(M) - 1,$$

while Corollary 11.11 gives

$$\operatorname{depth}(M/x_1M) = \operatorname{depth}(M) - 1.$$

The assertion in the proposition now follows from the definition.

Suppose now that M is Cohen-Macaulay, but R is not necessarily local. In order to deduce that $M/(x_1, \ldots, x_n)M$ is Cohen-Macaulay, it is enough to apply what we have already proved after localization at any maximal ideal in the support of $M/(x_1, \ldots, x_n)M$. □

The following result gives a very useful property of Cohen-Macaulay modules.

PROPOSITION 11.27. If M is a Cohen-Macaulay module over the Noetherian ring R, then every associated prime of M is minimal in $\operatorname{Supp}(M)$. Moreover, if R is local, then for every minimal prime $\mathfrak{p}$ in $\operatorname{Supp}(M)$, we have $\dim(R/\mathfrak{p}) = \dim(M)$.

PROOF. If $\mathfrak{p} \in \operatorname{Ass}_R(M)$, then after localizing at some maximal ideal containing $\mathfrak{p}$, we reduce to the case when R is a local ring. Since every associated prime of M contains a minimal prime in $\operatorname{Supp}(M)$, both assertions in the proposition follow if we show that for every associated prime $\mathfrak{p}$ of M, we have $\dim(R/\mathfrak{p}) = \dim(M)$.

Note that by Proposition 11.15, we have

$$\operatorname{depth}(M) \leq \dim(R/\mathfrak{p}) \leq \dim(M).$$

Since M is a Cohen-Macaulay module, it follows that the above inequalities are equalities. □

PROPOSITION 11.28. If M is a Cohen-Macaulay module over the Noetherian ring R, then for every prime ideal $\mathfrak{p}$ in R, the $R_{\mathfrak{p}}$-module $M_{\mathfrak{p}}$ is Cohen-Macaulay.

PROOF. We may and will assume that $\mathfrak{p} \in \operatorname{Supp}(M)$, since otherwise the assertion is trivial. Let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{p}$. After replacing R and M by $R_{\mathfrak{m}}$ and $M_{\mathfrak{m}}$, respectively, we may and will assume that R is a local ring. We need to show that $\operatorname{depth}(M_{\mathfrak{p}}) = \dim(M_{\mathfrak{p}})$. For this, we argue by induction on $r = \operatorname{depth}(M_{\mathfrak{p}})$. If $r = 0$, then $\mathfrak{p} \in \operatorname{Ass}_R(M)$. Since M is Cohen-Macaulay, it follows from Proposition 11.27 that $\mathfrak{p}$ is a minimal prime in $\operatorname{Supp}(M)$, and thus $\dim(M_{\mathfrak{p}}) = 0$.

Suppose now that $r \geq 1$. In this case $\mathfrak{p} \notin \operatorname{Ass}_R(M)$, and since all primes in $\operatorname{Ass}_R(M)$ are minimal in $\operatorname{Supp}(M)$ by Proposition 11.27, it follows that is $h \in \mathfrak{p}$ which is a non-zero-divisor on M. We then have $\operatorname{depth}(M_{\mathfrak{p}}/hM_{\mathfrak{p}}) = r - 1$ by Corollary 11.11. Since M/hM is a Cohen-Macaulay R-module by Proposition 11.26, we can apply the inductive hypothesis to conclude that $r - 1 = \dim(M_{\mathfrak{p}}/hM_{\mathfrak{p}})$. Since h is a non-zero-divisor on M, its image in $R_{\mathfrak{p}}$ is also a non-zero-divisor on $M_{\mathfrak{p}}$, hence Exercise 7.47 gives

$$\dim(M_{\mathfrak{p}}) = \dim(M_{\mathfrak{p}}/hM_{\mathfrak{p}}) + 1 = r.$$

This completes the proof of the induction step. □

COROLLARY 11.29. If M is a Cohen-Macaulay over the ring R and $S \subseteq R$ is a multiplicative system, then $S^{-1}M$ is a Cohen-Macaulay $S^{-1}R$-module.

PROOF. Any maximal ideal of $S^{-1}R$ is of the form $S^{-1}\mathfrak{p}$, for some prime ideal $\mathfrak{p}$ in R with $S \cap \mathfrak{p} = \emptyset$ and $(S^{-1}M)_{S^{-1}\mathfrak{p}} = M_{\mathfrak{p}}$ is Cohen-Macaulay by the proposition. □

PROPOSITION 11.30. A Noetherian ring R is Cohen-Macaulay if and only if for every ideal $\mathfrak{a} \subsetneq R$, we have

$$\operatorname{depth}(\mathfrak{a}, R) = \operatorname{codim}(\mathfrak{a}).$$

PROOF. Note that by Proposition 11.13, we have

$$\operatorname{depth}(\mathfrak{a}, R) = \min_{\mathfrak{p}} \operatorname{depth}(R_{\mathfrak{p}}),$$

where the minimum is over all prime ideals $\mathfrak{p}$ containing $\mathfrak{a}$. If R is Cohen-Macaulay, then every such $R_{\mathfrak{p}}$ is a Cohen-Macaulay ring by Proposition 11.28, hence

$$\min_{\mathfrak{p}} \operatorname{depth}(R_{\mathfrak{p}}) = \min_{\mathfrak{p}} \dim(R_{\mathfrak{p}}) = \operatorname{codim}(\mathfrak{a}).$$

Conversely, if $\operatorname{depth}(\mathfrak{a}, R) = \operatorname{codim}(\mathfrak{a})$ for all proper ideals $\mathfrak{a}$, then in particular it holds for all maximal ideals $\mathfrak{m}$. On the other hand, for every such $\mathfrak{m}$, we have

$$\operatorname{depth}(\mathfrak{m}, R) = \operatorname{depth}(R_{\mathfrak{m}}) \leq \dim(R_{\mathfrak{m}}) = \operatorname{codim}(\mathfrak{m}),$$

where the first equality follows from Proposition 11.13 and the inequality follows from Proposition 11.15. We thus conclude that $\operatorname{depth}(R_{\mathfrak{m}}) = \dim(R_{\mathfrak{m}})$ for every maximal ideal $\mathfrak{m}$, hence R is Cohen-Macaulay. □

EXAMPLE 11.31. If R is a reduced, Noetherian ring with $\dim(R) = 1$, then R is Cohen-Macaulay. Indeed, it is enough to show that if $\mathfrak{a}$ is not contained in any minimal prime, then $\operatorname{depth}(\mathfrak{a}) \geq 1$. This follows from the fact that since R is reduced, all associated primes of R are minimal, see Remark 5.19.

EXAMPLE 11.32. If R is a normal Noetherian ring, with $\dim(R) = 2$, then R is Cohen-Macaulay. Indeed, after localizing at a maximal ideal, we may and will assume that $(R, \mathfrak{m})$ is local and $\dim(R) = 2$ (if $\dim(R) = 1$, then we may apply the previous example). In this case R is a domain and any $a \in \mathfrak{m}$ is a non-zero-divisor. Moreover, $\mathfrak{m} \notin \operatorname{Ass}\big(R/(a)\big)$ by Proposition 8.41, hence $\operatorname{depth}(R) \geq 2$. Since $\dim(R) = 2$, we conclude that R is Cohen-Macaulay.

The following result will provide us with interesting examples of Cohen-Macaulay rings:

THEOREM 11.33. *If R is a Cohen-Macaulay ring, then $S = R[x]$ is a Cohen-Macaulay ring too.*

We begin with a lemma concerning the behavior of regular sequences under flat homomorphisms:

LEMMA 11.34. *If $f\colon R \to S$ is a flat homomorphism and $x_1, \ldots, x_n \in R$ form a regular sequence such that $(x_1, \ldots, x_n)S \neq S$, then $f(x_1), \ldots, f(x_n)$ form a regular sequence in S.*

PROOF. It is enough to show that for $1 \leq i \leq n$, $f(x_i)$ is a non-zero-divisor on $S/\big(f(x_1), \ldots, f(x_{i-1})\big)$. This follows from the fact that $R/(x_1, \ldots, x_{i-1}) \to S/\big(f(x_1), \ldots, f(x_{i-1})\big)$ is a flat homomorphism by Proposition 10.7i), hence multiplication by x_i on $R/(x_1, \ldots, x_{i-1})$ being injective implies that multiplication by $f(x_i)$ on $S/\big(f(x_1), \ldots, f(x_{i-1})\big)$ is injective. □

PROOF OF THEOREM 11.33. Let $\mathfrak{m}$ be a maximal ideal of S and let $\mathfrak{p} = \mathfrak{m} \cap R$. Since $R[x]_{\mathfrak{m}}$ is a localization of $R_{\mathfrak{p}}[x]$, it follows from Corollary 11.29 that it is enough to show that $R_{\mathfrak{p}}[x]$ is Cohen-Macaulay. Hence we may assume that $(R, \mathfrak{p})$ is a local ring. Let $n = \dim(R) = \operatorname{codim}(\mathfrak{p})$. If $k = R/\mathfrak{p}$, then $\mathfrak{m}/\mathfrak{p}[x]$ is a maximal ideal in $k[x]$, hence it is generated by some $\overline{u}$, where $u \in R[x]$ is a monic polynomial. Since R is Cohen-Macaulay, we have $\operatorname{depth}(\mathfrak{p}, R) = n$, and let $a_1, \ldots, a_n \in \mathfrak{p}$ be a regular sequence. Note that $\operatorname{codim}(a_1, \ldots, a_n) = n$ by Remark 11.17, hence $\mathfrak{p}$ is a minimal prime containing $(a_1, \ldots, a_n)$. Therefore $\mathfrak{m}$ is a minimal prime containing $(a_1, \ldots, a_n, u)$, and it follows that $\operatorname{codim}(\mathfrak{m}) \leq n + 1$ by Corollary 7.35. In order to complete the proof, it is enough to show that $\operatorname{depth}(\mathfrak{m}, S) \geq n + 1$ (this implies that $\operatorname{depth}(\mathfrak{m}S_{\mathfrak{m}}, S_{\mathfrak{m}}) \geq n + 1$). Since S is flat over R, it follows from the lemma that $a_1, \ldots, a_n$ form a regular sequence in S. Moreover, u is a non-zero-divisor on $R[x]/(a_1, \ldots, a_n)R[x] = R/(a_1, \ldots, a_n)[x]$ since it is monic. Therefore $\operatorname{depth}(\mathfrak{m}, S) \geq n + 1$. □

EXAMPLE 11.35. A field k is trivially Cohen-Macaulay, hence it follows from Theorem 11.33, by induction on n, that every polynomial ring $k[x_1, \ldots, x_n]$ is Cohen-Macaulay.

EXAMPLE 11.36. Note that the ring $\mathbf{Z}$ is Cohen-Macaulay: this follows, for example, from Example 11.31. We deduce from Theorem 11.33, by induction on n, that every polynomial ring $\mathbf{Z}[x_1, \ldots, x_n]$ is Cohen-Macaulay.

We end with two other properties that make Cohen-Macaulay rings very useful.

THEOREM 11.37. *If R is a local Cohen-Macaulay ring, then for every proper ideal $\mathfrak{a}$ of R, we have*

$$\operatorname{codim}(\mathfrak{a}) + \dim(R/\mathfrak{a}) = \dim(R).$$

PROOF. We argue by induction on $r = \operatorname{codim}(\mathfrak{a})$. If $r = 0$, then there is a minimal prime $\mathfrak{p}$ in R such that $\mathfrak{a} \subseteq \mathfrak{p}$. Since $\dim(R/\mathfrak{p}) = \dim(R)$ by Proposition 11.27, we are done in this case.

Suppose now that $r \geq 1$. Another application of Proposition 11.27 implies that since $\mathfrak{a}$ is not contained in any minimal prime of R, there is a non-zero-divisor $x \in \mathfrak{a}$. Let $\overline{R} = R/(x)$ and $\overline{\mathfrak{a}} = \mathfrak{a}/(x)$. Note that $\overline{R}$ is Cohen-Macaulay by Proposition 11.26 and $\dim(\overline{R}) = \dim(R) - 1$ by Exercise 7.47. Since $\overline{R}/\overline{\mathfrak{a}} \simeq R/\mathfrak{a}$, we are done by induction since

$$\operatorname{codim}(\overline{\mathfrak{a}}) = \operatorname{depth}(\overline{\mathfrak{a}}, R) = \operatorname{depth}(\mathfrak{a}, R) - 1 = \operatorname{codim}(\mathfrak{a}) - 1,$$

where the second equality follows from Remark 11.10 and Corollary 11.11, while the other equalities follow from the fact that both R and $\overline{R}$ are Cohen-Macaulay rings. □

COROLLARY 11.38. Every Cohen-Macaulay ring is catenary.

PROOF. Let R be a Cohen-Macaulay ring. In order to show that R is catenary, it is enough to show that if $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ are prime ideals such that there is no prime ideal $\mathfrak{p}'$ with $\mathfrak{p}_1 \subsetneq \mathfrak{p}' \subsetneq \mathfrak{p}_2$, then $\operatorname{codim}(\mathfrak{p}_2) = \operatorname{codim}(\mathfrak{p}_1) + 1$. After replacing R by $R_{\mathfrak{p}_2}$, we may assume that R is local, with maximal ideal $\mathfrak{p}_2$. It is then clear that $\dim(R/\mathfrak{p}_1) = 1$, hence it follows from Theorem 11.37 that

$$\operatorname{codim}(\mathfrak{p}_2) = \dim(R) - \dim(R/\mathfrak{p}_2) = \dim(R) - \dim(R/\mathfrak{p}_1) + 1 = \operatorname{codim}(\mathfrak{p}_1) + 1.$$

□

THEOREM 11.39. *If $(R, \mathfrak{m})$ is a local Cohen-Macaulay ring and $\mathfrak{a} = (x_1, \ldots, x_r)$ is a proper ideal in R, then* $\operatorname{codim}(\mathfrak{a}) = r$ *if and only if $x_1, \ldots, x_r$ form a regular sequence.*

PROOF. If $x_1, \ldots, x_r$ is a regular sequence, we always have $\operatorname{codim}(\mathfrak{a}) = r$ by Remark 11.17. In order to prove the converse, we may assume that $r = n$, where $n = \dim(R)$ Indeed, since all prime ideals containing $\mathfrak{a}$ have codimension $\geq r$, arguing as in the proof of Proposition 7.38, we can find $x_{r+1}, \ldots, x_n$ such that $\operatorname{codim}(x_1, \ldots, x_n) = n$. Of course, it is enough to show that $x_1, \ldots, x_n$ is a regular sequence.

We now prove the assertion by induction on n. Note that if $\mathfrak{p} \in \operatorname{Ass}(R)$, then $x_1 \notin \mathfrak{p}$. Indeed, otherwise it follows from the general form of the Principal ideal Theorem that $\operatorname{codim}(\mathfrak{m}/\mathfrak{p}) \leq n - 1$, contradicting the fact that $\dim(R/\mathfrak{p}) = n$ by Proposition 11.27. Therefore x_1 is a non-zero-divisor, hence $R/(x_1)$ is Cohen-Macaulay by Proposition 11.26, of dimension $n-1$, and $x_2, \ldots, x_n$ generate an ideal of codimension $n - 1$. We thus conclude, by induction, that $x_2, \ldots, x_n$ is a regular sequence in $R/(x_1)$. Therefore $x_1, \ldots, x_n$ is a regular sequence in R. □

EXERCISE 11.40. Show that if R is a domain of finite type over a field k, then for every prime ideal $\mathfrak{p}$ in R, we have

$$\dim(R) = \dim(R/\mathfrak{p}) + \operatorname{codim}(\mathfrak{p}).$$

Hint: reduce to the case when $R = k[x_1, \ldots, x_n]$ and then reduce to the fact that if $\mathfrak{m}$ is a maximal ideal in $\overline{k}[x_1, \ldots, x_n]$, where $\overline{k}$ is the algebraic closure of k, then $\operatorname{codim}(\mathfrak{m}) = n$.

EXERCISE 11.41. Compute $\operatorname{depth}(R)$ if $R = k[x, y, z, w]_{(x,y,z,w)}/(xz, xw, yz, yw)$, where k is a field. Is R Cohen-Macaulay?

EXERCISE 11.42. Let R be a Noetherian local ring and I and J two proper ideals in R such that $I \cap J = (0)$. We assume that both R/I and R/J are Cohen-Macaulay rings of dimension d and that $R/(I + J)$ has dimension $d - 1$. Show that R is a Cohen-Macaulay ring if and only if $R/(I + J)$ is a Cohen-Macaulay ring.

11.3. The Koszul complex

In this section we discuss an important complex which can be used to resolve ideals generated by regular sequences and which, over local rings, can be used to compute the depth of any ideal.

Let R be a commutative ring and $\underline{x} = x_1, \ldots, x_n$ a sequence of elements in R. We define a complex $K(\underline{x}) = K(x_1, \ldots, x_n)$:

$$0 \to K_n \to K_{n-1} \to \ldots \to K_1 \to K_0 \to 0,$$

as follows. For every $p \in \{0, \dots, n\}$, we take K_p to be a free R-module with basis $\{e_I \mid I \subseteq \{1, \dots, n\}, \#I = p\}$, so $\operatorname{rank}(K_p) = \binom{n}{p}$. For $1 \leq p \leq n$, we define $d\colon K_p \to K_{p-1}$, as follows: if $I = \{i_1, \dots, i_p\} \subseteq \{1, \dots, n\}$, with $i_1 < \dots < i_p$, we put

$$d(e_I) = \sum_{k=1}^{p} (-1)^{k-1} x_{i_k} e_{I \smallsetminus \{i_k\}}.$$

LEMMA 11.43. *We have $d \circ d = 0$, hence $K(\underline{x})$ is a complex.*

PROOF. Let $p \geq 2$ and consider $I = \{i_1, \dots, i_p\} \subseteq \{1, \dots, n\}$, with $i_1 < \dots < i_p$. By definition, we have

$$d \circ d(e_I) = \sum_{k=1}^{p} (-1)^{k-1} x_{i_k} d(e_{I \smallsetminus \{i_k\}}) = \sum_{k=1}^{p} \sum_{j<k} (-1)^{k+j} x_{i_k} x_{i_j} e_{I \smallsetminus \{i_k, i_j\}}$$

$$+ \sum_{k=1}^{p} \sum_{j>k} (-1)^{j+k-1} x_{i_k} x_{i_j} e_{I \smallsetminus \{i_k, i_j\}} = 0.$$

□

DEFINITION 11.44. The complex $K(\underline{x})$ is the *Koszul complex* associated to the sequence $\underline{x}$. If M is an R-module, then we put $K(\underline{x}; M) := K(\underline{x}) \otimes_R M$. For every i, with $0 \leq i \leq n$, we write $H_i(\underline{x}; M)$ for $H_i\big(K(\underline{x}; M)\big)$.

EXAMPLE 11.45. If we have only one element $x \in R$, then the Koszul complex $K(x; M)$ consists of

$$0 \to M \xrightarrow{\cdot x} M \to 0.$$

If we have 2 elements $x_1, x_2 \in R$, then the Koszul complex $K(x_1, x_2; M)$ is given by

$$0 \to M \xrightarrow{g} M \oplus M \xrightarrow{f} M \to 0,$$

where $g(u) = (-x_2 u, x_1 u)$ and $f(v_1, v_2) = x_1 v_1 + x_2 v_2$.

REMARK 11.46. It is clear from the definition that for every R-module M, we have

$$H_0(\underline{x}; M) \simeq M/(x_1, \dots, x_n)M.$$

EXERCISE 11.47. Show that if we permute the elements of the sequence, then we obtain isomorphic Koszul complexes: more precisely, given a permutation σ of $\{1, \dots, n\}$, we have an isomorphism of R-modules $\varphi_p\colon K_p(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \to K_p(x_1, \dots, x_n)$ that maps e_I to $\epsilon_I e_{\sigma(I)}$, where if $I = \{i_1, \dots, i_p\} \subseteq \{1, \dots, n\}$, with $i_1 < \dots < i_p$, we denote by ϵ_I the signature of the permutation that orders increasingly $\sigma(i_1), \dots, \sigma(i_p)$. Show that $(\varphi_i)_{0 \leq i \leq n}$ gives an isomorphism of complexes $K(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \to K(x_1, \dots, x_n)$.

EXERCISE 11.48. Given $\underline{x} = x_1, \dots, x_n \in R$, show that multiplication by $a \in (x_1, \dots, x_n)$ on $K(\underline{x})$ is homotopic to 0. In particular, if $(x_1, \dots, x_n) = R$, then for every R-module M and every $i \in \mathbf{Z}$, we have $H_i(\underline{x}; M) = 0$. Hint: show that if $a = \sum_{i=1}^{n} a_i x_i$, then we get the desired homotopy by defining for every $p \geq 0$ the map $\theta_p\colon K(\underline{x})_p \to K(\underline{x})_{p+1}$ such that

$$\theta_p(e_I) = \sum_{i \notin I} a_i \epsilon(i; I) e_{I \cup \{i\}},$$

where if $I = \{i_1, \ldots, i_p\} \subseteq \{1, \ldots, n\}$, with $i_1 < \ldots < i_p$, $\epsilon(i, I) = \#\{k \mid 1 \leq k \leq p, i_k < i\}$.

The main results concerning the Koszul complex are proved by induction on the length of the sequence. The next result provides the main ingredient for doing this. For any complex $F_\bullet$, we denote by $F_\bullet[1]$ the complex $G_\bullet$ with $G_n = F_{n-1}$ for all $n \in \mathbf{Z}$ and $d_G = d_F$.

PROPOSITION 11.49. Given a sequence $\underline{x} = x_1, \ldots, x_n$ of elements of R and an R-module M, we have a short exact sequence of complexes

$$0 \to K(\underline{x}'; M) \to K(\underline{x}; M) \to K(\underline{x}'; M)[1] \to 0,$$

where $\underline{x}' = x_1, \ldots, x_{n-1}$. Moreover, the corresponding long exact sequence of cohomology is given by

$$\ldots \to H_p(\underline{x}'; M) \to H_p(\underline{x}; M) \to H_{p-1}(\underline{x}'; M) \xrightarrow{\pm x_n} H_{p-1}(\underline{x}'; M) \to \ldots.$$

PROOF. It is clear that if we define $i_p \colon K_p(\underline{x}') \to K_p(\underline{x})$ by $i_n(e_J) = e_J$ for every $J \subseteq \{1, \ldots, n-1\}$ with $\#J = p$, we get an injective morphism of complexes $i \colon K(\underline{x}') \to K(\underline{x})$. If we define $\varphi_p \colon K_p(\underline{x}) \to K_{p-1}(\underline{x}')$ such that for every $J \subseteq \{1, \ldots, n\}$ with $\#J = p$ we have $\varphi(e_J) = 0$ if $n \notin J$ and $\varphi(e_J) = e_{J \smallsetminus \{n\}}$ if $n \in J$, we get a surjective morphism of complexes $\varphi \colon K(\underline{x}) \to K(\underline{x}')[1]$. Moreover, it is clear that for every p, the sequence

$$0 \to K_p(\underline{x}') \to K_p(\underline{x}) \to K_{p-1}(\underline{x}') \to 0$$

is split exact, hence after tensoring with M, we have a short exact sequence of complexes

$$0 \to K(\underline{x}'; M) \to K(\underline{x}; M) \to K(\underline{x}'; M)[1] \to 0.$$

We need to show that the boundary map $\delta \colon H_{p-1}(\underline{x}'; M) \to H_{p-1}(\underline{x}'; M)$ in the long exact sequence for cohomology is given by multiplication with $\pm x_n$. Recall that this is defined as follows. Given $u \in K_{p-1}(\underline{x}'; M)$ such that $d(u) = 0$, we write $u = \varphi_p(v)$, for some $v \in K_p(\underline{x}; M)$, and if $w \in K_{p-1}(\underline{x}'; M)$ is such that $i_{p-1}(w) = d(v)$, then $\delta(\overline{u}) = \overline{w}$. If we have $u = \sum_I e_I \otimes u_I$, with I running over the subsets of $\{1, \ldots, n-1\}$ of size $p-1$, then we may take $v = \sum_I e_{I \cup \{n\}} \otimes u_I$, so $d(v) = i(w)$, where $w = (-1)^{p-1} x_n \cdot \sum_I e_I \otimes u_I$. This gives the formula in the proposition. □

We next turn to the connection of the Koszul complex with regular sequences.

THEOREM 11.50. *Let M be an R-module and $\underline{x} = x_1, \ldots, x_n$ a sequence of elements of R.*

i) *If $\underline{x}$ is an M-regular sequence, then $H_i(\underline{x}; M) = 0$ for $i \geq 1$, while $H_0(\underline{x}; M) \simeq M/(x_1, \ldots, x_n)M \neq 0$.*
ii) *Conversely, if $(R, \mathfrak{m})$ is a local Noetherian ring, $x_1, \ldots, x_n \in \mathfrak{m}$, and $M \neq 0$ is a finitely generated R-module such that $H_i(\underline{x}; M) = 0$ for all $i \geq 1$, then $\underline{x}$ is an M-regular sequence.*

PROOF. We prove i) by induction on n. Note that the equality $H_0(\underline{x}; M) = M/(x_1, \ldots, x_n)M$ holds for all $\underline{x}$ by Remark 11.46, and $M/(x_1, \ldots, x_n)M \neq 0$ since $\underline{x}$ is an M-regular sequence. If $n = 1$, then the complex $K(x_1) \otimes_R M$ consists of

$$0 \to M \xrightarrow{x_1} M \to 0.$$

The map is injective since x_1 is a non-zero-divisor on M, hence $H_i(x_1; M) = 0$ for $i \neq 0$.

Suppose now that $n \geq 2$ and we know the assertion for $n-1$. We have seen that if $\underline{x}' = x_1, \ldots, x_{n-1}$, then we have a long exact sequence

$$\to H_i(\underline{x}'; M) \xrightarrow{\pm x_n} H_i(\underline{x}'; M) \to H_i(\underline{x}, M) \to H_{i-1}(\underline{x}'; M) \to \ldots.$$

By induction, we know that $H_i(\underline{x}'; M) = 0$ for $i \geq 1$, which immediately implies $H_i(\underline{x}; M) = 0$ for $i \geq 2$. Moreover, we have an exact sequence

$$0 \to H_1(\underline{x}; M) \to H_0(\underline{x}'; M) \xrightarrow{\pm x_n} H_0(\underline{x}'; M).$$

Since $H_0(\underline{x}'; M) \simeq M/(x_1, \ldots, x_{n-1})M$ and x_n is a non-zero-divisor on the R-module $M/(x_1, \ldots, x_{n-1})M$, we conclude that $H_1(\underline{x}; M) = 0$. This completes the proof of i).

Suppose now that we are under the assumptions of ii). Note that by Nakayama's lemma, we have $M/(x_1, \ldots, x_n)M \neq 0$, hence we only need to show that x_i is a non-zero-divisor on $M/(x_1, \ldots, x_{i-1})M$ for $1 \leq i \leq n$. We argue again by induction on n. If $n = 1$, then

$$0 = H_1(x_1; M) = \ker\left(M \xrightarrow{\cdot x_1} M\right),$$

hence x_1 is a non-zero-divisor on M.

For the induction step we use the following piece of the long exact sequence in cohomology provided by Proposition 11.49:

$$H_i(\underline{x}'; M) \xrightarrow{\pm x_n} H_i(\underline{x}'; M) \to H_i(\underline{x}; M) = 0,$$

where $i \geq 1$ and $\underline{x}' = x_1, \ldots, x_{n-1}$. Since $K(\underline{x}'; M)$ is a complex of finitely generated modules over the Noetherian ring R, $H_i(\underline{x}'; M)$ is a finitely generated R-module, and it follows from Nakayama's lemma that $H_i(\underline{x}'; M) = 0$ for all $i \geq 1$, hence by induction $x_1, \ldots, x_{n-1}$ is an M-regular sequence. Moreover, we have an exact sequence

$$0 = H_1(\underline{x}; M) \to H_0(\underline{x}'; M) \xrightarrow{\pm x_n} H_0(\underline{x}'; M).$$

Therefore x_n is a non-zero-divisor on $H_0(\underline{x}'; M) \simeq M/(x_1, \ldots, x_{n-1})M$, and thus $x_1, \ldots, x_n$ is an M-regular sequence. □

REMARK 11.51. Since the Koszul complex for a permutation of a sequence is isomorphic to the Koszul complex for the original sequence (see Exercise 11.47), using Theorem 11.50 we get another proof for the fact that if M is a finitely generated module over the Noetherian local ring $(R, \mathfrak{m})$ and $\underline{x}$ is an M-regular sequence, then every permutation of $\underline{x}$ is still M-regular (cf. Proposition 11.4).

When the ring is local, we can use the Koszul complex to compute the depth, as follows. The proof is similar to that of Theorem 11.50, see [**Mat89**, Theorem 16.8].

THEOREM 11.52. *If $(R, \mathfrak{m})$ is a Noetherian local ring, M is a nonzero finitely generated R-module, and $x_1, \ldots, x_n$ generate an ideal $\mathfrak{a} \subseteq \mathfrak{m}$ with $r = \operatorname{depth}(\mathfrak{a}, M)$, then*

$$H_i(\underline{x}; M) = 0 \quad \textit{for} \quad i > n - r, \quad \textit{and} \quad H_{n-r}(\underline{x}, M) \neq 0.$$

EXERCISE 11.53. Let R be a Noetherian ring, M a nonzero finitely generated module, and let $I = \operatorname{Ann}_R(M)$.

i) Show that $\operatorname{depth}(I, R) \leq \operatorname{pd}_R(M)$. The module M is *perfect* if this inequality is an equality.
ii) Show that if an ideal J in R is generated by a regular sequence, then R/J is a perfect R-module.
iii) Show that if M is perfect and $\mathfrak{p} \in \operatorname{Supp}(M)$, then $\mathfrak{p} \in \operatorname{Ass}(M)$ if and only if $\operatorname{depth}(R_p) = \operatorname{depth}(I, R)$.

CHAPTER 12

Regular rings

Our goal in this chapter is to discuss regular rings, their basic properties, and their homological characterization due to Auslander-Buchsbaum and Serre.

12.1. Definition and first properties

Let $(R, \mathfrak{m}, k)$ be a local Noetherian ring.

DEFINITION 12.1. A *system of parameters* of R is a sequence $x_1, \ldots, x_d \in \mathfrak{m}$, where $d = \dim(R)$, such that the ideal $(x_1, \ldots, x_d)$ is $\mathfrak{m}$-primary (or equivalently, it has codimension d).

REMARK 12.2. The existence of systems of parameters is guaranteed by Proposition 7.38.

DEFINITION 12.3. For a finitely generated R-module M, we denote by $\mu(M)$ the minimal number of elements of a system of generators of M. Recall that by Nakayama's lemma, we have $\mu(M) = \dim_k(M/\mathfrak{m}M)$ (moreover, $u_1, \ldots, u_n \in M$ is a minimal system of generators if and only if $\overline{u_1}, \ldots, \overline{u_n} \in M/\mathfrak{m}M$ is a k-basis of $M/\mathfrak{m}M$). The *embedding dimension* of R is $\operatorname{embdim}(R) := \mu(\mathfrak{m}) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$.

REMARK 12.4. It follows from the general form of the Principal Ideal theorem (see Corollary 7.35) that $\dim(R) \leq \mu(\mathfrak{m})$.

We now come to the main definition in this chapter. This is the "best" class of rings in commutative algebra.

DEFINITION 12.5. A Noetherian local ring $(R, \mathfrak{m})$ is a *regular ring* if $\mu(\mathfrak{m}) = \dim(R)$. In this case, a *regular system of parameters* of R is a minimal system of generators $x_1, \ldots, x_d$ of $\mathfrak{m}$ (so $d = \dim(R)$).

EXAMPLE 12.6. A 0-dimensional Noetherian local ring is regular if and only if it is a field.

We begin with two results concerning the behavior of regularity with respect to quotients.

PROPOSITION 12.7. If $(R, \mathfrak{m})$ is a regular local ring and $x \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$, then $R/(x)$ is a regular local ring, with $\dim\big(R/(x)\big) = \dim(R) - 1$.

PROOF. Since $x \notin \mathfrak{m}^2$, it follows that x can be completed to a regular system of parameters $x, x_2, \ldots, x_d$, where $d = \dim(R)$. Therefore $\operatorname{embdim}\big(R/(x)\big) \leq d-1$. On the other hand, we have $\dim\big(R/(x)\big) \geq d - 1$ (if $\overline{y_1}, \ldots, \overline{y_e}$ is a system of parameters of $R/(x)$, then it is clear that $(x, y_2, \ldots, y_e)$ is an $\mathfrak{m}$-primary ideal in R, hence $d \leq e + 1$ by the general form of the Principal Ideal theorem). We thus have $\operatorname{embdim}\big(R/(x)\big) \leq \dim\big(R/(x)\big)$ and since the opposite inequality always holds, it follows that $R/(x)$ is regular, of dimension $d - 1$. □

PROPOSITION 12.8. If $(R, \mathfrak{m})$ is a local Noetherian ring and $x \in \mathfrak{m}$ is a non-zero-divisor such that $R/(x)$ is regular, then R is regular.

PROOF. Let $d = \dim(R)$. Since x is a non-zero-divisor, it follows from Exercise 7.47 that $\dim\big(R/(x)\big) = d-1$. Since $R/(x)$ is regular, we can find $x_2, \ldots, x_d \in R$ such that $\mathfrak{m}/(x) = (\overline{x_1}, \ldots, \overline{x_{d-1}})$. We clearly have $\mathfrak{m} = (x, x_2, \ldots, x_d)$, hence $\operatorname{embdim}(R) \leq d$. Since the opposite inequality always holds, it follows that R is a regular ring. □

PROPOSITION 12.9. If R is a regular local ring, then R is a domain.

PROOF. We argue by induction on $d = \dim(R)$. If $d = 0$, then R is a field, and the assertion is clear. Suppose now that $d \geq 1$. If $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are the minimal primes of R, then there is $x \in \mathfrak{m} \smallsetminus (\mathfrak{m}^2 \cup \mathfrak{p}_1 \cup \ldots \mathfrak{p}_r)$ (this follows by Prime Avoidance, see Lemma 5.1). In this case it follows from Proposition 12.7 that $R/(x)$ is a regular ring of dimension $d-1$, hence it is a domain by induction. Therefore (x) is a prime ideal of R and by our choice of x, it is not minimal, hence it strictly contains one of the minimal primes, say $\mathfrak{p}_i$. Suppose now that $y \in \mathfrak{p}_i \smallsetminus \{0\}$. By Krull's Intersection theorem (see Corollary 4.22), there is $N \geq 0$ such that $y \in (x^N) \smallsetminus (x^{N+1})$. If we write $y = x^N z$, for some $z \in R$, since $x \notin \mathfrak{p}_i$, it follows that $z \in \mathfrak{p}_i \subseteq (x)$, hence $y \in (x^{N+1})$, a contradiction. Therefore $\mathfrak{p}_i = (0)$, hence R is a domain. □

EXAMPLE 12.10. A Noetherian local ring R of dimension 1 is regular if and only if it is a DVR (the "if" part is clear and the "only if" part follows since R regular implies that R is a domain, and we use the description of DVRs in Proposition 8.7.

PROPOSITION 12.11. Every regular local ring is Cohen-Macaulay.

PROOF. Let $(R, \mathfrak{m})$ be a regular local ring of dimension d. We argue by induction on d. If $d = 0$, then R is a field and the assertion is clear. Suppose now that $d \geq 1$ and let $x \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$. In this case $R/(x)$ is a regular ring of dimension $d-1$ by Proposition 12.7, hence Cohen-Macaulay by the inductive assumption. On the other hand, R is a domain by Proposition 12.9, hence x is a non-zero-divisor in R, and thus we conclude that R is Cohen-Macaulay by Proposition 11.26. □

REMARK 12.12. If $(R, \mathfrak{m})$ is a regular local ring, then every regular system of parameters in R is a regular sequence. More generally, if $(R, \mathfrak{m})$ is any Cohen-Macaulay ring of dimension n and $x_1, \ldots, x_n$ is a system of parameters, then $x_1, \ldots, x_n$ is a regular sequence. Indeed, we have $\operatorname{codim}(x_1, \ldots, x_n) = n$ and since R is Cohen-Macaulay, it follows from Proposition 11.39 that $x_1, \ldots, x_n$ is a regular sequence.

PROPOSITION 12.13. If $(R, \mathfrak{m}, k)$ is a regular local ring and $I \subseteq \mathfrak{m}$ is an ideal, then R/I is a regular ring if and only if I is generated by part of a regular system of parameters.

PROOF. Let $\overline{R} = R/I$ and $\overline{\mathfrak{m}} = \mathfrak{m}/I$. Note that $x_1, \ldots, x_r \in \mathfrak{m}$ form a part of a regular system of parameters if and only if their images in $\mathfrak{m}/\mathfrak{m}^2$ are linearly independent. In this case, a successive application of Proposition 12.7 implies that $R/(x_1, \ldots, x_r)$ is a regular local ring of dimension $\dim(R) - r$. This gives the "if" part of the proposition.

Conversely, suppose that $\overline{R}$ is a regular ring of dimension $\dim(R) - r$. Since

$$\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 = (\mathfrak{m}/I)/(\mathfrak{m}^2 + I/I) \simeq \mathfrak{m}/\mathfrak{m}^2 + I$$

and we have a short exact sequence of k-vector spaces

$$0 \to I/\mathfrak{m}^2 \cap I \simeq (\mathfrak{m}^2 + I)/\mathfrak{m}^2 \to \mathfrak{m}^2/\mathfrak{m}^2 \to \mathfrak{m}/\mathfrak{m}^2 + I \to 0,$$

it follows that

$$\mu(\overline{\mathfrak{m}}) = \dim_k(\mathfrak{m}/\mathfrak{m}^2 + I) = \mu(\mathfrak{m}) - \dim_k(I/\mathfrak{m}^2 \cap I).$$

We can thus choose $x_1, \ldots, x_r \in I$ whose images in $I/\mathfrak{m}^2 \cap I \hookrightarrow \mathfrak{m}/\mathfrak{m}^2$ are linearly independent. If $S = R/(x_1, \ldots, x_r)$, then by what we have already proved, S is a regular ring of dimension $\dim(R) - r$. In particular, it is a domain, hence if $J = I/(x_1, \ldots, x_r)$ is nonzero, then we have

$$\dim(R/I) = \dim(S/J) < \dim(R) - r,$$

a contradiction. We thus conclude that $I = (x_1, \ldots, x_r)$ and by construction $x_1, \ldots, x_r$ are part of a regular system of parameters of R. This completes the proof. □

One thing that is not clear at this point is that if R is a regular local ring and $\mathfrak{p}$ is a prime ideal in R, then $R_{\mathfrak{p}}$ is again a regular local ring. We will prove this in Section 12.4, after giving a homological characterization of regular local rings.

The notion of regular local ring that we discussed so far admits the following global version:

Definition 12.14. A Noetherian ring R is *regular* if $R_{\mathfrak{m}}$ is a regular local ring for all maximal ideals $\mathfrak{m}$ in R.

Remark 12.15. If R is a regular ring, then it follows from Proposition 12.9 that $R_{\mathfrak{m}}$ is a domain for every maximal ideal $\mathfrak{m}$ in R. In this case, arguing as in the proof of Proposition 8.38, we see that $R \simeq R_1 \times \ldots \times R_n$, where $R_1, \ldots, R_n$ are regular domains.

Exercise 12.16. Let $(R, \mathfrak{m})$ be a regular local ring. Recall that by Proposition 12.7, if $x \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$, then $R/(x)$ is again a regular ring. Show that conversely, if $x \in \mathfrak{m} \smallsetminus \{0\}$ is such that $R/(x)$ is regular, then $x \notin \mathfrak{m}^2$.

Exercise 12.17. Let $f \in k[x_1, \ldots, x_n]$, where k is an algebraically closed field, and let $R = k[x_1, \ldots, x_n]/(f)$. Show that if $\mathfrak{m}$ is a maximal ideal in R corresponding to the point P in the algebraic subset defined by f, then the ring $R_{\mathfrak{m}}$ is a regular ring if and only if $\frac{\partial f}{\partial x_i}(P) \neq 0$ for some i, with $1 \leq i \leq n$.

Exercise 12.18. Suppose that R is a Noetherian local ring with the property that there is some regular local ring S and a surjective homomorphism $S \to R$ (for example, R could be the localization of an algebra of finite type over a field). Show that the smallest dimension of such a ring S is precisely $\operatorname{embdim}(R)$ (this is the reason for the name of *embedding dimension*, note that such a surjection induces an "embedding" $\operatorname{Spec}(R) \hookrightarrow \operatorname{Spec}(S)$).

12.2. Projective dimension and minimal free resolutions

We begin this section by discussing the notions of projective and injective dimensions. Let R be an arbitrary (commutative) ring.

DEFINITION 12.19. If M is an R-module, then the *projective dimension* of M, denoted $\mathrm{pd}_R(M)$, is the smallest $n \geq 0$ such that there is a projective resolution of M with n terms:

$$0 \to F_n \to \ldots \to F_0 \to M \to 0$$

(if there is no such finite resolution, then $\mathrm{pd}_R(M) = \infty$). Similarly, the *injective dimension* of M, denoted $\mathrm{id}_R(M)$, is the smallest $n \geq 0$ such that there is an injective resolution of M with n terms:

$$0 \to M \to I^0 \to \ldots \to I^n \to 0$$

(again, if there is no such finite resolution, then $\mathrm{id}_R(M) = \infty$).

REMARK 12.20. Note that, by definition, we have $\mathrm{pd}_R(M) = 0$ if and only if M is projective and we have $\mathrm{id}_R(M) = 0$ if and only if M is injective.

PROPOSITION 12.21. For every R-module M, the following are equivalent:

i) $\mathrm{pd}_R(M) \leq n$.
ii) $\mathrm{Ext}^i_R(M, N) = 0$ for all $i > n$ and all R-modules N.
iii) $\mathrm{Ext}^{n+1}_R(M, N) = 0$ for all R-modules N.

Moreover, if R is Noetherian and M is finitely generated, then the above conditions are also equivalent with

iv) $\mathrm{Ext}^{n+1}_R(M, N) = 0$ for all finitely generated R-modules N.

PROOF. In order to prove the implication i)⇒ii), note that if $\mathrm{pd}_R(M) \leq n$, then we have a projective resolution of M given by

$$0 \to F_n \to \ldots F_0 \to M \to 0.$$

By Proposition 9.95, $\mathrm{Ext}^i_R(M, N)$ is the i-th cohomology of the complex

$$0 \to \mathrm{Hom}_R(F_0, N) \to \ldots \to \mathrm{Hom}_R(F_n, N) \to 0,$$

that only has nonzero entries in degrees $0, 1, \ldots, n$. Therefore it is clear that its i-th cohomology is 0 for $i > n$.

The implication ii)⇒iii) is trivial, hence it is enough to show the implications iii)⇒i) and, assuming that M is finitely generated and R is Noetherian, iv)⇒i). Consider a surjective morphism $p\colon F \to M$, with F a free module, and let $K = \ker(p)$. Therefore we have an exact sequence:

$$0 \to K \to F \to M \to 0. \tag{12.1}$$

If R is Noetherian and M is a finitely generated R-module, we may choose F to be finitely generated, so K is finitely generated as well.

We argue by induction on $n \geq 0$ and first treat the case $n = 0$. The long exact sequence for Ext modules associated to (12.1) gives

$$0 \to \mathrm{Hom}_R(M, K) \to \mathrm{Hom}_R(M, F) \to \mathrm{Hom}_R(M, M) \to \mathrm{Ext}^1_R(M, K) = 0.$$

Therefore there is a morphism $f\colon M \to F$ such that $p \circ f = 1_M$, hence the short exact sequence (12.1) is split, so $M \oplus K \simeq F$. Since F is free, it follows from Proposition 9.72 that M is projective.

Suppose now that $n \geq 1$. Note that it is enough to show that $\mathrm{pd}_R(K) \leq n-1$: indeed, given a projective resolution

$$0 \to P_{n-1} \to \ldots \to P_0 \to K \to 0$$

of K, we obtain a projective resolution

$$0 \to P_{n-1} \to \ldots \to P_0 \to F \to M \to 0$$

of M. On the other hand, for every R-module N, the long exact sequence of Ext modules associated to (12.1) gives an exact sequence

$$0 = \mathrm{Ext}^n_R(F, N) \to \mathrm{Ext}^n_R(K, N) \to \mathrm{Ext}^{n+1}_R(M, N)$$

where the vanishing of the first term follows from the fact that F is projective and the implication i)⇒ii), that we already proved. Therefore we conclude that $\mathrm{Ext}^n_R(K, N) = 0$ for all R-modules N (assumed to be finitely generated in the setting of iv)). By induction, we conclude that $\mathrm{pd}_R(K) \leq n-1$, which as we have seen implies $\mathrm{pd}_R(M) \leq n$. □

Corollary 12.22. Let R be an arbitrary ring.

i) For any exact sequence

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

we have $\mathrm{pd}_R(M') \leq \max\{\mathrm{pd}_R(M), \mathrm{pd}_R(M'') - 1\}$.

ii) Given an R-module M and an exact complex

$$0 \to P_n \to P_{n-1} \to \ldots \to P_1 \to P_0 \to M \to 0,$$

with $P_0, \ldots, P_{n-1}$ projective modules, we have $\mathrm{pd}_R(M) \leq n$ if and only if P_n is a projective module.

Proof. The assertion in i) follows from the characterization of projective dimension in condition iii) of the proposition and the following piece of the long exact sequence of Ext modules, where N is an arbitrary R-module:

$$\mathrm{Ext}^{n+1}_R(M, N) \to \mathrm{Ext}^n_R(M', N) \to \mathrm{Ext}^{n+1}_R(M'', N).$$

The "if" part in ii) is clear from the definition of projective dimension. For the converse, note that if $K_{j-1} = \mathrm{Im}(P_j \to P_{j-1})$ for $1 \leq j \leq n$, then we have short exact sequences

$$0 \to K_j \to P_j \to K_{j-1} \to 0$$

for $0 \leq j \leq n$ (where we put $K_{-1} = M$). Since $\mathrm{pd}(P_j) = 0$ for $0 \leq j \leq n-1$, using the assertion in i) and induction on j, with $0 \leq j \leq n-1$, we conclude that $\mathrm{pd}_R(K_j) \leq \max\{0, \mathrm{pd}_R(M) - j - 1\}$. We thus conclude that if $\mathrm{pd}_R(M) \leq n$, then $K_{n-1} \simeq P_n$ is projective. □

Corollary 12.23. If M is a finitely generated module over a Noetherian local ring R, we have

$$\mathrm{pd}_R(M) = \sup\{\mathrm{pd}_{R_\mathfrak{p}}(M_\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Spec}(R)\} \tag{12.2}$$

Proof. If $F_\bullet \to M$ is a projective resolution of M, then $F_\bullet \otimes_R R_\mathfrak{p} \to M_\mathfrak{p}$ is a projective resolution of $M_\mathfrak{p}$ for every $\mathfrak{p} \in \mathrm{Spec}(R)$. Therefore we have the inequality "$\geq$" in (12.2).

Suppose now that $\mathrm{pd}_{R_\mathfrak{p}}(M_\mathfrak{p}) \leq n$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$. Since M is a finitely generated module over a Noetherian ring, there is an exact complex

$$0 \to P_n \to \ldots \to P_1 \to P_0 \to M \to 0,$$

with all P_i finitely generated R-modules and with P_i free for $i \leq n-1$. For every prime ideal $\mathfrak{p}$, by tensoring with $R_\mathfrak{p}$ and applying Corollary 12.22, we deduce

that $(P_n)_{\mathfrak{p}}$ is a projective $R_{\mathfrak{p}}$-module. We conclude that P_n is projective using Theorem 9.74. We thus have the inequality "$\leq$" in (12.2) □

We next give a characterization of injective dimension:

PROPOSITION 12.24. For every R-module M, the following are equivalent:

i) $\mathrm{id}_R(M) \leq n$.
ii) $\mathrm{Ext}^i_R(N, M) = 0$ for all $i > n$ and all R-modules N.
iii) $\mathrm{Ext}^{n+1}_R(R/I, M) = 0$ for all ideals I in R.

PROOF. The proof is similar to that of Proposition 12.21, hence we omit it. We only mention that for the proof of the implication iii)⇒i) in the case $n = 0$, we use the fact that by Proposition 9.79, in order to prove that M is injective, it is enough to show that for every ideal I in R, the first morphism in the exact sequence below

$$\mathrm{Hom}_R(R, M) \to \mathrm{Hom}_R(I, R) \to \mathrm{Ext}^1_R(R/I, M)$$

is surjective. □

PROPOSITION 12.25. For every ring R, the following invariants are equal:

i) $\sup\{\mathrm{pd}_R(M) \mid M = R - \text{module}\}$.
ii) $\sup\{\mathrm{pd}_R(R/I) \mid I = \text{ideal in } R\}$.
iii) $\sup\{\mathrm{id}_R(M) \mid M = R - \text{module}\}$.

PROOF. By Proposition 12.21, we have $\mathrm{pd}_R(M) \leq n$ for all R-modules M if and only if $\mathrm{Ext}^{n+1}_R(M, N)$ for all R-modules M and N, which by Proposition 12.24 is equivalent to $\mathrm{id}_R(N) \leq n$ for all R-modules N. This proves the equality of the supremums in i) and iii). Furthermore, by Proposition 12.24, we have $\mathrm{id}_R(N) \leq n$ for all R-modules N if and only if $\mathrm{Ext}^{n+1}_R(R/I, N)$ for all R-modules N and all ideals I in R, which by Proposition 12.21 is equivalent to $\mathrm{pd}_R(R/I) \leq n$ for all ideals I in R. This gives the equality of the supremums in ii) and iii). □

DEFINITION 12.26. The common value of the invariant in Proposition 12.25 is the *global (homological) dimension* of R, denoted $\text{gl-dim}(R)$.

In what follows we focus on the case of a local Noetherian ring $(R, \mathfrak{m}, k)$ and give a description of projective dimension of finitely generated R-modules via Tor modules. We begin by discussing the important concept of *minimal free resolution*.

Let M be a finitely generated R-module. If $u_1, \ldots, u_n \in M$ give a minimal system of generators of M and if $\varphi_0 \colon F_0 = R^{\oplus n} \to M$ is given by $\varphi_0(e_i) = u_i$, then $\ker(\varphi_0) \subseteq \mathfrak{m}F_0$ (this follows from the fact that $\overline{u_1}, \ldots, \overline{u_n} \in M/\mathfrak{m}M$ are linearly independent over k). If we choose a minimal system of generators of $\ker(\varphi_0)$, we obtain a morphism $\varphi_1 \colon F_1 \to F_0$ such that $\mathrm{Im}(\varphi_1) = \ker(\varphi_0) \subseteq \mathfrak{m}F_0$. Continuing in this way we obtain a free resolution

$$F_\bullet : \ldots \to F_m \xrightarrow{\varphi_m} \ldots \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \to 0$$

of M, with all F_i finitely generated R-modules, such that $\varphi_i(F_i) \subseteq \mathfrak{m}F_{i-1}$ for all $i \geq 1$. A free resolution with this property is called *minimal*.

PROPOSITION 12.27. If $F_\bullet \to M$ is a minimal free resolution of M, then

$$\mathrm{rank}(F_i) = \dim_k \mathrm{Tor}^R_i(k, M).$$

PROOF. Note first that since k is annihilated by $\mathfrak{m}$, it follows from Exercise 9.100 that $\operatorname{Tor}_i^R(k,M)$ is annihilated by $\mathfrak{m}$, hence $\operatorname{Tor}_i^R(k,M)$ is indeed a k-vector space. Since $F_\bullet \to M$ is a free resolution, we have

$$\operatorname{Tor}_i^R(k,M) \simeq H_i(k \otimes_R F_\bullet).$$

On the other hand, with respect to suitable bases of F_i and F_{i-1}, the matrix of φ_i has entries in $\mathfrak{m}$; therefore all maps in $k \otimes_R F_\bullet$ are 0, hence

$$\operatorname{Tor}_i^R(k,M) \simeq k \otimes_R F_i.$$

This gives the assertion in the proposition. □

REMARK 12.28. The above proposition shows that the ranks of the free modules in a minimal free resolution do not depend on the resolution. In fact, any two minimal free resolutions of M are isomorphic (though the isomorphism is not unique). Indeed, suppose that $F_\bullet \to M$ and $G_\bullet \to M$ are two minimal free resolutions. In this case it follows from Proposition 9.84 that we have a morphism of complexes $F_\bullet \to G_\bullet$ that lifts the identity on M. By tensoring with k, we see that each morphism $k \otimes_R F_i \to k \otimes_R G_i$ is an isomorphism. Since R is local, it follows that each map $F_i \to G_i$ is an isomorphism, proving our assertion. Because of this, one often talks about *the* minimal free resolution of M.

COROLLARY 12.29. If M is a finitely generated module over the Noetherian local ring $(R,\mathfrak{m},k)$ and q is a non-negative integer, then the following are equivalent:

i) $\operatorname{pd}_R(M) \le q$.
ii) $\operatorname{Tor}_i^R(N,M) = 0$ for all $i \ge q+1$ and all R-modules N.
iii) $\operatorname{Tor}_{q+1}^R(k,M) = 0$.
iv) If $F_\bullet \to M$ is the minimal free resolution of M, then $F_{q+1} = 0$.

PROOF. The implication i)⇒ii) follows from the fact that if $G_\bullet \to M$ is a projective resolution of length $\le q$, then

$$\operatorname{Tor}_i^R(N,M) \simeq H_i(N \otimes_R G_\bullet)$$

vanishes for $i \ge q+1$. The implication ii)⇒iii) is trivial, iii)⇒iv) follows from Proposition 12.27, and iv)⇒i) is clear. □

COROLLARY 12.30. If $(R,\mathfrak{m},k)$ is a Noetherian local ring, then the global dimension of R is equal to $\operatorname{pd}_R(k)$.

PROOF. The fact that $\text{gl-dim}(R) \ge \operatorname{pd}_R(k)$ follows from the definition of global dimension. On the other hand, if $\operatorname{pd}_R(k) = n$, then we deduce from Corollary 12.29 first that $\operatorname{Tor}_i^R(N,k)$ for every $i > n$, and then that $\operatorname{pd}_R(N) \le n$ if N is finitely generated. By Proposition 12.25, this implies $\text{gl-dim}(R) \le n$. □

12.3. The Auslander-Buchsbaum formula

In this section we prove the following important result due to Auslander-Buchsbaum, which relates depth and projective dimension for modules of finite projective dimension.

THEOREM 12.31 (Auslander-Buchsbaum). *If $(R,\mathfrak{m})$ is a Noetherian local ring and M is a non-zero R-module with $\operatorname{pd}_R(M) < \infty$, then*

$$\operatorname{depth}(R) = \operatorname{depth}(M) + \operatorname{pd}_R(M). \tag{12.3}$$

We first give the following

LEMMA 12.32. *Given an R-module M, if $x \in R$ is a non-zero divisor on both R and M, we have* $\operatorname{Tor}_R^i\big(M, R/(x)\big) = 0$ *for* $i \geq 1$.

PROOF. Since x is a non-zero-divisor on R, we have the following free resolution of $R/(x)$:

$$0 \to R \xrightarrow{\cdot x} R \to R/(x) \to 0.$$

It is then clear that $\operatorname{Tor}_i^R\big(M, R/(x)\big) = 0$ for $i \geq 2$, while

$$\operatorname{Tor}_1^R\big(M, R/(x)\big) \simeq \ker\big(M \xrightarrow{\cdot x} M\big) = 0.$$

□

PROOF OF THEOREM 12.31. We argue by induction on $\operatorname{depth}(R)$ and treat separately different cases. Since $\operatorname{pd}_R(M) < \infty$, it follows from Corollary 12.29 that the minimal free resolution of M is finite:

$$0 \to F_n \xrightarrow{\varphi} F_{n-1} \to \ldots \to F_0 \to M \to 0.$$

Case 1. Suppose first that $\operatorname{depth}(R) = 0$. Therefore $\mathfrak{m} \in \operatorname{Ass}(R)$, hence there is a non-zero $u \in R$ such that $\mathfrak{m} \cdot u = 0$. If $n > 0$, then $\varphi(F_n) \subseteq \mathfrak{m}F_{n-1}$, hence $\varphi(u \cdot F_n) = 0$, contradicting the injectivity of φ. Therefore $n = 0$, that is, M is free, in which case it is clear that $\operatorname{depth}(M) = \operatorname{depth}(R) = 0$. This proves (12.3) in this case.

Case 2. Suppose now that $\operatorname{depth}(R) > 0$ and $\operatorname{depth}(M) > 0$. In this case, by Prime Avoidance, there is $x \in \mathfrak{m}$ which is a non-zero-divisor on both R and M. By the lemma, this implies that $\operatorname{Tor}_R^i\big(M, R/(x)\big) = 0$ for $i \geq 1$. Therefore $F_\bullet \otimes_R R/(x)$ is an exact complex, hence a minimal free resolution of M/xM. By Nakayama's lemma, we have $F_i = 0$ if and only if $F_i/xF_i = 0$, and we deduce using Corollary 12.29 that $\operatorname{pd}_{R/(x)}(M/xM) = \operatorname{pd}_R(M)$. On the other hand, using Corollary 11.11, we have

$$\operatorname{depth}(M/xM) = \operatorname{depth}(M) - 1 \quad \text{and} \quad \operatorname{depth}\big(R/(x)\big) = \operatorname{depth}(R) - 1.$$

We deduce the equality in (12.3) from the induction hypothesis.

Case 3. Suppose that $\operatorname{depth}(R) > 0$ and $\operatorname{depth}(M) = 0$. Note that in this case M can't be free, hence $N = \ker(F_0 \to M)$ is non-zero. Note that $\operatorname{pd}_R(N) = \operatorname{pd}_R(M) - 1$ by Corollary 12.29. On the other hand, it follows from Proposition 11.14 that

$$\operatorname{depth}(N) \geq \min\big\{\operatorname{depth}(F_0), \operatorname{depth}(M) + 1\big\} \geq 1 \quad \text{and}$$

$$0 = \operatorname{depth}(M) \geq \min\big\{\operatorname{depth}(F_0), \operatorname{depth}(N) - 1\big\} \geq \min\big\{1, \operatorname{depth}(N) - 1\big\},$$

hence $\operatorname{depth}(N) = 1$. We thus obtain the equality in (12.3) by applying Case 2 to N. □

12.4. The homological characterization of regular local rings

The following result, due independently to Auslander-Buchsbaum and Serre, was one of the first successes of homological techniques in commutative algebra.

THEOREM 12.33. *If $(R, \mathfrak{m}, k)$ is a Noetherian local ring, then R is regular if and only if* $\operatorname{gl-dim}(R) < \infty$. *Moreover, in this case we have* $\operatorname{gl-dim}(R) = \dim(R)$.

PROOF. If R is a regular local ring and $x_1, \dots, x_n$ is a regular system of parameters, then $\underline{x} = x_1, \dots, x_n$ form a regular sequence by Remark 12.12. In this case, it follows from Theorem 11.50 that the Koszul complex $K(\underline{x})$ is a free resolution of $R/(x_1, \dots, x_n) = k$. In particular, we have $\mathrm{pd}_R(k) < \infty$, hence $\text{gl-dim}(R) < \infty$ by Corollary 12.30. In fact, it follows from the definition of the Koszul complex that $K(\underline{x})$ is a minimal free resolution, hence $\text{gl-dim}(R) = \mathrm{pd}_R(k) = n = \dim(R)$.

Conversely, suppose that $\text{gl-dim}(R) < \infty$. By Corollary 12.30, this is equivalent to $\mathrm{pd}_R(k) < \infty$. We argue by induction on $n = \mathrm{depth}(R)$. If $n = 0$, then it follows from Theorem 12.31 that $\mathrm{pd}_R(k) = 0$, hence k is a free R-module by Proposition 9.74. In this case $R = k$ is a field and we are done (note that a nonzero element of R can't annihilate a nonzero free R-module).

Suppose now that $n \geq 1$. In particular, we have $\mathfrak{m} \neq (0)$, so $\mathfrak{m} \neq \mathfrak{m}^2$ by Nakayama's lemma. We deduce using Prime Avoidance (see Lemma 5.1) that there is $x \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$, which is a non-zero-divisor. The ring $\overline{R} = R/(x)$ is a local Noetherian ring, with maximal ideal $\overline{\mathfrak{m}} = \mathfrak{m}/(x)$. We have $\mathrm{depth}(\overline{R}) = \mathrm{depth}(R) - 1$ by Corollary 11.11. It follows that if we can show that $\mathrm{pd}_{\overline{R}}(k) < \infty$, then $\overline{R}$ is regular by the inductive hypothesis, hence R is regular by Proposition 12.8.

Note that if $F_\bullet \to \mathfrak{m}$ is a minimal free resolution of $\mathfrak{m}$, then $F_\bullet \to R \to k$ is a minimal free resolution of k. In particular, $F_\bullet$ has finitely many nonzero terms. Since x is a non-zero-divisor, it follows from Lemma 12.32 that $\mathrm{Tor}_i^R(\mathfrak{m}, \overline{R}) = 0$ for all $i \geq 1$. This implies that by tensoring $F_\bullet$ with $\overline{R}$, we obtain a finite free resolution of $\mathfrak{m}/x\mathfrak{m}$ over $\overline{R}$. Therefore $\mathrm{pd}_{\overline{R}}(\mathfrak{m}/x\mathfrak{m}) < \infty$.

Since $x \notin \mathfrak{m}^2$, we can find a minimal system of generators $x, x_2, \dots, x_d$ of $\mathfrak{m}$. Let $\mathfrak{a} = (x_2, \dots, x_d)$. Note that $(x) \cap \mathfrak{a} \subseteq x\mathfrak{m}$. Indeed, if $a_1 x = \sum_{i=2}^d a_i x_i$, since the classes of $x, x_2, \dots, x_n$ in $\mathfrak{m}/\mathfrak{m}^2$ are linearly independent over k, it follows that $a_1 \in \mathfrak{m}$, hence $a_1 x \in x\mathfrak{m}$. We thus have maps

$$\mathfrak{m}/(x) = \big(\mathfrak{a} + (x)\big)/(x) \simeq \mathfrak{a}/\big((x) \cap \mathfrak{a}\big) \xrightarrow{f} \mathfrak{m}/x\mathfrak{m} \xrightarrow{g} \mathfrak{m}/(x),$$

where g is the canonical projection and f is induced by the inclusion $\mathfrak{a} \hookrightarrow \mathfrak{m}$. It is clear that $g \circ f$ is the identity, hence $\overline{m} = \mathfrak{m}/(x)$ is a direct summand of $\mathfrak{m}/x\mathfrak{m}$. Since $\mathrm{pd}_{\overline{R}}(\mathfrak{m}/x\mathfrak{m}) < \infty$, it follows from the description of projective dimension in Proposition 12.21 that $\mathrm{pd}_{\overline{R}}(\overline{m}) < \infty$, hence $\mathrm{pd}_{\overline{R}}(k) < \infty$ (if $G_\bullet$ is a projective resolution of $\overline{\mathfrak{m}}$ over $\overline{R}$, then $G_\bullet \to \overline{R}$ is a projective resolution of k over $\overline{R}$). This completes the proof of the theorem. □

As an important corollary, we deduce the fact that the property of a local ring to be regular is preserved under localization.

COROLLARY 12.34. If R is a regular ring, then for every prime ideal $\mathfrak{p}$ in R, the ring $R_\mathfrak{p}$ is regular.

PROOF. If $\mathfrak{m}$ is a maximal ideal containing $\mathfrak{p}$, then $R_\mathfrak{m}$ is regular and $R_\mathfrak{p}$ is the localization of $R_\mathfrak{m}$ at $\mathfrak{p}R_\mathfrak{m}$. Therefore we may and will assume that R is local. Since R is a regular local ring, it follows from Theorem 12.33 that $R/\mathfrak{p}$ has a finite free resolution $F_\bullet$, which induces after tensoring with $R_\mathfrak{p}$ the finite free resolution $F_\bullet \otimes_R R_\mathfrak{p}$ of the residue field $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ of $R_\mathfrak{p}$. By Corollary 12.30, the global dimension of $R_\mathfrak{p}$ is finite and another application of Theorem 12.33 gives that $R_\mathfrak{p}$ is regular. □

COROLLARY 12.35. If R is any regular ring, then $\text{gl-dim}(R) = \dim(R)$.

PROOF. Let $n = \dim(R)$ (note that this may be infinite). For every prime ideal $\mathfrak{p}$ in R, we have

$$\mathrm{pd}_R(R/\mathfrak{p}) \geq \mathrm{pd}_{R_\mathfrak{p}}(R_p/\mathfrak{p}R_\mathfrak{p}) = \mathrm{codim}(\mathfrak{p}),$$

where the inequality follows from Corollary 12.23 and the equality follows from Theorem 12.33 and Corollary 12.30. We thus have $\text{gl-dim}(R) \geq n$.

In order to prove the reverse inequality, it is enough to show that $\mathrm{pd}_R(M) \leq n$ for all finitely generated R-modules M (see Proposition 12.25). Note that it follows from Theorem 12.33 that $\mathrm{pd}_{R_\mathfrak{p}}(M_\mathfrak{p}) \leq n$ for every prime ideal $\mathfrak{p}$, and we conclude that $\mathrm{pd}_R(M) \leq n$ by Corollary 12.23. This completes the proof. □

We can now prove a result that will provide us with many examples of regular rings.

PROPOSITION 12.36. If R is a regular ring, then so is $R[x]$.

PROOF. We need to show that for every maximal ideal $\mathfrak{m}$ in $R[x]$, the localization $R[x]_\mathfrak{m}$ is regular. If $\mathfrak{p} = \mathfrak{m} \cap R$, we may replace R by $R_\mathfrak{p}$ to assume that $(R, \mathfrak{p})$ is a local regular ring (note that we use here Corollary 12.34). Since R is regular, we can write $\mathfrak{p} = (y_1, \ldots, y_n)$, where $n = \dim(R)$. Note that $R[x]/\mathfrak{p}[x] \simeq (R/\mathfrak{p})[x]$ is a PID, hence $\mathfrak{m} = \mathfrak{p}[x] + (f)$, for some polynomial $f \in R[x]$. Moreover, since $\mathfrak{m}$ is a maximal ideal we have $\mathrm{codim}\big(\mathfrak{m}/\mathfrak{p}[x]\big) = 1$; since $R \to R[x]$ is a flat homomorphism, it follows from Corollary 10.15 that $\mathrm{codim}(\mathfrak{m}) = \mathrm{codim}(\mathfrak{p}) + 1 = n + 1$. Since $\mathfrak{m}$ can be generated by $n + 1$ elements, it follows that $R[x]_\mathfrak{m}$ is regular. □

EXAMPLE 12.37. If k is a field, then it is a regular ring, and we deduce from Proposition 12.36, by induction on n, that $k[x_1, \ldots, x_n]$ is a regular ring. Similarly, if R is a Dedekind domain, then it is a regular ring, and we deduce again from Proposition 12.36, by induction on n, that $R[x_1, \ldots, x_n]$ is a regular ring.

PROPOSITION 12.38. If R is a regular ring, then R is normal.

PROOF. It is enough to show that $R_\mathfrak{m}$ is a normal ring for every maximal ideal $\mathfrak{m}$ in R, hence we may assume that R is local. Since we already know that R is a domain by Proposition 12.9, in order to check that R is normal, we may use the criterion in Proposition 8.41. First, we need to show that $R_\mathfrak{p}$ is a DVR for every prime ideal $\mathfrak{p}$ in R of codimension 1: this follows from the fact that $R_\mathfrak{p}$ is again a regular local ring by Corollary 12.34, and having dimension 1, it is a DVR (see Example 12.10).

The second property we need to check is that for every nonzero $a \in R$, and every $\mathfrak{p} \in \mathrm{Ass}_R\big(R/(a)\big)$, we have $\mathrm{codim}(\mathfrak{p}) = 1$. Note that the condition on $\mathfrak{p}$ implies that $\mathrm{depth}(\mathfrak{p}, R) = 1$. Since R is Cohen-Macaulay by Proposition 12.11, we see that indeed $\mathrm{codim}(\mathfrak{p}) = 1$ (see Proposition 11.30). This completes the proof. □

REMARK 12.39. It is an important theorem of Auslander-Buchsbaum that, in fact, every regular local ring is a UFD. For a proof, see for example [**Eis95**, Theorem 19.19].

EXERCISE 12.40. Let $f\colon (R, \mathfrak{m}) \to (S, \mathfrak{n})$ be a flat, local homomorphism of Noetherian local rings.

i) Show that if R and $S/\mathfrak{m}S$ are regular, then S is regular.
ii) Show that if S is regular, then R is regular.

iii) Give an example to show that if S is regular, it does not imply that $S/\mathfrak{m}S$ is regular.

EXERCISE 12.41. Let $(A, \mathfrak{m}) \hookrightarrow (B, \mathfrak{n})$ be an injective, finite, local ring homomorphism of Noetherian local rings, with A regular. Show that B is a Cohen-Macaulay ring if and only if it is a free A-module.

CHAPTER 13

Graded modules

13.1. Basic properties of graded modules

DEFINITION 13.1. A *graded ring* is a (commutative) ring R, together with a direct sum decomposition

$$R = \bigoplus_{i \in \mathbf{Z}} R_i,$$

as Abelian groups, such that if $a \in R_i$ and $b \in R_j$, then $ab \in R_{i+j}$. An element of R_i is *homogeneous of degree* i. We will mostly be interested in $\mathbf{N}$*-graded rings*, that is, graded rings such that $R_i = 0$ for $i < 0$.

REMARK 13.2. It follows from the above definition that if $R = \bigoplus_{i \in \mathbf{Z}} R_i$ is a graded ring, then $R_0 \subseteq R$ is a subring and every R_i is an R_0-submodule of R.

EXAMPLE 13.3. If A is any ring, then the polynomial ring $R = A[x_1, \ldots, x_n]$ can be viewed as an $\mathbf{N}$-graded ring, with R_i generated over A by the monomials of degree i. We will refer to this as the *standard grading* of the polynomial ring.

DEFINITION 13.4. If R and S are graded rings, a *homomorphism of graded rings* $f\colon R \to S$ is a ring homomorphism such that $f(R_i) \subseteq S_i$ for all $i \in \mathbf{Z}$.

REMARK 13.5. It is clear that a composition of homomorphisms of graded rings is a homomorphism of graded rings, hence graded rings form a category.

EXAMPLE 13.6. If R is a graded ring and $S \subseteq R$ is a multiplicative system that consists of homogeneous elements, then $S^{-1}R$ is naturally a graded ring such that the canonical homomorphism $R \to S^{-1}R$ is a homomorphism of graded rings: if $u \in R_m$ and $s \in S \cap R_q$, then $\frac{u}{s} \in S^{-1}R_{m-q}$. Note that even if R is $\mathbf{N}$-graded, its localization $S^{-1}R$ is typically not $\mathbf{N}$-graded.

EXAMPLE 13.7. The analogue of a field in the graded setting is a graded ring R with the property that every nonzero homogeneous element is invertible. In this case R_0 is clearly a field. If $R \neq R_0$ and t is a nonzero homogeneous element of smallest positive degree, then we have a homomorphism of R_0-algebras $f\colon R_0[x, x^{-1}] \to R$ given by $f(x) = t$. We leave as an exercise checking that if we consider on $R_0[x, x^{-1}]$ the grading such that $\deg(x) = \deg(t)$, then f is an isomorphism of graded rings.

DEFINITION 13.8. Let $R = \bigoplus_{i \in \mathbf{Z}} R_i$ be a graded ring. A *graded R-module* is an R-module M, together with a decomposition $M = \bigoplus_{i \in \mathbf{Z}} M_i$ as Abelian groups, such that if $a \in R_i$ and $u \in M_j$, then $au \in M_{i+j}$. The elements of M_i are *homogeneous of degree* i (note that by assumption, every $u \in M$ can be uniquely written as $u = \sum_i u_i$, with $u_i \in M_i$ for all $i \in \mathbf{Z}$, and all but finitely many of the u_i being 0).

REMARK 13.9. With the notation in the above definition, note that each M_i is an R_0-submodule of M.

REMARK 13.10. Often, when considering a graded R-module M, we consider a system of homogeneous generators of M. In fact, given any system $(u_\alpha)_{\alpha\in\Lambda}$ of generators of M, if we write $u_\alpha = \sum_i u_{\alpha,i}$, with $u_{\alpha,i} \in M_i$, then the nonzero $u_{\alpha,i}$ give a system of homogeneous generators of M (note that this is a finite set if the original system of generators was finite).

DEFINITION 13.11. If $R = \bigoplus_{i\in\mathbf{Z}} R_i$ is a graded ring and $M = \bigoplus_{i\in\mathbf{Z}} M_i$ and $N = \bigoplus_{i\in\mathbf{Z}} N_i$ are graded R-modules, then a *morphism of graded R-modules* $f\colon M \to N$ is an R-linear map such that $f(M_i) \subseteq N_i$ for all $i \in \mathbf{Z}$. It is clear that a composition of morphisms of graded R-modules is again a morphism of graded R-modules. Therefore graded R-modules form a category and it is straightforward to check that this is, in fact, an additive category.

EXAMPLE 13.12. We have seen that if I is an ideal in a ring A, then we have considered in Section 4.3 the Rees algebra $R(I, A) = \bigoplus_{n\geq 0} I^n$, which is a graded ring. Moreover, if M is an A-module, then $R(I, M) = \bigoplus_{n\geq 0} I^n M$ is a graded $R(I, A)$-module.

EXAMPLE 13.13. If M is a graded R-module and $a \in \mathbf{Z}$, then $M(a)$ is the graded module with the same underlying R-module, but with the grading such that $M(a)_i = M_{a+i}$.

DEFINITION 13.14. If M is a graded module over the graded ring R, then a *graded submodule* of M is a submodule N of M, which is a graded R-module, such that the inclusion map $N \hookrightarrow M$ is a homomorphism of graded modules; equivalently, we have $N = \bigoplus_{i\in\mathbf{Z}}(N \cap M_i)$. This applies in particular if $M = R$, in which case we talk about graded (also called *homogeneous*) ideals.

REMARK 13.15. Note that if M is a graded module over the graded ring R, then a submodule N of M is a graded submodule if and only if for every $u \in N$, if we write $u = \sum_i u_i$, with $u_i \in M_i$, then $u_i \in N$ for all i. This is further equivalent to the fact that N is generated as an Abelian group by homogeneous elements of M (note also that if it is generated as an R-module by homogeneous elements of M, it is also generated as an Abelian group by homogeneous elements). In what follows we will freely use these two characterizations of homogeneous submodules.

REMARK 13.16. It is clear that if N is a graded submodule of the graded R-module M, then the quotient M/N has an induced structure of graded module given by $M/N = \bigoplus_{i\in\mathbf{Z}} \big(M_i/(M_i \cap N)\big)$ and the canonical projection $M \to M/N$ is a morphism of graded modules. Similarly, if I is a homogeneous ideal in the graded ring R, then R/I has a natural structure of graded ring such that the canonical projection $R \to R/I$ is a graded ring homomorphism.

REMARK 13.17. It is straightforward to see that if $f\colon R \to S$ is a homomorphism of graded rings, then $\ker(f)$ is a homogeneous ideal of R. Similarly, if $\varphi\colon M \to N$ is a morphism of graded modules over a graded ring R, then $\ker(f)$ is a graded submodule of M (and as such it is the kernel in the category of graded R-modules) and $\mathrm{Im}(f)$ is a graded submodule of N, hence $\mathrm{coker}(f)$ has a canonical structure of graded module (and as such, it is the cokernel in the category of graded R-modules). It is then straightforward to check that the category of graded R-modules is an Abelian category.

The next result shows that when dealing with graded modules, various basic constructions still live in the graded category.

PROPOSITION 13.18. Let $M = \bigoplus_{i\in\mathbf{Z}} M_i$ be a graded module over a graded ring $R = \bigoplus_{i\in\mathbf{Z}} R_i$.

i) If $(N_\alpha)_{\alpha\in\Lambda}$ is a family of graded submodules of M, then $\sum_{\alpha\in\Lambda} N_\alpha$ and $\bigcap_{\alpha\in\Lambda} N_\alpha$ are graded submodules of M.
ii) If I is a homogeneous ideal of R, then IM is a graded submodule of M.
iii) If $u \in M$ is homogeneous, then $\mathrm{Ann}_R(u)$ is a homogeneous ideal.
iv) $\mathrm{Ann}_R(M)$ is a homogeneous ideal.

PROOF. For the first assertion in i), note that since each N_α is generated by homogeneous elements of M, the same holds for $\sum_{\alpha\in\Lambda} N_\alpha$, hence this is a graded submodule of M. The second assertion in i) follows from the fact that if $u \in \bigcap_{\alpha\in\Lambda} N_\alpha$ and we write $u = \sum_i u_i$, with $u_i \in M_i$ for all i, then $u_i \in N_\alpha$ for all i and all α, since N_α is a graded submodule; therefore $u_i \in \bigcap_{\alpha\in\Lambda} N_\alpha$ for all $i \in \mathbf{Z}$. This implies that $\bigcap_{\alpha\in\Lambda} N_\alpha$ is a graded submodule of M.

The assertion in ii) follows from the fact that if $(a_j)_{j\in J}$ are homogeneous generators of I and $(u_k)_{k\in K}$ are homogeneous generators of M, then IM is generated by the homogeneous elements $a_j u_k$, for $j \in J$ and $k \in K$, hence IM is a graded submodule.

For the assertion in iii), note that if $a \in \mathrm{Ann}_R(u)$ and $a = \sum_i a_i$ is the decomposition of a in homogeneous components, we have $0 = au = \sum_i (a_i u)$, hence $a_i u = 0$ for all i. Therefore $a_i \in \mathrm{Ann}_R(u)$ for all i and thus $\mathrm{Ann}_R(u)$ is a homogeneous ideal.

If $(u_j)_{j\in J}$ is a system of homogeneous generators of M as an R-module, then $\mathrm{Ann}_R(M) = \bigcap_{j\in J} \mathrm{Ann}_R(u_j)$ is a homogeneous ideal by iii) and i). □

For any ideal I in a graded ring R, we denote by I^* the ideal generated by all homogeneous elements of I (hence I^* is the largest homogeneous ideal contained in I).

PROPOSITION 13.19. Let I be a homogeneous ideal of a graded ring R.

i) Show that I is a prime ideal if and only if for every *homogeneous* $x, y \in R$, with $xy \in I$, we have $x \in I$ or $y \in I$.
ii) Show that I is a reduced ideal if and only if for every homogeneous $x \in R$ such that $x^n \in I$ for some positive integer n, we have $x \in I$.
iii) For every prime ideal $\mathfrak{p}$ in R, the ideal $\mathfrak{p}^*$ is a prime ideal.
iv) Every minimal prime ideal containing I is homogeneous. In particular, $\mathrm{rad}(I)$ is homogeneous, and it is an intersection of homogeneous prime ideals.

PROOF. Suppose first that we know that if $xy \in I$ and x, y are homogeneous, then $x \in I$ or $y \in I$. Suppose now that $a, b \in R \smallsetminus I$ are such that $ab \in I$. Let us write $a = \sum_i a_i$ and $b = \sum_i b_i$, with $a_i, b_i \in R_i$. Let $i_1 = \min\{i \mid a_i \notin I\}$ and $i_2 = \min\{i \mid b_i \notin I\}$. Since $ab \in I$ and I is homogeneous, by looking at the homogeneous term of degree $i_1 + i_2$ in ab, we see that $\sum_j a_{i_1+j} b_{i_2-j} \in I$. If $j > 0$, then $b_{i_2-j} \in I$ and if $j < 0$, then $a_{i_1+j} \in I$. We thus conclude that $a_{i_1} b_{i_2} \in I$, a contradiction. This proves i) and the proof of ii) is similar, so we leave it as an exercise.

By definition, $\mathfrak{p}^*$ is a homogeneous ideal. By i), in order to show that $\mathfrak{p}^*$ is prime, it is enough to show that if $x, y \in R$ are homogeneous elements and $xy \in \mathfrak{p}^*$, then $x \in \mathfrak{p}^*$ or $y \in \mathfrak{p}^*$. This is clear, since $\mathfrak{p}$ is prime, hence $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$, and a homogeneous element lies in $\mathfrak{p}$ if and only if it lies in $\mathfrak{p}^*$.

If $\mathfrak{p}$ is a minimal prime containing I, we clearly have $I \subseteq \mathfrak{p}^*$. Since $\mathfrak{p}^*$ is a prime ideal by iii), it follows that $\mathfrak{p} = \mathfrak{p}^*$, hence $\mathfrak{p}$ is a homogeneous ideal. The other assertions are clear, since $\operatorname{rad}(I)$ is the intersection of the minimal prime ideals containing I. □

PROPOSITION 13.20. If M is a graded module over the graded ring R and $\mathfrak{p} \in \operatorname{Ass}(M)$, then $\mathfrak{p}$ is a homogeneous ideal. Moreover, there is a homogeneous element $u \in M$ such that $\mathfrak{p} = \operatorname{Ann}_R(u)$.

PROOF. By hypothesis, there is $x \in M$ such that $\mathfrak{p} = \operatorname{Ann}_R(x)$. Let $a \in \mathfrak{p}$ and consider the decomposition into homogeneous terms

$$a = a_m + a_{m+1} + \ldots + a_{m+r} \quad \text{and} \quad x = x_n + x_{n+1} + \ldots + x_{n+s}.$$

In order to prove the first assertion, we need to show that $a_i x = 0$ for all i. In fact, it is enough to show that for every such a, we have $a_m x = 0$ (then replace a by $a - a_m$, and repeat the argument). We know that

$$a_m x_{n+i} + a_{m+1} x_{n+i-1} + \ldots + a_{m+i} x_n = 0 \quad \text{for all} \quad 0 \leq i \leq s.$$

We easily see by induction on i that $a_m^{i+1} x_{n+i} = 0$ for $0 \leq i \leq s$. Therefore $a_m^{s+1} \in \mathfrak{p}$ and since $\mathfrak{p}$ is prime, we conclude that $a_m \in \mathfrak{p}$. We conclude that $\mathfrak{p}$ is prime.

If $b \in \mathfrak{p}$ is homogeneous, it is clear that $b x_i = 0$ for all i. Since $\mathfrak{p}$ is generated by homogeneous elements, it follows that $\mathfrak{p} \subseteq \bigcap_{i=0}^{s} \operatorname{Ann}_R(x_{n+i})$. On the other hand, the reverse inclusion is clear, hence $\mathfrak{p} = \bigcap_{i=0}^{s} \operatorname{Ann}_R(x_{n+i})$. Since $\mathfrak{p}$ is a prime ideal, it follows that there is i, with $0 \leq i \leq s$ such that $\mathfrak{p} = \operatorname{Ann}_R(x_{n+i})$, completing the proof. □

It is a useful fact that any prime ideal in a graded ring is "close to" a homogeneous prime ideal. This is the content of the next lemma.

LEMMA 13.21. *If $\mathfrak{p}$ is a prime ideal in a graded ring R and $\mathfrak{p}$ is not homogeneous, then* $\operatorname{codim}(\mathfrak{p}/\mathfrak{p}^*) = 1$.

PROOF. After replacing R by $R/\mathfrak{p}^*$, we may assume that $\mathfrak{p}^* = (0)$ and after localizing at the set of all homogeneous elements in $R \smallsetminus \mathfrak{p}$, we may assume that every nonzero homogeneous element of R is invertible. In this case, it follows from Example 13.7 that R_0 is a field and $R \simeq R_0[x, x^{-1}]$ hence $\dim(R) = 1$. This implies the assertion in the proposition. □

The next proposition relates the codimension of a prime ideal in a Noetherian graded ring to chains of homogeneous ideals.

PROPOSITION 13.22. Let R be a Noetherian graded ring and $\mathfrak{p}$ a prime ideal in R.

i) If $\mathfrak{p}$ is homogeneous and $r = \operatorname{codim}(\mathfrak{p})$, then there is a chain of homogeneous prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_r = \mathfrak{p}. \tag{13.1}$$

ii) If $\mathfrak{p}$ is not homogeneous, then $\operatorname{codim}(\mathfrak{p}) = \operatorname{codim}(\mathfrak{p}^*) + 1$.

PROOF. Both assertions follow if we show that if $\operatorname{codim}(\mathfrak{p}) = r$, then we can find a chain of prime ideals as in (13.1), with $\mathfrak{p}_0, \ldots, \mathfrak{p}_{r-1}$ homogeneous. Indeed, in the setting of ii), we have $\mathfrak{p}_{r-1} \subseteq \mathfrak{p}^*$, hence $\operatorname{codim}(\mathfrak{p}^*) \geq r-1$, and the opposite inequality is obvious.

We argue by induction on r. The assertion is trivial if $r = 0$ and in the case $r = 1$ it follows from the fact that every minimal prime ideal contained in $\mathfrak{p}$ is homogeneous by Proposition 13.19iv). Suppose now that $r \geq 2$ and we know the assertion for $r-1$. Starting with an arbitrary chain of prime ideals as in (13.1), and applying the inductive hypothesis to $\mathfrak{p}_{r-1}$, we see that we may assume that $\mathfrak{p}_0, \ldots, \mathfrak{p}_{r-2}$ are homogeneous.

If $\mathfrak{p}$ is not homogeneous, then $\mathfrak{p}_{r-2} \subseteq \mathfrak{p}^* \subsetneq \mathfrak{p}$ and the first inclusion is strict since $\operatorname{codim}(\mathfrak{p}/\mathfrak{p}^*) = 1$ by Lemma 13.21. Therefore we can replace $\mathfrak{p}_{r-1}$ by $\mathfrak{p}^*$ and we are done in this case. Suppose now that $\mathfrak{p}$ is homogeneous. In this case there is $a \in \mathfrak{p}$ homogeneous that does not lie in $\mathfrak{p}_{r-1}$. If $\mathfrak{q} \subseteq \mathfrak{p}$ is a minimal prime ideal that contains $\mathfrak{p}_{r-2} + (a)$, then $\mathfrak{q}$ is homogeneous by Proposition 13.19iv). Since $\mathfrak{q} \neq \mathfrak{p}$ by the Principal Ideal theorem, we may replace $\mathfrak{p}_{r-1}$ by $\mathfrak{q}$ to complete the proof of the induction step. □

We end with a proposition describing when graded rings are Noetherian. For the sake of simplicity, we only consider the $\mathbf{N}$-graded case, which is the one we will be interested in.

PROPOSITION 13.23. Let $R = \bigoplus_{i \geq 0} R_i$ be an $\mathbf{N}$-graded ring.

i) R is a Noetherian ring if and only if R_0 is a Noetherian ring and R is a finitely generated R_0-algebra.
ii) If the condition in i) holds and $M = \bigoplus_{i \in \mathbf{Z}} M_i$ is a finitely generated graded R-module, then M_j is a finitely generated R_0-module for all $j \in \mathbf{Z}$.

PROOF. The "if" part in i) is a consequence of the fact that every algebra of finite type over a Noetherian ring is Noetherian (see Corollary 4.16). Suppose now that R is Noetherian. Since R_0 is isomorphic to the quotient of R by the ideal $I = \bigoplus_{i>0} R_i$, it follows that R_0 is Noetherian. Furthermore, since I is a finitely generated homogeneous ideal, we may choose a system of homogeneous generators $x_1, \ldots, x_n$ of I. Let $d_i = \deg(x_i) > 0$. We will show that R is generated as an R_0-algebra by $x_1, \ldots, x_n$. Clearly, it is enough to show that for every $m \geq 0$, any $f \in R_m$ lies in the R_0-submodule generated by the monomials $x_1^{i_1} \cdots x_n^{i_n}$ with $\sum_{k=1}^n i_k d_k = m$. We argue by induction on m, with the case $m = 0$ being clear. By assumption, given any $f \in R_m$, we can write $f = \sum_{i=1}^n f_i x_i$ and after only keeping the term in each f_i that is homogeneous of degree $m - d_i$, we may assume that $f_i \in R_{m-d_i}$ (in particular, we have $f_i = 0$ if $m > d_i$). By the inductive assumption, each f_i lies in the R_0-submodule generated by the monomials $x_1^{i_1} \cdots x_n^{i_n}$ with $\sum_{k=1}^n i_k d_k = m - d_i$, which immediately implies the assertion about f.

Suppose now that the assertion in i) holds, $x_1, \ldots, x_n$ are as above, and M is a finitely generated graded R-module. We may choose a system of homogeneous generators $u_1, \ldots, u_N$ of M, with $\deg(u_j) = a_j$ for $1 \leq j \leq N$. For every $j \in \mathbf{Z}$ and every $u \in M_j$, we may thus write $u = \sum_{i=1}^N g_i u_i$, where $g_i \in R$, and we may clearly assume that g_i is homogeneous of degree $j - a_i$. As we have seen, R_{j-a_i} is generated as an R_0-module by the monomials $x_1^{i_1} \cdots x_n^{i_n}$, with $\sum_{k=1}^n i_k d_k = j - a_i$. This implies that M_j is generated as an R_0-module by the elements $x_1^{i_1} \cdots x_n^{i_n} u_i$,

with $1 \leq i \leq N$ and $\sum_{k=1}^{n} i_k d_k = j - a_i$. In particular, M is a finitely generated R_0-module. □

13.2. Hilbert series and Hilbert polynomial

Consider an $\mathbf{N}$-graded ring $R = \bigoplus_{i \geq 0} R_i$ such that $(R_0, \mathfrak{m}_0, k)$ is a local ring. Note that the homogeneous ideal $\mathfrak{m} = \mathfrak{m}_0 \oplus \bigoplus_{i>0} R_i$ is a maximal ideal (since $R/\mathfrak{m} \simeq k$) and every proper homogeneous ideal of R is contained in $\mathfrak{m}$: this is due to the fact that every homogeneous element in $R \smallsetminus \mathfrak{m}$ is invertible. From many points of view, graded modules over such a ring behave like modules over a local ring. We will discuss this in more detail in the next section, but we now give a result that allows us to reduce to the local case when considering the dimension of a module.

PROPOSITION 13.24. Let R be a Noetherian $\mathbf{N}$-graded ring such that $(R_0, \mathfrak{m}_0)$ is a local ring and let $\mathfrak{m} = \mathfrak{m}_0 \oplus \bigoplus_{i>0} R_i$. For every nonzero finitely generated R-module M, we have

$$\dim(M) = \dim(M_{\mathfrak{m}}).$$

PROOF. Recall that $I = \operatorname{Ann}_R(M)$ is a homogeneous ideal by Proposition 13.18, hence it is contained in $\mathfrak{m}$. We need to show that for every prime ideal $\mathfrak{p}$ in $\operatorname{Supp}(M)$, we have $\operatorname{codim}(\mathfrak{p}/I) \leq \operatorname{codim}(\mathfrak{m}/I)$. This is clear if $\mathfrak{p}$ is homogeneous. Otherwise, since $\mathfrak{m}$ is a maximal ideal we have $\mathfrak{p}^* \subsetneq \mathfrak{m}$ and thus

$$\operatorname{codim}(\mathfrak{p}/I) = 1 + \operatorname{codim}(\mathfrak{p}^*/I) \leq \operatorname{codim}(\mathfrak{m}/I),$$

where the first equality follows by applying Proposition 13.22 in R/I. This completes the proof. □

From now on, in this section we assume that R is a Noetherian $\mathbf{N}$-graded ring, with R_0 local and 0-dimensional (note that R_0 is automatically Noetherian by Proposition 13.23). If M is a finitely generated graded R-module, then it follows from Proposition 13.23 that all M_i are finitely generated R_0-modules. Since $\dim(R_0) = 0$, we have $\ell_{R_0}(M_i) < \infty$ for all i by Proposition 7.23.

We now introduce a very important invariant of finitely generated graded modules:

DEFINITION 13.25. For a finitely generated R-module M, we put $H(M, i) = \ell_{R_0}(M_i)$ for $i \in \mathbf{Z}$, and the *Hilbert series* of M is the series

$$H_M(t) := \sum_{i \in \mathbf{Z}} H(M, i) t^i.$$

REMARK 13.26. Note that $H_M(t)$ is a Laurent power series, that is, we have $\ell_{R_0}(M_i) = 0$ for $i \ll 0$. Indeed, if M is generated by the homogeneous elements $u_1, \ldots, u_N$, with $\deg(u_i) = d_i$, since R is $\mathbf{N}$-graded, it follows that $M_i = 0$ if $i < \min\{d_j \mid 1 \leq j \leq N\}$.

EXAMPLE 13.27. Note that for every R-module M and every $a \in \mathbf{Z}$, we have $H\big(M(a), i\big) = H(M, a + i)$, hence $H_{M(a)}(t) = t^{-a} \cdot H_M(t)$.

PROPOSITION 13.28. Given a short exact sequence of finitely generated R-modules

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

we have $H_M(t) = H_{M'}(t) + H_{M''}(t)$.

PROOF. The assertion follows from the additivity of length in short exact sequences. □

COROLLARY 13.29. If M is a finitely generated R-module and $f \in R_d$ is a non-zero-divisor on M, then

$$H_{M/fM}(t) = (1 - t^d) \cdot H_M(t).$$

PROOF. Since f is a non-zero-divisor on M, multiplication by f gives a short exact sequence of graded R-modules

$$0 \to M(-d) \xrightarrow{\cdot f} M \longrightarrow M/fM \to 0.$$

The assertion then follows from the proposition, together with Example 13.27. □

EXAMPLE 13.30. Let $R = R_0[x_1, \ldots, x_n]$, with the standard grading. Since $x_1, \ldots, x_n$ is a regular sequence in R, applying Corollary 13.29 n times and using the fact that $H_{R_0}(t) = \ell(R_0)$, we conclude that

$$H_R(t) = \ell(R_0) \cdot \frac{1}{(1-t)^n}.$$

The formula

$$\frac{1}{(1-t)} = \sum_{k \geq 0} t^k$$

gives after differentiating $(n-1)$ times

$$\frac{1}{(1-t)^n} = \sum_{k \geq 0} \binom{k+n-1}{n-1} t^k.$$

We thus conclude that the number $N(n,k)$ of monomials of degree k in n variables is $\binom{k+n-1}{n-1}$.

Note that since R is Noetherian, it follows from Proposition 13.23 that R is a finitely generated R_0-algebra. From now on, for the sake of simplicity, we may one more assumption: we assume that R is generated over R_0 by finitely many elements of degree 1. Equivalently, R is isomorphic, as a graded ring, to a quotient of some $R_0[x_1, \ldots, x_n]$, where we consider $R_0[x_1, \ldots, x_n]$ with the standard grading. We note that for a finitely generated R-module M, the Hilbert series is the same whether we consider M as an R-module or as an $R_0[x_1, \ldots, x_n]$-module. The following is the main result of this section.

THEOREM 13.31. *Let R be an $\mathbf{N}$-graded ring, generated over R_0 by finitely many elements of degree 1, with R_0 local, Noetherian, and 0-dimensional. If M is a graded nonzero R-module, then there is a polynomial $P_M \in \mathbf{Q}[x]$ of degree*[1] $\dim(M) - 1$ *such that $H_M(i) = P_M(i)$ for $i \gg 0$.*

The polynomial P_M in the theorem is the *Hilbert polynomial* of M.

PROOF OF THEOREM 13.31. We argue by induction on $\dim(M) = d$. Let us first show that we get the assertion for M if we know it for all quotients $R/\mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal with $\dim(R/\mathfrak{p}) \leq d$. Indeed, we have seen in Proposition 13.20 that if $\mathfrak{p}_1$ is an associated prime of M, then $\mathfrak{p}_1$ is a homogeneous ideal and there is $u \in M$ homogeneous such that $\mathfrak{p}_1 = \mathrm{Ann}_R(u)$. If $d_1 = \deg(u)$, then we have an

[1] We make the convention here that the degree of the zero polynomial is equal to -1.

injective graded homomorphism $R/\mathfrak{p}_1(-d_1) \hookrightarrow M$ that maps the class of 1 to u. Iterating this observation and using the fact that M is Noetherian as in the proof of Theorem 5.5, we get a sequence of graded submodules

$$0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_r = M$$

such that $M_j/M_{j-1} \simeq R/\mathfrak{p}_j(-d_j)$ for $1 \leq j \leq r$, where $\mathfrak{p}_j$ is a homogeneous prime ideal and $d_j \in \mathbf{Z}$. By Proposition 13.28, we have

$$H(M,n) = \sum_{j=1}^{r} H(M_j/M_{j-1},n) = \sum_{j=1}^{r} H(R/\mathfrak{p}_j, n-d_j) \quad \text{for all} \quad n \in \mathbf{Z}.$$

Note that $\dim(M) = \max\big\{\dim(R/\mathfrak{p}_j) \mid 1 \leq j \leq r\big\}$ since we have

$$\operatorname{Supp}(M) = \bigcup_{j=1}^{r} \operatorname{Supp}(R/\mathfrak{p}_j)$$

by Exercise 5.12. It follows that if we know the assertion in the theorem for each $R/\mathfrak{p}_j$, then we get the assertion for M (note that each $P_{R/\mathfrak{p}_j}$ has positive leading term since $P_{R/\mathfrak{p}_j}(i) \geq 0$ for $i \gg 0$, hence the degree of $\sum_{j=1}^{r} P_{R/\mathfrak{p}_j}(m-d_j)$ is $\max\big\{\deg(P_j) \mid 1 \leq j \leq r\big\}$).

In order to prove the case $d = 0$, it is thus enough to consider a homogeneous prime ideal $\mathfrak{p}$ in R with $\dim(R/\mathfrak{p}) = 0$, so $\mathfrak{p}$ is a maximal ideal. Since $\mathfrak{p} \subseteq \mathfrak{m} = \mathfrak{m}_0 \oplus \bigoplus_{i>0} R_i$, it follows that $\mathfrak{p} = \mathfrak{m}$. In this case we have $H(R/\mathfrak{p}, i) = 0$ for $i \geq 1$, hence $P_{R/\mathfrak{p}_j} = 0$.

Suppose now that we know the assertion in the theorem for modules of dimension $< d$ and let us consider a homogeneous prime ideal $\mathfrak{p}$ in R, with $\dim(R/\mathfrak{p}) = d > 0$. Since R is generated as an R_0-algebra by R_1 and $\mathfrak{p} \neq \mathfrak{m}$, it follows that there is $f \in R_1 \smallsetminus \mathfrak{p}$. In this case we have a short exact sequence

$$0 \to R/\mathfrak{p}(-1) \xrightarrow{\cdot f} R/\mathfrak{p} \to N \to 0,$$

where $N = R/(\mathfrak{p} + Rx)$. Note that it follows from Proposition 13.28 that

$$H(R/\mathfrak{p}, i) - H(R/\mathfrak{p}, i-1) = H(N,i) \quad \text{for all} \quad i \in \mathbf{Z}.$$

Moreover, we have $\dim(N) = \dim(R/\mathfrak{p}) - 1$ (this follows by applying Exercise 7.47 for the corresponding localizations at $\mathfrak{m}$ and using Proposition 13.24). The assertion in the proposition now follows from the following elementary fact: if $f\colon \mathbf{Z} \to \mathbf{Z}$ is a function and P is a polynomial of degree $d-1$ such that $f(i) - f(i-1) = P(i)$ for all $i \gg 0$, then there is a polynomial P of degree d such that $f(i) = P(i)$ for all $i \gg 0$. □

Remark 13.32. It is elementary to deduce from the theorem that if R and M are as in the statement of the theorem, then the Hilbert series $H_M(t)$ is a rational function. However, by arguing as in the proof of the theorem, we can be more precise: if $d = \dim(M)$, then we can write $H_M(t) = \frac{Q(t)}{(1-t)^d}$, for some Laurent polynomial $Q \in \mathbf{Z}[t, t^{-1}]$.

13.3. Graded free resolutions

We begin by discussing in more detail the case of an $\mathbf{N}$-graded ring $R = \bigoplus_{i \geq 0} R_i$ such that $(R_0, \mathfrak{m}_0, k)$ is a local ring. Let $\mathfrak{m} = \mathfrak{m}_0 \oplus \bigoplus_{i>0} R_i$. We first

show that for graded modules, we don't lose information by localizing at $\mathfrak{m}$ (we have already seen an instance of this in Proposition 13.24).

PROPOSITION 13.33. With the above notation, if M is a graded R-module, then $M = 0$ if and only if $M_{\mathfrak{m}} = 0$.

PROOF. It is enough to prove the 'if' part. If $M_{\mathfrak{m}} = 0$, it follows that for every homogeneous element $u \in M$, we have $\mathrm{Ann}_R(u) \not\subseteq \mathfrak{m}$ Since $\mathrm{Ann}_R(u)$ is a homogeneous ideal, it follows that $\mathrm{Ann}_R(u) = R$, hence $u = 0$. Using the fact that M is generated by homogeneous elements, we conclude that $M = 0$. □

COROLLARY 13.34 (Graded Nakayama's lemma). Let M be a finitely generated graded R-module and N a graded submodule. If $M = N + \mathfrak{m}M$, then $M = N$.

PROOF. After replacing M by M/N, we see that we may assume $N = 0$. The hypothesis and Nakayama's lemma implies that $M_{\mathfrak{m}} = 0$, hence $M = 0$ by the proposition. □

REMARK 13.35. It is a consequence of the above corollary that if $u_1, \ldots, u_n \in M$ are homogeneous elements, then $u_1, \ldots, u_n$ generate M if and only if their classes in $M/\mathfrak{m}M$ generate this module over $R/\mathfrak{m} \simeq k$. In particular, a minimal system of homogeneous generators corresponds to a k-basis of $M/\mathfrak{m}M$.

COROLLARY 13.36. A sequence of graded modules

$$M' \xrightarrow{f} M \xrightarrow{g} M'',$$

is exact if and only the corresponding sequence of $R_{\mathfrak{m}}$-modules

$$M'_{\mathfrak{m}} \to M_{\mathfrak{m}} \to M''_{\mathfrak{m}}$$

is exact.

PROOF. It is enough to show that if A and B are two submodules of M such that $A_{\mathfrak{m}} \subseteq B_{\mathfrak{m}}$, then $A \subseteq B$ (apply this with A and B being $\ker(g)$ and $\mathrm{Im}(f)$ and vice versa). This follows by applying Proposition 13.34 with $M = (A + B)/B$. □

DEFINITION 13.37. A *free graded R-module* is a graded module M that has a basis given by homogeneous elements; equivalently, M is isomorphic to a direct sum of graded modules of the form $R(a)$, with $a \in \mathbf{Z}$.

Suppose now that R is also Noetherian. Given any finitely generated R-module M, if $u_1, \ldots, u_n$ is a system of homogeneous generators of M, with $\deg(u_i) = d_i$, then we get a surjective morphism of graded R-modules $p\colon F = \bigoplus_{i=1}^n R(-d_i) \to M$, that maps the standard generators e_i of $R(-d_i)$ to u_i. Note that if $u_1, \ldots, u_n$ is a minimal system of homogeneous generators, then $\ker(p) \subseteq \mathfrak{m}F$. Since R is Noetherian, $\ker(p)$ is a finitely generated graded R-module and we can iterate this construction to get an exact complex

$$\ldots \to F_n \xrightarrow{d_n} F_{n-1} \to \ldots \to F_1 \xrightarrow{d_1} F_0 \to M \to 0,$$

such that each F_n is a finitely generated free graded R-module and $d_n(F_n) \subseteq \mathfrak{m}F_{n-1}$ for all $n \geq 1$. Such a complex is a *minimal graded free resolution* of M. Note that $F_\bullet \otimes_R R_{\mathfrak{m}}$ is a minimal free resolution of $M_{\mathfrak{m}}$.

REMARK 13.38. As in the local case, such a minimal graded free resolution is unique, up to a non-canonical isomorphism. Indeed, given two such minimal resolutions, it follows from Proposition 9.84 that there is a morphism of complexes $\varphi\colon F_\bullet \to G_\bullet$ that induces the identity on M. Moreover, it is easy to see, from the construction of φ, that we may assume that each φ_m is a morphism of graded modules. It follows from Remark 12.28 that $\varphi \otimes_R R_{\mathfrak{m}}$ is an isomorphism between the corresponding minimal free resolutions of $M_{\mathfrak{m}}$, and thus φ is an isomorphism by Corollary 13.36.

In particular, this implies that each graded free R-module F_i in the minimal free resolution of M is uniquely determined, up to isomorphism. If we write

$$F_i \simeq \bigoplus_{j\in\mathbf{Z}} R(-j)^{b_{i,j}(M)},$$

then the numbers $b_{i,j}(M)$ are the *graded Betti numbers* of M and they are important invariants of M (note that $b_{i,j}(M) = \dim_k(F_i/\mathfrak{m}F_i)_j$, hence it is independent of any choices).

PROPOSITION 13.39. Let $R = \bigoplus_{i\geq 0} R_i$ be a Noetherian $\mathbf{N}$-graded ring, with $(R_0, \mathfrak{m}_0)$ a local ring, and let $\mathfrak{m} = \mathfrak{m}_0 \oplus \bigoplus_{i>0} R_i$. For every finitely generated graded R-module M and every $n \in \mathbf{Z}_{\geq 0}$, the following are equivalent:

i) $\mathrm{pd}_R(M) \leq n$.
ii) $\mathrm{pd}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}}) \leq n$.
iii) If $F_\bullet$ is the minimal graded free resolution of M, then $F_{n+1} = 0$.

PROOF. The implication i)⇒ii) is a general fact (see Corollary 12.23). The implication ii)⇒iii) follows from Corollary 12.29, since $F_\bullet \otimes_R R_{\mathfrak{m}}$ is a minimal free resolution of $M_{\mathfrak{m}}$ over $R_{\mathfrak{m}}$. We use here that $F_i \otimes_R R_{\mathfrak{m}} = 0$ if an only if $F_i = 0$ (we don't even need Proposition 13.33 since each F_i is a free R-module). Finally, the implication iii)⇒i) is clear. □

REMARK 13.40. A special case of the above proposition is that if M is a finitely generated graded R-module, then M is projective if and only if it is a free graded module.

The following result is *Hilbert's Syzygy Theorem.*

THEOREM 13.41. *If k is a field, $R = k[x_1, \ldots, x_n]$ is a polynomial ring with the standard grading*[2]*, and M is a finitely generated R-module, then M has a finite graded free resolution*

$$0 \to F_n \to \ldots \to F_0 \to M \to 0.$$

PROOF. We know that R is a regular ring (see Example 12.37) and $\dim(R) = n$, hence $\text{gl-dim}(R) = n$ by Corollary 12.34. In particular, we have $\mathrm{pd}_R(M) \leq n$, so if $F_\bullet$ is the graded free resolution of M, we have $F_{n+1} = 0$ by Proposition 13.39, and we get the assertion in the theorem. □

REMARK 13.42. If M is a finitely generated graded R-module, where $R = k[x_1, \ldots, x_n]$, with the standard grading, then the graded Betti numbers of M give

[2]In fact, we may consider on R any grading such that $R_0 = k$.

a more refined information than the Hilbert series $H_M(t)$. Indeed, suppose that $F_\bullet$ is the minimal graded free resolution of M. If we write

$$F_i = \bigoplus_j R(-j)^{b_{i,j}(M)} \quad \text{for} \quad 0 \leq i \leq n,$$

then it follows from Proposition 13.28 that

$$H_M(t) = \sum_{i=0}^{n} (-1)^i H_{F_i}(t) = \frac{1}{(1-t)^n} \cdot \sum_{i=0}^{n} \sum_{j \in \mathbf{Z}} (-1)^i b_{i,j}(M) t^j.$$

In particular, we get another proof of the rationality of the Hilbert function of M in this case.

Bibliography

[DF04] D. Dummit and R. Foote, *Abstract algebra* third edition, John Wiley & Sons, Inc., Hoboken, NJ, 2004. 54

[Eis95] D. Eisenbud, *Commutative algebra. With a view toward algebraic geometry*, Graduate Texts in Mathematics, 150, Springer-Verlag, New York, 1995 vii, 58, 124

[Mat89] H. Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics, 8, second edition, translated from the Japanese by M. Reid, Cambridge University Press, Cambridge, 1989. vii, 41, 60, 113

[Mum99] D. Mumford, The red book of varieties and schemes, Lecture Notes in Mathematics, 1358, second, expanded edition, includes the Michigan lectures (1974) on curves and their Jacobians; with contributions by Enrico Arbarello, Springer-Verlag, Berlin, 1999. 27, 45