Commutative Algebra: an introductory course

Luís Duarte

November 13, 2026

These are notes for the course on Commutative Algebra I will teach in the Fall of 2026 at Stockholm University. This is intended to be an introductory course to the topic of commutative rings, with some emphasis on homological tools. As such, it is mostly recommended for graduate students who are relatively new to the topics of Commutative Algebra or Homological Algebra. The notes are written to be self contained and are heavily inspired by the following famous books on Commutative Algebra: Atiyah&McDonald [AM69], Matsumura [Mat86] and Bruns&Herzog [BH98] (all of which I recommend). The content of this document will be constantly updated and expanded. For now, you might find typos or innacuracies. Please inform me of them.

Contents

1 The basics **3**
1.1 Basic definitions . . . 3
1.1.1 Commutative rings . . . 3
1.1.2 Ideals . . . 3
1.1.3 Modules . . . 6
1.2 Maximal ideals, prime ideals and Spectrum . . . 8
1.3 Nakayama's lemma and minimal generating sets . . . 10
1.4 Localization . . . 12
1.5 Complexes and short exact sequences . . . 15
1.6 Hom and tensor . . . 16
1.6.1 The Hom functor . . . 16
1.6.2 The tensor product . . . 18
1.6.3 Tensor-Hom adjointness and exactness of the tensor product . . . 20
1.7 Noetherian rings and modules . . . 22
1.8 Artinian rings and modules . . . 25
1.8.1 Length . . . 25
1.8.2 The Artinian property . . . 27

2 Primary decomposition **30**
2.1 The radical of an ideal . . . 30
2.2 Minimal primes . . . 31
2.3 Associated primes . . . 32
2.4 Primary ideals . . . 35
2.5 Primary decomposition . . . 36

3 Graded Rings **38**
3.1 Graded rings and modules . . . 38
3.2 Hilbert functions . . . 40
3.3 The associated graded ring . . . 42

4 Dimension theory **45**
4.1 Height and dimension . . . 45
4.2 A local perspective of dimension . . . 47
4.3 Height theorems . . . 49
4.4 A graded perspective of dimension . . . 50

5 Basics of homological algebra **53**
5.1 Maps of complexes . . . 53
5.2 Projective and injective resolutions . . . 56
5.3 Tor and Ext . . . 59
5.4 Minimal free resolutions . . . 63

6 Regular sequences **68**
6.1 Regular sequences . . . 68
6.2 Depth . . . 70
6.3 The Koszul complex . . . 72

1 The basics

1.1 Basic definitions

1.1.1 Commutative rings

Definition 1.1.1. (Ring) A *ring* is an abelian group $(R, +)$ together with a multiplication operation $(a, b) \mapsto ab$ satisfying the distributive property:

$$\begin{aligned}(a+b)c &= ac+bc \quad \forall a,b,c \in R \\ a(b+c) &= ab+ac \quad \forall a,b,c \in R.\end{aligned}$$

R is said to contain an *identity element* if there exists an element $1 \in R$ such that

$$1r = r1 = r \quad \forall r \in R.$$

A ring R is said to be *commutative* if the multiplication operation is commutative, i.e.,

$$ab = ba \quad \forall a, b \in R.$$

In this course, 'ring' will *always* mean a commutative ring with identity.

Definition 1.1.2. A *ring homomorphism* is a map $f : R \to S$ from a (commutative) ring R to a (commutative) ring S satisfying, for every $r_1, r_2 \in R$,

$$\begin{aligned}f(r_1+r_2) &= f(r_1)+f(r_2) \\ f(r_1r_2) &= f(r_1)f(r_2) \\ f(1) &= 1.\end{aligned}$$

Definition 1.1.3. A subset S of a ring R is said to be a *subring* of R is it is closed under addition and multiplication and if it contains the identity of R.

Let $R_1, R_2, \ldots$ be commutative rings. Their *direct product*

$$R = \prod_{i=1}^{\infty} R_i$$

is the set of all sequences $r = (r_1, r_2, \ldots)$ with $r_i \in R_i$ for every $i \geq 0$. R is a ring with componentwise addition and multiplication and identity given by $(1, 1, \ldots)$. The projections $p_i : R \to R_i$ given by $p_i(r) = r_i$ are ring homomorphisms.

Example 1.1.4.

1. Fields are examples of rings. However, these are very uninteresting for the kind analysis of rings we will be making.
2. $\mathbb{Z}$ is a commutative ring.
3. The polynomial ring $k[x_1, \ldots, x_n]$ in n variables over a field k is a commutative ring. More generally, we can consider the ring $R[x_1, \ldots, x_n]$ of polynomials with coefficients in a commutative ring R.
4. The power series ring $k[\![x_1, \ldots, x_n]\!]$, whose elements are infinite power series $\sum_{\alpha \in \mathbb{N}^n} a_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with coefficients a_α in a field k, with the usual sum and multiplication of power series, is a commutative ring ($0 \in \mathbb{N}$).

1.1.2 Ideals

Definition 1.1.5. A subset I of a ring R is called an *ideal* of R if I is closed under addition and is invariant under multiplication by any element of R, i.e., if

$$\begin{aligned}a+b &\in I \quad \forall a,b \in I \\ ra &\in I \quad \forall a \in I, r \in R.\end{aligned}$$

An ideal I can be defined by giving a set of generators for it.

Definition 1.1.6. We say that a subset $\{a_\lambda\}_{\lambda\in\Lambda}$ of R is a *generating set* (or a *set of generators*) for an ideal I if the set of all finite R-linear combinations of elements a_λ equals I. i.e., if

$$I = \{r_1 a_{\lambda_1} + \cdots + r_n a_{\lambda_n} : n \geq 1, r_1, \ldots, r_n \in R, \lambda_1, \ldots, \lambda_n \in \Lambda\}.$$

In this case we write $I = (a_\lambda : \lambda \in \Lambda)$ to say that I is *generated by* $\{a_\lambda\}_{\lambda\in\Lambda}$.

We say that I is *finitely generated* if I has a finite set of generators. In other terms, if there exist $a_1, \ldots, a_n \in R$ such that $I = (a_1, \ldots, a_n)$.

An ideal is said to be *principal* if it can be generated by a single element.

Example 1.1.7.

1. If R is a field, then R only has two ideals: (0) and R.
2. In $\mathbb{Z}[x]$, the ideal $(2, x)$ consists of the set of polynomials in x with coefficients in $\mathbb{Z}$ whose constant terms are even.
3. Every ideal in $\mathbb{Z}$ is of the form (n) with $n \in \mathbb{Z}$. In other words, every ideal of $\mathbb{Z}$ is principal.

Operations on ideals: Let I and J be ideals of a ring R.

- *(sum)* The sum of I and J is the ideal

  $$I + J = \{a + b : a \in I, b \in J\}.$$

  More generally, if $(I_i)_{i\in\Lambda}$ is a (possibly infinite) family of ideals of R, then the ideal $\sum_{i\in\lambda} I_i$ is the ideal consisting of all finite sums of the form $r_{i_1} + \cdots + r_{i_n}$, where $n \geq 1$ and $r_{i_j} \in I_{i_j}$, with $i_1, \ldots, i_n \in \Lambda$.

- *(product)* The product IJ of I and J is the ideal of R generated by all products of elements of I with elements of J:

  $$IJ = (ab : a \in I, b \in J).$$

  (Notice that this is not the set $\{ab : a \in I, b \in J\}$, as this would not be an ideal in general). If I is generated by $a_1, \ldots, a_r$ and J is generated by $b_1, \ldots, b_s$, then one can check that IJ is generated by all the elements $a_i b_j$ with $1 \leq i \leq r$ and $1 \leq j \leq s$.

  Similarly, one can define the product of any finite number of ideals and, consequently, the powers I^n of an ideal I:

  $$I^n = (r_1 \cdots r_n : r_1, \ldots, r_n \in I).$$

  Notice that the sum and product of ideals is distributive: $I(J + K) = IJ + IK$ for all ideals I, J, K of R.

- *(intersection)* For any family $(I_i)_{i\in\Lambda}$ of ideals of R, the intersection $\bigcap_{i\in\lambda} I_i$ is also an ideal of R. Observe that $IJ \subseteq I \cap J$ always holds.

- *(union)* If $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ is an ascending chain of ideals of R, then the union $\bigcup_{i=1}^{\infty} I_i$ is also an ideal of R. In general, however, the union of ideals is not an ideal.

- *(colon)* The *colon ideal* $I : J$ is defined as

  $$I : J = \{r \in R : rJ \subseteq I\}.$$

  This is an ideal of R. The following identities can be checked easily from the definition:

  (1) $I \subseteq (I : J)$.

  (2) $J(I : J) \subseteq I$.

  (3) $(I : JK) = ((I : J) : K) = ((I : K) : J)$.

  (4) $(\bigcap_i I_i : J) = \bigcap_i (I_i : J)$.

  (5) $(I : \sum_i J_i) = \bigcap_i (I : J_i)$.

The quotient ring:

If I is an ideal of the ring R, then the quotient group $R/I = \{r + I : r \in R\}$ inherits the structure of a ring, with multiplication induced by the multiplication in R, i.e., multiplication in R/I is given by

$$(r_1 + I)(r_2 + I) = r_1 r_2 + I \quad \forall r_1, r_2 \in R$$

(check that this is well defined). R/I is called the *quotient ring* or *residue class ring* of I.

Proposition 1.1.8. *Let I be an ideal of a ring R. There exists a one to one correspondence between the ideals of R/I and the ideals of R that contain I.*

Proof. Consider the projection ring homomorphism $\pi : R \longrightarrow R/I$. If J is an ideal of R that contains I, then $\pi(J)$ is an ideal of R/I. Conversely, Let J' be an ideal of R/I and take $J = \pi^{-1}(J')$. One easily verifies that J is an ideal of R. Moreover, since $\pi(I) = 0 \subseteq J'$, we have that $I \subseteq J$. We conclude that π provides a bijection between the ideals of R that contain I and the ideals of R/I. □

Hence, when one wants to focus on studying ideals that contain I, it is useful to shift focus to the study of the ring R/I.

Generalizing the chinese remainder theorem:

Definition 1.1.9. We say that two ideals I and J of a ring R are *coprime* if $I + J = R$. Equivalently, if we can write the identity of R as $1 = a + b$ with $a \in I$ and $b \in J$.

This matches the notion of coprime integer numbers since, given $n, m \in \mathbb{Z}$, one can write $1 = an + bm$ with $a, b \in \mathbb{Z}$ if and only if $\gcd(n, m) = 1$.

Notice that if I and J are coprime ideals, then $IJ = I \cap J$. Indeed, the inclusion $IJ \subseteq I \cap J$ always holds. For the reverse inclusion, suppose $x \in I \cap J$. Write $1 = a + b$ with $a \in I, b \in J$. Then $x = 1x = (a + b)x = ax + bx \in IJ$ since $ax \in I(I \cap J) \subseteq IJ$ and $bx \in J(I \cap J) \subseteq IJ$. This can be generalized.

Proposition 1.1.10. *Let $I_1, \ldots, I_n$ be pairwise coprime ideals of a ring R (i.e., such that I_i and I_j are coprime whenever $i \neq j$). Then*

$$\bigcap_{i=1}^{n} I_i = \prod_{i=1}^{n} I_i.$$

Proof. The proof goes by induction on n. We have already discussed the case $n = 2$. Suppose $n > 2$ and that the result is valid for $n - 1$. Then $J = I_1 \cdots I_{n-1} = I_1 \cap \cdots \cap I_{n-1}$. The identity we want to show can thus be stated as $I_n \cap J = I_n J$ and, by the $n = 2$ case, it will follow if we show that $I_n + J = R$. As I_n is coprime with I_j for any $1 \leq j \leq n - 1$, there exist $a_j \in I_n$ and $b_j \in I_j$ such that $a_j + b_j = 1$. Thus

$$b = b_1 \cdots b_{n-1} = (1 - a_1) \cdots (1 - a_{n-1}) = 1 - a$$

for some $a \in I_n$. As $b \in I_1 \cdots I_{n-1} = J$, this shows that I_n and J are coprime. □

Theorem 1.1.11. *Let R be a ring and $I_1, \ldots, I_n$ ideals of R. Consider the ring homomorphism*

$$\begin{aligned} \phi \colon R &\longrightarrow R/I_1 \oplus \cdots \oplus R/I_n \\ r &\longmapsto (r + I_1, \ldots, r + I_n) \end{aligned}.$$

Then ϕ is surjective if and only if $I_1, \ldots, I_n$ are pairwise coprime.

Proof. ($\Rightarrow$) : It is enough to show that if ϕ is surjective then $I_1 + I_2 = R$. There must exist $r \in R$ such that $\phi(r) = (1 + I_1, 0 + I_2, \ldots)$. Such an r must satisfy $r \in I_2$ and $1 - r \in I_1$. Thus $1 = (1 - r) + r \in I_1 + I_2$.

($\Leftarrow$) : It is easy to see that it is enough to show that $(1 + I_1, 0 + I_2, \ldots, 0 + I_n)$ is in the image of ϕ. For that, we must show that there exists $r \in R$ such that $1 - r \in I_1$ and $r \in I_2 \cap \cdots \cap I_n =: J$. Such an r exists if and only if I_1 and J are coprime. By the proof of Proposition 1.1.10, this holds if $I_1, \ldots, I_n$ are pairwise coprime. □

Remark 1.1.12. Notice that the homomorphism ϕ of Theorem 1.1.11 has kernel equal to $I_1 \cap \cdots \cap I_n$. Thus, it is injective if and only if $I_1 \cap \cdots \cap I_n = 0$.

1.1.3 Modules

Definition 1.1.13. Let R be a (commutative) ring. An *R-module* M is an additive group M together with an action of R on M which satisfies the following axioms for all $a, b \in R$ and all $x, y \in M$:

$$\begin{aligned} a(x+y) &= ax + ay \\ (a+b)x &= ax + bx \\ (ab)x &= a(bx) \\ 1x &= x. \end{aligned}$$

A module over a ring is the analogue of a vector space over a field. In fact, if R is a field, the R-modules are exactly the vector spaces over R.

Definition 1.1.14. Let M be an R-module. A subset M' of M is a *submodule* of M is M' is closed under addition and under multiplications by elements of R.

If M' is a submodule of M, then the abelian group M/M' inherits the structure of an R-module, with the action of R on M/M' being given by

$$a(x + M') = (ax) + M'$$

for all $a \in R$, $x \in M$. The module

$$M/M'$$

is called the *quotient* module of M by M'.

Definition 1.1.15. Let M and N be R-modules. An R-homomorphism (or an R-linear map) from M to N is a mapping $f : M \to N$ such that

$$\begin{aligned} f(x+y) &= f(x) + f(y) \\ f(ax) &= af(x) \end{aligned}$$

for all $a \in R$ and all $x, y \in M$. The *kernel* and *cokernel* of f are, respectively,

$$\begin{aligned} \ker f &= \{x \in M : f(x) = 0\} \\ \operatorname{coker} f &= N/\operatorname{im} f. \end{aligned}$$

Proposition 1.1.16. (The isomorphism theorems) *Let R be a ring.*

1. *If $f : M \to N$ is an R-module homomorphism, then*

$$M/\ker f \cong \operatorname{im} f.$$

2. *If $M \supseteq N \supseteq L$ are R-modules, then*

$$(M/L)/(N/L) \cong M/N.$$

3. *If M_1 and M_2 are submodules of M, then*

$$\frac{M_1 + M_2}{M_2} \cong \frac{M_1}{M_1 \cap M_2}.$$

Direct sums of modules:

Given a family of R-modules $\{M_\lambda\}_{\lambda \in \Lambda}$, we can form their *direct product*

$$M = \prod_{\lambda \in \Lambda} M_\lambda,$$

which, as a set, consists of all tuples $r = (r_\lambda)$ with $r_\lambda \in M_\lambda$. M is an R-modules componentwise addition and scalar multiplication. The projections $\pi_\lambda : M \to M_\lambda$ given by $p_\lambda(r) = r_\lambda$ are R-modules homomorphisms.

The *direct sum*

$$S = \bigoplus_{\lambda \in \Lambda} M_\lambda$$

of the family $\{M_\lambda\}_{\lambda \in \Lambda}$ consists of all tuples $r = (r_\lambda)$ with $r_\lambda \in M_\lambda$ for which only a finite number of the r_λ are non-zero. Again with componentwise addition and scalar multiplication, M is a new R-module. Naturally, the direct sum and direct product coincide for a finite family of R-modules.

We denote by M^n the direct sum $M \oplus \cdots \oplus M$ of n copies of an R-module M.

Generating sets and free modules:

Given a subset $\Gamma \subseteq M$, the smallest submodule of M that contains Γ is the submodule $\sum_{m \in \Gamma} Rm$, which consists of all finite R-linear combinations of elements of Γ:

$$\sum_{m \in \Gamma} Rm = \{a_1 m_1 + \cdots + a_s m_s : s \geq 1, a_i \in R, m_i \in \Gamma\}.$$

We say that Γ *generates* M (or is a *generating set of* M), if $M = \sum_{m \in \Gamma} Rm$.

M is said to be *finitely generated* if there exists a finite generating set of M, that is, if there exists a finite number of elements $m_1, \ldots, m_s \in M$ such that $M = Rm_1 + \cdots + Rm_s$.

Definition 1.1.17. A *basis* for an R-module M is a generating set Γ of M such that, given any $a_1, \ldots, a_s \in R$ and $m_1, \ldots, m_s \in \Gamma$, $a_1 m_1 + \cdots + a_s m_s = 0$ implies $a_1, \ldots, a_s = 0$. An R-module M is said to be *free* if it has a basis.

Remark 1.1.18. An R-module M is free if and only if it is isomorphic to a direct sum of copies of R. Indeed, suppose M is free with basis $\Gamma = \{\gamma_i\}_{i \in \mathcal{I}}$ and consider the R module homomorphism

$$\begin{array}{ccc} \bigoplus_{i \in \mathcal{I}} R & \xrightarrow{\quad \varphi \quad} & M \\ (r_i)_{i \in \mathcal{I}} & \longmapsto & \sum_{i \in \mathcal{I}} r_i \gamma_i \end{array} .$$

φ is surjective because Γ generates M and it is injective due to Γ being a basis. Thus $M \cong \bigoplus_{i \in \mathcal{I}} R$. Conversely, if this isomorphism holds, it is clear that M is free.

For $r \in R$, rM denotes the set $\{rx : x \in M\}$, which is also a submodule of M.

More generaly, if I is an ideal of R, then IM denotes the following submodule of M:

$$IM = \{a_1 x_1 + \cdot + a_r x_r : r \in \mathbb{N}, a_1, \ldots, a_r \in I, x_1, \ldots, x_r \in M\}.$$

Annihilator of a module:

Definition 1.1.19. If N, P are submodules of an R-module M, we define $(N : P)$ as

$$(N : P) = \{r \in R : rP \subseteq N\}.$$

$(N : P)$ is an ideal of R. In particular, $(0 : M)$ denotes the set of all $r \in R$ such that $rM = 0$, i.e., the set of all *annihilators* of M. $(0 : M)$ is also denoted by

$$\mathrm{Ann}(M).$$

If m is an element of M, we will also use the notation $\mathrm{Ann}(m)$ to denote the set $(0 : m)$ of annihilators of m, i.e.

$$\mathrm{Ann}(m) = (0 : m) = \{r \in R : rm = 0\}.$$

Observation 1.1.20. *A trivial, but very useful remark is the following:* If an ideal I of R is such that $I \subseteq \mathrm{Ann}(M)$, then M is also an R/I-module. Indeed, the action of R/I on M given by $(r + I)x = rx$ for all $r \in R, x \in M$ is well defined whenever $IM = 0$. This way, the module structure of M is exactly the same whether we view it as an R-module or as an R/I-module. In some cases it can be very useful to think of M as an R/I-module (specially if R/I is a field).

For example, for any ideal I of R, the module M/IM is an R-module, but also an R/I-module.

1.2 Maximal ideals, prime ideals and Spectrum

The notions of maximal ideals and prime ideals are crucial in the study of commutative rings. Before introducing them however, we will define a few other concepts.

Definition 1.2.1. An element r of a ring R is said to be a *zerodivisor* in R if there exists $0 \neq a \in R$ such that $ra = 0$. Otherwise, r is said to be a *nonzerodivisor* in R.

An element $r \in R$ is said to be invertible if there exists $u \in R$ such that $ru = 1$.

Definition 1.2.2. A ring R is a *domain* if every nonzero element of R is a nonzero divisor. In other words, if for every $a, b \in R$ we have that $ab = 0$ implies $a = 0$ of $b = 0$.

Now we define maximal and prime ideals. We will say that an ideal I of a ring R is *proper* if $I \neq R$.

Definition 1.2.3. A proper ideal $\mathfrak{m} \subsetneq R$ of R is said to be a *maximal ideal* of R if there is no ideal J of R such that $\mathfrak{m} \subsetneq J \subsetneq R$ (strict inclusions).

An ideal $P \subseteq R$ is said to be a *prime ideal* of R if it is a proper ideal of R and if the following holds for every $a, b \in R$:

$$\text{if } ab \in P, \text{ then } a \in P \text{ or } b \in P.$$

Remark 1.2.4. (1) R is a domain if and only if (0) is a prime ideal.

(2) $\mathfrak{m}$ is a maximal ideal of R is equivalent to saying that $R/\mathfrak{m}$ has only two ideals (0 and $R/\mathfrak{m}$), i.e., $\mathfrak{m}$ is a maximal ideal of R if and only if $R/\mathfrak{m}$ is a field.

(3) Note also that P is a prime ideal of R if and only if R/P is a domain. This is immediate from the definitions.

(4) Suppose I is a proper ideal of R. Since ideals of R/I correspond to ideals of R that contain I, also the maximal ideals of R/I correspond to the maximal ideals of R that contain I. Similarly, the prime ideals of R/I correspond to the prime ideals of R that contain I.

Proposition 1.2.5. *Let $R \neq 0$ be a ring.*

(1) R has at least one maximal ideal.

(2) Every maximal ideal of R is a prime ideal.

(3) Every proper ideal of R is contained in a maximal ideal.

(4) Every non invertible element in R belongs to a maximal ideal of R.

Proof. (1): We will resort to Zorn's Lemma. Let $\mathcal{S}$ be the set of all proper ideals of R, partially ordered using the inclusion order $\subseteq$. $\mathcal{S}$ is nonempty since $(0) \in \mathcal{S}$. If $\{I_i\}_i$ is a chain of proper ideals of R, notice that $I = \bigcup_i I_i$ is also an ideal. In fact, I is also a proper ideal since $1 \notin I_i$ for all i. Therefore, the ideal I is an upper bound in $\mathcal{S}$ for the chain $\{I_i\}_i$. By Zorn's Lemma, $\mathcal{S}$ has a maximal element, i.e., there exists a maximal ideal of R.

(2): Let $\mathfrak{m}$ be a maximal ideal of R and let $a, b \in R$ be such that $ab \in \mathfrak{m}$, with $a \notin \mathfrak{m}$. We must show that $b \in \mathfrak{m}$. The inclusion $\mathfrak{m} \subset \mathfrak{m} + (a)$ is strict because $a \notin \mathfrak{m}$, hence the maximality of $\mathfrak{m}$ implies that $\mathfrak{m} + (a) = R$. As such, there exist $y \in \mathfrak{m}$ and $c \in R$ such that $1 = y + ac$. Therefore,

$$b = b(y + ac) = by + (ab)c \in \mathfrak{m},$$

concluding the proof.

(3): If I is a proper ideal of $\mathfrak{m}$, applying (1) to R/I, we conclude that R/I has a maximal ideal. This corresponds to a maximal ideal of R that contains I.

(4): If $a \in R$ is not invertible, then (a) is a proper ideal of R, hence by (3) it must be contained in a maximal ideal. □

Example 1.2.6.

1. The ring $\mathbb{Z}$ is a domain. In $\mathbb{Z}$ every ideal is principal (i.e., can be generated by a single element). You can easily verify that the prime ideals of $\mathbb{Z}$ coincide with the ideals (p), where p is a prime number. Plus, these are exactly the maximal ideals of $\mathbb{Z}$.

2. A *principal ideal domain* (PID) is a domain R in which every ideal is principal. In a PID (such as $k[x]$, where k is a field), every non-zero prime ideal is maximal (exercise).

3. In $R = k[x_1, \ldots, x_n]$, where k is a field, an ideal of the form (f) is prime if and only if f is an irreducible polynomial.

   Given $a_1, \ldots, a_n \in k$, the ideal $(x_1 - a_1, \ldots, x_n - a_n)$ is a maximal ideal of R. This can be seen the following way: the nonzero ring homomorphism $\varphi : R \longrightarrow k$ given by $\varphi(f) = f(a_1, \ldots, a_n)$ has kernel $(x_1 - a_1, \ldots, x_n - a_n)$ (which follows easily from polynomial division, which tells us that every polynomial $f \in R$ can be written as $f = f_1(x_1 - a_1) + \cdots + f_n(x_n - a_n) + c$ with $c \in k$). Thus $R/(x_1 - a_1, \ldots, x_n - a_n) \cong k$. As this is a field, $(x_1 - a_1, \ldots, x_n - a_n)$ must be a prime ideal of R.

   If k is algebraically closed, then these are in fact all the maximal ideals of R. This result is known as the weak Hilbert Nullstelensatz

4. Given a ring R, consider the ring $S = R[\![X]\!]$ of power series in X with coefficients in R. The invertible elements in S coincide with the power series $f = a_0 + a_1X + a_2X^2 + \cdots$ in which a_0 is invertible in R. Indeed, if f is invertible with inverse $g = b_0 + b_1X + b_2X^2 + \cdots$, then $1 = fg = a_0b_0 + X(\cdots)$, hence $1 = a_0b_0$. Conversely, if a_0 is invertible in R with inverse b_0, then, since

   $$fg = 1 + (b_0a_1 + a_0b_1)X + (\cdots + a_0b_2)X^2 + (\cdots + a_0b_3)X^3 + \cdots,$$

   one can choose $b_1, b_2, \ldots$ such that the coefficients of $X, X^2, \ldots$ in fg are all zero, making $fg = 1$.

   We now characterize the maximal ideals of S.

   Claim 1.2.7. *The maximal ideals of S coincide with the ideals of the form*

   $$\mathfrak{m} + (X),$$

   where $\mathfrak{m}$ is a maximal ideal of R.

   Proof. From the isomorphism

   $$R[\![X]\!]/(\mathfrak{m} + (X)) \cong R/\mathfrak{m}$$

   we see that an ideal J of S of the form $J = \mathfrak{m} + (X)$, with $\mathfrak{m}$ an ideal of R, is maximal if and only if $\mathfrak{m}$ is a maximal ideal of R.

   Let J be a maximal ideal of S. We need to show that J is of this form. We begin by observing that $X \in J$. Indeed, if $X \notin J$, then X is invertible in the field $R[\![X]\!]/(J)$, so that there exists $f \in R[\![X]\!]$ such that $1 + Xf \in J$. However, $1 + Xf$ is invertible in $R[\![X]\!]$, which contradicts the fact that J is maximal. Thus $X \in J$. Now let I be the set of all elements $a \in R$ such that there exists an element in J of the form $a + a_1X + a_2X^2 + \cdots$. Then I is an ideal of R and $J = I + (X)$. The isomorphism $R[\![X]\!]/(I + (X)) \cong R/I$ implies that I is a maximal ideal of R, concluding the proof. □

Definition 1.2.8. A ring R is said to be *local* if it has only one maximal ideal.

To say that a ring R is local with unique maximal ideal $\mathfrak{m}$, we sometimes condense it into the form "let $(R, \mathfrak{m})$ be a local ring". Plus, if we want to add that $R/\mathfrak{m} \cong k$ ($R/\mathfrak{m}$ is called the *residue field* of a local ring $(R, \mathfrak{m})$), we can denote this in the form "let $(R, \mathfrak{m}, k)$ be a local ring".

Example 1.2.9.

1. By Example 1.2.6, if $(R, \mathfrak{m})$ is local, then the power series ring $R[\![x_1, \ldots, x_n]\!]$ is a local ring with unique maximal ideal $\mathfrak{m} + (x_1, \ldots, x_n)$. In particular, if k is a field, then $k[\![x_1, \ldots, x_n]\!]$ is local with unique maximal ideal $(x_1, \ldots, x_n)$.

2. In Section 1.4 we will see that we can build local rings from any ring R by *localizing* at prime ideals of R.

Definition 1.2.10. A ring R which has only a finite number of maximal primes is called *semilocal*.

We now introduce the Spectrum of a ring.

Definition 1.2.11. The *Spectrum* of a ring R is the set of all its prime ideals. It is denoted by

$$\mathrm{Spec}(R) = \{P : P \text{ is a prime ideal of } R\}.$$

For any ideal I of R, we set

$$V(I) = \{P \in \mathrm{Spec}(R) : I \subseteq P\}.$$

The following properties are fairly easy to show and are left as an exercise.

Proposition 1.2.12. *Let R be a ring and I, J be ideals of R. Then*

(1) $V(R) = \emptyset$ *and* $V(0) = R$.

(2) If $I \subseteq J$, *then* $V(J) \subseteq V(I)$.

(3) $V(I) \cup V(J) = V(I \cap J) = V(IJ)$.

(4) If $\{I_\lambda\}_{\lambda \in \Lambda}$ *is a family of ideals of* R, *then* $\bigcap_{\lambda \in \Lambda} V(I_\lambda) = V(\sum_{\lambda \in \Lambda} I_\lambda)$.

Remark 1.2.13. *(The Zariski topology)* Thanks to Proposition 1.2.12, $\mathrm{Spec}(R)$ becomes a topological space in which its closed sets are precisely the sets of the form $V(I)$. This is called the *Zariski topology* on $\mathrm{Spec}(R)$.

Notice that the closed points in $\mathrm{Spec}(R)$ are precisely the maximal ideals of R.

We finish this section with a really useful property of prime ideals, which we will use several times.

Theorem 1.2.14. (Prime avoidance) *Let R be a ring.*

(i) Let $P_1, \dots, P_n$ be prime ideals of R and I an ideal such that $I \subseteq \bigcup_{i=1}^n P_i$. Then $I \subseteq P_i$ for some i.

(ii) Let $I_1, \dots, I_n$ be ideals of R and P a prime ideal such that $\bigcap_{j=1}^n I_j \subseteq P$. Then $I_j \subseteq P$ for some j. If $\bigcap_{j=1}^n I_j = P$, then $I_j = P$ for some j.

Proof. (i): The proof goes by induction on n. If $n = 1$ the result is a triviality. Suppose $n = 2$. Assume $I \not\subseteq P_1$ and $I \not\subseteq P_2$. We must show that $I \not\subseteq P_1 \cup P_2$. Take $a_1 \in I \backslash P_1$ and $a_2 \in I \backslash P_2$. If $a_1 \notin P_2$ or $a_2 \notin P_1$, we are done, as a_1 or a_2 will provide, respectively, an element in $I \backslash P_1 \cup P_2$. Thus, suppose $a_1 \in P_2$ and $a_2 \in P_1$. Then $a = a_1 + a_2$ is an element of I that does not belong to P_1 or P_2. This concludes the proof in the $n = 2$ case. Note that for this case we did not even require the assumption that P_1, P_2 are prime ideals.

Suppose now $n \geq 3$ and that the result is valid for $n - 1 \geq 2$. Supposing $I \not\subseteq P_i$ for all $i = 1, \dots, n$, the goal is to find an element $a \in I \backslash \cup_{i=1}^n P_i$. By induction, we have that

$$I \not\subseteq \bigcup_{i \neq j} P_i$$

for each $j = 1, \dots, n$. Hence, for each j we can find an element

$$a_j \in I \backslash \bigcup_{i \neq j} P_j.$$

Plus, we can assume $a_j \in P_j$, otherwise the proof is done by choosing $a = a_j$. Notice that

$$a_1 \cdots a_{n-1} \in P_1 \cap \cdots \cap P_{n-1} \backslash P_n.$$

Here we are using the fact that P_n is a prime ideals to conclude that $a_1 \cdots a_{n-1} \notin P_n$ from the fact that $a_j \notin P_n$ for each $j = 1, \dots, n - 1$. We consider the element

$$a = a_n + a_1 \cdots a_{n-1}.$$

$a \notin P_n$ because $a_n \in P_n$ but $a_1 \cdots a_{n-1} \notin P_n$. Also, $a \notin P_j$ with $j \leq n - 1$ because $a_1 \cdots a_{n-1} \in P_j$ but $a_n \notin P_j$. Thus a is an element of I that does not belong to $P_1, P_2, \dots$ or P_n.

(2): First, assuming that $I_j \not\subseteq P$ for all j, we must show that $\bigcap_{j=1}^n I_j \not\subseteq P$. Take $a_j \in I_j \backslash P$. As P is prime, $a_1 \cdots a_n \notin P$. But $a_1 \cdots a_n \in \bigcap_{j=1}^n I_j$. Hence we are done. Suppose now $\bigcap_{j=1}^n I_j = P$. Then $P \subseteq I_j$ for every j. Since $I_j \subseteq P$ for some j, it then follows that $I_j = P$ for such j. □

1.3 Nakayama's lemma and minimal generating sets

Here we introduce a simple but really useful result in commutative algebra, which will be particularly handy when working over local rings. This result, known as Nakayama's lemma, will then allow us to define the "minimal number of generators" for ideals over local rings.

Proposition 1.3.1. *Let R be a ring, I an ideal and M a finitely generated R-module. If*

$$IM = M$$

then there exists a element $r \in 1 + I$ such that $rM = 0$.

Proof. Let $m_1, \ldots, m_s$ be generators of M, so that $M = Rm_1 + \cdots + Rm_s$. Since $M = IM$, there exist $a_{ij} \in I$, $1 \leq i, j \leq s$, such that

$$m_1 = a_{11}m_1 + \cdots + a_{1s}m_s, \ldots, m_s = a_{s1}m_1 + \cdots + a_{ss}m_s.$$

Let A denote the matrix $[a_{ij}]$ and v the column vector $[m_i]$. Then $Av = v$, i.e., $(\mathrm{Id} - A)v = 0$. Applying the determinantal trick (meaning, multiplying by the adjoint of $\mathrm{Id} - A$ on both sides), we conclude that $\det(\mathrm{Id} - A)$ annihilates each m_i, hence it also annihilates M. Finnaly, since all the entries of A belong to I, we observe that $\det(\mathrm{Id} - A) \equiv \det(\mathrm{Id}) = 1 \bmod I$. Thus, the element $r = \det(\mathrm{Id} - A)$ satisfies our requirement. □

Definition 1.3.2. *(Jacobson radical)* The intersection of all the maximal ideals of a ring $R \neq 0$ is called the *Jacobson radical* of R (or simply the *radical* of R) and is denoted $\mathrm{rad}(R)$. Notice that if $a \in \mathrm{rad}(R)$, then $1 + a$ does not belong to any maximal ideal of R, hence it must be an invertible element, by Proposition 1.2.5.

The following immediate consequences of Proposition 1.3.1 are known as Nakayama's Lemma (even though we will state them as separate results and as theorems, not lemmas).

Theorem 1.3.3. *Let $R \neq 0$ be a ring, M a finitely generated R-module and I an ideal of R such that $I \subseteq rad(R)$. If $IM = M$ then $M = 0$.*

Proof. By Proposition 1.3.1 there exists $r \in 1 + I$ such that $rM = 0$. But since $I \subseteq \mathrm{rad}(R)$, r must be invertible. Hence $M = 0$. □

Theorem 1.3.4. *Let $(R, \mathfrak{m})$ be a local ring and M a finitely generated R-module. If $\mathfrak{m}M = M$ then $M = 0$.*

Proof. Immediate corollary of Theorem 1.3.3, since $\mathrm{rad}(R) = \mathfrak{m}$ for a local ring $(R, \mathfrak{m})$. □

Theorem 1.3.5. *Let $(R, \mathfrak{m})$ be a local ring, M a finitely generated R-module and N a submodule of M. If $M = N + \mathfrak{m}M$ then $N = M$.*

Proof. If $M = N + \mathfrak{m}M$, then $\mathfrak{m}(M/N) = (N + \mathfrak{m}M)/N = M/N$. By Theorem 1.3.4, applied to the module M/N, it follows that $M/N = 0$, that is, $N = M$. □

Definition 1.3.6. Let R be a ring and M an R-module. A set of generators of M is said to be *minimal* if no strict subset of it is a set of generators of M.

Notice that, in general, an R-module can have minimal generating sets of different cardinalities. For instance, in $\mathbb{Z}$, we have $I = (4) = (8, 12)$ and both $\{4\}$ and $\{8, 12\}$ are minimal generating sets of I. Over local rings, however, this is a situation that cannot occur, thanks to the following observation.

Proposition 1.3.7. *Let $(R, \mathfrak{m}, k)$ be a local ring and M a finitely generated R-module. For elements $m_1, \ldots, m_s \in M$ the following holds:*

$$m_1, \ldots, m_s \text{ generate } M \iff \overline{m_1}, \ldots, \overline{m_s} \in M/\mathfrak{m}M \text{ generate } M/\mathfrak{m}M.$$

Proof. The implication $(\Rightarrow)$ is clear. We show $(\Leftarrow)$. Let $N = Rm_1 + \cdots Rm_s \subseteq M$. If $\overline{m_1}, \ldots, \overline{m_s}$ generate $M/\mathfrak{m}M$, that means that the image of N in $M/\mathfrak{m}M$ equals $M/\mathfrak{m}M$, i.e., $M = N + \mathfrak{m}M$. By Theorem 1.3.5 it follows that $M = N$, meaning that $m_1, \ldots, m_s$ generate M. □

Notice that, since $M/\mathfrak{m}M$ is annihilated by $\mathfrak{m}$, $M/\mathfrak{m}M$ is a $k = R/\mathfrak{m}$-vector space. The statement of Proposition 1.3.7 can therefore be stated in the following way for minimal generating sets:

$$\begin{aligned} m_1, \ldots, m_s \text{ minimally generate } M &\iff \overline{m_1}, \ldots, \overline{m_s} \text{ minimally generate } M/\mathfrak{m}M \\ &\iff \{\overline{m_1}, \ldots, \overline{m_s}\} \text{ is a basis of the } k \text{ vector space } M/\mathfrak{m}M. \end{aligned}$$

Therefore, every minimal generating set of a finitely generated module over a local ring $(R, \mathfrak{m}, k)$ must have cardinality equal to the dimension of $M/\mathfrak{m}M$ as a k-vector space. This prompts us to make the following definition.

Definition 1.3.8. Let $(R, \mathfrak{m}, k)$ be a local ring and M a finitely generated R-module. Then the *minimal number of generators of* M is defined as

$$\mu(M) = \dim_k(M/\mathfrak{m}M).$$

This coincides with the cardinality of any minimal generating set of M.

Proposition 1.3.7 also gives us the following description of minimal generating sets of a finitely generated module M over a local ring $(R, \mathfrak{m}, k)$: $\{m_1, \ldots, m_s\} \subseteq M$ is a minimal generating set of M if and only if

1. $s = \dim_k(M/\mathfrak{m}M)$ and
2. if $a_1, \ldots, a_s \in R$ are such that $a_1 m_1 + \cdots + a_s m_s = 0$, then $a_1, \ldots, a_s \in \mathfrak{m}$.

1.4 Localization

Definition 1.4.1. A *multiplicative subset* of a ring R is a subset $S \subset R$ satisfying the following two properties:

$$1 \in S \quad \text{and} \quad s, w \in S \Rightarrow sw \in S.$$

The following are very important examples of multiplicative subsets:

Example 1.4.2.

1. Given any $s \in R$, the set $S = \{1, s, s^2, s^3, \ldots\}$ of powers of r is a multiplicative subset of R.
2. Given a prime ideal P of R, the complement $S = R \backslash P$ of P is a multiplicative subset of P. This follows immediately from the defining property of prime ideals.
3. The set S of nonzerodivisors of R is a multiplicative subset of R. Indeed 1 is a nonzerodivisor in R and if r, s are nonzerodivisors, then so is rs (if $a \in R$ is such that $(rs)a = r(sa) = 0$, then we must have $sa = 0$, because r is a nonzerodivisor; but since s is also a nonzerodivisor, this forces $a = 0$).
4. An arbitrary intersection of multiplicative subsets of R is also a multiplicative subset of R. As a consequence, if $\{P_\lambda\}$ is a family of prime ideals of R, then $R \backslash (\bigcup_\lambda P_\lambda)$ is a multiplicative subset of R.

We now define the localization of a ring R at a multiplicative subset S.

Definition 1.4.3. Let R be a ring and S a multiplicative subset of R with $0 \notin S$. The *locatization* of R at S is formally defined as the ring

$$S^{-1}R = \left\{ \frac{r}{s} : r \in R, s \in S \right\} / \sim$$

where $\sim$ is the equivalence relation between the formal fractions $\frac{r}{s}$ given by

$$\frac{r}{s} \sim \frac{r'}{s'} \text{ if there exists } w \in S \text{ such that } w(rs' - r's) = 0.$$

Addition and multiplication in $S^{-1}R$ are given by

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'} \quad \text{and} \quad \frac{r}{s}\frac{r'}{s'} = \frac{rr'}{ss'}.$$

(Exercise: check that these operations are well defined.)

There is a canonical ring homomorphism

$$\begin{aligned} R &\longrightarrow S^{-1}R \\ r &\longmapsto \tfrac{r}{1} \end{aligned}.$$

Remark 1.4.4. The localization $S^{-1}R$ of R at a multiplicative subset S is the smallest ring extension of R in which every element $s \in S$ becomes invertible. In precise terms, you can check that $S^{-1}R$ is characterized by the following universal property:

If $f : R \longrightarrow R'$ is a ring homomorphism such that $f(s)$ is invertible in R' for all $s \in S$, then there exists a ring homomorphism $g : S^{-1}R \longrightarrow R'$ such that the following diagram commutes

$$\begin{array}{ccc} R & \longrightarrow & S^{-1}R \\ {\scriptstyle f}\downarrow & \swarrow_{g} & \\ R' & & \end{array}$$

where the horizontal map is the canonical homomorphism $R \longrightarrow S^{-1}R$.

If J is an ideal of the ring $S^{-1}R$, then we will write $J \cap R$ for the contraction of J to R under the canonical homomorphism $R \longrightarrow S^{-1}R$. That is, $J \cap R$ is the ideal

$$J \cap R = \left\{ r \in R : \frac{r}{1} \in J \right\}.$$

On the other hand, if I is an ideal of R, we denote

$$S^{-1}I = \left\{ \frac{r}{s} : r \in I, s \in S \right\}.$$

$S^{-1}I$ is an ideal of the ring $S^{-1}R$.

Lemma 1.4.5. *Let R be a ring and S a multiplicative subset of R.*

(1) If I is an ideal of R, then $S^{-1}I = I(S^{-1}R)$.

(2) If I is an ideal of R, then $S^{-1}I \cap R = \{r \in R : sr \in I \text{ for some } s \in S\}$.

(3) If J is an ideal of $S^{-1}R$, then $S^{-1}(J \cap R) = J$.

Proof. (1) For every element $\frac{r}{s} \in S^{-1}I$, with $r \in I, s \in S$, we have $\frac{r}{s} = \frac{r}{1}\frac{1}{s} = r\frac{1}{s}$, hence $\frac{r}{s} \in I(S^{-1}R)$. On the other hand, the ideal $I(S^{-1}R)$ is generated by elements of the form $r\frac{a}{s} = \frac{r}{1}\frac{a}{s} = \frac{ra}{s}$ with $r \in I, a \in R$ and $s \in S$. As I is an ideal, $ra \in I$, and thus $\frac{ra}{s} \in S^{-1}I$.

(2) If $rs \in I$ for some $s \in S$, then $\frac{r}{1} = \frac{r}{1}\frac{s}{s} = \frac{rs}{s} \in S^{-1}I$. Conversely, suppose $r \in R$ is such that $\frac{r}{1} \in S^{-1}I$. Then there exists $a \in I$ and $s \in S$ such that $\frac{r}{1} = \frac{a}{s}$. This means there exists $w \in S$ satisfying $w(rs - a) = 0$. Therefore $r(ws) = aw \in I$. As $ws \in S$, since S is multiplicatively closed, we are done.

(3) The inclusion $S^{-1}(J \cap R) \subseteq J$ is an easy check (and is in fact a simple consequence of $R \to S^{-1}R$ being a ring homomorphism). Conversely, given $\frac{r}{s} \in J$, with $r \in S$ and $s \in S$, we get that $\frac{r}{1} = \frac{r}{s}\frac{s}{1}$ also belongs to J. Thus $r \in J \cap R$ and we conclude that $\frac{r}{s} \in S^{-1}(J \cap R)$. □

We now characterize the ideals and the prime ideals in the localization. The following result is one of the reasons why localization is such a useful tool in commutative algebra.

Theorem 1.4.6. *Let R be a ring and S a multiplicative subset of R.*

(1) Every ideal of $S^{-1}R$ is of the form $S^{-1}I$, where I is an ideal of R.

(2) There is a one to one correspondence

$$\begin{aligned} \{\text{prime ideals of } S^{-1}R\} &\longleftrightarrow \{\text{prime ideals } P \text{ of } R \text{ such that } P \cap S = \emptyset\} \\ Q &\longrightarrow Q \cap R \\ S^{-1}P &\longleftarrow P. \end{aligned}$$

Proof. (1): follows immediately from Lemma 1.4.5.

(2): Given a prime ideal Q of $S^{-1}R$, it is easy to verify that $Q \cap R$ is a prime ideal of R. We notice also that $Q \cap R$ does not intersect S, since otherwise there would exist $s \in S$ such that $\frac{s}{1} \in Q$; but then Q would contain an invertible element in $S^{-1}R$, which would imply $Q = S^{-1}R$, contradicting the fact that Q is a prime ideal of $S^{-1}R$.

Suppose P is a prime ideal of R such that $P \cap S = \emptyset$. Then $sr \in P$ with $r \in R, s \in S$ must imply that $r \in P$. Therefore, by Lemma 1.4.5, it follows that $(S^{-1}P) \cap R = P$. It remains to show that $S^{-1}P$ is a prime ideal of $S^{-1}R$.

Suppose $\frac{a}{s}, \frac{b}{w} \in S^{-1}R$ are such that $\frac{a}{s}\frac{b}{w} = \frac{ab}{sw} \in S^{-1}P$, so that there exists $r \in P, t \in S$ such that $\frac{ab}{sw} = \frac{r}{t}$. Then there exists $u \in S$ satisfying

$$u(abt - rsw) = 0.$$

It follows that $(ab)(ut) = rswu \in P$. As $ut \in S$ and P is a prime ideal that does not intersect S, this implies $ab \in P$. Thus $a \in P$ or $b \in P$. This is telling us that $\frac{a}{s}$ or $\frac{b}{w}$ is in $S^{-1}P$. Thus $S^{-1}P$ is a prime ideal of $S^{-1}R$. □

Example 1.4.7. (And Notation)

1. When S is the multiplicative subset $S = \{1, s, s^2, s^3, \ldots\}$, for some $s \in R$, then we will denote $S^{-1}R$ by

   $$R_s.$$

   The prime ideals of R_s are in one to one correspondence with the prime ideals of R that do not contain s.

2. When S is the multiplicative subset $S = R \backslash P$, for a prime ideal P of R, we will denote $S^{-1}R$ by

   $$R_P.$$

   The prime ideals of R_P are in one to one correspondence with the prime ideals Q of R such that $Q \subseteq P$. From this, it follows that R_P is a local ring with unique maximal ideal PR_P. We call R_P the localization of R at the prime P.

3. When S is the set of nonzerodivisors of R, we call $S^{-1}R$ the *total ring of fractions* of R. If R is a domain, then the total ring of fractions of R coincides with the field of fractions of R, $\mathrm{Frac}(R)$, which is the localization of R at the prime (0).

Remark 1.4.8. Let S be a multiplicative subset of a ring R. The canonical map

$$R \longrightarrow S^{-1}R$$

is not necessarily injective (for instance, if $R = k[x, y]/(xy)$, then $R \to R_x$ is not injective since $\frac{y}{1} = \frac{y}{1}\frac{x}{x} = \frac{yx}{1} = \frac{0}{1}$ in R_x.) One can check easily check that

$$\ker(R \longrightarrow S^{-1}R) = \{r \in R : sr = 0 \text{ for some } s \in S\}.$$

Therefore, $R \longrightarrow S^{-1}R$ is injective if and only if S does not contain any zerodivisors. In particular, if R is a domain then $R \longrightarrow S^{-1}R$ is injective.

Similar to rings, we define localization of modules as follows.

Definition 1.4.9. Let R be a ring, S a multiplicative subset of R with $0 \notin S$ and M an R-module. The *locatization* of M at S is formally defined as the $S^{-1}R$-module

$$S^{-1}M = \left\{ \frac{m}{s} : m \in M, s \in S \right\} / \sim$$

where $\sim$ is the equivalence relation between the formal fractions $\frac{m}{s}$ given by

$$\frac{m}{s} \sim \frac{m'}{s'} \text{ if there exists } w \in S \text{ such that } w(s'm - sm') = 0.$$

Addition and scalar multiplication in $S^{-1}M$ are given by

$$\frac{m}{s} + \frac{m'}{s'} = \frac{s'm + sm'}{ss'} \quad \text{and} \quad \frac{r}{s}\frac{m}{s'} = \frac{rm}{ss'}$$

for any $m, m' \in M, s, s' \in S$ and $r \in R$.

We will use the notations M_s and M_P, if $s \in R$ or if P is a prime ideal of R, similarly to R_s and R_P.

Notice that there is a canonical homomorphism of R-modules

$$M \longrightarrow S^{-1}M$$

$$m \longmapsto \frac{m}{1}$$

with kernel

$$\{m \in M : sm = 0 \text{ for some } s \in S\}.$$

If $f : M_1 \longrightarrow M_2$ if an homomorphism of R-modules, then f induces an homomorphism of $S^{-1}R$-modules

$$\begin{array}{ccc} S^{-1}M_1 & \xrightarrow{S^{-1}f} & S^{-1}M_2 \\ \frac{m}{s} & \longmapsto & \frac{f(m)}{s} \end{array}.$$

Notice that if $f : M_1 \longrightarrow M_2$ and $g : M_2 \longrightarrow M_3$ are R-module homomorphisms, then $S^{-1}(g \circ f) = (S^{-1}g) \circ (S^{-1}f)$. The functor $S^{-1}(-)$ is therefore a covariant functor from the category of R-modules to the category of $S^{-1}R$-modules.

Definition 1.4.10. The *support* of an R-module M is defined as

$$\operatorname{Supp}(M) = \{P \in \operatorname{Spec}(R) : M_P \neq 0\}.$$

Remark 1.4.11. Let P be a prime ideal of R, M an R-module and $m \in M$. Notice that $\frac{m}{1} = 0$ in M_P is equivalent to $sm = 0$ for some $s \notin P$. In other words,

$$\frac{m}{1} = 0 \text{ in } M_P \iff \operatorname{Ann}(m) \not\subseteq P.$$

Suppose M is finitely generated, so that there exist $m_1, \ldots, m_n \in M$ such that $M = Rm_1 + \cdots + Rm_n$. Having $M_P \neq 0$ is equivalent to having $\frac{m_i}{1} \neq 0$ for some i, i.e., $\operatorname{Ann}(m_i) \subseteq P$ for some i. By Theorem 1.2.14, this is equivalent to

$$\operatorname{Ann}(M) = \bigcap_{i=1}^{n} \operatorname{Ann}(m_i) \subseteq P.$$

This shows that, when M is finitely generated,

$$\operatorname{Supp}(M) = \{P \in \operatorname{Spec}(R) : \operatorname{Ann}(M) \subseteq P\} = V(\operatorname{Ann}(M)).$$

The property of a module being zero is one that can be checked locally, meaning that it can be checked at the localizations at every prime ideal of the ring.

Proposition 1.4.12. *Let R be a ring and M a finitely generated R-module. The following are equivalent:*

(1) $M = 0$.

(2) $M_P = 0$ *for all prime ideals* P *of* R.

(3) $M_{\mathfrak{m}} = 0$ *for all maximal ideals* $\mathfrak{m}$ *of* R.

Proof. (1) $\Rightarrow$ (2) $\Rightarrow$ (3) is obvious. We show (3) $\Rightarrow$ (1) by contradiction. Suppose $M \neq 0$ and take $0 \neq x \in M$. Then $\operatorname{Ann}(x) \neq R$, so that there exists a maximal ideal $\mathfrak{m}$ of R such that $\operatorname{Ann}(x) \subseteq \mathfrak{m}$. Then, by Remark 1.4.11 we have $\frac{x}{1} \neq 0$ in $M_{\mathfrak{m}}$, contracting the assumption that $M_{\mathfrak{m}} = 0$. □

1.5 Complexes and short exact sequences

Definition 1.5.1. Let R be a ring. A *complex* is a sequence

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

of R-modules and R-homomorphisms such that $f_{i+1} \circ f_i = 0$ for all i, that is,

$$\operatorname{im}(f_i) \subseteq \ker(f_{i+1})$$

for all i. The complex is said to be *exact at* M_i if

$$\operatorname{im}(f_i) = \ker(f_{i+1}).$$

We say that the (whole) complex is *exact* if it is exact at M_i for every i.

Example 1.5.2. Let $R = k[X]/(X^2)$, where k is a field. Then the complex

$$\cdots \xrightarrow{\cdot X} \frac{k[X]}{(X^2)} \xrightarrow{\cdot X} \frac{k[X]}{(X^2)} \xrightarrow{\cdot X} \cdots$$

is exact since both the image and kernel of $\cdot X : R \to R$ coincide with $(X)/(X^2)$.

Definition 1.5.3. Let R be a ring. A *short exact sequence* (SES) is an exact complex of the form

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0.$$

If such a complex is not necessarily exact, we will simply call it a *short sequence*.

Remark 1.5.4. Saying that the sequence

$$0 \longrightarrow A \xrightarrow{f} B$$

is exact is equivalent to saying that f is injective. On the other hand, saying that

$$B \xrightarrow{g} C \longrightarrow 0$$

is exact is equivalent to saying that g is surjective. Therefore, a short sequence

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is exact exactly (pun intended) when f is injective, g is surjective and $\operatorname{im} f = \ker g$. In this case we have that

$$A \cong \ker g \quad \text{and} \quad C \cong \operatorname{coker} f = B/\operatorname{im} f \cong B/A.$$

Remark 1.5.5. Notice also that the sequence $0 \longrightarrow M \longrightarrow 0$ is exact if and only if $M = 0$.

1.6 Hom and tensor

1.6.1 The Hom functor

Definition 1.6.1. Let M and N be R-modules. We denote by $\operatorname{Hom}_R(M, N)$ the set of all R-module homomorphisms from M to N.

Given $f, g \in \operatorname{Hom}_R(M, N)$, define $f + g : M \longrightarrow N$ by

$$(f + g)(m) = f(m) + g(m)$$

for every $m \in M$. Also, given $r \in R$, define $rf : M \longrightarrow N$ by setting

$$(rf)(m) = rf(m)$$

for every $m \in M$. It is an easy check to verify that $f + g$ and rf are elements of $\operatorname{Hom}_R(M, N)$. However, we point out that the commutativity of R is a crucial assumption to have when verifying the R-linearity of rf. Indeed, for any $a \in R$ and $m \in M$,

$$(rf)(am) = rf(am) = raf(m) = a(rf(m)) = a(rf)(m)$$

holds thanks to R being commutative. This way $\operatorname{Hom}_R(M, N)$ is itself an R-module.

Example 1.6.2.

1. For any R-module M we have
$$\operatorname{Hom}_R(R, M) \cong M.$$
This follows since any R-homomorphism from R to M is completely determined by the image of 1.
2. More generally, if I is an ideal of R, we have
$$\operatorname{Hom}_R(R/I, M) \cong (0 :_M I)$$
for any R-module M, where
$$(0 :_M I) = \{m \in M : Im = 0\}.$$

Indeed, as $R/I = R\overline{1}$, where $\overline{1} = 1 + I$, any R-homomorphism $f : R/I \longrightarrow M$ is completely determined by the image $m = f(\overline{1})$. Notice that we must have $m \in (0 :_M I)$ since

$$am = af(\overline{1}) = f(\overline{a}) = f(0) = 0$$

for any $a \in I$. On the other hand, if $m \in (0 :_M I)$, defining $f : R/I \longrightarrow M$ by $f(r + I) = rm$ yields a well defined map $f \in \mathrm{Hom}_R(R/I, M)$.

This indicates that Hom detects annihilators.

Proposition 1.6.3. *(*Hom and direct sum*)*

(1) Suppose $\{M_i\}_{i\in\Lambda}$ is a family of R-modules and N is another R-module. Then

$$\mathrm{Hom}_R(\bigoplus_{i\in\Lambda} M_i, N) \cong \prod_{i\in\Lambda} \mathrm{Hom}_R(M_i, N).$$

(2) Suppose $\{N_i\}_{i\in\Lambda}$ is a family of R-modules and M is a finitely generated R-module. Then

$$\mathrm{Hom}_R(M, \bigoplus_{i\in\Lambda} N_i) \cong \bigoplus_{i\in\Lambda} \mathrm{Hom}_R(M, N_i).$$

Consequently, $\mathrm{Hom}_R(R^n, M) \cong M^n$ *for any* $n \geq 1$.

Proof. I leave this one as an exercise. □

The Hom construction is functorial in both variables. Suppose $\alpha : M' \to M$ is an R-module homomorphism. Then α induces a map

$$\alpha^* : \mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_R(M', N)$$

$$f \longmapsto f \circ \alpha$$

Notice that the direction of the arrow has been reversed. Similarly, if $\beta : N \to N'$ is an R-module homomorphism, then β induces a map

$$\beta^* : \mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_R(M, N')$$

$$g \longmapsto \beta \circ g$$

α^* and β^* are both R-module homomorphisms.

The Hom functor enjoys important exactness properties.

Theorem 1.6.4. (Left exactness of Hom)

(1) A complex $0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N''$ of R-modules is exact if and only if

$$0 \longrightarrow \mathrm{Hom}_R(M, N') \xrightarrow{f^*} \mathrm{Hom}_R(M, N) \xrightarrow{g^*} \mathrm{Hom}_R(M, N'')$$

is exact for every R-modules M.

(2) A complex $M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ of R-modules is exact if and only if

$$0 \longrightarrow \mathrm{Hom}_R(M'', N) \xrightarrow{g^*} \mathrm{Hom}_R(M, N) \xrightarrow{f^*} \mathrm{Hom}_R(M', N)$$

is exact for every R-modules N.

Proof. We prove only (1). The proof of (2) can be seen in [AM69, Proposition 2.9].

($\Rightarrow$) : Suppose the first sequence is exact. Since $g \circ f = 0$, it follows that $g^* \circ f^* = 0$, thus $\operatorname{im} f^* \subseteq \ker g^*$. To verify the opposite inclusion, let $h \in \ker g^*$, so that $g \circ h = 0$. Then

$$\operatorname{im} h \subseteq \ker g = \operatorname{im} f.$$

As f is injective, f is an isomorphism between N' and $\operatorname{im} f$, thus f^{-1} is well defined on $\operatorname{im} f$ (and, consequently, on $\operatorname{im} h$). As such, we can write

$$h = (f \circ f^{-1}) \circ h = f \circ (f^{-1} \circ h).$$

Given that $f^{-1} \circ h \in \operatorname{Hom}_R(M, N')$, this tells us that $h \in \operatorname{im} f^*$. It remains to show that f^* is injective, but this follows easily from just the injectivity of f.

($\Leftarrow$) : Simply take $M = R$. □

In sum, we have the following:

- $\operatorname{Hom}_R(-, N)$ is a contravariant left-exact functor.
- $\operatorname{Hom}_R(M, -)$ is a covariant left-exact functor.

Later we will delve into the topic of *projective* and *injective* modules. These will be the modules that make the Hom functor exact, not just left-exact.

1.6.2 The tensor product

We begin by recalling the notion of bilinearity.

Definition 1.6.5. Let R be a ring and let M, N, and P be R-modules. A map

$$\beta : M \times N \longrightarrow P$$

is called *R-bilinear* if the following relations hold for all $m, m' \in M$, $n, n' \in N$, and $r \in R$:

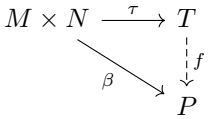
$$\begin{aligned} \beta(m + m', n) &= \beta(m, n) + \beta(m', n), \\ \beta(m, n + n') &= \beta(m, n) + \beta(m, n'), \\ \beta(rm, n) &= r\beta(m, n) = \beta(m, rn). \end{aligned}$$

Example 1.6.6. If I is an ideal of R, then the multiplication map $I \times R \longrightarrow I$ given by $(x, r) \mapsto xr$ is bilinear.

Although bilinear maps occur naturally, the collection of all bilinear maps from $M \times N$ to P has no immediate module structure comparable to that of linear maps. The tensor product $M \otimes N$, defined by a universal property, remedies this difficulty by introducing a module that represents all bilinear maps simultaneously.

Definition 1.6.7. Let R be a ring and M, N be R-modules. A *tensor product* of M and N consists of an R-module T together with a bilinear map $\tau : M \times N \longrightarrow T$ satisfying the following universal property:

Whenever $\beta : M \times N \longrightarrow P$ is an R-bilinear map, there exists a unique R-module homomorphism $f : T \longrightarrow P$ such that the diagram

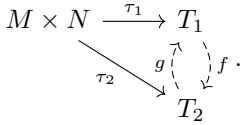


commutes. The module T is denoted by

$$M \otimes_R N.$$

Thus every bilinear map factors uniquely through the tensor product.

Uniqueness of the tensor product: Suppose T_1, T_2, together with R-bilinear maps $\tau_1 : M \times N \longrightarrow T_1$ and $\tau_2 : M \times N \longrightarrow T_2$ are tensor products of M and N. By the universal product there exist R-homomorphisms $f : T_1 \longrightarrow T_2$ and $g : T_2 \longrightarrow T_1$ such that the following diagram commutes:



Then

$$\tau_2 = f \circ \tau_1 = (f \circ g) \circ r_2$$

and again by the universal product of the tensor product T_2, we conclude that $f \circ g = \mathrm{id}_{T_2}$. Similarly, $g \circ f = \mathrm{id}_{T_1}$. Thus T_1 and T_2 are isomorphic.

Existence of the tensor product: Let F be the free R-module generated by the set $M \times N$. Thus every element of F is a finite formal sum $\sum_i r_i(m_i, n_i)$. Let K be the submodule generated by all elements of the form

$$\begin{gathered}(m + m', n) - (m, n) - (m', n),\\ (m, n + n') - (m, n) - (m, n'),\\ (rm, n) - r(m, n),\\ (m, rn) - r(m, n)\end{gathered}$$

with $m, m' \in M$, $n, n' \in N$, and $r \in R$. Define

$$M \otimes_R N := F/K.$$

One can check that $M \otimes_R N$, defined this way, satisfies the universal property of Definition 1.6.7 (see [AM69, Proposition 2.12]), hence it is the tensor product of M and N.

The image of (m, n) in the quotient F/K is denoted by $m \otimes n$. This element is called a *simple tensor*. The tensor product $M \otimes_R N$ is generated as an R-module by these simple tensors.

The defining relations of $M \otimes_R N$ immediately imply

$$\begin{gathered}(m + m') \otimes n = m \otimes n + m' \otimes n,\\ m \otimes (n + n') = m \otimes n + m \otimes n',\\ (rm) \otimes n = m \otimes (rn) = r(m \otimes n).\end{gathered}$$

Example 1.6.8.

1. $2\mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) = 0$ since for every $n \in \mathbb{Z}$ and $x \in \mathbb{Z}/2\mathbb{Z}$ we have

$$(2n) \otimes x = 2(n \otimes x) = n \otimes (2x) = n \otimes 0 = 0.$$

2. If M is an R-module and I is an ideal of R, then

$$M \otimes_R R/I \cong M/IM.$$

Indeed, the map $\beta : M \times R/I \longrightarrow M/IM$ given by $(m, \overline{r}) \longmapsto \overline{rm}$ is well defined and is R-bilinear, hence there exists an R-homomorphism $f : M \otimes_R R/I \longrightarrow M/IM$ such that $f(m \otimes \overline{r}) = \overline{rm}$ for every $m \in M, r \in R$. Notice also that the map $g : M/IM \longrightarrow M \otimes_R R/I$ given by $g(\overline{m}) = m \otimes \overline{1}$ is a well defined R-homomorphism. We easily observe that $f \circ g = \mathrm{id}$ and $g \circ f = \mathrm{id}$, from which the isomorphism follows.

As a corollary of this, note that $R/J \otimes_R R/I \cong R/(I + J)$ whenever I and J are two ideals of R.

3. If M is an R-module and S a multiplicative subset of R such that $0 \notin S$, then

$$S^{-1}M \cong M \otimes_R S^{-1}R.$$

To check this, observe that the map the map $\beta : M \times S^{-1}R \longrightarrow S^{-1}M$ given by $(m, \frac{r}{s}) \longmapsto \frac{rm}{s}$ is R-bilinear (check also that it is well defined), hence there exists an R-homomorphism $f : M \otimes_R S^{-1}R \longrightarrow S^{-1}M$ such that

$f(m \otimes \frac{r}{s}) = \frac{rm}{s}$ for every $m \in M, r \in R$ and $s \in S$. Finally, one checks that the map $g : S^{-1}M \longrightarrow M \otimes_R S^{-1}R$ defined by $\frac{m}{s} \longmapsto m \otimes \frac{1}{s}$ is a well defined R-homomorphism that provides an inverse to the map f.

In fact, observe that the maps f and g are $S^{-1}R$-homomorphisms, hence $S^{-1}M$ and $M \otimes_R S^{-1}R$ are isomorphic as $S^{-1}R$-modules.

Remark 1.6.9. Similarly to how we defined R-bilinear maps, one can define R-multilinear maps and, consequently, we can also define the multi-tensor product $M_1 \otimes_R M_2 \otimes_R \cdots \otimes_R M_r$ of multiple R-modules $M_1, \ldots, M_r$.

The following properties can be checked as an exercise (or see [AM69, Proposition 2.14]).

Proposition 1.6.10. *(Properties of the tensor product) Let R be a ring and M, N, P be R-modules. Then*

(1) $M \otimes_R N \cong N \otimes_R M$.

(2) $(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R P) \cong M \otimes_R N \otimes_R P$.

(3) $(M \oplus N) \otimes_R P \cong (M \otimes_R P) \oplus (N \otimes_R P)$.

(4) $R \otimes_R M \cong M$. *Consequently,* $R^n \otimes M \cong M^n$ *for any* $n \geq 1$.

Suppose $f : M \longrightarrow M'$ and $g : N \longrightarrow N'$ are homomorphisms of R-modules. Then the map $h : M \times N \longrightarrow M' \otimes_R N'$ defined by $(m, n) \longmapsto f(m) \otimes g(n)$ for all $m \in M, n \in N$ is an R-bilinear map. Hence it gives rise to an R-module homomorphism

$$f \otimes g : M \otimes_R N \longrightarrow M' \otimes_R N'$$

such that

$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n) \quad \text{for all} \quad m \in M, n \in N.$$

The following is an easy check: if $f' : M' \longrightarrow M''$ and $g' : N' \longrightarrow N''$ are two other R-module homomorphisms, then

$$(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g).$$

Remark 1.6.11. If $f : M \longrightarrow N$ is an R-module homomorphism and S is a multiplicatively closed subset of R with $0 \notin S$, then the map $S^{-1}f : S^{-1}M \longrightarrow S^{-1}N$ arises as $f \otimes \mathrm{id}$ under the isomorphisms $S^{-1}M \cong M \otimes_R S^{-1}R$ and $S^{-1}N \cong N \otimes_R S^{-1}R$ of Example 1.6.8.

1.6.3 Tensor-Hom adjointness and exactness of the tensor product

Hom and $\otimes_R$ are related via the following relation.

Lemma 1.6.12. (Tensor-Hom adjointness) *Let M, N and P be R-modules. Then*

$$\mathrm{Hom}_R(M \otimes N, P) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)).$$

Proof. The isomorphism will follow if we are able to identify both sides with the set $\mathcal{S}$ of R-bilinear maps $\beta : M \times N \longrightarrow P$. It is clear, from the universal property that defines the tensor product, that $\mathrm{Hom}_R(M \otimes N, P)$ is isomorphic to $\mathcal{S}$. We now observe that the same holds for $\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$.

If $\beta : M \times N \longrightarrow P$ is bilinear, then β defines an R-linear map $\beta' : M \longrightarrow \mathrm{Hom}_R(N, P)$ given by $\beta'(m)(x) = \beta(m, x)$ for every $m \in M, x \in N$. Indeed, the bilinearity of β makes $\beta'(m)$ an R-homomorphism for every $m \in M$. On the other hand, if $\varphi : M \longrightarrow \mathrm{Hom}_R(N, P)$ is an R-linear map, then $\phi : M \times N \longrightarrow P$ given by $\phi(m, x) = \varphi(m)(x)$ is bilinear. The maps $\beta \mapsto \beta'$ and $\varphi \mapsto \phi$ are inverses of one another, hence we have the desired isomorphism between $\mathcal{S}$ and $\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$. □

We are now able to show that the tensor product is right-exact.

Proposition 1.6.13. *Suppose*

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

is an exact sequence of R-modules and let N be an R-module. Then

$$M' \otimes_R N \xrightarrow{f \otimes 1} M \otimes_R N \xrightarrow{g \otimes 1} M'' \otimes_R N \longrightarrow 0$$

is also exact. Here 1 stands for the identity map on N.

Proof. By Theorem 1.6.4, the second sequence is exact if and only if

$$0 \longrightarrow \mathrm{Hom}_R(M'' \otimes_R N, P) \xrightarrow{(g\otimes 1)^*} \mathrm{Hom}_R(M \otimes_R N, P) \xrightarrow{(g\otimes 1)^*} \mathrm{Hom}_R(M' \otimes_R N, P)$$

is exact for every R-module P. By tensor-hom adjointness, this sequence is isomorphic to

$$0 \longrightarrow \mathrm{Hom}_R(M'', E) \xrightarrow{g^*} \mathrm{Hom}_R(M, E) \xrightarrow{f^*} \mathrm{Hom}_R(M', E) \ ,$$

where $E = \mathrm{Hom}_R(N, P)$. But, again by Theorem 1.6.4, this sequence is exact, since by assumption

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

is exact. □

The functor $(-) \otimes_R N$ may not be exact, as it can fail to preserve injectivity of maps. For instance, take $R = \mathbb{Z}$ and the injective map $\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}$. Tensoring with $N = \mathbb{Z}/2\mathbb{Z}$ yields the map $\mathbb{Z}/2\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}/2\mathbb{Z}$, which is the zero map. In certain cases, however, an R-module N may be such that $(-) \otimes_R N$ is exact. When this happens, N receives a special name.

Definition 1.6.14. We say that an R-module N is *flat* if $(-) \otimes_R N$ is an exact functor, i.e., if for every exact sequence

$$0 \longrightarrow M \xrightarrow{f} M'$$

we have that

$$0 \longrightarrow M \otimes_R N \xrightarrow{f\otimes 1} M' \otimes_R N$$

is also exact.

Example 1.6.15. Free R-modules are flat. This is immediate from the isomorphism $R^n \otimes_R M \cong M^n$.

The most important example of flat R-modules for us will be the localizations $S^{-1}R$ of R.

Theorem 1.6.16. *Let R be a ring, S a multiplicative subset of R with $0 \notin S$ and*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

an exact sequence of R-modules. Then

$$0 \longrightarrow S^{-1}A \xrightarrow{S^{-1}f} S^{-1}B \xrightarrow{S^{-1}g} S^{-1}C \longrightarrow 0$$

is also exact. In other words, $S^{-1}R$ is a flat R-module.

Proof. Since $S^{-1}M \cong M \otimes_R S^{-1}R$ for every R-module M, the exactness of

$$S^{-1}A \xrightarrow{S^{-1}f} S^{-1}B \xrightarrow{S^{-1}g} S^{-1}C \longrightarrow 0$$

follows from Proposition 1.6.13. Thus it remains to show that $S^{-1}A \xrightarrow{S^{-1}f} S^{-1}B$ is injective. Suppose $\frac{x}{s} \in S^{-1}A$ is such that $\frac{f(x)}{s} = 0$. Then there exists $u \in S$ such that $0 = uf(x) = f(ux)$. As f is injective, this implies $ux = 0$. Thus $\frac{x}{s} = 0$, proving that $S^{-1}f$ is injective. □

Corollary 1.6.17. *Let*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be an exact sequence of R-modules. Then $\mathrm{Supp}(B) = \mathrm{Supp}(A) \cup \mathrm{Supp}(C)$.

Proof. Thanks to Theorem 1.6.16, for any $P \in \mathrm{Spec}(R)$ we have that

$$0 \longrightarrow A_P \longrightarrow B_P \longrightarrow C_P \longrightarrow 0$$

is exact. Thus, if $P \in \mathrm{Supp}(A) \cup \mathrm{Supp}(C)$, then $A_P \neq 0$ or $C_P \neq 0$, which forces $B_P \neq 0$, i.e, $P \in \mathrm{Supp}(B)$. Conversely, if $P \notin \mathrm{Supp}(A) \cup \mathrm{Supp}(C)$, then $A_P = 0$ and $C_P = 0$, implying $B_P = 0$, i.e., $P \notin \mathrm{Supp}(B)$. □

Remark 1.6.18. The other very important example of a flat R-module, when R is local, is the completion $\widehat{R}$ of R. However, that is a topic we will not go into in this course. I recommend [Mat86, Section 8] or [AM69, Chapter 10] for those interested in learning about completion.

1.7 Noetherian rings and modules

We now introduce the concept of Noetherian rings. These are the kind of rings that most commutative algebraists focus on studying. In fact, throughout the rest of this course, we will be working over Noetherian rings essentially 100% of the time. What makes this property so nice to work with is that it will allow us to obtain several finiteness properties from infinite rings.

Definition 1.7.1. A ring R is said to be *Noetherian* if every ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

eventually stabilizes, i.e., if there exists N such that $I_n = I_{n+1}$ for every $n \geq N$.

Proposition 1.7.2. *Let R be a ring. The following are equivalent:*

1. *R is a Noetherian ring.*
2. *Every nonempty family of ideals of R has a maximal element (under $\subseteq$).*
3. *Every ascending chain of finitely generated ideals of R stabilizes.*
4. *Given any generating set S for an ideal I, I is generated by a finite subset of S.*
5. *Every ideal of R is finitely generated.*

Proof. (1) $\Rightarrow$ (2) : By contradiction. Suppose there exists a nonempty family of ideals of R without a maximal element. Then one can inductively pick elements $I_1, I_2, \ldots$ from that family such that $I_i \subsetneq I_{i+1}$ for all $i \geq 1$. The chain $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ does not stabilize and therefore R is not Noetherian.

(2) $\Rightarrow$ (1) : An ascending chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ must have a maximal element I_N by (2). Hence it stabilizes at I_N.

(1) $\Rightarrow$ (3) : Clear.

(3) $\Rightarrow$ (4) : By contradiction. Suppose an ideal I is generated by a set S, but not by any finite subset of S. Pick $s_1 \in S$. Then $(s_1) \subsetneq (S) = I$, hence we can pick $s_2 \in S$ such that $s_2 \notin (s_1)$. Thus $(s_1) \subsetneq (s_1, s_2)$. As $(s_1, s_2) \subsetneq (S) = I$, we can pick $s_3 \in S$ such that $s_3 \notin (s_1, s_2)$. Thus $(s_1) \subsetneq (s_1, s_2) \subsetneq (s_1, s_2, s_3)$. Continuing in this way, we construct an ascending chain of finitely generated ideals of R that does not stabilize, contradicting (3).

(4) $\Rightarrow$ (5) : Clear.

(5) $\Rightarrow$ (1) : Given an ascending chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ of ideals of R, let $I = \bigcup_{i=1}^{\infty} I_n$. I is an ideal of R, hence by (5) it must be finitely generated. Let $a_1, \ldots, a_r \in I$ be such that $I = (a_1, \ldots, a_r)$. For each $1 \leq i \leq r$ there must exist n_i such that $a_i \in I_{n_i}$. If $N = \max\{n_1, \ldots, n_r\}$, we have that, for all $n \geq N$,

$$I_N \subseteq I_n \subseteq I = (a_1, \ldots, a_r) \subseteq I_N.$$

Hence $I_n = I_N$ for all $n \geq N$. □

Example 1.7.3. (1) Every field k is a Noetherian ring, as its only ideals are (0) and k.

(2) $\mathbb{Z}$ is a Noetherian ring, as every ideal of $\mathbb{Z}$ is finitely generated. In fact, $\mathbb{Z}$ is a PID, so every ideal is generated by a single element.

(3) Let k be a field. The polynomial ring $k[x_1, x_2, x_3, \ldots]$ over k in infinitely many variables is not Noetherian. The following is an ascending chain of ideals in $k[x_1, x_2, x_3, \ldots]$ that does not stabilize:

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

(4) The ring $\mathcal{C}(\mathbb{R},\mathbb{R})$ of continuous real-valued functions is not Noetherian. The ideals

$$I_n = \{f \in \mathcal{C}(\mathbb{R},\mathbb{R}) : f|_{[-1/n,1/n]} = 0\}$$

form a strictly increasing chain.

The following couple of results show how one can obtain Noetherian rings from known Noetherian rings.

Proposition 1.7.4. *If R is a Noetherian ring and I is an ideal of R, then R/I is also a Noetherian ring.*

Proof. By Proposition 1.1.8, ideals in R/I correspond to ideals of R that contain I. Hence if every ideal in R is finitely generated, so must be every ideal in R/I. □

Theorem 1.7.5. (Hilbert's Basis Theorem) *Let R be a Noetherian ring. Then the polynomial ring $R[X]$ and the power series ring $R[\![X]\!]$ are Noetherian rings.*

Proof. We will prove the result for $R[X]$ and in the end we will indicate the necessary changes one needs to do to adapt it to $R[\![X]\!]$.

Let I be an ideal of $R[X]$. We will show that I is finitely generated. Every $f \in R[X]$ can be written as $aX^m +$ (terms of degree lower than m in X). We call a the leading coefficient of f. For each $n \geq 0$ let

$$J_n = \{a \in R : a \text{ is the leading coefficient of some } f \in I \text{ of degree} \leq n\}.$$

One easily checks that each J_n is an ideal of R. As R is Noetherian, J_n is finitely generated. Let $J_n = (a_{n1}, \ldots, a_{nr_n})$ with $a_{n1}, \ldots, a_{nr_n} \in R$. There exist $f_{n1}, \ldots, f_{nr_n} \in I$ of degree $\leq n$ such that a_{ni} is the leading coefficient of f_{ni} for all $1 \leq i \leq r_n$. The ideals J_n form a chain

$$J_0 \subseteq J_1 \subseteq J_2 \subseteq \cdots .$$

Since R, is Noetherian, this chain must stabilize, so there exists N such that $J_n = J_N$ for all $n \geq N$. We will show that

$$\{f_{ni} : 0 \leq n \leq N, 1 \leq i \leq r_n\}$$

is a generating set of I. Let $f \in I$. We show by induction on $\deg f$ that $f \in (f_{ni} : 0 \leq n \leq N, 1 \leq i \leq r_n)$. If $\deg f = 0$, then $f \in R$ and f must be an R-linear combination of $f_{01}, \ldots, f_{0r_0}$. If $1 \leq \deg f = d < N$, then the leading coefficient a of f is in J_d, and thus it is an R-linear combination of $a_{d1}, \ldots a_{dr_d}$. Therefore, we can find a suitable $R[X]$-linear combination g of $f_{d1}, \ldots f_{dr_d}$ that cancels the leading term of f, i.e., such that $\deg(f-g) < d$. Since $f - g \in I$, by the induction hypothesis we have that $f - g \in (f_{ni} : 0 \leq n \leq d-1, 1 \leq i \leq r_n)$. Thus $f \in (f_{ni} : 0 \leq n \leq d, 1 \leq i \leq r_n)$. Finnaly, if $\deg f \geq N$, in a similar way we can find a suitable $R[X]$-linear combination g of $f_{N1}, \ldots f_{Nr_N}$ such that $\deg(f-g) \leq N-1$. By the induction hypothesis we conclude that $f \in (f_{ni} : 0 \leq n \leq N, 1 \leq i \leq r_n)$. This concludes the proof.

The proof for $R[\![X]\!]$ requires a bit of a different approach, so we will skip it here. □

Corollary 1.7.6. *Let k be a field or $k = \mathbb{Z}$. Then every quotient of $k[X_1, \ldots, X_n]$ and of $k[\![X_1, \ldots, X_n]\!]$ is a Noetherian ring.*

For modules, the Noetherian property is defined in a similar way to rings.

Definition 1.7.7. Let R be a ring. An R-module M is said to be *Noetherian* if every ascending chain of submodules of M eventually stabilizes.

The following criteria for an R-module to be Noetherian can be shown in the same way as Proposition 1.7.2.

Proposition 1.7.8. *Let R be a ring and M an R-module. The following are equivalent:*

1. *M is a Noetherian R-module.*
2. *Every nonempty family of submodules of M has a maximal element (under $\subseteq$).*
3. *Every ascending chain of finitely generated submodules of M stabilizes.*
4. *Given any generating set S for a submodule P of M, P is generated by a finite subset of S.*
5. *Every submodule of M is finitely generated.*

In particular, if M if a Noetherian R-module, M must be finitely generated.

Example 1.7.9. (1) A ring R is Noetherian if and only if is Noetherian as a module over itself.

(2) $\mathbb{Z} \subseteq \mathbb{Q}$ is an inclusion of Noetherian rings. However, $\mathbb{Q}$ is not Noetherian as an $\mathbb{Z}$-module. In fact, $\mathbb{Q}$ is not even finitely generated over $\mathbb{Z}$. Indeed, given any finitely generated submodule $P = \frac{a_1}{b_1}\mathbb{Z} + \cdots + \frac{a_r}{b_r}\mathbb{Z}$ of $\mathbb{Q}$, P will not contain $\frac{1}{p}$ for every prime $p > \max\{b_1, \ldots, b_r\}$.

The Noetherian property for modules behaves well with respect to short exact sequences in the following way:

Lemma 1.7.10. *Let R be a ring and*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

a short exact sequence of R-modules. Then B is Noetherian if and only if A and C are both Noetherian.

Proof. Suppose first that B is Noetherian. As $A \cong \operatorname{im} f$, A is isomorphic to a submodule of B. Therefore, an ascending chain of submodules of A is isomorphic to an ascending chain of submodules of B, hence it must stabilize. On the other hand, C is isomorphic to a quotient of B as $C \cong B/A$. Consequently, an ascending chain of submodules of C corresponds to as ascending chain of submodules of B which contain A, hence it must also stabilize.

Assume now that A and C are Noetherian. We will identify A with $\operatorname{im} f$ throughout the rest of the proof. Suppose

$$M_1 \subseteq M_2 \subseteq \cdots$$

is an ascending chain of submodules of B. Then

$$M_1 \cap A \subseteq M_2 \cap A \subseteq \cdots$$

is an ascending chain of submodules of A, while

$$g(M_1) \subseteq g(M_2) \subseteq \cdots$$

is an ascending chain of submodules of C. By hypothesis, both of these chains must stabilize. Hence, for $n \gg 0$ we have

$$M_n \subseteq M_{n+1}, \quad g(M_n) = g(M_{n+1}) \quad \text{and} \quad M_n \cap A = M_{n+1} \cap A.$$

It is now enough to show that these conditions imply $M_n = M_{n+1}$. Let $x \in M_{n+1}$. Since $g(x) \in g(M_{n+1}) = g(M_n)$, there exists $y \in M_n$ such that $g(x) = g(y)$, that is, $x - y \in \ker g = \operatorname{im} f = A$. As $y \in M_{n+1}$, we have in fact that

$$x - y \in M_{n+1} \cap A = M_n \cap A.$$

Hence $x - y \in M_n$. Given that $y \in M_n$, we conclude that $x \in M_n$. This proves the inclusion $M_{n+1} \subseteq M_n$. □

Corollary 1.7.11. *Let R be a ring and A and C be R-modules. Then A and C are Noetherian if and only if so is $A \oplus C$.*

Proof. Apply Lemma 1.7.10 to the short exact sequence $0 \longrightarrow A \longrightarrow A \oplus C \longrightarrow C \longrightarrow 0$. □

Corollary 1.7.12. *Let R be a ring and M be an R-module. Then M is Noetherian if and only if M^n is Noetherian for every $n \geq 1$. In particular, R is a Noetherian ring if and only if R^n is a Noetherian R-module for every $n \geq 1$.*

Proof. By induction on n. There is nothing to prove for $n = 1$. For $n > 1$ consider the short exact sequence $0 \longrightarrow M \longrightarrow M^n \longrightarrow M^{n-1} \longrightarrow 0$ and apply Lemma 1.7.10 and the induction hypothesis. □

Proposition 1.7.13. *Let R be a Noetherian ring and M be an R-module. Then M is Noetherian if and only if M is finitely generated.*

Proof. If M is Noetherian, then M needs to be a finitely generated R-module by Proposition 1.7.8.

Suppose now M is finitely generated, so that there exist $x_1, \dots, x_n \in M$ such that $M = Rx_1 + \cdots + Rx_n$. Consider the R-homomorphism $\varphi : R^n \to M$ given by

$$\varphi(a_1, \dots, a_n) = a_1x_1 + \cdots + a_nx_n.$$

Then φ is surjective. Hence M is isomorphic to a quotient of R^n. Since, by Corollary 1.7.12, R^n is a Noetherian R-module, M must also be Noetherian. □

The above result implies that, over a Noetherian ring, submodules of finitely generated modules are also finitely generated.

1.8 Artinian rings and modules

1.8.1 Length

Definition 1.8.1. An R-module $M \neq 0$ is *simple* if its only submodules are 0 and M.

Remark 1.8.2. A simple R-module must be cyclic, for if $0 \neq m \in M$, then Rm must be all of M. Thus every simple module is isomorphic to R/I, for an ideal I of R. But then I must be maximal, otherwise if $\mathfrak{m}$ is a maximal ideal of R such that $I \subsetneq \mathfrak{m} \subsetneq R$, R/I would contain the proper submodule $\mathfrak{m}/I$. We conclude that an R-module M is simple if and only if it is isomorphic to $R/\mathfrak{m}$, for a maximal ideal $\mathfrak{m}$ of R.

Definition 1.8.3. *(Length)* An R-module M has *finite length* if it has a filtration of the form

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$$

with M_{i+1}/M_i simple for every i. Such a filtration is called a *composition series of* M of *length* n. We say that a composition series is *strict* if $M_{i+1} \neq M_i$ for each i. Two composition series of M are said to be *equivalent* if the collections of the simple modules M_{i+1}/M_i are the same up to reordering.

The *length* of a finite length module M, denoted $\ell(M)$, if the minimum of the lengths of all composition series of M. If M does not have finite length, we set $\ell(M) = \infty$.

Theorem 1.8.4. (Jordan-Holder theorem) *Let M be an R-module of finite length. Then*

(1) Any proper submodule N of M satisfies $\ell(N) < \ell(M)$.

(2) Any filtration of M can be refined to a composition series.

(3) All strict composition series for M have the same length $\ell(M)$.

Proof. (1): Let $n = \ell(M)$. Consider a strict composition series of M of length n

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M.$$

Then

$$0 = M_0 \cap N \subseteq M_1 \cap N \subseteq M_2 \cap N \subseteq \cdots \subseteq M_n \cap N = N$$

is a filtration of N. The successive quotients of this filtration are, by the second isomorphism theorem,

$$(M_{i+1} \cap N)/(M_i \cap N) \cong (M_{i+1} \cap N + M_i)/M_i \subseteq M_{i+1}/M_i.$$

As M_{i+1}/M_i, for each i two cases can occur:

1. $M_i \cap N = M_{i+1} \cap N$. This means that the inclusion $M_i \cap N \subseteq M_{i+1} \cap N$ can be removed from the filtration.
2. $M_{i+1} \cap N + M_i = M_{i+1}$.

Thus, after removing the redundant inclusions relative to the i such that 1. occurs, we are left with a strict composition series for $M \cap N$. This shows that $\ell(N) \leq \ell(M)$. Plus, equality holds if and only if case 2. holds for every $i = 0, \dots, n-1$. But this means the following:

$M_1 = M_1 \cap N + M_0 = M_1 \cap N$,

$M_2 = M_2 \cap N + M_1 = M_2 \cap N + M_1 \cap N = M_2 \cap N,$

$M_3 = M_3 \cap N + M_2 = M_3 \cap N + M_2 \cap N = M_3 \cap N,$

$\vdots$

$M = M_n = M_n \cap N + M_{n-1} = M_n \cap N + M_{n-1} \cap N = M_n \cap N = M \cap N = N.$

This contradicts the assumption that $N \subseteq M$ is strict. Hence $\ell(N) < \ell(M)$.

(2): We claim that every filtration

$$\mathcal{F} : N_0 \subsetneq N_1 \subsetneq N_2 \subsetneq \cdots \subsetneq N_k$$

of submodules of M must satisfy $k \leq \ell(M)$. This will prove the result because

1. If $k < \ell(M)$, then $\mathcal{F}$ cannot be a composition series (by the definition of $\ell(M)$), thus one of the inclusions $N_i \subsetneq N_{i+1}$ must be such that N_{i+1}/N_i is not simple, hence it can be extended to $N_i \subsetneq N \subsetneq N_{i+1}$.
2. If $k = \ell(M)$, then $\mathcal{F}$ must be a composition series, because otherwise, similar to the previous case, we would be able to extent it to a filtration of size bigger that $\ell(M)$.

We prove the claim by induction on $\ell(M)$. If $\ell(M) = 0$, then $M = 0$ and the claim is trivial. Now suppose $\ell(M) \geq 1$ and that the statement holds for modules of length $< \ell(M)$. N_{k-1} must be a strict submodule of M, hence by (1) we have $\ell(N_{k-1}) < \ell(M)$. By induction, $k - 1 \leq \ell(N_{k-1})$ and we conclude that $k \leq \ell(M)$.

(3) Let

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$$

be a strict composition series of M. By definition of $\ell(M)$ we have $\ell(M) \leq n$. On the other hand, by (1) we see that

$$0 = \ell(M_0) < \ell(M_1) < \ell(M_2) < \cdots < \ell(M_{n-1}) < \ell(M)$$

which forces $\ell(M) \geq n$. Thus every strict composition series of M has length $\ell(M)$. □

Notice that, if M is a finitely generated module over a local ring $(R, \mathfrak{m}, k)$ such that $\mathfrak{m}M = 0$ (so that M is a k-vector space), then $\ell(M) = \dim_k M$.

Length also behaves well with respect to short exact sequences.

Proposition 1.8.5. *Let*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be an exact sequence of R-modules. Then $\ell(B) = \ell(A) + \ell(C)$.

Proof. We begin by assuming that $\ell(B) < \infty$. Then $\ell(A) < \infty$ since $A \subseteq B$ and also $\ell(C) < \infty$ since $C \cong B/A$.

Let

$$0 = A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots \subseteq A_n = A$$

be a strict composition series for A ($n = \ell(A)$) and let

$$0 = B_0/A \subseteq B_1/A \subseteq B_2/A \subseteq \cdots \subseteq B_k/A = B/A$$

be a strict composition series for $B/A \cong C$ ($k = \ell(C)$). Then

$$0 = A_0 \subseteq A_1 \subseteq \cdots \subseteq A_n = A \subseteq B_1 \subseteq B_2 \subseteq \cdots \subseteq B_k = B$$

is a strict composition series for B. Indeed, every successive quotient must a simple module since it is isomorphic to a successive quotient from one of the two previous composition series. This shows that $\ell(B) = \ell(A) + \ell(C)$.

If $\ell(B) = \infty$, then $\ell(A) = \infty$ or $\ell(C) = \infty$, since otherwise the same argument would show that $\ell(B) < \infty$. □

In the following remark we list some direct consequences of the previous results, which you can check yourself.

Remark 1.8.6.

(1) If

$$0 \longrightarrow A_1 \longrightarrow \cdots \longrightarrow A_n \longrightarrow 0$$

is an exact sequence of R-modules of finite length, then $\sum_{i=1}^{n} (-1)^i \ell(A_i) = 0$.

(2) Given a chain of submodules $M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$, we have

$$\ell(M) = \ell(M_0) + \sum_{i=0}^{n-1} \ell(M_{i+1}/M_i).$$

(3) If M has finite length and $N \subseteq M$ is a submodule of N, then $\ell(N) \leq \ell(M)$. The equality $N = M$ holds if and only if $\ell(N) = \ell(M)$.

Note: Sometimes, for clarity, we may write $\ell_R(M)$ instead of just $\ell(M)$ to empathize that we are taking the length of M viewed as an R-module.

1.8.2 The Artinian property

Here we define Artinian rings and modules. While the Noetherian property was defined based on the ascending chain condition (a.c.c.), the Artinian property is defined based on the descending chain condition (d.c.c.).

Definition 1.8.7. A ring R is said to be *Artinian* if every descending chain of ideals of R

$$I_0 \supseteq I_1 \supseteq I_2 \supseteq \cdots$$

eventually stabilizes, i.e., there exists N such that $I_n = I_{n+1}$ for all $n \geq N$.

An R-module M is *Artinian* if it satisfies the d.c.c. for submodules of M, that is, if every descending chain of submodules of M eventually stabilizes.

The following remarks are analogous to ones we made previously for Noetherian rings:

1. If R is an Artinian ring, then so is R/I, for an ideal $I \subseteq R$.
2. A ring R is Artinian if and only if every nonempty family of ideals of R has a minimal element.
3. If M is an Artinian R-module, then so if N and M/N for any submodule $N \subseteq M$.

The Artinian property, together with the Noetherian property, characterize modules of finite length.

Lemma 1.8.8. *An R-module M has finite length if and only if M is both Artinian and Noetherian.*

Proof. ($\Rightarrow$) : If M has finite length, every strict chain of submodules of M can have length at most $\ell(M)$. In particular, every ascending or descending chains of submodules of M must eventually stabilize.

($\Leftarrow$) : Suppose now $M \neq 0$ is both Artinian and Noetherian. The set of proper submodules of M is then nonempty and thus, by the Noetherian property, must have a maximal element M_1. Therefore, M/M_1 must be a simple module. Applying the same reasoning to M_1, we have that either $M_1 = 0$ or there exists a submodule $M_2 \subset M_1$ such that M_1/M_2 is simple. We can continue in this way, building a chain

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq M_3 \supsetneq \cdots$$

such that M_i/M_{i+1} is simple for every i, as long as $M_j \neq 0$ at every step j. But since M is Artinian, this descending chain cannot be infinite. Therefore, eventually we must end up with $M_j = 0$. Then

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots \supseteq M_j = 0$$

is a composition series for M, showing that $\ell(M) < \infty$. □

We also have the following characterization for modules of finite length over Noetherian local rings:

Corollary 1.8.9. *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring. An R-module M has finite length if and only if M is finitely generated and $\mathfrak{m}^n M = 0$ for some $n \geq 0$.*

Proof. ($\Rightarrow$) : By Lemma 1.8.8, if M has finite length, M needs to be Noetherian, which implies that M is finitely generated. Also, M must be Artinian, so that the chain $M \supseteq \mathfrak{m}M \supseteq \mathfrak{m}^2M \supseteq \cdots$ must eventually stabilize. Thus, there exists $n \geq 0$ such that $\mathfrak{m}^nM = \mathfrak{m}^{n+1}M = \mathfrak{m}(\mathfrak{m}^nM)$. As $\mathfrak{m}^nM$ is a finitely generated R-module, by Nakayama's Lemma we conclude that $\mathfrak{m}^nM = 0$.

($\Leftarrow$) : As $\mathfrak{m}^nM = 0$, by Remark 1.8.6 2., we have that $\ell(M) = \sum_{i=0}^{n-1} \ell(\mathfrak{m}^iM/\mathfrak{m}^{i+1}M)$. As M is finitely generated and R is Noetherian, M is a Noetherian R-module, thus all the $\mathfrak{m}^iM$ are finitely generated modules. Therefore $\ell(\mathfrak{m}^iM/\mathfrak{m}^{i+1}M) = \dim_k(\mathfrak{m}^iM/\mathfrak{m}^{i+1}M) = \mu(\mathfrak{m}^iM)$ is finite for every i. We conclude that $\ell(M) < \infty$. □

Remark 1.8.10. One consequence of Corollary 1.8.9 is the following:

If $(R, \mathfrak{m})$ is a Noetherian local ring and I is an ideal of R, then

$$R/I \text{ is an Artinian ring } \iff \mathfrak{m}^n \subseteq I \text{ for some } n \geq 0.$$

We now provide a full description of Artinian rings. We will not be able to give the full proof yet, though, as it requires tools and results we will introduce in Section 2.

Theorem 1.8.11. *Let R be a ring. The following are equivalent*

(1) R is Artinian.

(2) R is Noetherian and every prime ideal of R is maximal.

Proof. We won't prove (2) $\Rightarrow$ (1) here. We will come back to it in Section 2. We show (1) $\Rightarrow$ (2). So, suppose R is Artinian.

Step 1: Show that every prime ideal of R is maximal.

Let P be a prime ideal of R. Then $A = R/P$ is an Artinian domain. Let a be a nonzero element of A. The decreasing chain $(a) \supseteq (a^2) \supseteq (a^3) \supseteq \cdots$ must eventually stabilize, so that there exists n such that $(a^n) = (a^{n+1})$. Hence, there exists $b \in A$ such that $a^n = a^{n+1}b$. As A is a domain, a is a nonzero divisor in A, hence we can cancel a^n on both sides to obtain $1 = ab$. This shows that every nonzero element of A is invertible. Thus $A = R/P$ is a field, meaning that P is a maximal ideal of R.

Step 2: Show that R has a finite number of maximal ideals.

Suppose there are an infinite number of maximal ideals of R, namely $\mathfrak{m}_1, \mathfrak{m}_2, \ldots$ (all distinct). Consider the decreasing chain

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

This chain must stabilize, so that there exists k such that $\mathfrak{m}_1 \cdots \mathfrak{m}_k = \mathfrak{m}_1 \cdots \mathfrak{m}_k\mathfrak{m}_{k+1} \subseteq \mathfrak{m}_{k+1}$. As $\mathfrak{m}_{k+1}$ is prime, there must exist $1 \leq i \leq k$ such that $\mathfrak{m}_i \subseteq \mathfrak{m}_{k+1}$. But this contradicts the assumption that $\mathfrak{m}_i$ and $\mathfrak{m}_{k+1}$ are distinct maximal primes of R. Thus, let $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ be all the maximal ideals of R.

Step 3: Let $I = \mathfrak{m}_1 \cdots \mathfrak{m}_r$. Then there exists n such that $I^n = 0$.

The chain $I \supseteq I^2 \supseteq I^3 \supseteq \cdots$ must eventually stabilize, so that there exists n such that $I^n = I^{n+1}$. Note, however, that we cannot use Nakayama's Lemma to conclude that $I^n = 0$ since at this point we don't know that I^n is finitely generated. Suppose $I^n \neq 0$. Consider the family $\mathcal{S}$ of all the ideals J of R such that $JI^n \neq 0$. $\mathcal{S}$ is nonempty since $I \in \mathcal{S}$. As R is Artinian, there must exist a minimal element J in $\mathcal{S}$.

There exists $x \in J$ such that $xI^n \neq 0$. Hence $(x)I^n \neq 0$. Thus, the minimality of J implies that $J = (x)$. Observe now that

$$((x)I)I^n = (x)I^{n+1} = (x)I^n \neq 0.$$

Thus $(x)I \neq 0$ and $(x)I \in \mathcal{S}$. Hence, by the minimality of (x) in $\mathcal{S}$, we have that $(x) = (x)I$. As $I \subseteq \text{rad}(R)$, we can now use Nakayama's Lemma to conclude that $(x) = (0)$. But this contradicts the assumption that $(x)I^n \neq 0$.

Step 4: R is Noetherian.

By Lemma 1.8.8 it is enough to show that R has finite length as a module over itself. Consider the following chain of ideals of R:

$$\begin{aligned}\mathcal{F} : R \supseteq \mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \cdots \supseteq I \supseteq I\mathfrak{m}_1 \supseteq I\mathfrak{m}_1\mathfrak{m}_2 \supseteq \cdots \supseteq I^2 \supseteq \cdots \\ \supseteq I^{n-1} \supseteq I^{n-1}\mathfrak{m}_1 \supseteq \cdots \supseteq I^n = 0.\end{aligned}$$

Every inclusion in the chain is of the form $J \supseteq \mathfrak{m}_i J$. The quotient $J/\mathfrak{m}_i J$ is a vector space over the field $R/\mathfrak{m}_i$. Plus, as $J/\mathfrak{m}_i J$ is Artinian, it must be a finite dimensional $R/\mathfrak{m}_i$-vector space (if it was infinite dimensional we would be able to find an infinitely decreasing chain of subspaces of $J/\mathfrak{m}_i J$). Thus every successive quotient in the filtration $\mathcal{F}$ has finite length. We conclude that R has finite length. □

Example 1.8.12.

1. Let k be a field. Then $k[\![x, y]\!]/(x^3, y^3)$ and $k[x, y]/(x^2, xy, y^2)$ are examples of Artinian rings.
2. $k[\![x_1, x_2, \ldots]\!]/(x_1^2, x_2^2, \ldots)$ is an example of a ring which only has one prime ideal, but is neither Noetherian or Artinian.
3. While Theorem 1.8.11 says that every Artinian ring must be Noetherian, this is a statement that does not hold true for modules. As an example, let k be a field, $R = k[\![x]\!]$ and $M = R_x/R$. You can check (exercise) that M is an Artinian R-module, but M is not Noetherian (it is not even finitely generated).

2 Primary decomposition

2.1 The radical of an ideal

Definition 2.1.1. Given an ideal I of a ring R, the *radical* of I is

$$\sqrt{I} = \{f \in R : f^n \in I \text{ for some } n \in \mathbb{N}\}.$$

I is said to be *radical* if $I = \sqrt{I}$.

Observe that the radical of an ideal is also an ideal. Clearly if $f \in \sqrt{I}$ then also $af \in \sqrt{I}$ for every $a \in R$. On the other hand, if $f_1, f_2 \in \sqrt{I}$, then $f_1^n, f_2^m \in I$ for some n, m, then also $(f_1 + f_2)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} f_1^i f_2^{n+m-i} \in I$, which implies $f_1 + f_2 \in \sqrt{I}$. Note that we can use Newton's binomial expansion because R is commutative.

The following properties of the radical are easy to show.

Proposition 2.1.2. *Let I, J be ideals of a ring R. Then*

(1) $I \subseteq \sqrt{I}$. Also $\sqrt{\sqrt{I}} = \sqrt{I} = \sqrt{I^n}$ for all $n \geq 1$.

(2) If $I \subseteq J$ then $\sqrt{I} \subseteq \sqrt{J}$.

(3) $\sqrt{I \cap J} = \sqrt{IJ} = \sqrt{I} \cap \sqrt{J}$

(4) $\sqrt{P} = P$ if P is a prime ideal.

(5) If R is Noetherian, then there exists $n \geq 1$ such that $(\sqrt{I})^n \subseteq I$.

If I is an ideal of R, recall that $V(I)$ denotes the closed subset $\{P \in \operatorname{Spec}(R) : I \subseteq P\}$ of $\operatorname{Spec}(R)$. Notice that for every ideal I we have

$$V(I) = V(\sqrt{I}).$$

Indeed, if $P \in V(\sqrt{I})$, then $I \subseteq \sqrt{I} \subseteq P$ imples $P \in V(I)$. Conversely, suppose $P \in V(I)$. Given any $f \in \sqrt{I}$, there exists $n \geq 1$ such that $f^n \in I \subseteq P$. As P is prime, we must have $f \in P$. This shows that $\sqrt{I} \subseteq P$, i.e., $P \in V(\sqrt{I})$.

We now prove a closer relationship between $\sqrt{I}$ and $V(I)$.

Theorem 2.1.3. *Let I be an ideal of a ring R. Then*

$$\sqrt{I} = \bigcap_{p \in V(I)} P.$$

Proof. $(\subseteq)$: Suppose $f \in \sqrt{I}$. Then, for some $n \geq 1$, $f^n \in I$. Thus $f^n \in P$ for every $P \in V(I)$. As every such P is prime, we must have $f \in P$ for every $P \in V(I)$.

$(\supseteq)$: Suppose $f \notin \sqrt{I}$. Then I does not intersect the multiplicatively closed set $S = \{1, f, f^2, \ldots\}$. Consider the localization R_f of R at S. Denote $I_f = S^{-1}I \subseteq R_f$. As I does not intersect S, I_f is a proper ideal of R_f. Thus, there exists a maximal (hence prime) ideal Q of R_f such that $I_f \subseteq Q$. By Theorem 1.4.6, Q must be of the form $S^{-1}P$, where P is a prime ideal of R that does not intersect S and such that $I \subseteq P$. Therefore, there exists $P \in V(I)$ such that $f \notin P$. □

As a consequence, notice that we have the following equivalences for any $f \in R$ and any ideal I:

$$f \in \sqrt{I} \iff f \in P \quad \forall P \in V(I) \iff V(I) \subseteq V(f).$$

Corollary 2.1.4. *Let R be a ring. There is an order reversing bijection between the Zariski closed subsets of* $\operatorname{Spec}(R)$ *and the radical ideals of R. In particular, for two ideals I and J, we have that*

$$V(I) = V(J) \iff \sqrt{I} = \sqrt{J}.$$

Proof. $(\Rightarrow)$: Follows directly from Theorem 2.1.3.

$(\Leftarrow)$: Let $P \in V(I)$. Then $J \subseteq \sqrt{J} = \sqrt{I} \subseteq P$. Thus $P \in V(J)$. This shows that $V(I) \subseteq V(J)$. In the same way we can show $V(I) \supseteq V(J)$. □

We close this small subsection with the notion of the nilradical.

Definition 2.1.5. Let R be a ring. The *nilradical* of R is the ideal $\mathcal{N}(R) = \sqrt{(0)} = \{a \in R : a^n = 0 \text{ for some } n \geq 1\}$.

An element $a \in R$ is said to be *nilpotent* if $a \in \mathcal{N}(R)$.

R is said to be *reduced* if its nilradical is (0), i.e., if for every $a \in R$ and $n \in \mathbb{N}$, $a^n = 0$ implies $a = 0$.

By Theorem 2.1.3, the nilradical of R consists of the intersection of all the prime ideals of R. Observe also that if I is an ideal of R, then R/I is reduced if and only if I is radical.

2.2 Minimal primes

Definition 2.2.1. Let I be an ideal in a ring R. A *minimal prime* of I is a minimal element in $V(I)$ (with respect to inclusion). In other words, P is a minimal prime of I if P is a prime ideal such that $I \subseteq P$ and such that if Q is a prime ideal satisfying $I \subseteq Q \subseteq P$, then $Q = P$.

The set of minimal primes of I is denoted $\text{Min}(I)$.

By the set of minimal primes of the ring R we mean the set of minimal primes of (0).

Notice that $\text{Min}(P) = \{P\}$ if P is a prime ideal. Also, since $V(I) = V(\sqrt{I})$, we have that $\text{Min}(I) = \text{Min}(\sqrt{I})$ for any ideal I. Plus, we can restate the statement of Theorem 2.1.3 as

$$\sqrt{I} = \bigcap_{p \in \text{Min}(I)} P.$$

Example 2.2.2. Let $R = k[x, y, z]$, where k is a field. Then $\text{Min}((x^2z^2, y^3, xyz)) = \{(x, y), (y, z)\}$ and $\sqrt{(x^2z^2, y^3, xyz)} = (x, y) \cap (y, z) = (xz, y)$.

It turns out that the Noetherian property implies a nice finiteness condition on minimal primes.

Lemma 2.2.3. *Let I be an ideal of R. If $I = P_1 \cap \cdots \cap P_r$ with $P_1, \ldots, P_r$ prime ideals, then* $\text{Min}(I) \subseteq \{P_1, \ldots, P_r\}$. *In particular, I is radical and* $\text{Min}(I)$ *is finite.*

Proof. I must be radical, since $\sqrt{I} = \sqrt{P_1} \cap \cdots \cap \sqrt{P_r} = P_1 \cap \cdots \cap P_r = I$ by Proposition 2.1.2.

Notice that $P_i \in V(I)$ for every i. Let Q be a minimal prime of I. As $P_1 \cap \cdots \cap P_r \subseteq Q$, by Theorem 1.2.14 there exists j such that $P_j \subseteq Q$. The minimality of Q in $V(I)$ implies $Q = P_j$. This proves the lemma. □

Theorem 2.2.4. *Let R be a Noetherian ring. Then* $\text{Min}(I)$ *is a finite set for every ideal I of R.*

Proof. Let $\mathcal{S} = \{\text{ideals } I \text{ of } R : \text{Min}(I) \text{ is infinite}\}$ and suppose, by means of contradiction, that $\mathcal{S} \neq \emptyset$. Since R is Noetherian, $\mathcal{S}$ has a maximal element J. Notice that J is not prime, since otherwise $\text{Min}(P) = \{P\}$. Also, since $\text{Min}(J) = \text{Min}(\sqrt{J})$, we have $\sqrt{J} \in \mathcal{S}$. The inclusion $J \subseteq \sqrt{J}$ and the maximality of J in $\mathcal{S}$ imply that $J = \sqrt{J}$. As J is not prime, there exist $a, b \notin J$ such that $ab \in J$. Notice that

$$(J + (a))(J + (b)) \subseteq J^2 + J(a) + J(b) + (ab) \subseteq J.$$

Therefore, using Proposition 2.1.2,

$$J \subseteq \sqrt{J + (a)} \cap \sqrt{J + (b)} = \sqrt{(J + (a))(J + (b))} \subseteq \sqrt{J} = J.$$

So

$$J = \sqrt{J + (a)} \cap \sqrt{J + (b)}.$$

Plus, $J \subsetneq J + (a) \subseteq \sqrt{J + (a)}$, hence the maximality of J in $\mathcal{S}$ implies that $\text{Min}(\sqrt{J + (a)}) = \text{Min}(J + (a))$ is finite. Thus, by Theorem 2.1.3, $\sqrt{J + (a)}$ is the intersection of finitely many primes (and similarly for $\sqrt{J + (b)}$). We conclude that $J = \sqrt{J + (a)} \cap \sqrt{J + (b)}$ is also the intersection of finitely many primes. By Lemma 2.2.3 we conclude that $\text{Min}(J)$ is finite, which is a contradiction with $J \in \mathcal{S}$. □

The minimal primes of an ideal I correspond to the irreducible components of $V(I)$, i.e., If $\mathrm{Min}(I) = \{P_1, \ldots, P_r\}$, then

$$V(I) = V(P_1) \cup \cdots \cup V(P_r)$$

and each $V(P_i)$ is an irreducible closed subset of $\mathrm{Spec}(R)$. Indeed, $V(P)$ is irreducible for every prime ideal P, in the sense that if $V(P) = V(J_1) \cup V(J_2)$, then $V(P) = V(J_1)$ or $V(P) = V(J_2)$ (exercise).

We now have the tools required to finish the proof of Theorem 1.8.11.

Proof. Conclusion of the proof of Theorem 1.8.11:

We need to show that if R is a Noetherian ring in which every ideal is maximal, then R is Artinian.

The hypothesis can be rephrased as saying that R is Noetherian and every maximal ideal is a minimal prime of the ideal (0). Thus, by Theorem 2.2.4, R has finitely many maximal primes, say $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$. Also, $\mathcal{N}(R) = \sqrt{(0)} = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r$.

For n sufficiently large we have that $(\sqrt{(0)})^n \subseteq (0)$, i.e, $(\sqrt{(0)})^n = 0$. Therefore, $(\mathfrak{m}_1 \cdots \mathfrak{m}_r)^n \subseteq (\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r)^n = (0)$, i.e., $(\mathfrak{m}_1 \cdots \mathfrak{m}_r)^n = (0)$. We now consider the chain

$$\begin{aligned} R \supseteq \mathfrak{m}_1 \supseteq \mathfrak{m}_1^2 \supseteq \cdots \supseteq \mathfrak{m}_1^n \supseteq & \mathfrak{m}_1^n \mathfrak{m}_2 \supseteq \mathfrak{m}_1^n \mathfrak{m}_2^2 \supseteq \cdots \supseteq \mathfrak{m}_1^n \mathfrak{m}_2^n \supseteq \\ & \cdots \supseteq \mathfrak{m}_1^n \cdots \mathfrak{m}_{r-1}^n \mathfrak{m}_r \supseteq \cdots \supseteq \mathfrak{m}_1^n \cdots \mathfrak{m}_r^n = (0). \end{aligned}$$

Every successive quotient in this chain is a $R/\mathfrak{m}_i$-vector space for some i, hence it has finite length. We conclude that R has finite length as an R-module, hence it is an Artinian ring. □

2.3 Associated primes

Definition 2.3.1. Let M be an R-module. An *associated prime* of M is a prime ideal P such that

$$P = \mathrm{Ann}(x) \subseteq R$$

for some $x \in M$. The set of associated primes of M is denoted by $\mathrm{Ass}_R(M)$ or just $\mathrm{Ass}(M)$.

Notice that, for an ideal I of R, a homomorphism $f : R/I \longrightarrow M$ is determined by the image x of $1 + I$, which must satisfy $I \subseteq \mathrm{Ann}(x)$. f is injective if and only if $I = \ker f = \mathrm{Ann}(x)$. Thus, we see that

$$P \in \mathrm{Ass}(M) \iff P \text{ is a prime ideal such that } R/P \text{ can be embedded in } M.$$

Remark 2.3.2. If I is an ideal of R, then we will use a particular language: we will refer to the set of associated primes of the ideal I to mean the set of associated primes of the R-module R/I (and not the R-module I).

Notice that the associated prime ideals of I (i.e., of the module R/I) coincide with the prime ideals P of the form $P = (I : x)$ for some $x \notin I$. Observe that $\mathrm{Ass}(R/I) \subseteq V(I)$.

Example 2.3.3.

1. If P is a prime ideal of R, then $\mathrm{Ass}(R/P) = \{P\}$. Indeed, $P = (P : 1)$ and if Q is a prime ideal such that $Q = (P : x)$ with $x \notin P$, then $xQ \subseteq P$. As $x \notin P$ and P is prime, this implies $Q \subseteq P$. Since also $P \subseteq Q$, we must have $Q = P$.
2. Let $R = k[x, y]$, where k is a field. Then (x, y) is an associated prime ideal of $I = (x^2, xy)$ since (x, y) is prime and $(x, y) = ((x^2, xy) : x)$.

Under the Noetherian assumption on R and M, $\mathrm{Ass}(M)$ has rather nice properties, and provides a way to detect the zerodivisors of M.

Lemma 2.3.4. *Let R be a Noetherian ring and M a nonzero R-module. Then* $\mathrm{Ass}(M) \neq \emptyset$.

Proof. Let $\mathcal{S} = \{\mathrm{Ann}(x) : 0 \neq x \in M\}$. As R is Noetherian, $\mathcal{S}$ has a maximal element $\mathrm{Ann}(y)$. Notice that $\mathrm{Ann}(y) \neq R$ because $y \neq 0$. We show that $\mathrm{Ann}(y)$ is a prime ideal, and thus that $\mathrm{Ann}(y) \in \mathrm{Ass}(M)$. Let $a, b \in R$ be such that $ab \in \mathrm{Ann}(y)$ and suppose $a \notin \mathrm{Ann}(y)$, so that $ay \neq 0$. Then $\mathrm{Ann}(ay) \in \mathcal{S}$. The inclusion $\mathrm{Ann}(y) \subseteq \mathrm{Ann}(ay)$ and the maximality of $\mathrm{Ann}(y)$ in $\mathcal{S}$ implies that $\mathrm{Ann}(ay) = \mathrm{Ann}(y)$. Since $b(ay) = (ab)y = 0$, we have that $b \in \mathrm{Ann}(ay) = \mathrm{Ann}(y)$. We conclude that $\mathrm{Ann}(y)$ is a prime ideal. □

Lemma 2.3.5. *Let*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be an exact sequence of R-modules. Then $\operatorname{Ass}(A) \subseteq \operatorname{Ass}(B) \subseteq \operatorname{Ass}(A) \cup \operatorname{Ass}(C)$.

Proof. Let $P \in \operatorname{Ass}(A)$. Then there is an embedding $R/P \subseteq A$. As $A \subseteq B$, we see that R/P can be embedded in B, i.e., $P \in \operatorname{Ass}(B)$. Suppose now $P \in \operatorname{Ass}(B)$, so that there exists $x \in B$ such that $P = \operatorname{Ann}(x)$. Observe that for every $r \in R \backslash P$ we have $P = \operatorname{Ann}(x) = \operatorname{Ann}(rx)$. Indeed, the inclusion $\operatorname{Ann}(x) \subseteq \operatorname{Ann}(rx)$ is obvious; conversely, if $s \in \operatorname{Ann}(rx)$, then $0 = s(rx) = (sr)x$, which implies $sr \in P$ and, as $r \notin P$, we must have $s \in P = \operatorname{Ann}(x)$. Therefore we have two cases:

(1): There exists $r \notin P$ such that $rx \in A$. Then $P = \operatorname{Ann}(x) = \operatorname{Ann}(rx) \in \operatorname{Ass}(A)$.

(2): For every $r \notin P$ we have $rx \notin A$.

We claim that $P = \operatorname{Ann}(x) = \operatorname{Ann}(g(x))$. This will show that $P \in \operatorname{Ass}(C)$. The inclusion $P = \operatorname{Ann}(x) \subseteq \operatorname{Ann}(g(x))$ is trivial. Now suppose $r \notin P$. Then $rg(x) = g(rx) \neq 0$ because $rx \notin A = \ker g$, thus showing that $r \notin \operatorname{Ann}(g(x))$. □

Corollary 2.3.6. *Let A and C be R-modules. Then* $\operatorname{Ass}(A \oplus C) = \operatorname{Ass}(A) \cup \operatorname{Ass}(C)$.

Proof. Apply Lemma 2.3.5 to the short exact sequences $0 \longrightarrow A \longrightarrow A \oplus C \longrightarrow C \longrightarrow 0$ and $0 \longrightarrow C \longrightarrow A \oplus C \longrightarrow A \longrightarrow 0$. □

Corollary 2.3.7. *Let $I_1, \ldots, I_r$ be ideals of a ring R. Then*

$$\operatorname{Ass}(R/\bigcap_{j=1}^{r} I_j) \subseteq \bigcup_{j=1}^{r} \operatorname{Ass}(R/I_j).$$

Proof. It is enough to show the result for $r = 2$. The general result will follow by induction on r. The homomorphism $R \longrightarrow R/I_1 \oplus R/I_2$ given by $r \longmapsto (r + I_1, r + I_2)$ has kernel $I_1 \cap I_2$. Thus, there is an injective map $R/(I_1 \cap I_2) \longrightarrow R/I_1 \oplus R/I_2$. Lemma 2.3.5 now gives

$$\operatorname{Ass}(R/(I_1 \cap I_2)) \subseteq \operatorname{Ass}(R/I_1 \oplus R/I_2) = \operatorname{Ass}(R/I_1) \cup \operatorname{Ass}(R/I_2).$$

□

Theorem 2.3.8. *Let R be a Noetherian ring and M a nonzero finitely generated R-module. There exists a filtration*

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M$$

of submodules of M such that for every i we have $M_i/M_{i-1} \cong R/P_i$ with $P_i \in \operatorname{Spec}(R)$.

Such a filtration is called a prime filtration *of M.*

Given such a prime filtration of M we have that $\operatorname{Ass}(M) \subseteq \{P_1, \ldots, P_n\}$. *Thus* $\operatorname{Ass}(M)$ *is finite.*

Proof. By Lemma 2.3.4 there exists an associated prime P_1 of M. This means there exists a submodule M_1 of M such that $M \cong R/P_1$. If $M_1 = M$, we are done. Otherwise there exists an associated prime P_2 of M/M_1 and a submodule M_2/M_1 of M/M_1 such that $M_2/M_1 \cong R/P_2$. If $M_2 = M$ we are done. If not, then we can continue this process, building a chain $0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq \cdots$ of submodules of M such that $M_i/M_{i-1} \cong R/P_i$ with P_i prime ideals. But since M is Noetherian, this chain must be finite, meaning that $M_n = M$ for some $n \geq 1$.

Applying Lemma 2.3.5 to the short exact sequence

$$0 \longrightarrow M_{i-1} \longrightarrow M_i \longrightarrow M_i/M_{i-1} \longrightarrow 0$$

we see that $\operatorname{Ass}(M_i) \subseteq \operatorname{Ass}(M_{i-1}) \cup \operatorname{Ass}(M_i/M_{i-1}) = \operatorname{Ass}(M_{i-1}) \cup \operatorname{Ass}(R/P_i) = \operatorname{Ass}(M_{i-1}) \cup \{P_i\}$. Since $\operatorname{Ass}(0) = \emptyset$, using this successively with $i = n, n-1, \ldots, 1$ yields $\operatorname{Ass}(M) = \operatorname{Ass}(M_n) \subseteq \{P_1, \ldots, P_n\}$. □

Theorem 2.3.8 is very useful, as very often it will allow us to reduce problems about modules to problems about just modules of the form R/P with P prime.

We now recall the notion of *zerodivisors* and *nonzerodivisors* (also called *regular* elements).

Definition 2.3.9. Let M be an R-module. An element $r \in R$ is said to be a *zerodivisor* in M if there exists $0 \neq m \in M$ such that $am = 0$. The set of zerodivisors of M is denoted $\mathcal{Z}(M)$.

If r is not a zerodivisor of M, then r is called a *nonzerodivisor* of M.

Nonzerodivisors of M are also called M-*regular* elements.

Proposition 2.3.10. *Let R be a Noetherian ring and $0 \neq M$ an R-module. Then*

$$\mathcal{Z}(M) = \bigcup_{P \in \operatorname{Ass}(M)} P.$$

Proof. ($\supseteq$): If $P \in \operatorname{Ass}(M)$, then $P = \operatorname{Ann}(m)$, with $m \neq 0$, thus P consists of zerodivisors of M.

($\subseteq$): If r is a zerodivisor of M, there exists $0 \neq m \in M$ such that $r \in \operatorname{Ann}(m)$. $\operatorname{Ann}(m)$ must be contained in a maximal element $\operatorname{Ann}(m')$ of the set $\mathcal{S} = \{\operatorname{Ann}(x) : 0 \neq x \in M\}$. By the proof of Lemma 2.3.4, $\operatorname{Ann}(m')$ is an associated prime of M. This r belongs to an associated prime of M. □

Proposition 2.3.10 can be also be interpreted the following way: $r \in R$ is M-regular if and only if $r \notin P$ for every $P \in \operatorname{Ass}(M)$.

We know show how associated primes behave under localization.

Lemma 2.3.11. *Let R be a Noetherian ring, S a multiplicative subset of R with $0 \notin S$ and M an R-module. Then*

$$\operatorname{Ass}_{S^{-1}R}(S^{-1}M) = \{S^{-1}P : P \in \operatorname{Ass}(M) \text{ and } P \cap S = \emptyset\}$$

Proof. ($\supseteq$): If $P \in \operatorname{Ass}(M)$ is such that $P \cap S = \emptyset$, then we know that $S^{-1}P$ is a prime ideal of $S^{-1}R$. Since there is an embedding of $R/P \hookrightarrow M$, by exactness of localization there is also an embedding $S^{-1}R/S^{-1}P \cong S^{-1}(R/P) \hookrightarrow S^{-1}M$. Thus $S^{-1}P \in \operatorname{Ass}_{S^{-1}R}(S^{-1}M)$.

($\subseteq$): Suppose $Q \in \operatorname{Ass}_{S^{-1}R}(S^{-1}M)$, so that $Q = \operatorname{Ann}_{S^{-1}R}(\frac{x}{s})$ with $x \in R, s \in S$. We know that $Q = S^{-1}P$ with P a prime ideal of R such that $P \cap S = \emptyset$. It remains to show that $P \in \operatorname{Ass}(M)$.

Since R is Noetherian, P is finitely generated, say $P = (r_1, \ldots, r_n)$. As $S^{-1}P = Q$ annihilates $\frac{x}{s}$, we have that, for each i,

$$\frac{r_i}{1}\frac{x}{s} = 0 \iff w_i r_i x = 0 \text{ for some } w_i \in S.$$

If we let $0 \neq w = w_1 \cdots w_n \in S$, we then have that $r_i(wx) = 0$ for all i. Thus $P \subseteq \operatorname{Ann}(wx)$. We claim that, in fact, $P = \operatorname{Ann}(wx)$. Indeed, suppose $r \in R$ is such that $rwx = 0$. Then $\frac{r}{1}\frac{x}{s} = 0$, meaning that $\frac{r}{1} \in Q = S^{-1}P$ and, by Theorem 1.4.6 we must have $r \in R \cap S^{-1}P = P$. □

If M is a finitely generated R-module, recall that $\operatorname{Supp}(M) = \{P \in \operatorname{Spec}(R) : M_P \neq 0\} = V(\operatorname{Ann}(M))$. In the next theorem we show that $\operatorname{Ass}(M)$ and $\operatorname{Supp}(M)$ have the same set of minimal elements.

Theorem 2.3.12. *Let R be a Noetherian ring and M a finitely generated R-module. Then*

(1) $\operatorname{Ass}(M) \subseteq \operatorname{Supp}(M)$.

(2) $\operatorname{Min}(\operatorname{Ann}(M)) \subseteq \operatorname{Ass}(M)$.

Proof. (1) We can assume $M \neq 0$. If $P \in \operatorname{Ass}(M)$, there is an embedding $R/P \hookrightarrow M$. Localizing at P, and using exactness of localization, we obtain that $0 \neq R_P/PR_P$ embeds into M_p. Thus $M_P \neq 0$, meaning $P \in \operatorname{Supp}(M)$.

(2) Suppose P is a minimal element of $V(\operatorname{Ann}(M)) = \operatorname{Supp}(M)$. Then $M_P \neq 0$ and, by Lemma 2.3.11 we have that

$$\begin{aligned} 0 &\neq \operatorname{Ass}_{R_P}(M_P) \\ &= \{QR_P : Q \in \operatorname{Ass}(M) \text{ and } Q \subseteq P\} \\ &\subseteq \{QR_P : Q \in \operatorname{Supp}(M) \text{ and } Q \subseteq P\} = \{PR_P\}. \end{aligned}$$

Thus $P \in \mathrm{Ass}(M)$. $\square$

Consequently, if R is Noetherian and I is an ideal of R, we have that the minimal primes of I are associated primes of I, i.e., $\mathrm{Min}(I) \subseteq \mathrm{Ass}(R/I)$. As $\mathrm{Ass}(R/I)$ is finite by Theorem 2.3.8, this gives an alternate proof of Theorem 2.2.4.

If M is a finitely generated module over a Noetherian ring R, the minimal elements of $\mathrm{Ass}(M)$ are called the *isolated associated primes* of M. The elements of $\mathrm{Ass}(M)$ that are not minimal are called the *embedded primes* of M.

2.4 Primary ideals

In this section we introduce the ideals which are the building blocks for any ideal in a Noetherian ring, just like the ideals (p^n), with p prime, are the building blocks for any ideal in $\mathbb{Z}$. Indeed, given any ideal $I = (n)$ of $\mathbb{Z}$, if $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is a prime decomposition of n, then $(n) = (p_1^{\alpha_1}) \cap \cdots \cap (p_r^{\alpha_r})$. In fact, we will see that the ideals (p^n), with p prime, are the primary ideals of $\mathbb{Z}$.

Definition 2.4.1. We say that an ideal I of a ring R is *primary* if the following holds for all $a, b \in R$:

$$ab \in I \Longrightarrow a \in I \text{ or } b \in \sqrt{I}.$$

Lemma 2.4.2. *If Q is a primary ideal, then $\sqrt{Q}$ is prime.*

Proof. Suppose $ab \in \sqrt{Q}$. Then $a^n b^n \in Q$ for some $n \geq 1$. As Q is primary, we either have $a^n \in Q$, in which case $a \in \sqrt{Q}$, or $b^n \in \sqrt{Q}$, in which case $y \in \sqrt{Q}$ since $\sqrt{Q}$ is radical. $\square$

Therefore, if Q is a primary ideal of R with $\sqrt{Q} = P$, we will actually say that Q is a *P-primary* ideal.

Notice, however, that $\sqrt{Q} = P$ being prime does not imply that Q is P-primary. Also, not every primary ideal is a power of a prime ideal (in fact, powers of a prime ideal P may not even be P-primary).

Example 2.4.3.

1. In $\mathbb{Z}$, the primary ideals are those of the form (p^k) with p prime. Indeed, these are easily checked to be primary, and these are the only ideals in $\mathbb{Z}$ whose radical is prime, since if $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is a prime decomposition of n, then $\sqrt{(n)} = (p_1 \cdots p_r)$, which is prime if and only if $r = 1$.
2. Consider $R = k[x, y]$, with k a field and $Q = (x^2, xy)$. Then $\sqrt{Q} = (x)$ is a prime ideal, but Q is not primary, since $xy \in Q$, but $x \notin Q$ and $y \notin \sqrt{Q} = (x)$. *Note: this explanation of why Q is not primary might be confusing, since if we viewed xy as yx, then this product would satisfy the condition of Definition 2.4.1. Indeed, the non-symmetry of the definition might be confusing at first. However, we will soon give an equivalent definition for an ideal to be primary which will not cause these kind of problems.*
3. In $k[x, y]$, consider $Q = (x, y^2)$. Then Q is (x, y)-primary. However, Q is not a power of (x, y).
4. Let $R = k[x, y, z]/(xy - z^2)$. Consider the prime $P = (\overline{x}, \overline{z})$ of R. We observe that P^2 is not primary. Indeed, $\overline{xy} = \overline{z}^2 \in P^2$, but $\overline{x} \notin P^2$ and $\overline{y} \notin \sqrt{P^2} = P$.

We now give the following characterization of primary ideals.

Theorem 2.4.4. *Let R be a Noetherian ring and Q an ideal of R. The following are equivalent.*

(1) Q is P-primary.

(2) $\sqrt{Q} = P$ and every zerodivisor in R/Q is nilpotent in R/Q.

(3) $\mathrm{Ass}(R/Q) = \{P\}$.

Proof. (1) $\Leftrightarrow$ (2) is just a rephrasing of Definition 2.4.1. If $xy \in Q$ and $x \notin Q$, this means precisely that $\overline{y}$ is a zerodivisor in R/Q. Q is primary if and only if for such x, y this implies $\overline{y}^n \in Q$ for some $n \geq 1$, i.e., $\overline{y}$ is nilpotent in R/Q.

(2) $\Rightarrow$ (3): Since nilpotent elements are always zerodivisors, (2) is equivalent to saying that $\mathcal{Z}(R/Q) = \mathcal{N}(R/Q)$. Recall that the nilradical of a ring coincides with the intersection of all its prime ideals, which coincides with the

intersection of all its minimal primes (or the intersection of all its associated primes). Using this and Proposition 2.3.10 we then have that

$$\bigcup_{P\in \mathrm{Ass}(R/Q)} P = \mathcal{Z}(R/Q) = \mathcal{N}(R/Q) = \bigcap_{P\in \mathrm{Ass}(R/Q)} P.$$

It is now easy to verify that this implies that the set $\mathrm{Ass}(R/Q)$ consists of only one element P. This P has to be the unique minimal prime of Q, so that $\sqrt{Q} = P$.

Conversely, the same argument tells us that if $\mathrm{Ass}(R/Q) = \{P\}$, then $\mathcal{Z}(R/Q) = \mathcal{N}(R/Q)$. □

Remark 2.4.5. Suppose $\mathfrak{m}$ is a maximal ideal of a Noetherian ring R. If an ideal I is such that $\sqrt{I} = \mathfrak{m}$, then I is $\mathfrak{m}$-primary. This follows from $\emptyset \neq \mathrm{Ass}(R/I) \subseteq \mathrm{Supp}(R/I) = V(I) = V(\sqrt{I}) = \{\mathfrak{m}\}$.

In Theorem 1.4.6 we saw that $PR_P \cap R = P$ for a prime ideal P of R. We now show that a similar equality holds for P-primary ideals.

Theorem 2.4.6. *Let R be a Noetherian ring and Q an ideal of R. The following are equivalent.*

(1) Q is P-primary.

(2) $\sqrt{Q} = P$ and $QR_P \cap R = Q$.

Proof. (1) ⇒ (2): We see that, given $r \in R$, $\frac{r}{1} \in QR_P \cap R$ if and only if there exists $a \in Q$ and $s \notin P$ such that $\frac{r}{1} = \frac{a}{s}$ if and only if there exists $w \notin P$ such that $r(ws) = wa \in Q$. As Q is P-primary and $ws \notin P = \sqrt{Q}$, we must have $r \in Q$.

(2) ⇒ (1): Suppose $ab \in Q$ and $b \notin \sqrt{Q} = P$. Then $\frac{a}{1} = \frac{ab}{b} \in QR_P$, meaning $a \in QR_P \cap R = Q$. Thus Q is P-primary. □

Lemma 2.4.7. *Let R be a Noetherian ring and $I_1, \ldots, I_r$ be P-primary ideals of R. Then $I_1 \cap \cdots \cap I_r$ is also a P-primary ideal.*

Proof. First note that $I_1 \cap \cdots \cap I_r \neq R$ and $\sqrt{I_1 \cap \cdots \cap I_r} = \sqrt{I_1} \cap \cdot \cap \sqrt{I_r} = P$. By Corollary 2.3.7 and Theorem 2.4.4 we have that

$$\emptyset \neq \mathrm{Ass}(R/(I_1 \cap \cdots \cap I_r)) \subseteq \mathrm{Ass}(R/I_1) \cup \cdots \cup \mathrm{Ass}(R/I_r) = \{P\}.$$

Thus $\mathrm{Ass}(R/(I_1 \cap \cdots \cap I_r)) = \{P\}$ and, by Theorem 2.4.4, we conclude that $I_1 \cap \cdots \cap I_r$ is P-primary. □

2.5 Primary decomposition

Definition 2.5.1. Let I be an ideal of a ring R. A *primary decomposition* of I is an expression of the form

$$I = Q_1 \cap \cdots \cap Q_r$$

where each Q_i is a primary ideal. The primary decomposition is said to be *irredundant* if $\sqrt{Q_i} \neq \sqrt{Q_j}$ for every $i \neq j$ and if no Q_j contains the intersection of all the Q_i with $i \neq j$ (meaning that Q_j cannot be removed from the intersection without changing it).

Notice that every primary decomposition of I can be reduced to an irredundant one by removing any unnecessary Q_j and by grouping together all the terms with the same radical (since, by Lemma 2.4.7, intersection of P-primary ideals is also P-primary).

We now prove that irredundant primary decompositions exist in Noetherian rings. This was one of Emmy Noether's biggest discovery in her initial research on Noetherian rings.

Theorem 2.5.2. *Every ideal in a Noetherian ring admits a primary decomposition.*

Proof. We say that an ideal I is irreducible if it cannot be written as an intersection of two strictly larger ideals. We claim that if R is a Noetherian ring, then every ideal of R can be written as a finite intersection of irreducible ideals. Indeed, let $\mathcal{S} = \{\text{ideals } I \subseteq R : I \text{ is not a finite intersection of irreducible ideals }\}$. If $\mathcal{S} \neq \emptyset$, then $\mathcal{S}$ must have a maximal element J. J is not irreducible, so it can be written as $J = J_1 \cap J_2$ with $J \subsetneq J_1$ and $J \subsetneq J_2$. The maximality of J in $\mathcal{S}$ implies that J_1 and J_2 can both be written as finite intersections of irreducible ideals. This contradicts the assumption that J is not the finite intersection of irreducible ideals.

It is now enough to prove that every irreducible ideal Q in a Noetherian ring R must be primary. Note that Q is irreducible if and only the ideal (0) is irreducible in R/Q. Suppose Q is not primary. By Theorem 2.4.4 $\mathrm{Ass}(R/Q)$ contains at least two distinct elements P_1 and P_2. Then R/P_1 and R/P_2 are isomorphic to nonzero submodules Rx and Ry of R/Q ($x, y \in R/Q$), where $P_1 = \mathrm{Ann}(x)$ and $P_2 = \mathrm{Ann}(y)$.

Wlog assume $P_1 \not\subseteq P_2$. We claim that $Rx \cap Ry = 0$. Indeed, if $z \in Rx \cap Ry$, there are $a, b \in R$ such that $z = ax = by$. Let $c \in P_1 \backslash P_2$. Then $0 = cax = cby$, so that $cb \in \mathrm{Ann}(y) = P_2$. As P_2 is prime and $c \notin P_2$, we conclude that $b \in P_2$; but this means that $z = by = 0$. This contradicts the assumption that (0) is irreducible in R/Q. □

Example 2.5.3. If I is radical, then $I = \sqrt{I} = P_1 \cap \cdots \cap P_r$, where $\mathrm{Min}(I) = \{P_1, \ldots, P_r\}$. This is an irredundant primary decomposition of I, as no P_i can be removed from the intersection by Lemma 2.2.3.

Example 2.5.4. Take $R = k[x, y]$, where k is a field. Notice that the following are two irredundant primary decompositions of (x^2, xy):

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

However, $(x^2, xy, y^2) \neq (x^2, y)$. Thus primary decompositions, even when irredundant, are not unique. Notice, however, that $\mathrm{Ass}(R/(x^2, xy)) = \{(x), (x, y)\}$ and that $\sqrt{(x^2, xy, y^2)} = \sqrt{(x^2, y)} = (x, y)$. The primary component corresponding to the minimal associated prime (x) is the same on both decompositions ((x)).

Theorem 2.5.5. (Uniqueness of primary decompositions) *Let I be an ideal of a Noetherian ring R and suppose*

$$I = Q_1 \cap \cdots \cap Q_r$$

is an irredundant primary decomposition of I with $\sqrt{Q_i} = P_i$ for all i. Then

(1) $\mathrm{Ass}(R/I) = \{P_1, \ldots, P_r\}$.

(2) If $P_i \in \mathrm{Min}(I)$, then $Q_i = IR_{P_i} \cap R$. Thus the primary components corresponding to the minimal primes of I are unique in any irredundant primary decomposition of I.

Proof. (1): The inclusion $\mathrm{Ass}(R/I) \subseteq \{P_1, \ldots, P_r\}$ follows directly from Lemma 2.4.7. We now show $\supseteq$. Fixing $1 \leq j \leq r$, we will show that $P_j \in \mathrm{Ass}(R/I)$. Let

$$I_j = \bigcap_{i \neq j} Q_i \supseteq I.$$

Because the primary decomposition is irredundant, I_j/I is nonzero. Thus it has some associated prime $P = \mathrm{Ann}(x+I)$ with $x \in I_j \backslash I$. Notice that $Q_j \subset \mathrm{Ann}(I_j/I)$ since $Q_j I_j \subseteq Q_j \cap I_j = I$. Thus $Q_j \subseteq P$ and we conclude that $P_j = \sqrt{Q_j} \subseteq \sqrt{P} = P$ We now show that in fact $P_j = P$.

Suppose there exists $r \in P \backslash P_j$. Observe that $xr \in I \subseteq Q_j$. As Q_j is P_j-primary and $r \notin P_j$, this forces $x \in Q_j$. But then $x \in I_j \cap Q_j = I$, which is a contradiction.

We have shown that $P = P_j$, so that $P_j \in \mathrm{Ass}(I_j/I)$, meaning there is an embedding $R/P_j \hookrightarrow I_j/I$. But I_j/I is a submodule of R/I. Hence there is an embedding $R/P_j \hookrightarrow R/I$, meaning that $P_j \in \mathrm{Ass}(R/I)$.

(2): Let i be such that $P = P_i$ is a minimal prime of I. Since finite intersections commute with localizations (exercise: this is a consequence of the flatness of localization), we have

$$IR_P = Q_1 R_P \cap \cdots \cap Q_r R_P.$$

As P is minimal in $\{\sqrt{Q_1}, \ldots, \sqrt{Q_r}\} = \mathrm{Ass}(R/I)$, for every $j \neq i$ we have $\sqrt{Q_j} \not\subseteq P$, which is equivalent to $Q_j \not\subseteq P$. Thus $Q_j R_P = R_P$ for all $j \neq i$. We conclude that

$$IR_P = Q_i R_P.$$

Therefore, $IR_P \cap R = Q_i R_P \cap R = Q_i$, the last equality following from Theorem 2.4.6. □

3 Graded Rings

3.1 Graded rings and modules

In the polynomial ring $k[x_1, \ldots, x_n]$ we have the concept of homogeneous elements. Every polynomial can be uniquely written as a finite sum of homogeneous polynomials. Graded rings are rings for which a similar decomposition holds.

Definition 3.1.1. Let G be an abelian semigroup with identity 0. A ring R is *graded* (or *G-graded*) if R admits a decomposition

$$R = \bigoplus_{i \in G} R_i$$

as a direct sum of additive groups such that, for all $i, j \in G$,

$$R_i R_j \subseteq R_{i+j}.$$

An element $f \in R$ is said to be homogeneous if $f \in R_i$ for some $i \in G$. In this case, $\deg(f) = i$ is called the *degree* of f.

If R is a graded ring, then R_0 is a subring of R and each R_i is an R_0-module (Exercise: show that we must have $1 \in R_0$).

Example 3.1.2.

1. Let k be a field. $R = k[x_1, \ldots, x_n]$ is an $\mathbb{N}$ graded ring by setting R_i to be the k-vector space generated by all monomials $x_1^{a_1} \cdots x_n^{a_n}$ with $a_1 + \cdots + a_n = i$. This is called the *standard grading* of the polynomial ring R.
2. We can give a different $\mathbb{N}$-grading to $R = k[x_1, \ldots, x_n]$ by choosing $(d_1, \ldots, d_n) \in \mathbb{N}^n$ and setting $\deg(x_j) = d_j$. In this case, R_i will be the k-vector space generated by all monomials $x_1^{a_1} \cdots x_n^{a_n}$ with $a_1 d_1 + \cdots + a_n d_n = i$. For instance, in $k[x, y]$, $x^2 + y^3$ is not homogeneous with respect to the standard grading, but is homogeneous of degree 6 if the grading is given by $\deg(x) = 3$ and $\deg(y) = 2$.
3. One can give $R = k[x_1, \ldots, x_n]$ an $\mathbb{N}^n$-grading by setting $\deg(x_j) = (0, \ldots, 1, \ldots, 0)$ with the 1 in position j. Given $\underline{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n$, the degree $\underline{a}$ piece of R is the one dimensional k-vector space generated by the monomial $x_1^{a_1} \cdots x_n^{a_n}$.

We define graded modules in a similar way.

Definition 3.1.3. Let G be an abelian semigroup with identity 0 and R be a G-graded ring. An R-module M is *graded* if M admits a decomposition

$$M = \bigoplus_{j \in G} M_j$$

as a direct sum of additive groups such that, for all $i, j \in G$,

$$R_i M_j \subseteq M_{i+j}.$$

An element $y \in M$ is said to be homogeneous if $y \in M_j$ for some $j \in G$.

A submodule N of M is called a *graded* (or *homogeneous*) submodule of M is N can be generated by homogeneous elements of M.

Proposition 3.1.4. *Let R be a $\mathbb{Z}$-graded ring, M a graded R-module and N a submodule of M. The following are equivalent:*

(1) N is a graded submodule of M.

(2) Given $f \in N$, every homogeneous component of f is also in N.

(3) $N = \bigoplus_{j \in \mathbb{Z}} (N \cap M_j)$.

Proof. It is easy to verify that (3) is just a rephrasing of (2).

(2) $\Rightarrow$ (1) is also trivial: If (2) holds, then given a generating set Λ of N, the set set Λ', consisting of all the homogeneous components of all the elements of Λ, will be a set of homogeneous generators of N.

(1) $\Rightarrow$ (2) : Let Λ be a homogeneous set of generators of N. Given $f \in N$, it can be writen as $f = a_1 g_1 + \cdots + a_r g_r$ with $a_i \in R$ and $g_i \in \Lambda$ of degree d_i. Denote by $a_{i,e}$ the homogeneous component of a_i of degree e. Then, for each $d \in G$, the homogeneous component of degree d of f equals $f = a_{1,d-d_1} g_1 + \cdots + a_{r,d-d_r} g_r$, which belongs to N. $\square$

If R is $\mathbb{Z}$-graded and N is a graded submodule of a graded R-module M, then M/N innherits the structure of a graded module since $M/N = \bigoplus_{j\in\mathbb{Z}} M_j / \bigoplus_{j\in\mathbb{Z}}(N\cap M_j) \cong \bigoplus_{j\in\mathbb{Z}} M_j/(N\cap M_j)$. In the particular case where $M = R$ and $N = I$ is a graded ideal of R, then we see that R/I inherits the structure of a graded ring.

Definition 3.1.5. Given an $\mathbb{N}$-graded ring R, we set $R_+ = \bigoplus_{n\geq 1}^{\infty} R_n$. R_+ is a homogeneous ideal of R and $R/R_+ \cong R_0$. R_+ is called the *irrelevant homogeneous ideal* of R.

A graded version of Nakayama's lemma exists for graded rings and finitely generated graded modules. The proof is left as an exercise.

Theorem 3.1.6. (Nakayama's lemma-graded version) *Let R be an $\mathbb{N}$-graded ring and M be a finitely generated graded R-module. If $R_+M = M$ then $M = 0$.*

Corollary 3.1.7. *Let R be an $\mathbb{N}$-graded ring and M be a finitely generated graded R-module. Homogeneous elements $y_1, \ldots, y_r \in M$ generate M if and only if their images in M/R_+M generate M/R_+M as an $R/R_+ \cong R_0$-module. Consequently, if R_0 is a field, then $\{y_1, \ldots, y_r\}$ is a minimal set of homogeneous generators of M is and only if the images of $y_1, \ldots, y_r$ in M/R_+M are a basis for the R_0-vector space M/R_+M.*

We now characterize when an $\mathbb{N}$-graded ring is Noetherian.

Theorem 3.1.8. *A graded ring $R = \bigoplus_{n=0}^{\infty} R_n$ is Noetherian if and only if R_0 is Noetherian and R is finitely generated as an R_0-algebra.*

Proof. ($\Leftarrow$) : If R is a finitely generated R_0-algebra, then R is a quotient of a polynomial ring over R_0 in finitely many variables. By Theorem 1.7.5, R is Noetherian.

($\Rightarrow$) : If R is Noetherian, then so is $R_0 \cong R/R_+$. As R_+ is a homogeneous ideal of R, it must be generated by finitely many homogeneous elements $x_1, \ldots, x_r$. We claim that $R = R_0[x_1, \ldots, x_r]$.

For this, it is enough to show, by induction on n, that $R_n \subset R_0[x_1, \ldots, x_r]$. This is obvious for $n = 0$. Suppose $n > 0$ and that the claim holds for all $n' < n$. Given $f \in R_n$, we can write $f = x_1h_1 + \cdots + x_rh_r$ with $h_1, \ldots, h_r \in R$. If we let g_i denote the component of h_i of degree $n - d_i$, where $d_i = \deg(x_i)$, then $f = x_1g_1 + \cdots + x_rg_r$. By the induction hypothesis, each g_i is in $R_{n-d_i} \subset R_0[x_1, \ldots, x_r]$. Thus, $f \in R_0[x_1, \ldots, x_r]$. □

There is also a graded version of prime avoidance

Theorem 3.1.9. (Prime avoidance-graded version) *Let R be an $\mathbb{N}$-graded ring and I a homogeneous ideal of R generated by elements of positive degree. Let $P_1, \ldots, P_n$ be prime ideals of R such that $I \not\subseteq P_j$ for all j. Then there exists a homogeneous element $x \in I$ such that $x \notin P_1 \cup \cdots \cup P_n$.*

Proof. Exercise: make necessary adaptations to the proof Theorem 1.2.14. □

Definition 3.1.10. Let R and S be G-graded rings. A ring homomorphism $\varphi : R \longrightarrow S$ is said to be *degree-preserving* is $\varphi(R_i) \subseteq S_i$ for all $i \in G$.

Definition 3.1.11. Let M and T be graded modules over a G-graded ring R. A homomorphism of R-modules $\varphi : M \longrightarrow T$ is said to be *graded* (of *homogeneous*) of *degree* $d \in G$ is $\varphi(M_i) \subseteq T_{i+d}$ for all $i \in G$. If φ is homogeneous of degree 0, we also say φ is *degree-preserving*.

Notice that if

$$\cdots \xrightarrow{f_{i-2}} M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \cdots$$

is an exact complex of graded modules over a graded ring R, such that f_i is degree-preserving for all i, then for all $a \in G$,

$$\cdots \xrightarrow{f'_{i-2}} (M_{i-1})_a \xrightarrow{f'_{i-1}} (M_i)_a \xrightarrow{f'_i} (M_{i+1})_a \xrightarrow{f_{i+1}} \cdots$$

is also an exact complex of R_0-modules where, for each i, f'_i denotes the restriction of f_i to $(M_i)_a$.

Remark 3.1.12. If $\varphi : M \longrightarrow T$ is a graded homomorphism of graded R-modules, then $\ker\varphi$, $\operatorname{im}\varphi$ and $\operatorname{coker}\varphi$ are also graded R-modules. (This is not hard to check. Something nice to think about next time you are in the shower).

3.2 Hilbert functions

Suppose $R = \bigoplus_{n=0}^{\infty} R_n$ is a Noetherian graded ring and that $M = \bigoplus_{n=0}^{\infty} M_n$ is a finitely generated graded R-module.

Claim: Each M_n is a finitely generated R_0-module.

Proof. First notice that each R_a is a finitely generated R_0-module. This is because, by Theorem 3.1.8, R is a quotient of a polynomial ring over R_0 in finitely many variables. Now suppose $y_1, \ldots, y_r \in M$ are homogeneous elements of M generating M. If $d_i = \deg(y_i)$, then $M_n = R_{n-d_1}y_1 + \cdots + R_{n-d_r}y_r$ (the argument for this is similar to one used in the proof of Theorem 3.1.8). Therefore, the R_0-module homomorphism $\varphi : R_{n-d_1} \oplus \cdots \oplus R_{n-d_r} \longrightarrow M_n$ given by $\varphi(a_1, \ldots, a_r) = a_1y_1 + \cdots + a_ry_r$ is surjective, so that M_n is a quotient of $R_{n-d_1} \oplus \cdots \oplus R_{n-d_r}$. As each R_{n-d_i} is a finitely generated R_0-module, so is $R_{n-d_1} \oplus \cdots \oplus R_{n-d_r}$ and, as a consequence, M_n. □

Suppose that, in addition, R_0 is Artinian. Then, by the claim, each M_n is an Artinian and Noetherian R_0-module, so that $\ell(M_n) < \infty$ (here ℓ denotes length as an R_0-module). The *Hilbert function* of M, denoted HF_M, is the function that measures these lengths, i.e., $\mathrm{HF}_M : \mathbb{Z}_{\geq 0} \longrightarrow \mathbb{Z}_{\geq 0}$ is given by

$$\mathrm{HF}_M(n) = \ell(M_n)$$

for all $n \geq 0$. The *Hilbert series* of M, denoted $\mathrm{HS}_M(t)$, is the generating function of HF_M, so that it is defined as

$$\mathrm{HS}_M(t) = \sum_{n \geq 0} \mathrm{HF}_M(n)t^n = \sum_{n \geq 0} \ell(M_n)t^n.$$

Theorem 3.2.1. *Let $R = \bigoplus_{n=0}^{\infty} R_n$ be a Noetherian graded ring with R_0 Artinian and let $M = \bigoplus_{n=0}^{\infty} M_n$ be a finitely generated graded R-module. Then $\mathrm{HS}_M(t)$ is a rational function of t. More concretely, if $R = R_0[x_1, \ldots, x_r]$ with $x_i \in R$ of degree d_i, then there exists $f(t) \in \mathbb{Z}[t]$ such that*

$$HS_M(t) = \frac{f(t)}{\prod_{i=1}^{r}(1 - t^{d_i})}.$$

Proof. By induction on r. If $r = 0$, then $R = R_0$ is Artinian and, being a finitely generated R_0-module, M must have finite length, so that $\ell(M_n) = 0$ for $n \gg 0$. Thus, in this case, $\mathrm{HS}_M(t)$ is a polynomial.

Suppose $r \geq 1$. Let L and $K = M/x_rM$ be the kernel and cokernel of the multiplication by x_r map $\cdot x_r : M \longrightarrow M$, respectively. Then L and K are graded R-modules, both of which are annihilated by x_r. Hence, L and K can be viewed as graded R/x_rR-modules and, consequently, as $R[x_1, \ldots, x_{r-1}]$-modules. For each $n \geq 0$ we have a short exact sequence of R_0-modules

$$0 \longrightarrow L_n \longrightarrow M_n \xrightarrow{\cdot x_r} M_{n+d_r} \longrightarrow K_{n+d_r} \longrightarrow 0 \ ,$$

so that

$$\ell(M_{n+d_r}) - \ell(M_n) = \ell(K_{n+d_r}) - \ell(L_n).$$

This gives the relation

$$HS_M(t) - t^{d_r}HS_M(t) = HS_K(t) - t^{d_r}HS_L(t).$$

By the induction hypothesis, the right hand side is of the form $f(t)/\prod_{i=1}^{r-1}(1 - t^{d_i})$ for some $f(t) \in \mathbb{Z}[t]$. The result now follows. □

An important particular case of Theorem 3.2.1 is when $d_1 = \cdots = d_r = 1$ (i.e., when R is standard graded). In this case the Hilbert series of any finitely generated graded R-module M has the form

$$HS_M(t) = \frac{f(t)}{(1 - t)^r}.$$

After canceling out all the factors of $(1 - t)$ from $f(t)$, the Hilbert series of M takes the form

$$HS_M(t) = \frac{f(t)}{(1 - t)^d}$$

with the following property: either $d = 0$ or $d > 0$ and $f(1) \neq 0$.

Recall the following identity for all $d \geq 1$:

$$\frac{1}{(1-t)^d} = \sum_{n=0}^{\infty} \binom{n+d-1}{d-1} t^n.$$

Consequently, if $f(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_s t^s$, then

$$\ell(M_n) = a_0 \binom{n+d-1}{d-1} + a_1 \binom{n+d-2}{d-1} + \cdots + a_s \binom{n+d-s-1}{d-1}$$

where we set $\binom{k}{d-1} = 0$ if $k < d-1$. Since $\binom{k}{d-1} = k(k-1)\cdots(k-d+2)/(d-1)!$ for $k \geq 0$, each term $\binom{n+d-i}{d-1}$ can be viewed as a polynomial in n of degree $d-1$ with rational coefficients as long as $n \geq i-d$. Thus, if $d \geq 1$ then the above expression for $\ell(M_n)$ can be written as

$$\ell(M_n) = \frac{e}{(d-1)!} n^{d-1} + (\text{lower degree terms})$$

for all $n \geq s+1-d$. Notice that $e = a_0 + a_1 + \cdots + a_s = f(1)$. These observations can be stated as follows.

Theorem 3.2.2. *Let $R = \bigoplus_{n=0}^{\infty} R_n$ be a standard graded Noetherian ring and M a finitely generated graded R-module. Let d be the smallest non-negative integer such that $(1-t)^d \operatorname{HS}_M(t)$ is a polynomial $f(t) \in \mathbb{Z}[t]$ and let $s = \deg(f)$. There exists a polynomial $P_M(t) \in \mathbb{Q}[t]$ of degree $d-1$ such that*

$$\ell(M_n) = P_M(n)$$

for all $n \geq s+1-d$. (If $d = 0$, then $P_M(t) = 0$. This is equivalent to M being Artinian.)

Definition 3.2.3. Following the notation of Theorem 3.2.2, the polynomial $P_M(t)$ is called the *Hilbert polynomial* of M. The *multiplicity* of M, denoted $e_R(M)$ (or simply $e(M)$) is the number $e \geq 0$ such that $P_M(t) = \frac{e}{(d-1)!} t^{d-1} + \cdots$. Equivalently,

$$e(M) = \lim_{n \to \infty} \frac{(d-1)!}{n^{d-1}} \ell(M_n) = f(1).$$

Example 3.2.4. 1. Take $M = R = R_0[x_1, \ldots, x_d]$, where R_0 is an Artinian ring and $x_1, \ldots, x_d$ are variables. Since there are $\binom{n+d-1}{d-1}$ monomials of degree n, we have $\ell(R_n) = \ell(R_0)\binom{n+d-1}{d-1}$ for all $n \geq 0$. Thus

$$\operatorname{HS}_R(t) = \frac{\ell(R_0)}{(1-t)^d}.$$

The Hilbert polynomial of R is $P_R(t) = \ell(R_0)(t+d-1)\cdots(t+1)/(d-1)!$ and the multiplicity of R is $e(R) = \ell(R_0)$.

2. Let k be a field and let F be a nonzero homogeneous polynomial of degree s of the polynomial ring $R = k[x_1, \ldots, x_d]$. Take $M = R/(F)$. As R is a domain, F is a nonzerodivisor of R, so that for each $n \geq 0$ we have a short exact sequence of k-vector spaces

$$0 \longrightarrow R_n \xrightarrow{\cdot F} R_{n+s} \longrightarrow M_{n+s} \longrightarrow 0 \ ,$$

so that $\ell(M_{n+s}) = \ell(R_{n+s}) - \ell(R_n)$. This translates to

$$\operatorname{HS}_{R/(F)}(t) = \operatorname{HS}_M(t) = (1-t^s)\operatorname{HS}_R(t) = \frac{1-t^s}{(1-t)^d} = \frac{1+t+\cdots+t^{s-1}}{(1-t)^{d-1}}.$$

The multiplicity of $R/(F)$ is $e(R/(F)) = s = \deg(F)$.

3.3 The associated graded ring

We now introduce a crucial idea in Commutative Algebra, that of associating graded rings and graded modules to commutative rings and ideals.

Definition 3.3.1. Let R be a ring and I an ideal of R. We define the *associated graded ring of R with respect to I* to be the graded ring

$$\mathrm{gr}_I(R) = \bigoplus_{n=0}^{\infty} \frac{I^n}{I^{n+1}}.$$

Multiplication of graded elements in $\mathrm{gr}_I(R)$ is defined by

$$(a + I^{n+1})(b + I^{m+1}) = (ab + I^{n+m+1})$$

for all $a \in I^n$ and $b \in I^m$ (check that this well defined).

Notice that if I is finitely generated, so that $I = (a_1, \ldots, a_r)$, and if we let $\overline{a_1}, \ldots, \overline{a_r}$ denote the images of the a_i in I/I^2, then $\mathrm{gr}_I(R) = (R/I)[\overline{a_1}, \ldots, \overline{a_r}]$. This follows from that definition of I^n: every element in I^n is an R-linear combination of products of n elements from $a_1, \ldots, a_r$.

If R is Noetherian, then every ideal I of R is finitely generated. Also, R/I is Noetherian, from which it follows that $(R/I)[\overline{a_1}, \ldots, \overline{a_r}]$ is Noetherian. Consequently,

$$R \text{ Noetherian} \Longrightarrow \mathrm{gr}_I(R) \text{ Noetherian}.$$

Let M be an R-module. A filtration $\mathcal{F} : M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$ of submodules of M is said to be an *I-filtration* if $I^n M_i \subseteq M_{i+n}$ for all $i, n \geq 0$. For such a filtration, the *associated graded module* of M with respect to $\mathcal{F}$ is defined as

$$\mathrm{gr}_{\mathcal{F}}(M) = \bigoplus_{n=0}^{\infty} \frac{M_n}{M_{n+1}}.$$

$\mathrm{gr}_{\mathcal{F}}(M)$ is a $\mathrm{gr}_I(R)$-module with scalar multiplication given by

$$(a + I^{n+1})(x + M_{m+1}) = (ax + M_{n+m+1})$$

for all $a \in I^n$ and $x \in M_m$. Furthermore, the filtration $\mathcal{F}$ is said to be *I-stable* if there exists $n_0 \geq 0$ such that $M_{n+1} = IM_n$ for all $n \geq n_0$. In this case, $\mathrm{gr}_{\mathcal{F}}(M)$ is generated as a $\mathrm{gr}_I(R)$-module by $(M_0/M_1) \oplus \cdots \oplus (M_{n_0}/M_{n_0+1})$. Consequently, if $\mathcal{F}$ is I-stable and M is a Noetherian R-module, then $\mathrm{gr}_{\mathcal{F}}(M)$ is a finitely generated $\mathrm{gr}_I(R)$-module.

The most important I-stable filtration we can consider on M is the I-adic filtration of M, i.e., the filtration $M \supseteq IM \supseteq I^2M \supseteq I^3M \supseteq \cdots$. The associated graded module of M with respect to the I-adic filtration is simply denoted by

$$\mathrm{gr}_I(M) = \bigoplus_{n=0}^{\infty} \frac{I^n M}{I^{n+1} M}.$$

If R is Noetherian and M is a finitely generated R-module, then, by the observations already made, $\mathrm{gr}_I(M)$ is a finitely generated $\mathrm{gr}_I(R)$-module, hence a Notherian $\mathrm{gr}_I(R)$-module.

If N is a submodule of M, the I-adic filtration on M induces the filtration $N \supseteq IM \cap N \supseteq I^2M \cap N \supseteq I^3M \cap N \supseteq \cdots$ on N. This is an I-filtration. Turns out that, if R is Noetherian and M is finitely generated, then this filtration on N is also I-stable. This is another finitess type property of Noetherian rings, known as the Artin-Rees lemma.

Theorem 3.3.2. (Artin-Rees lemma) *Suppose R is Noetherian and I is an ideal of R. Let M be a finitely generated R-module and N a submodule of M. Then there exists $s \geq 0$ such that*

$$I^n M \cap N = I^{n-s}(I^s M \cap N) \quad \textit{for all } n \geq s.$$

Proof. We consider the associated graded ring of N with respect to the filtration $\mathcal{F}$ of N induced by the I-adic filtration of M. By the isomorphism theorems, we have $(I^n M \cap N)/(I^{n+1} M \cap N) \cong (I^n M \cap N + I^{n+1} M)/I^{n+1} M$. Thus

$$\mathrm{gr}_{\mathcal{F}}(N) = \bigoplus_{n=0}^{\infty} \frac{I^n M \cap N}{I^{n+1} M \cap N} \cong \bigoplus_{n=0}^{\infty} \frac{I^n M \cap N + I^{n+1} M}{I^{n+1} M} \subseteq \bigoplus_{n=0}^{\infty} \frac{I^n M}{I^{n+1} M} = \mathrm{gr}_I(M).$$

As we have seen. $\mathrm{gr}_I(M)$ is a Noetherian $\mathrm{gr}_I(R)$-module. Thus $\mathrm{gr}_{\mathcal{F}}(N)$ is must be a finitely generated graded $\mathrm{gr}_I(R)$-module. Let $y_1, \ldots, y_r \in \mathrm{gr}_{\mathcal{F}}(N)$ be a set of minimal homogeneous generators of degrees $d_1 \leq \cdots \leq d_r$. Then, for all $n \geq d_r$,

$$\begin{aligned}
\frac{I^n M \cap N}{I^{n+1} M \cap N} &= (\mathrm{gr}_{\mathcal{F}}(N))_n = (\mathrm{gr}_I(R))_{n-d_1} y_1 + \cdots + (\mathrm{gr}_I(R))_{n-d_r} y_r. \\
&= \left(\frac{I^{n-d_1}}{I^{n+1-d_1}}\right) y_1 + \cdots + \left(\frac{I^{n-d_r}}{I^{n+1-d_r}}\right) y_r. \\
&= \left(\frac{I^{n-d_r}}{I^{n+1-d_r}}\right) \left(\left(\frac{I^{d_r-d_1}}{I^{d_r-d_1+1}}\right) y_1 + \cdots + \left(\frac{R}{I}\right) y_r\right) \\
&\subseteq \left(\frac{I^{n-d_r}}{I^{n+1-d_r}}\right) \frac{I^{d_r} M \cap N}{I^{d_r+1} M \cap N}.
\end{aligned}$$

We choose $s = d_r$. Then the above inclusion shows that $I^n M \cap N \subseteq I^{n-s}(I^s M \cap N)$ for all $n \geq s$. The inclusion $I^n M \cap N \supseteq I^{n-s}(I^s M \cap N)$ is obvious, hence the proof is concluded. □

Remark 3.3.3. In the setting of Theorem 3.3.2, the smallest s for which $I^n M \cap N = I^{n-s}(I^s M \cap N)$ holds for all $n \geq s$ is called the *Artin-Rees number* of I *with respect to* $N \subseteq M$. Some authors denote it by $\mathrm{AR}(I, N \subseteq M)$.

With this, we can now prove the following

Theorem 3.3.4. (Krull intersection theorem) *Let $(R, \mathfrak{m})$ be a Noetherian local ring, I a proper ideal of R and M a finitely generated R-module. Then*

$$\bigcap_{n=1}^{\infty} I^n M = 0.$$

Proof. Let $N = \bigcap_{n=1}^{\infty} I^n M \subseteq M$. By the Artin-Rees lemma there exists $s \geq 0$. such that

$$I^{s+1} M \cap N = I(I^s M \cap N) \subseteq IN.$$

But $I^{s+1} M \cap N = N$. Thus $N = IN$. By Nakayama's lemma, we conclude that $N = 0$. □

Suppose now $(R, \mathfrak{m}, k)$ is a Noetherian local ring. $\mathrm{gr}_{\mathfrak{m}}(R)$ is simply called the *associated graded ring* of R. In particular, $(\mathrm{gr}_{\mathfrak{m}}(R))_0 = R/\mathfrak{m} = k$ is Artinian. Thus, for a finitely generated graded nonzero R-module M, the Hilbert function of the associaded graded module $\mathrm{gr}_{\mathfrak{m}}(M)$ is well defined. In this case

$$\mathrm{HF}_{\mathrm{gr}_{\mathfrak{m}}(M)}(n) = \ell\left(\frac{\mathfrak{m}^n M}{\mathfrak{m}^{n+1} M}\right) = \dim_k\left(\frac{\mathfrak{m}^n M}{\mathfrak{m}^{n+1} M}\right) = \mu(\mathfrak{m}^n M)$$

gives the minimal number of generators of $\mathfrak{m}^n M$. From what we have seen in Section 3.2, the Hilbert series of $\mathrm{gr}_{\mathfrak{m}}(M)$ can be written as $f(t)/(1-t)^d$ with $f(1) \neq 0$. If $f = a_0 + a_1 t + a_2 t^2 + \cdots + a_s t^s$, then

$$\mathrm{HF}_{\mathrm{gr}_{\mathfrak{m}}(M)}(n) = a_0\binom{n+d-1}{d-1} + a_1\binom{n+d-2}{d-1} + \cdots + a_s\binom{n+d-s-1}{d-1}.$$

Using the identity $\sum_{i=0}^{n}\binom{i+d-1}{d-1} = \binom{n+d}{d}$ we then get

$$\ell\left(\frac{M}{\mathfrak{m}^{n+1} M}\right) = \sum_{i=0}^{n} \ell\left(\frac{\mathfrak{m}^i M}{\mathfrak{m}^{i+1} M}\right) = a_0\binom{n+d}{d} + a_1\binom{n+d-1}{d} + \cdots + a_s\binom{n+d-s}{d}$$

The function

$$n \longmapsto \ell\left(\frac{M}{\mathfrak{m}^{n+1} M}\right)$$

is sometimes more convenient to consider than the Hilbert function of $\mathrm{gr}_{\mathfrak{m}}(M)$. This function is called the *Samuel function* of M. By the above expression, we see that, for $n \geq s - d$, $\ell\left(\frac{M}{\mathfrak{m}^{n+1} M}\right)$ coincides with a polynomial $\varphi_M^{\mathfrak{m}}$ of degree d evaluated at n (the argument for this is analogous to the the argument used to show that the Hilbert polynomial exists). The polynomial $\varphi_M^{\mathfrak{m}}$, which we can call the *Samuel polynomial* of M, has the form $\varphi_M^{\mathfrak{m}}(t) = \frac{e}{d!} t^d + \cdots$, where $e = a_0 + \cdots + a_s = e(\mathrm{gr}_{\mathfrak{m}}(M))$.

Definition 3.3.5. Given a finitely generated nonzero module M over a Noetherin local ring $(R, \mathfrak{m})$, we define $d(M)$ to be the degree of the Samuel polynomial of M. Equivalently, $d(M)$ is such that the degree of the Hilbert polynomial of $\mathrm{gr}_{\mathfrak{m}}(M)$ is $d(M) - 1$.

This number $d(M)$ is a measure of the size of M. It is in fact intrinsically related to the concept of "dimension", which we will explore in the next section. The following lemma will be useful there.

Lemma 3.3.6. *Let $(R, \mathfrak{m})$ be a Noetherian local ring and let $0 \longrightarrow N \longrightarrow M \longrightarrow P \longrightarrow 0$ be a short exact sequence of finitely generated R-modules. Then*

$$d(M) = \max\{d(N), d(P)\}.$$

Proof. Since $P \cong M/N$, the second isomorphism theorem gives

$$P/\mathfrak{m}^n P \cong (M/N)/((\mathfrak{m}^n M + N)/N) \cong M/(\mathfrak{m}^n M + N)$$

and the third isomorphism theorem gives

$$(\mathfrak{m}^n M + N)/\mathfrak{m}^n M \cong N/(\mathfrak{m}^n M \cap N).$$

Thus

$$\begin{aligned} \ell(M/\mathfrak{m}^n M) &= \ell(M/(\mathfrak{m}^n M + N)) + \ell((\mathfrak{m}^n M + N)/\mathfrak{m}^n M) \\ &= \ell(P/\mathfrak{m}^n P) + \ell(N/(\mathfrak{m}^n M \cap N)). \end{aligned}$$

From this, we see that, for large values of n, $n \longmapsto \ell(N/(\mathfrak{m}^n M \cap N))$ coincides with a polynomial function $\lambda(t) \in \mathbb{Q}[t]$ evaluated at n. Since both $\varphi_P^{\mathfrak{m}}$ and λ take on positive values at all $n \geq 1$, both have positive leading coefficients, so that we immediately get $d(M) = \max\{d(P), \deg(\lambda)\}$. It remains to show that $\deg(\lambda) = d(N)$. By the Artin-Rees lemma, there exists $r \geq 0$ such that for all $n \gg 0$ we have

$$\mathfrak{m}^n N \subseteq \mathfrak{m}^n M \cap N \subseteq \mathfrak{m}^{n-r} N.$$

Therefore

$$\varphi_N^{\mathfrak{m}}(n - r - 1) = \ell\left(\frac{N}{\mathfrak{m}^{n-r} N}\right) \leq \ell\left(\frac{N}{\mathfrak{m}^n M \cap N}\right) = \lambda(n) \leq \ell\left(\frac{N}{\mathfrak{m}^n N}\right) = \varphi_N^{\mathfrak{m}}(n - 1).$$

This forces $\deg(\lambda) = \deg(\varphi_N^{\mathfrak{m}}) = d(N)$. □

Remark 3.3.7. Instead of considering the maximal ideal $\mathfrak{m}$, we could consider an $\mathfrak{m}$-primary ideal I, so that R/I is Artinian. This way, the Hilbert function of $\mathrm{gr}_I(M)$ as a $\mathrm{gr}_I(R)$-module is well defined, as well as the Samuel function $n \longmapsto \ell\left(\frac{M}{I^{n+1}M}\right)$ of M over I. In a similar way, for large values of n, $\ell\left(\frac{M}{I^{n+1}M}\right)$ coincides with a polynomial $\varphi_M^I \in \mathbb{Q}[t]$ of degree d' evaluated at n. One can see, however, that $d' = d(M)$. Indeed, since I is $\mathfrak{m}$-primary, there exists $a \geq 1$ such that $\mathfrak{m}^a \subseteq I \subseteq \mathfrak{m}$. Hence

$$\varphi_M^{\mathfrak{m}}(n) = \ell(M/\mathfrak{m}^{n+1}M) \leq \ell(M/I^{n+1}M) = \varphi_M^I(n) \leq \ell(M/\mathfrak{m}^{a(n+1)}M) = \varphi_M^{\mathfrak{m}}(an + a - 1)$$

which implies $d(M) = \deg(\varphi_M^{\mathfrak{m}}) = \deg(\varphi_M^I)$.

4 Dimension theory

4.1 Height and dimension

We introduce here the concepts of height and dimension, which are measures of the size of ideals and rings. They are motivated by the concepts of dimension of vector spaces and combinatorial dimension of varieties.

If V is a vector space over a field k, then we know that the dimension of V coincides with the supremum of all r for which there is a strictly increasing chain $V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_r$ of subspaces of V. On the other hand, if X is a topological space, it doesn't make sense to define the dimension of X as the supremum of lengths of strictly increasing chains of subspaces of X (this way, points would not have dimension zero, and thus that would be a dumb definition of dimension). Instead, we should consider irreducible subspaces of X and define $\dim X$ as the supremum of all r such that there exists a strictly increasing chain $Y_0 \subsetneq Y_1 \subsetneq \cdots \subsetneq Y_r$ of irreducible subspaces of X.

If R is a ring, we consider the topological space $\operatorname{Spec}(R)$ associated to it. The irreducible closed subspaces of $\operatorname{Spec}(R)$, as we have seen, coincide with the varieties $V(P)$, where P is a prime ideal of R. This motivates the following definitions.

Definition 4.1.1. *(height)* Let R be a ring and P a prime ideal of R. The *height* of P is defined as

$$\operatorname{ht}(P) = \sup\{r : \text{there exists a strictly increasing chain of prime ideals } P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_r = P\}.$$

If I is a proper ideal of I, then we define the *height* of I as

$$\operatorname{ht}(I) = \inf\{\operatorname{ht}(P) : P \text{ is prime and } I \subseteq P\} = \inf\{\operatorname{ht}(P) : P \in \operatorname{Min}(I)\}.$$

Definition 4.1.2. *(dimension)* Let R be a ring. We define

$$\dim(R) = \sup\{\operatorname{ht}(P) : P \in \operatorname{Spec}(R)\}.$$

We say that a strict chain of prime ideals $P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_r$ has length r. We say that the chain is *saturated* if for each i there is no prime ideal Q such that $P_i \subsetneq Q \subsetneq P_{i+1}$.

Example 4.1.3.

1. A field has dimension zero. In fact, a ring R has dimension zero if and only if every prime ideal of R is maximal. This way, we can rephrase Theorem 1.8.11 in the following way:

$$R \text{ is Artinian } \iff R \text{ is Noetherian and } \dim(R) = 0.$$

2. $\mathbb{Z}$ has dimension 1 since every nonzero prime ideal is of the form (p) with p prime, and thus is maximal. Every saturated chain of prime ideals of $\mathbb{Z}$ is of the form $(0) \subsetneq (p)$ with p prime.

3. In any polynomial ring $S[x_1, \ldots, x_n]$ or power series ring $S[\![x_1, \ldots, x_n]\!]$, where S is a domain, there is always a strictly increasing chain of prime ideals

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

   Thus these rings have dimension $\geq n$. We will later see that if $S = k$ is a field, then the dimension of these rings is actually equal to n.

   By a similar argument, $S[x_1, x_2, x_3, \ldots]$ and $S[\![x_1, x_2, x_3, \ldots]\!]$ always have infinite dimension.

4. However, if we consider $R = k[x_1, x_2, x_3, \ldots]/(x_1^2, x_2^2, x_3^2, \ldots)$, where k is a field, then R has dimension zero (even tough R is not Noetherian), since $(x_1, x_2, x_3, \ldots)$ is its only prime ideal.

5. Conversely, there exist Noetherian rings that have infinite dimension. Take the following example by Nagata: Let k be a field and $R = k[x_{1,1}, x_{2,1}, x_{2,2}, x_{3,1}, x_{3,2}, x_{3,3}, x_{4,1}, \ldots]$. For each i let P_i be the prime ideal $P_i = (x_{i,1}, \ldots, x_{i,i})$. Consider the multiplicative subset $W = R \setminus \bigcup_{i=1}^{\infty} P_i$ and the ring

$$A = W^{-1}R.$$

   Then A is Noetherian (the proof is intricate, so I won't include it) but $\dim(A) = \infty$. Indeed, for each i,

$$(x_{i,1}) \subsetneq (x_{i,1}, x_{i,2}) \subsetneq \cdots \subsetneq (x_{i,1}, \ldots, x_{i,i})$$

   is a strictly increasing chain of prime ideals of R of length $i - 1$, none of which intersect W. This shows that $\dim(A) \geq i - 1$ for all i.

The following is a list of properties of height and dimension that follow directly from the definitions and from the characterization of the primes of R/I, for an ideal I of R, and the characterization of the primes of R_P, when P is a prime ideal of R.

Proposition 4.1.4. *Let R be a ring.*

(1) A prime ideal has height zero if and only if it is a minimal prime of R. An ideal of R has height zero if and only if it is contained in a minimal prime of R.

(2) $\dim(R) = \sup\{\dim(R/P) : P \in \operatorname{Spec}(R)\}$.

(3) $\dim(R) = \sup\{\operatorname{ht}(P) : P \in \operatorname{Spec}(R)\} = \sup\{\operatorname{ht}(\mathfrak{m}) : \mathfrak{m}$ *is a maximal ideal of* $R\}$.

(4) If I is an ideal, then $\dim(R/I)$ *is the supremum of all r for which there exists a strictly increasing chain $I \subseteq P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_r$ of primes in $V(I)$.*

(5) If I is an ideal of R, then $\dim(R/I) + \operatorname{ht}(I) \leq \dim(R)$.

(6) If W is a multiplicatively closed subset of R, then $\dim(W^{-1}R) \leq \dim(R)$.

(7) If P is a prime ideal of R, then $\dim(R_P) = \operatorname{ht}(P)$.

(8) If $Q \subseteq P$ are prime ideals of R, then $\dim(R_P/QR_P)$ *equals the supremum of the lengths of chains of prime ideals of R of the form $Q = P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_r = P$.*

(9) If $I \subseteq J$ are ideals, then $\dim(R/J) \leq \dim(R/I)$.

(10) If R is Noetherian and I is an ideal of R, then $\dim(R/I) = \dim(R/\sqrt{I})$ *(follows from* $\operatorname{Min}(I) = \operatorname{Min}(\sqrt{I})$*).*

We specify some properties of rings that are related to the behavior of saturated chains of prime ideals when we fix some of the endpoints.

Definition 4.1.5. A ring is said to be *catenary* if, for every pair of prime ideals $Q \subseteq P$, every saturated chain of prime ideals starting at Q and ending at P have the same finite length.

A ring R is said to be *equidimensional* if all its maximal ideals have the same (finite) height and $\dim(R) = \dim(R/P) < \infty$ for every minimal prime ideal P of R.

Example 4.1.6. Here is an example of a ring that is not equidimensional. Consider $R = \mathbb{C}[x, y, z]/(xy, xz)$. $(xy, xz) = (x) \cap (y, z)$ is an irredundant primary decomposition of (xy, xz). Plus, (x) and (y, z) are incomparable, thus $\operatorname{Min}(R) = \{(x), (y, z)\}$. However, $\dim(R/(x)) = \dim(\mathbb{C}[y, z]) = 2$ and $\dim(R/(y, z)) = \dim(\mathbb{C}[x]) = 1$. Thus, R is not equidimensional. (Here we are using the fact that $\dim(k[x_1, \ldots, x_n] = n$ when k is a field, which is something we will eventually prove).

Catenary rings can be easily found in nature. Any quotient of $k[x_1, \ldots, x_n]$, where k is a field, is a catenary ring. In fact, any quotient of a Cohen-Macaulay ring is catenary. However, such discussions related to Cohen-Macaulay rings will be left for later, in a section dedicated specifically to those types of rings. For a local ring $(R, \mathfrak{m})$, it actually holds true that R is catenary if and only if $\dim(R/P) + \operatorname{ht}(P) = \dim(R)$ for all $P \in \operatorname{Spec}(R)$. The proof of this, however, requires a lot of work and thus it will not be included in these notes (if you want, you can find it in [Mat86, Theorem 31.4]).

We now see how dimension is defined for modules.

Definition 4.1.7. Let R be a ring and M be an R-module. The *dimension* of M is defined as

$$\dim(M) = \dim(R/\operatorname{Ann}(M)).$$

Notice that if M is finitely generated, then $\operatorname{Supp}(M) = V(\operatorname{Ann}(M))$, so that in this case $\dim(M)$ coincides with the combinatorial dimension of $\operatorname{Supp}(M)$.

Remark 4.1.8. If $(R, \mathfrak{m})$ is a Noetherian local ring and M a finitely generated R-module, then $\dim(M) = \dim(R/\operatorname{Ann}(M)) = 0$ is equivalent to $\operatorname{Ann}(M)$ being $\mathfrak{m}$-primary. Thus

$$\dim(M) = 0 \iff \ell(M) < \infty.$$

Indeed, if $\operatorname{Ann}(M)$ is $\mathfrak{m}$-primary, $R/\operatorname{Ann}(M)$ is Artinian, so that M, being a finitely generated $R/\operatorname{Ann}(M)$-module, must have finite length. Conversely, assume $\ell(M) = l < \infty$. We show that $\mathfrak{m}^l \subseteq \operatorname{Ann}(M)$. Suppose not. Then by Nakayama's lemma we have that $\mathfrak{m}^i M \neq \mathfrak{m}^{i+1} M$ for all $0 \leq i \leq l$. But then

$$\ell(M) \geq \ell(M/\mathfrak{m}M) + \ell(\mathfrak{m}M/\mathfrak{m}^2 M) + \cdots + \ell(\mathfrak{m}^l M/\mathfrak{m}^{l+1} M) \geq l + 1,$$

a contradiction.

4.2 A local perspective of dimension

Another measure of the size of a module M could be based on the following question: how many elements do I need to reduce M to a zero dimensional module? In the local case, this yields the following definition.

Definition 4.2.1. Let $(R, \mathfrak{m})$ be a Noetherian local ring and M is a finitely generated R-module. We define

$$\delta(M) = \inf\{r : \text{there exist } a_1, \ldots, a_r \in \mathfrak{m} \text{ such that } \dim(M/a_1 M + \cdots + a_r M) = 0\}.$$

If $\dim(M) = 0$, we simply set $\delta(M) = 0$.

Let $I = (a_1, \ldots, a_r)$ be an $\mathfrak{m}$-primary ideal of R, so that R/I is Artinian. This way, since I is contained in the annihilator of $M/IM = M/a_1 M + \cdots + a_r M$, we have

$$0 \leq \dim(M/IM) = \dim(R/\operatorname{Ann}(M/IM)) \leq \dim(R/I) = 0.$$

This shows that $\delta(M)$ is finite and $\delta(M) \leq r$. Also, by Remark 4.1.8, we actually have

$$\delta(M) = \min\{r : \text{there exist } a_1, \ldots, a_r \in \mathfrak{m} \text{ such that } \ell(M/a_1 M + \cdots + a_r M) < \infty\}.$$

In the particular case $M = R$ we have the following description of $\delta(R)$:

$$\delta(R) = \min\{r : \text{there exists an } \mathfrak{m}\text{-primary ideal of } R \text{ generated by } r \text{ elements}\}.$$

Turns out that Noetherian local rings actually have finite dimension. In the local setting, we will also show that the invariants $d(M), \dim(M)$ and $\delta(M)$ we have introduced so far actually coincide when M is finitely generated. We start with a couple of observations:

Remark 4.2.2.

1. Suppose
$$0 \longrightarrow N \longrightarrow M \longrightarrow P \longrightarrow 0$$
is a short exact sequence of finitely generated R-modules. Then
$$\operatorname{Supp}(M) = \operatorname{Supp}(N) \cup \operatorname{Supp}(P).$$
From this one sees that
$$\dim(M) = \max\{\dim(N), \dim(P)\}.$$

2. Suppose $(R, \mathfrak{m})$ is local and M is finitely generated. Given $x \in \mathfrak{m}$ we claim that
$$d(M/xM) \geq d(M) - 1.$$
To see this, let $M' = M/xM$. Then
$$\begin{aligned}\ell(M'/\mathfrak{m}^n M') &= \ell(M/xM + \mathfrak{m}^n M) = \ell(M/\mathfrak{m}^n M) - \ell(\mathfrak{m}^n M + xM/\mathfrak{m}^n M) \\ &= \ell(M/\mathfrak{m}^n M) - \ell(xM/xM \cap \mathfrak{m}^n M).\end{aligned}$$
Multiplication by x induces an isomorphism $M/(\mathfrak{m}^n M : x) \cong xM/xM \cap \mathfrak{m}^n M$. Thus
$$\ell(M'/\mathfrak{m}^n M') = \ell(M/\mathfrak{m}^n M) - \ell(M/(\mathfrak{m}^n M : x)) \geq \ell(M/\mathfrak{m}^n M) - \ell(M/\mathfrak{m}^{n-1} M).$$
For $n \gg 0$ we have that $\ell(M/\mathfrak{m}^n M) - \ell(M/\mathfrak{m}^{n-1} M)$ coincides with a polynomial of degree $d(M) - 1$ evaluated at n. Thus $d(M') \geq d(M) - 1$.

Theorem 4.2.3. (Fundamental theorem of dimension theory) *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring and M a finitely generated R-module. Then*

$$\dim(M) = d(M) = \delta(M) < \infty.$$

Proof. Step 1: $\dim(M) \leq d(M)$. (Consequently, $\dim(M)$ is finite).

Step 1.1: We prove Step 1 for the case $M = R$, by induction on $d(R)$.

Suppose $d(R) = 0$. This means that $\ell(R/\mathfrak{m}^n) = \ell(R/\mathfrak{m}^{n+1})$ for all $n \gg 0$. But this is equivalent to $\ell(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = 0$, i.e., $\mathfrak{m}^n = \mathfrak{m}^{n+1}$, which by Nakayama's lemma implies $\mathfrak{m}^n = 0$. Thereore, R is Artinian and thus $\dim(R) = 0$.

Suppose now $d(R) > 0$. If $\dim(R) = 0$, there is nothing to prove. So, assuming $\dim(R) > 0$, take any strictly increasing chain $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_e$ of prime ideals of R. We must show that $e \leq d(R)$. Consider an element $x \in P_1 \backslash P_0$. Let $S = R/(P_0, x)$, so that we have a short exact sequence

$$0 \longrightarrow R/P_0 \xrightarrow{\cdot x} R/P_0 \longrightarrow R/(P_0, x) = S \longrightarrow 0 \ .$$

Let $A = R/P_0$. By Lemma 3.3.6, we get that $d(A) = \max(d(A), d(S))$, so that $d(S) \leq d(A)$. But the proof of Lemma 3.3.6 also tells us that $\varphi_A^{\mathfrak{m}} - \varphi_S^{\mathfrak{m}}$ has the same leading coefficient as $\varphi_A^{\mathfrak{m}}$. Thus, we can actually conclude that $d(S) < d(A)$. Also, since A is a quotient of R, is easy to see that $d(A) \leq d(R)$. Thus $d(S) \leq d(R) - 1$. By the induction hypothesis we get

$$\dim(S) \leq d(S) \leq d(R) - 1.$$

As $P_1 \subsetneq \cdots \subsetneq P_e$ provides a strictly increasing chain of prime ideals in S, we obtain

$$e - 1 \leq \dim(S) \leq d(R) - 1.$$

Thus $e \leq d(R)$ as we wanted to show.

Step 1.2: We prove Step 1 for the general case of a finitely generated R-module M.

By Theorem 2.3.8 there exists a filtration $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_r = M$ of submodules of M such that for all i we have $M_{i+1}/M_i \cong R/P_i$ for prime ideals P_i of R. Using Remark 4.2.2, Lemma 3.3.6 and Step 1 we get

$$\dim(M) = \max\{\dim(R/P_i)\} \leq \max\{d(R/P_i)\} = d(M).$$

Step 2: $d(M) \leq \delta(M)$.

If $\delta(M) = 0$, this means that $\ell(M) < \infty$. Since $\ell(M/\mathfrak{m}^n M) \leq \ell(M)$ for all n, $n \longmapsto \ell(M/\mathfrak{m}^n M)$ must be bounded, so that $d(M) = 0$. Suppose now that $\delta(M) = r > 0$ and let $a_1, \ldots, a_r \in \mathfrak{m}$ be such that $M' = M/a_1 M + \cdots + a_r M$ has finite length. Then, by repeated use of Remark 4.2.2, we get $0 = d(M') \geq d(M) - s$, i.e., $d(M) \leq s = \delta(M)$.

Step 3: $\delta(M) \leq \dim(M)$.

We prove this part by induction on $\dim(M)$. If $\dim(M) = 0$, then as, we have seen before, this is equivalent to $\ell(M) = 0$, so that $\delta(M) = 0$. Suppose now $\dim(M) > 0$. Let $P_1, \ldots, P_r$ the the minimal primes of $\mathrm{Ann}(M)$ for which $\dim(M) = \dim(R/P_i)$ for all i. Since $\dim(M) > 0$, $P_i \neq \mathfrak{m}$ for all i. By prime avoidance there exists $x \in \mathfrak{m} \backslash P_1 \cup \cdots \cup P_r$. Set $M' = M/xM$. The choice of x guarantees that $\dim(M') \leq \dim(M) - 1$. Also, the inequality $\delta(M) \leq \delta(M') + 1$ is clear from the definition of δ. Thus, by the induction hypothesis it follows that

$$\delta(M) \leq \delta(M') + 1 \leq \dim(M') + 1 \leq \dim(M).$$

This concludes the proof of the theorem. □

This leads to the following definition.

Definition 4.2.4. *(System of parameters)* Let $(R, \mathfrak{m})$ be a Noetherian local ring and M a finitely generated R-module of dimension d. We say that a sequence $x_1, \ldots, x_d$ in $\mathfrak{m}$ is a *system of parameters (s.o.p.)* of M if

$$\ell(M/(x_1 M + \cdots + x_d M)) < \infty.$$

If a sequence $x_1, \ldots, x_i \in \mathfrak{m}$ with $1 \leq i \leq d$ can be completed to be a s.o.p. of M, we say that $x_1, \ldots, x_i$ is a *parameter sequence* (or *part of a s.o.p.*) of M.

In particular, if $(R,\mathfrak{m})$ is Noetherian of dimension d, then $x_1,\dots,x_d \in \mathfrak{m}$ are a s.o.p. of R if and only if $(x_1,\dots,x_d)$ is $\mathfrak{m}$-primary if and only if $R/(x_1,\dots,x_d)$ is Artinian (has dimension zero).

Example 4.2.5. 1. We can now see that if k is a field then $R = k[\![X_1,\dots,X_n]\!]$ has dimension exactly n. Indeed, $X_1,\dots,X_n$ is such that $\dim(R/(X_1,\dots,X_n)) = \dim(k) = 0$, so that $\dim(R) = \delta(R) \leq n$. But we have already seen before that $\dim(R) \geq n$. Thus $\dim(R) = n$ and $X_1,\dots,X_n$ is a s.o.p. of R.

$X_1^2,\dots,X_n^2$ is also a s.o.p. of R since $(X_1^2,\dots,X_n^2)$ is $(X_1,\dots,X_n)$-primary.

2. Consider $R = k[\![x,y,z]\!]/(xy,xz,x^2)$. Check that $\dim(R) = 2$ and that y^2, z^2 is a s.o.p. of R.

4.3 Height theorems

One consequence of Theorem 4.2.3 is that all ideals in a Noetherian ring have finite height, which can be controled by the number of generators of the ideal.

Theorem 4.3.1. *Let R be a Noetherian ring and $I = (a_1,\dots,a_r)$ a proper ideal of R generated by r elements. Then*

$$\operatorname{ht}(I) \leq r.$$

Proof. Let P be a minimal prime of I. We must show that $\operatorname{ht}(P) \leq r$. Consider the local ring R_P. By Theorem 4.2.3 we have that $\operatorname{ht}(P) = \dim(R_P) = \delta(R_P)$. This coincides with

$$\inf\{s : R_P \text{ contains a } PR_P\text{-primary ideal generated by } s \text{ elements}\}.$$

Since P is a minimal prime over I, there is no prime ideal in R_P strictly between IR_P and PR_P. Thus IR_P is PR_P-primary. Since IR_P can be generated by r elements, we conclude that $\delta(R_P) \leq r$. □

Theorem 4.3.2. *Let R be a Noetherian ring and P a prime ideal of R of height r. Then*

(1) There exist $a_1,\dots,a_r \in R$ such that P is a minimal prime of $(a_1,\dots,a_r)$.

(2) For any $b_1,\dots,b_s \in P$ we have that $\operatorname{ht}(P/(b_1,\dots,b_s)) \geq r - s$.

(3) If $a_1,\dots,a_r$ are as in (1), then $\operatorname{ht}(P/(a_1,\dots,a_i)) = r - i$ for all $1 \leq i \leq r$.

Proof. (1) R_P is a ring of dimension r. By Theorem 4.2.3 there exist elements $a_1,\dots,a_r \in R_P$ such that PR_P is a minimal prime over $a_1R_P + \cdots a_rR_P$. We can pick these a_i in R. Then P must be a minimal prime of $(a_1,\dots,a_r)$.

(2) Denote $\overline{R} = R/(b_1,\dots,b_s)$ and $\overline{P} = P/(b_1,\dots,b_s)$. Let $t = \operatorname{ht}(\overline{P})$. By (1) there exist $a_1,\dots,a_t \in \overline{R}$ such that $\overline{P}$ is minimal over $(a_1,\dots,a_t)$. Let c_i denote the preimage of a_i in R. Then P is minimal over $(c_1,\dots,c_t,b_1,\dots,b_s)$. It follows by Theorem 4.3.1 that $r = \operatorname{ht}(P) \leq t + s$.

(3) If P is minimal over $(a_1,\dots,a_r)$, then $P/(a_1,\dots,a_i)$ is minimal over $(\overline{a_{i+1}},\dots,\overline{a_r})$ in $R/(a_1,\dots,a_i)$. Thus $\operatorname{ht}(P/(a_1,\dots,a_i)) \leq r - i$. The opposite inequality follows from (2). □

In fact, parameter sequences are determined by a property similar to the one in Theorem 4.3.2.

Theorem 4.3.3. *Let $(R,\mathfrak{m})$ be a Noetherian local ring of dimension d and $x_1,\dots,x_d \in \mathfrak{m}$. Then*

(1) $x_1,\dots,x_d$ is a s.o.p. of R if and only if $\dim(R/(x_1,\dots,x_i)) = d - i$ for all $1 \leq i \leq d$.

(2) One can choose a s.o.p. $x_1,\dots,x_d$ of R with the property that every subset $F \subseteq \{x_1,\dots,x_d\}$ generates an ideal of height $|F|$.

Proof. (1) Follows easily from Theorem 4.3.2 (3).

(2): If $d = 1$ the statement is obvious. Suppose $d \geq 2$. Let $\mathcal{P}_0$ be the set of prime ideals of R of height zero. The elements in $\mathcal{P}_0$ are the minimal primes of R, hence $\mathcal{P}_0$ is finite. By prime avoidance we can pick $x_1 \in \mathfrak{m}$ such that x_1 does not belong to any prime in $\mathcal{P}_0$. This guarantees that $\operatorname{ht}(x_1) = 1$. Let now $\mathcal{P}_1$ denote the set of minimal primes of (x_1) of height 1. As $\mathfrak{m} \notin \mathcal{P}_1 \cup P_0$, by prime avoidance we can pick $x_2 \in \mathfrak{m}$ such that x_2 does not belong to any prime of $\mathcal{P}_0$ (which guarantees $\operatorname{ht}(x_2) = 1$) or $\mathcal{P}_1$ ($\operatorname{ht}(x_1,x_2) = 2$). If $d = 2$ we are done. Otherwise we can keep this process going, choosing x_2 not in any minimal prime of R of height zero, in any minimal prime of (x_1) or (x_2) of height one, or in any minimal prime of (x_1,x_2) of height two, and so on. □

The following example show that if we do not choose our system of parameters $x_1, \dots, x_d$ carefully, it can indeed happen that $\operatorname{ht}(x_1, \dots, x_i) < i$.

Example 4.3.4. Take $R = k[\![x, y, z]\!]/(xy, xz)$, where k is a field. The minimal primes of R are (x) and (y, z). $R/(x) \cong k[\![y, z]\!]$ has dimension 2, while $R/(y, z) \cong k[\![x]\!]$ has dimension 1. Thus $\dim(R) = 2$. Notice that $\{y, x + z\}$ is a s.o.p. of R. Indeed $R/(y, x + z) \cong k[\![x, y, z]\!]/(xy, xz, y, x + z) \cong k[\![x, z]\!]/(xz, x + z) \cong k[\![x]\!]/(x^2)$ is zero dimensional. However, (y) has height zero since y is contained in a minimal prime of R.

4.4 A graded perspective of dimension

Our goal here is essentially to show that if $(R_0, \mathfrak{m})$ is a Noetherian local ring, then $R = R_0[x_1, \dots, x_n]$ has finite dimension. In fact, the dimension of R will equal the height of $\mathfrak{m} + R_+$ and can be measured by the largest size of a saturated chain of homogeneous prime ideals in R.

Definition 4.4.1. Let R be a graded ring and I an arbitrary ideal of R. We define I^* to be the homogeneous ideal of R generated by all homogeneous elements $a \in I$. I^* is the largest homogeneous ideal that sits inside I.

Proposition 4.4.2. *Let R be a $\mathbb{Z}$-graded ring. If P is a prime ideal of R, then P^* is also a prime ideal.*

Proof. This can be a fun exercise. □

Given a prime ideal P of a $\mathbb{Z}$-graded ring R, let S denote the set of homogeneous elements that do not belong to P. Then S is a multiplicatively closed subset of R. If M is a graded R-module, define

$$M_{(P)} = S^{-1}M.$$

Then one can define a grading on $M_{(P)}$ by setting $\deg(x/a) = \deg(x) - \deg(a)$ for all homogeneous $x \in R$ and all homogeneous $a \in S$. The piece of degree n of $M_{(P)}$ is then

$$(M_{(P)})_n = \{x/a \in M_{(P)} : x \text{ homogeneous and } \deg(x/a) = n\}.$$

$R_{(P)}$ is a $\mathbb{Z}$-graded ring and $M_{(P)}$ is a graded $R_{(P)}$-module. Notice that $P^*R_{(P)}$ is a graded prime ideal of $R_{(P)}$ and that every nonzero homogeneous element in $R_{(P)}/P^*R_{(P)}$ is invertible.

Lemma 4.4.3. *Let R be a $\mathbb{Z}$-graded ring. The following are equivalent.*

(1) Every nonzero homogeneous element in R is invertible.

(2) $R_0 = k$ is a field and either $R = k$ (if R has no elements of positive degree) or $R = k[t, t^{-1}]$ with $t \in R$ homogeneous of positive degree and transcendental over k.

Proof. I refer to [BH98, Lemma 1.5.7]. □

With this we can now prove the following.

Proposition 4.4.4. *Let R be a $\mathbb{Z}$-graded ring and P a prime ideal of R. If P is not homogeneous, then* $\operatorname{ht}(P/P^*) = 1$.

Proof. Let $A = R_{(P)}/P^*R_{(P)}$. Then $\operatorname{ht}(P/P^*) = \operatorname{ht}(PA)$ (the height of the ideal PA in A). By the previous lemma and previous observations, A is either k or $k[t, t^{-1}]$, for a field k and a variable t. But since PA is a nonzero proper ideal in A, the latter must be the case. Now, as $k[t, t^{-1}]$ is a principal ideal domain, we conclude that $\operatorname{ht}(PA) = 1$. □

Associated primes behave well with respect to grading.

Lemma 4.4.5. *Let R be a Noetherian $\mathbb{Z}$-graded ring. If I is a proper homogeneous ideal of R and $P \in \operatorname{Ass}(R/I)$, then P is also homogeneous.*

Proof. P is a prime ideal of R of the form $P = (I : x)$ for some $x \in R$. Let $x = x_s + \cdots + x_r$ be the decomposition of x into homogeneous components ($s \leq r, x_i \in R_i$). Suppose $a \in P$. We must show that each homogeneous component of a is also in P. Let $a = a_p + \cdots + a_q$ be the decomposition of a into homogeneous components ($p \leq q, a_j \in R_j$). As $ax \in I$ and I is homogeneous, we have

$$a_p x_s \in I, \quad a_p x_{s+1} + a_{p+1} x_s \in I, \quad a_p x_{s+2} + a_{p+1} x_{s+1} + a_{p+2} x_s \in I, \cdots .$$

Multiplying the i-th equation by a_p^i we successively get $a_p^2 x_{s+1} \in I$, $a_p^3 x_{s+2} \in I, \ldots, a_p^{r-s+1} x_r \in I$. Thus $a_p^{r-s+1} x \in I$, meaning $a_p^{r-s+1} \in P$. As P is a prime ideal, we must have $a_p \in P$. Therefore, $a_{p+1} + \cdots + a_q \in P$ and, by the same argument, we conclude that $a_{p+1} \in P$. Continuing in this way, we see that all the homogeneous components of a belong to P. □

We can now investigate properties of chains of prime ideals in graded rings.

Proposition 4.4.6. *Let R be a Noetherian $\mathbb{Z}$-graded ring and P a prime ideal of R of finite height r. Then there exists a chain*

$$P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_{r-1} \subsetneq P$$

with $P_0, P_1, \ldots, P_{r-1}$ homogeneous prime ideals.

Proof. By induction on r. If $r = 0$ there is nothing to prove. Also, for $r = 1$ the result follows because in any saturated chain $P_0 \subsetneq P$ of prime ideals, the prime P_0 must be a minimal, and thus an associated, prime of (0) (as (0) is homogeneous, Lemma 4.4.5 guarantees that P_0 is an homogeneous ideal).

Suppose now that $r > 1$. There is a saturated chain of prime ideals $Q_0 \subsetneq Q_1 \subsetneq Q_2 \subsetneq \cdots \subsetneq Q_{r-1} \subsetneq P$. The prime Q_{r-1} has height $r - 1$, so that, by induction, there is a chain

$$P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_{r-2} \subsetneq Q_{r-1} \subsetneq P$$

where $P_0, P_1, \ldots, P_{r-2}$ are homogeneous primes. It remains to find a homogeneous prime ideal P_{r-1} such that $P_{r-2} \subsetneq P_{r-1} \subsetneq P$.

Case 1: P is not homogeneous. In this case pick $P_{r-1} = P^*$. P^* is strictly contained in P because P is not homogeneous. Also, as P_{r-2} is homogeneous, $P_{r-2} \subseteq P^*$. But this last inclusion must be strict, otherwise $\operatorname{ht}(P/P^*) = \operatorname{ht}(P/P_{r-2}) = 2$, which would contradict the fact that $\operatorname{ht}(P/P^*) = 1$, from Lemma 4.4.4.

Case 2: P is homogeneous. In this case we can pick a homogeneous element $a \in P \backslash P_{r-2}$ and let P_{r-1} be a minimal prime of $P_{r-2} + (a)$ contained in P. As P_{r-1} is an associated prime of the homogeneous ideal $P_{r-2} + (a)$, it must be homogeneous by Lemma 4.4.4. It remains to notice that $P_{r-1} \neq P$. Indeed, if $P = P_{r-1}$ then, by the definition of P_{r-1}, the prime P/P_{r-2} would be a minimal prime of the principal ideal $(P_{r-2} + (a))/P_{r-2}$ in R/P_{r-2}. By Theorem 4.3.1, this would imply $\operatorname{ht}(P/P_{r-2}) \leq 1$, contradicting the fact that $\operatorname{ht}(P/P_{r-2}) = 2$. □

Definition 4.4.7. Let R be a graded ring. A proper homogeneous ideal $\mathfrak{m}$ of R is said to be **-maximal* if there is no homogeneous ideal J of R such that $\mathfrak{m} \subsetneq J \subsetneq R$. R is said to be **-local* if it has a unique $*$-maximal ideal $\mathfrak{m}$. In this case we say $(R, \mathfrak{m})$ is a *-local ring.

Remark 4.4.8. Suppose $R = \bigoplus_{n \geq 0} R_n$ is $\mathbb{N}$-graded.

(1) Every *-maximal ideal $\mathfrak{m}$ of R is maximal. Indeed, if $\mathfrak{m}$ is *-maximal, every homogeneous element of $R/\mathfrak{m}$ must be invertible, so that, by Lemma 4.4.3, either $R/\mathfrak{m} \cong k$ or $R/\mathfrak{m} \cong k[t, t^{-1}]$, where k is a field. But since $R/\mathfrak{m}$ is positively graded, we must fall on the case $R/\mathfrak{m} \cong k$. This tells us that $\mathfrak{m}$ is a maximal ideal of R.

(2) Every *-maximal ideal of R is of the form $\mathfrak{m}_0 + R_+$ where $\mathfrak{m}_0$ is a maximal ideal of R_0 (recall that $R_+ = R_1 \oplus R_2 \oplus \cdots$). Indeed, if $\mathfrak{m}$ is *-maximal, clearly it must contain R_+. Thus $\mathfrak{m} = \mathfrak{m}_0 \oplus R_+$ where $\mathfrak{m}_0 = \mathfrak{m} \cap R_0$. Since $R/\mathfrak{m} \cong R_0/\mathfrak{m}_0$ must be maximal, $\mathfrak{m}_0$ is a maximal ideal of R_0.

Consequently, if R_0 is local, R is *-local.

Now we can see that positively graded Noetherian *-local rings have finite dimension and that their dimension equals the height of the *-maximal ideal.

Theorem 4.4.9. *Let $R = \bigoplus_{n \geq 0} R_n$ be a Noetherian *-local ring with *-maximal ideal $\mathfrak{m}$. Then*

$$\dim(R) = \operatorname{ht}(\mathfrak{m}) < \infty.$$

This coincides with the maximum length of a saturated chain of homogeneous prime ideals of R.

Proof. Since R is Noetherian, $\mathfrak{m}$ is finitely generated and so $\operatorname{ht}(\mathfrak{m}) < \infty$. $\dim(R) \geq \operatorname{ht}(\mathfrak{m})$ is obvious. We show the opposite inequality. Let P be a prime ideal of R. If P is homogeneous, then $P \subseteq \mathfrak{m}$ and thus $\operatorname{ht}(P) \leq \operatorname{ht}(\mathfrak{m})$. If P is not homogeneous, then $\operatorname{ht}(P) = \operatorname{ht}(P^*) + 1$ by Propositions 4.4.4 and 4.4.6. As $P^* \subsetneq P$, P^* is not maximal, and thus not *-maximal. Hence $P^* \subsetneq \mathfrak{m}$, so that $\operatorname{ht}(P^*) \leq \operatorname{ht}(\mathfrak{m}) - 1$. From this we conclude that $\operatorname{ht}(P) \leq \operatorname{ht}(\mathfrak{m})$.

The last statement of the theorem follows from Proposition 4.4.6. □

If k is a field, we can now see that $\dim(k[x_1,\dots,x_n]) = n$. Indeed, by the previous theorem $\dim(k[x_1,\dots,x_n]) = \mathrm{ht}(x_1,\dots,x_n) \leq n$, while $\dim(k[x_1,\dots,x_n]) \geq n$ can be seen from the chain of prime ideals $(0) \subsetneq (x_1) \subsetneq (x_1,x_2) \subsetneq \cdots \subsetneq (x_1,\dots,x_n)$.

Definition 4.4.10. Let $(R,\mathfrak{m})$ be an $\mathbb{N}$-graded Noetherian *-local ring of dimension d. A *homogeneous system of parameters of* R is a sequence $y_1,\dots,y_d$ of homogeneous elements of R such that $\dim(R/(y_1,\dots,y_d)) = 0$ (or, equivalently, such that $(y_1,\dots,y_d)$ is $\mathfrak{m}$-primary).

Notice that homogeneous systems of parameters do exist in $\mathbb{N}$-graded Noetherian *-local rings. They can be picked in a similar way to that of Theorem 4.3.3 (2), using the fact that minimal primes of homogeneous ideals are homogeneous and using the graded version of prime avoidance.

We finish this section by mentioning that there is a graded version of the fundamental theorem of dimension theory (Theorem 4.2.3).

Recall that if M is a nonzero finitely generated graded module over a graded Noetherian ring R which is standard graded ($R = R_0[R_1]$) and such that R_0 is Artinian, then the Hilbert series of M can be written as $\mathrm{HS}_M(t) = f(t)/(1-t)^d$ with $f(1) \neq 0$. We denote $d(M) = d$. This is such that the Hilbert polynomial of M has degree $d-1$.

Theorem 4.4.11. *Let $R = R_0[R_1]$ be a standard graded Noetherian ring with R_0 Artinian and let M be a finitely generated graded R-module. Then*

$$\dim(M) = d(M).$$

Proof. I refer to [BH98, Theorem 4.1.3] for a proof of this. It is similar to the proof of Theorem 4.2.3 (but even simpler, I would say). □

With this we can show the following.

Theorem 4.4.12. *Let $(R,\mathfrak{m})$ be a Noetherian local ring. Then*

$$\dim(R) = \dim(\mathrm{gr}_{\mathfrak{m}}(R)).$$

Proof. By Theorem 4.2.3 we know that $\dim(R) = d$, where d is the degree of the Samuel polynomial of R. By what we have seen in Section 3.3, this coincides with the number d such that the Hilbert series of $\mathrm{gr}_{\mathfrak{m}}(R)$ can be written as $f(t)/(1-t)^d$ with $f(1) \neq 0$. Now, by Theorem 4.4.11, this equals $\dim(\mathrm{gr}_{\mathfrak{m}}(R))$. □

Remark 4.4.13. Take $R = k[\![X_1,\dots,X_n]\!]$, where k is a field. Then $\mathrm{gr}_{(x_1,\dots,x_n)}(R) = k[x_1,\dots,x_n]$. We have seen that the Hilbert series of $k[x_1,\dots,x_n]$ is $1/(1-t)^n$. This is another way to see that $\dim(k[\![X_1,\dots,X_n]\!]) = \dim(k[x_1,\dots,x_n]) = n$.

5 Basics of homological algebra

Let R be a ring. Recall that a *complex* is a sequence

$$C_\bullet : \cdots \longrightarrow C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \longrightarrow \cdots$$

of R-modules and R-homomorphisms such that $d_n \circ d_{n+1} = 0$ for all n. In other terms, $\operatorname{im}(d_{n+1}) \subseteq \ker(d_n)$ for all n. As such, for each n we can associate to $C_\bullet$ the R-module

$$H_n(C_\bullet) = \frac{\ker(d_n)}{\operatorname{im}(d_{n+1})}.$$

This is called the *n-th homology module of $C_\bullet$*. Recall that $C_\bullet$ is *exact* at position n if $\operatorname{im}(d_{n+1}) = \ker(d_n)$, i.e., if $H_n(C_\bullet) = 0$. As such, the modules $H_n(C_\bullet)$ are a measure of how far the complex is from being exact.

$d = (\ldots, d_{n+1}, d_n, \ldots)$ is called the *differential* of $C_\bullet$. It is also common to omit the indexes when referring to the maps $d_n : C_n \longrightarrow C_{n-1}$ (instead we may just write $d : C_n \longrightarrow C_{n-1}$). With this abuse of notation, the property of being a complex can be stated as just $d \circ d = 0$. Also, we may use the expression "let $(C_\bullet, d)$ be a complex" to mean that $C_\bullet$ is a complex with differential d. Another piece of terminology that is used is the following: $\ker(d_n)$ can be denoted by $Z_n(C_\bullet)$ and its elements are called *cycles*; $\operatorname{im}(d_{n+1})$ can be denoted by $B_n(C_\bullet)$ and its elements are called *boundaries*. This way, $H_n(C_\bullet) = Z_n(C_\bullet)/B_n(C_\bullet)$.

Remark 5.0.1. (and definition) We will also consider complexes with the indexes going up, instead of down:

$$\cdots \longrightarrow C_{n-1} \xrightarrow{d_{n-1}} C_n \xrightarrow{d_n} C_{n+1} \longrightarrow \cdots .$$

We will use the notation $C^\bullet$ for such complexes. In this situation, the homology modules of $C^\bullet$ are actually called *cohomology modules of $C^\bullet$* and they are denoted by $H^n(C^\bullet) = \ker(d_n)/\operatorname{im}(d_{n-1})$.

In this section I will leave quite a few statements as exercises (as doing everything here and going over every detail would ruin the rhythm of the exposition). If you are interested in learning this theory in a more detailed manner, I recommend [Wei94] as a good reference for learning about homological algebra.

5.1 Maps of complexes

A *map of complexes* (or *chain map*) $f : A_\bullet \longrightarrow B_\bullet$ between two complexes $(A_\bullet, d^A)$ and $(B_\bullet, d^B)$ is a sequence of R-module homomorphisms $f_n : A_n \longrightarrow B_n$ such that $d^B_n f_n = f_{n-1} d^A_n$ for all n. In other words, such that the following diagram commutes:

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & A_{n+1} & \longrightarrow & A_n & \longrightarrow & A_{n-1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \\
\cdots & \longrightarrow & B_{n+1} & \longrightarrow & B_n & \longrightarrow & B_{n-1} & \longrightarrow & \cdots
\end{array}.$$

The commutativity of this diagram forces $f_n(\ker d^A_n) \subseteq \ker d^B_n$ and $f_n(\operatorname{im} d^A_{n+1}) \subseteq \operatorname{im} d^B_{n+1}$. Consequently, f induces a well defined map $H_n(f) : H_n(A_\bullet) \longrightarrow H_n(B_\bullet)$ given by

$$\begin{array}{ccc}
H_n(A_\bullet) & \longrightarrow & H_n(B_\bullet) \\
z + \operatorname{im}(d^A_{n+1}) & \longmapsto & f_n(z) + \operatorname{im}(d^B_{n+1})
\end{array}.$$

The map $H_n(f)$ can be denoted by f_{*n} (or even simply by f if there is no confusion).

We say that a map of complexes $f : A_\bullet \longrightarrow B_\bullet$ is a *quasi-isomorphism* if $H_n(f)$ is an isomorphism for every n.

Definition 5.1.1. We say that two maps of complexes $f, g : A_\bullet \longrightarrow B_\bullet$ are *homotopic* (denoted $f \sim g$) if for each n there exists R-module homomorphisms $h_n : A_n \longrightarrow B_{n+1}$ such that $f_n - g_n = d^B_{n+1} h_n + h_{n-1} d^A_n$.

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & A_{n+1} & \longrightarrow & A_n & \longrightarrow & A_{n-1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f_{n+1}} & \swarrow{\scriptstyle h_n} & \downarrow{\scriptstyle f_n} & \swarrow{\scriptstyle h_{n-1}} & \downarrow{\scriptstyle f_{n-1}} & & \\
\cdots & \longrightarrow & B_{n+1} & \longrightarrow & B_n & \longrightarrow & B_{n-1} & \longrightarrow & \cdots
\end{array}$$

$h = (\ldots, h_{n+1}, h_n, \ldots)$ is called a *homotopy* between f and g.

Two complexes $A_\bullet$ and $B_\bullet$ are said to be *homotopy equivalent* if there exist chain maps $f : A_\bullet \longrightarrow B_\bullet$ and $g : B_\bullet \longrightarrow A_\bullet$ such that $gf \sim 1_A$ and $fg \sim 1_B$. In this case we say that f and g are *homotopy equivalences* between $A_\bullet$ and $B_\bullet$.

Exercise 5.1.2. (a) Show that $\sim$ is an equivalence relation.

(b) Show that if two maps of complexes $f, g : A_\bullet \longrightarrow B_\bullet$ are homotopic, then f and g induce the same maps $H_n(A_\bullet) \longrightarrow H_n(B_\bullet)$ in homology, for every n.

(c) Show that homotopy equivalences are quasi-isomorphisms

The converse, however, is not true. For example, the following map of complexes is a quasi-isomorphism.

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\times 2} & \mathbb{Z} & \longrightarrow & 0 & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \pi} & & \downarrow & & \\
\cdots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 & \longrightarrow & \cdots
\end{array}$$

(where π is the projection) but it is not a homotopy equivalence (essentialy because every $\mathbb{Z}$-module homomorphism from $\mathbb{Z}/2\mathbb{Z}$ to $\mathbb{Z}$ must be the zero map).

Of course, the composition of two chain maps is also a chain map. As such, there is a category whose objects are the complexes of R-modules and whose arrows are the maps of complexes. This is the *category of chain complexes*, denoted $\mathrm{Ch}(R)$.

Given a map of complexes $f : A_\bullet \longrightarrow B_\bullet$, its *kernel* is the complex

$$\cdots \longrightarrow \ker f_{n+1} \longrightarrow \ker f_n \longrightarrow \ker f_{n-1} \longrightarrow \cdots$$

where the differential is the restriction of the differential of $A_\bullet$, and the *image* of f is the complex

$$\cdots \longrightarrow \operatorname{im} f_{n+1} \longrightarrow \operatorname{im} f_n \longrightarrow \operatorname{im} f_{n-1} \longrightarrow \cdots$$

where the differential is the restriction of the differential of $B_\bullet$. (*Exercise:* Check that these are indeed complexes of R-modules). With these notions, one can consider complexes in $\mathrm{Ch}(R)$ (i.e., complexes of complexes). We will mostly be interested, however, in short exact sequences of complexes.

Definition 5.1.3. A *short exact sequence of complexes* is an exact sequence of the form

$$0 \longrightarrow A_\bullet \xrightarrow{f} B_\bullet \xrightarrow{g} C_\bullet \longrightarrow 0$$

where $A_\bullet, B_\bullet$ and $C_\bullet$ are complexes of R-modules and f and g are maps of complexes. Equivalently, a short exact sequence of complexes is a commutative diagram of the form

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A_{n+1} & \xrightarrow{f_{n+1}} & B_{n+1} & \xrightarrow{g_{n+1}} & C_{n+1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A_n & \xrightarrow{f_n} & B_n & \xrightarrow{g_n} & C_n & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A_{n-1} & \xrightarrow{f_{n-1}} & B_{n-1} & \xrightarrow{g_{n-1}} & C_{n-1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

where every row is a short exact sequence of R-modules.

The big thing here is that a short exact sequence of complexes $0 \longrightarrow A_\bullet \xrightarrow{f} B_\bullet \xrightarrow{g} C_\bullet \longrightarrow 0$ can help us compute the homology modules of $A_\bullet, B_\bullet$ and $C_\bullet$. This is because this short exact sequence will induce a long exact sequence in homology. This is what we now want to show. For this, we need the famous Snake lemma. Recall that the cokernel of an R-module homomorphism $h : M \longrightarrow N$ is $\operatorname{coker} h = N/\operatorname{im} h$.

Lemma 5.1.4. (the Snake lemma) *Suppose we have a commutative diagram of R-modules as follows:*

$$\begin{array}{ccccccc} & & A & \xrightarrow{i} & B & \xrightarrow{p} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A' & \xrightarrow{i'} & B' & \xrightarrow{p'} & C' & & \end{array}$$

where both rows are exact. Then there exists an exact sequence

$$\ker f \longrightarrow \ker g \longrightarrow \ker h \xrightarrow{\partial} \operatorname{coker} f \longrightarrow \operatorname{coker} g \longrightarrow \operatorname{coker} h$$

where ∂ is defined as follows: given $c \in C$ with $c \in \ker h$, pick $b \in B$ such that $p(b) = c$. Then $g(b) \in \ker p' = \operatorname{im} i'$, so that there exists a unique $a' \in A'$ such that $g(b) = i'(a')$. Define

$$\partial(c) = a' + \operatorname{im} f \in \operatorname{coker} f.$$

∂ is called the connecting homomorphism.

Proof. There is a lot of stuff to check here. I leave it as an exercise to prove exactness at $\ker g$ and $\operatorname{coker} g$. Also, you should try to prove that ∂ is indeed a homomorphism and that it is well defined (i.e., the choice of b does not matter).

Let's show exactness at $\ker h$. We need to show that $\ker g \xrightarrow{p} \ker h \xrightarrow{\partial} \operatorname{coker} f$ is exact.

Given $b \in \ker g$, we must show that $\partial(p(b)) = 0$. By the definition of ∂, $\partial(p(c)) = a' + \operatorname{im} f$ where a' is such that $i'(a') = g(b)$. But since $g(b) = 0$, the only choice for a' is $a' = 0$.

Next we must show that if $c \in \ker h$ is such that $\partial(c) = 0$, then $c \in p(\ker g)$. Indeed, pick $b \in B$ such that $p(b) = c$. Then $\partial(c) = a' + \operatorname{im}(f)$ where $i'(a') = g(b)$. The hypothesis $\partial(c) = 0$, which tells us that $a' \in \operatorname{im}(f)$, so write $a' = f(a)$ with $a \in A$. Then $g(b) = i'(a') = i'(f(a)) = g(i(a))$, meaning $b_0 := b - i(a) \in \ker g$. Thus $c = p(b) = p(b_0) \in p(\ker g)$, as we wanted to show.

Finally, one must show exactness at $\operatorname{coker} f$. This one is more diagram chasing and I also leave it as an exercise. $\square$

We can now see how short exact sequences of complexes induce long exact sequences in homology.

Theorem 5.1.5. (the long exact sequence) *Let*

$$0 \longrightarrow A_\bullet \xrightarrow{f} B_\bullet \xrightarrow{g} C_\bullet \longrightarrow 0$$

be a short exact sequence of complexes. There exist connecting homomorphisms $\partial : H_n(C_\bullet) \longrightarrow H_{n-1}(A_\bullet)$, for all n, such that

$$\cdots \longrightarrow H_{n+1}(C_\bullet) \xrightarrow{\partial} H_n(A_\bullet) \xrightarrow{f_*} H_n(B_\bullet) \xrightarrow{g_*} H_n(C_\bullet) \xrightarrow{\partial} H_{n-1}(A_\bullet) \longrightarrow \cdots$$

is an exact sequence.

Proof. Given a complex $F_\bullet$, note that the differential d induces well defined maps $\overline{d_n} : F_n/\operatorname{im} d_{n+1} \longrightarrow \ker d_{n-1}$ given by $\overline{d_n}(x + \operatorname{im} d_{n+1}) = d_n(x)$. Plus, notice that $\ker \overline{d_n} = \ker d_n/\operatorname{im} d_{n+1} = H_n(F_\bullet)$ and $\operatorname{coker} \overline{d_n} = \ker d_{n-1}/\operatorname{im} d_n = H_{n-1}(F_\bullet)$.

The maps f and g send cycles to cycles and boundaries to boundaries. Hence, they induce a diagram

$$\begin{array}{ccccccccc} & & A_n/\operatorname{im} d^A_{n+1} & \xrightarrow{f} & B_n/\operatorname{im} d^B_{n+1} & \xrightarrow{g} & C_n/\operatorname{im} d^C_{n+1} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \overline{d^A_n}} & & \downarrow{\scriptstyle \overline{d^B_n}} & & \downarrow{\scriptstyle \overline{d^C_n}} & & \\ 0 & \longrightarrow & \ker d^A_{n-1} & \xrightarrow{f} & \ker d^B_{n-1} & \xrightarrow{g} & \ker d^C_{n-1} & & \end{array}.$$

(*Exercise:* Check that this diagram is commutative and that the rows are exact.) Applying now the Snake lemma to this diagram gives an exact sequence

$$H_n(A_\bullet) \xrightarrow{f_*} H_n(B_\bullet) \xrightarrow{g_*} H_n(C_\bullet) \xrightarrow{\partial} H_{n-1}(A_\bullet) \xrightarrow{f_*} H_{n-1}(B_\bullet) \xrightarrow{g_*} H_{n-1}(C_\bullet) \ .$$

□

Remark 5.1.6. From the Snake lemma, here is how one defines the connecting homomorphism $\partial : H_n(C_\bullet) \longrightarrow H_{n-1}(A_\bullet)$ in Theorem 5.1.5: Given an element $z \in H_n(C_\bullet)$, take a representative $c \in C_n$ (actually, $c \in \ker d_n^C$). As g is surjective, we can pick $b \in B_n$ such that $g(b) = c$. Then we see that $g(d_n^B(b)) = d_n^C(g(b)) = d_n^C(c) = 0$, so that $d_n^B(b) \in \ker g = \operatorname{im} f$. Therefore there exists a unique $a \in \ker d_{n-1}^A$ such that $f(a) = d_n^B(b)$. Then ∂ is defined by

$$\partial(z) = a + \operatorname{im} d_n^A \in H_{n-1}(A_\bullet).$$

5.2 Projective and injective resolutions

Recall that in Section 1.6 we have seen that Hom and tensor are not exact functors. We saw that $\operatorname{Hom}_R(-, N)$ is a contravariant left-exact functor, while $\operatorname{Hom}_R(M, -)$ is a covariant left-exact functor. Plus, we saw that $(-) \otimes_R M$ is only right-exact. We will now see that for special choices of M and N, these functors will actually be exact.

Projective modules:

Definition 5.2.1. Let R be a ring. An R-module P is said to be *projective* if given any surjective homomorphism $\pi : A \longrightarrow B$ and any homomorphism $f : P \longrightarrow B$, then there exists an homomorphism $g : P \longrightarrow A$ such that $f = \pi \circ g$.

$$\begin{array}{ccccc} & & P & & \\ & \swarrow^{g} & \downarrow{\scriptstyle f} & & \\ A & \xrightarrow{\pi} & B & \longrightarrow & 0 \end{array}$$

Exercise 5.2.2. Show that free modules are projective. *(And to be honest, for the purposes of this course, these are the projective modules that we actually care about)*

Proposition 5.2.3. *Let P be an R-module. Then P is projective if and only if $\operatorname{Hom}_R(P, -)$ is an exact functor.*

Proof. We have seen in Section 1.6 that $\operatorname{Hom}_R(P, -)$ is left-exact. Thus, $\operatorname{Hom}_R(P, -)$ is exact if and only if we have the following: given a short exact sequence

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 0$$

then the induced map $\operatorname{Hom}_R(P, B) \longrightarrow \operatorname{Hom}_R(P, C)$ given by $g \longmapsto p \circ g$ is surjective. On the other hand, by definition, P is projective if and only if, given any surjective map $p : B \longrightarrow C$, any $f : P \longrightarrow C$ can be written as $f = p \circ g$ for some $g \in \operatorname{Hom}_R(P, B)$, i.e., if $\operatorname{Hom}_R(P, B) \longrightarrow \operatorname{Hom}_R(P, C)$ given by $g \longmapsto p \circ g$ is surjective. Thus exactness of $\operatorname{Hom}_R(P, -)$ coincides with P being projective. □

The following is a characterization of projective modules. We will skip the proof, however.

Proposition 5.2.4. *An R-module P is projective if and only if it is a direct summand of a free module, i.e., if there is a module N and a free module F such that $F \cong P \oplus N$. A finitely generated R-module P is projective if and only if it is a direct summand of R^n for some n.*

With this, you can show the following:

1. Direct summands of projective modules are projective.
2. The direct sum of projective modules is projective.
3. If P is a projective module, then $(-) \otimes_R P$ is an exact functor.

Example 5.2.5. Here is an example of a projective module which is not free. Let $R = \mathbb{Z}/6\mathbb{Z}$. Consider $I = (2)$ and $J = (3)$, ideals (hence submodules) of R. Since $I + J = R$ and $I \cap J = 0$, by the chinese remainder theorem we have $R \cong (R/I) \oplus (R/J)$. Thus R/I and R/J are projective R-modules. However, they are not free (because, for instance, they have less than 6 elements).

The following result is something we have seen in the beginning of the course. Due to its importance in this sections, I restate it here.

Proposition 5.2.6. *For every R-module M there exists a free (hence projective) module F surjecting onto M. If M is finitely generated, F can be taken finitely generated as well.*

Injective modules:

Definition 5.2.7. Let R be a ring. An R-module E is said to be *injective* if given any injective homomorphism $\iota : N \longrightarrow M$ and any homomorphism $f : N \longrightarrow E$, then there exists an homomorphism $g : M \longrightarrow E$ such that $f = g \circ \iota$ (in other words, if f can be extended to the whole of M).

$$\begin{array}{ccccc} & & E & & \\ & & \uparrow{\scriptstyle f} & \nwarrow{\scriptstyle g} & \\ 0 & \longrightarrow & N & \xrightarrow{\iota} & M \end{array}$$

Proposition 5.2.8. *Let E be an R-module. Then E is injective if and only if $\mathrm{Hom}_R(-, E)$ is an exact functor.*

Proof. It is analogous to the proof of Proposition 5.2.3. □

To check that a module is injective, turns out that it is enough to check that a homomorphism from an ideal to it can be extended to the whole of R.

Theorem 5.2.9. (Baer's criterion) *An R-module E is injective if and only if every homomorphism $f : I \longrightarrow E$ from an ideal I of R to E can be extended to the whole ring. In other words, if there exists $g : R \longrightarrow E$ making the following diagram commute:*

$$\begin{array}{ccccc} & & E & & \\ & & \uparrow{\scriptstyle f} & \nwarrow{\scriptstyle g} & \\ 0 & \longrightarrow & I & \longrightarrow & R \end{array} .$$

With this we can now see an example of an injective module.

Proposition 5.2.10. *Let R be a domain. Then $R_{(0)}$, the field of fractions of R, is an injective R-module.*

Proof. We use Baer's criterion. Let I be an ideal of R. We need to show that every R-homomorphism $f : I \longrightarrow R_{(0)}$ can be extended to R. If $I = 0$ that is obvious, so suppose $I \neq 0$. For each nonzero $a, b \in I$ notice that $af(b) = f(ab) = bf(a)$. Thus $f(a)/a = f(b)/b$ for all nonzero $a, b \in I$. Let $c = f(a)/a \in R_{(0)}$ for all nonzero $a \in I$. Define the R-homomorphism $g : R \longrightarrow R_{(0)}$ by $r \longmapsto rc$. Then g is an extension of f. Indeed, for every $a \in I$ (nonzero) we have $g(a) = ac = a(f(a)/a) = f(a)$. □

Injective modules are indeed much harder to picture than projective modules. In fact, in general they are not even finitely generated.

I leave the following properties of injective modules as an exercise:

1. Prove Baer's criterion.
2. If $\{M_\lambda\}_{\lambda \in \Lambda}$ is a family of injective R-modules, then $\prod_{\lambda \in \Lambda} M_\lambda$ is also injective. Furtherore, if R is Noetherian, then $\bigoplus_{\lambda \in \Lambda} M_\lambda$ is also injective.
3. If $M \oplus N = E$ is an injective R-module, then so are M and N.

The following property of injective modules is crucial for the construction of injective resolutions ahead.

Theorem 5.2.11. *Every R-module M is a submodule of some injective R-module.*

Proof. For this proof I refer to [BH98, Theorem 3.1.8]. □

Projective resolutions:

Given an R-module M, we can find a free module P_0 and a surjection $f_0 : P_0 \longrightarrow M$. Let $K_0 = \ker f_0$. We can now find a free module P_1 and a surjection $f_1' : P_1 \longrightarrow K_0$. Composing f_1' with the identity $K_0 \hookrightarrow P_0$ we get a homomorphism $f_1 : P_1 \longrightarrow P_0$ such that $\operatorname{im} f_1 = K_0 = \ker f_0$, i.e.,

$$P_1 \xrightarrow{f_1} P_0 \xrightarrow{f_0} M \longrightarrow 0$$

is exact. Now let $K_1 = \ker f_1$, find a free module P_2 and a surjection $f_2' : P_2 \longrightarrow K_1$, and so on. Continuing in this manner, we obtain an exact complex

$$\cdots \xrightarrow{f_3} P_2 \xrightarrow{f_2} P_1 \xrightarrow{f_1} P_0 \xrightarrow{f_0} M \longrightarrow 0$$

where all the P_i are free R-modules.

Definition 5.2.12. Let M be an R-module. A *projective resolution* of M is a complex

$$P_\bullet : \cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow 0$$

where all the P_i are projective and such that $H_0(P_\bullet) = M$ and $H_n(P_\bullet) = 0$ for all $n \geq 1$. We can also write a projective resolution of M in its *augmented form*, i.e., as an exact complex

$$P_\bullet : \cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0 \ .$$

The resolution is said to be *free* if all the P_i are free.

By the construction above, every R-module M has a free (hence projective) resolution.

Example 5.2.13.

1. $0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$ is free a resolution of $\mathbb{Z}/2\mathbb{Z}$ over $\mathbb{Z}$ (in its augmented form).
2. Let $R = k[X]/(X^3)$, where k is a field, and let M be the R-module $k[X]/(X^2)$. Then

$$\cdots \xrightarrow{\cdot X} R \xrightarrow{\cdot X^2} R \xrightarrow{\cdot X} R \xrightarrow{\cdot X^2} R \longrightarrow M \longrightarrow 0$$

is a free resolution of M, also in its augmented form.

The following is a useful property of complexes of projective modules.

Proposition 5.2.14. *Let M and N be R-modules. Let*

$$P_\bullet : \cdots \xrightarrow{f_3} P_2 \xrightarrow{f_2} P_1 \xrightarrow{f_1} P_0 \xrightarrow{f_0} M \longrightarrow 0$$

be a complex, where all the P_i are projective (not necessarily exact). Let also

$$A_\bullet : \cdots \xrightarrow{g_3} A_2 \xrightarrow{g_2} A_1 \xrightarrow{g_1} A_0 \xrightarrow{g_0} N \longrightarrow 0$$

be any exact complex. Then every R-module homomorphism $f : M \longrightarrow N$ lifts to a map of complexes $\varphi : P_\bullet \longrightarrow A_\bullet$:

$$\begin{array}{ccccccccccc}
\cdots & \xrightarrow{f_3} & P_2 & \xrightarrow{f_2} & P_1 & \xrightarrow{f_1} & P_0 & \xrightarrow{f_0} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_0} & & \downarrow{\scriptstyle f} & & \\
\cdots & \xrightarrow[g_3]{} & A_2 & \xrightarrow[g_2]{} & A_1 & \xrightarrow[g_1]{} & A_0 & \xrightarrow[g_0]{} & N & \longrightarrow & 0
\end{array} .$$

Furthermore, any two such liftings are homotopic.

Proof. I show how to construct φ_0 and φ_1. The construction of the rest of the φ_i is similar. I will leave the last statement of the proposition as an exercise.

As g_0 is surjective, the projectivity of P_0 guarantees that there exists $\varphi_0 : P_0 \longrightarrow A_0$ such that $ff_0 = g_0\varphi_0$. Now observe that $g_0\varphi_0 f_1(P_1) = ff_0 f_1(P_1) = 0$, meaning $\varphi_0 f_1(P_1) \subseteq \ker g_0$. As the bottom complex is exact, we have that $\ker g_0 = g_1(A_1)$. We conclude that $\varphi_0 f_1$ has image in $g_1(A_1)$. Now, the projectivity of P_1 guarantees that there exists $\varphi_1 : P_1 \longrightarrow A_1$ such that $\varphi_0 f_1 = g_1\varphi_1$. $\square$

Injective resolutions:

These are defined in an analogous way to projective resolutions.

Definition 5.2.15. Let M be an R-module. An *injective resolution* of M is a complex

$$E^\bullet : 0 \longrightarrow E_0 \longrightarrow E_1 \longrightarrow E_2 \longrightarrow E_3 \longrightarrow \cdots$$

where all the E_i are injective and such that $H^0(E^\bullet) = M$ and $H^n(E^\bullet) = 0$ for all $n \geq 1$. We can also write an injective resolution of M in its *augmented form*, i.e., as an exact complex

$$E^\bullet : 0 \longrightarrow M \longrightarrow E_0 \longrightarrow E_1 \longrightarrow E_2 \longrightarrow E_3 \longrightarrow \cdots .$$

Thanks to Theorem 5.2.11, one can show that an injective resolution of M always exists, in a similar way to how we saw that projective resolutions always exist.

There is also an analogous of Proposition 5.2.14 for complexes of injective modules (can you state it?).

5.3 Tor and Ext

The constructions we will present in this section are a particular case of right and left derived functors. In general, given a covariant right exact functor F in the category of R-modules, one can associate to it its *left derived functors* $\mathcal{L}^iF$. For a given R-module M these are defined as $\mathcal{L}^iF(M) = H_i(F(P_\bullet))$ where $P_\bullet$ is a projective resolution of M. Similarly, if F is covariant left exact functor, we can associate to it its *right derived functors* $\mathcal{R}^iF$ defined as $\mathcal{R}^iF(M) = H^i(F(E^\bullet))$ where $E^\bullet$ is an injective resolution of M.

We will do this here for the case of the right exact functors $(-) \otimes N$ and the left exact functors $\mathrm{Hom}_R(N, -)$.

The Tor functor:

Definition 5.3.1. Let M and N be R-modules and let

$$P_\bullet : \cdots \xrightarrow{f_3} P_2 \xrightarrow{f_2} P_1 \xrightarrow{f_1} P_0 \longrightarrow 0$$

be a projective resolution of M. Define $P_\bullet \otimes N$ as the complex

$$P_\bullet \otimes N : \cdots \xrightarrow{f_3 \otimes \mathrm{id}} P_2 \otimes_R N \xrightarrow{f_2 \otimes \mathrm{id}} P_1 \otimes_R N \xrightarrow{f_1 \otimes \mathrm{id}} P_0 \otimes_R N \longrightarrow 0 \ .$$

For each $i \geq 0$ we define

$$\mathrm{Tor}_i^R(M, N) = H_i(P_\bullet \otimes N).$$

Remark 5.3.2. We show that the definition of Tor does not depend on the projective resolution chosen for M, up to isomorphism. Suppose $Q_\bullet$ is another projective resolution of M. By Proposition 5.2.14 there are maps of complexes $f : P_\bullet \longrightarrow Q_\bullet$ and $g : Q_\bullet \longrightarrow P_\bullet$, both being liftings of the identity map 1_M of M. Consequently, $f' = f \otimes \mathrm{id} : P_\bullet \otimes N \longrightarrow Q_\bullet \otimes N$ and $g' = g \otimes \mathrm{id} : Q_\bullet \otimes N \longrightarrow P_\bullet \otimes N$, are both liftings of the identity map $1_{M \otimes_R N}$ of $M \otimes_R N$.

In particular, $g'f' : P_\bullet \otimes N \longrightarrow P_\bullet \otimes N$ is also a lifting $1_{M \otimes_R N}$. Since $1_{P_\bullet \otimes N}$ is obviously a lifting of $1_{M \otimes_R N}$, by Proposition 5.2.14 we conclude that $f'g' \sim 1_{P_\bullet \otimes N}$. Similarly, $g'f' \sim 1_{Q_\bullet \otimes N}$. We conclude that f' and g' are homotopy equivalences. Consequently, they are quasi-isomorphisms, from which it follows that

$$H_i(P_\bullet \otimes N) \cong H_i(Q_\bullet \otimes N).$$

The following properties of Tor follow from the definition and are left as an exercise:

1. $\mathrm{Tor}_0^R(M, N) = M \otimes_R N$ (follows from the right exactness of $(-) \otimes_R N$).
2. If N is a flat R-module (i.e., $(-) \otimes_R N$ is exact), then $\mathrm{Tor}_i^R(M, N) = 0$ for all R-modules M and all $i > 0$.
3. $\mathrm{Tor}_i^R(M_1 \oplus M_2, N) \cong \mathrm{Tor}_i^R(M_1, N) \oplus \mathrm{Tor}_i^R(M_2, N)$ for all i.
4. $\mathrm{Ann}(N) \subseteq \mathrm{Ann}(\mathrm{Tor}_i^R(M, N))$ for all i.

The following result is the most useful property of Tor. Further ahead we will see that it has some really crucial consequences.

Theorem 5.3.3. (Balancing Tor) *Let M and N be R-modules, $P_\bullet$ a projective resolution of M and $Q_\bullet$ a projective resolution of N. Then for all $i \geq 0$ we have*

$$H_i(P_\bullet \otimes N) \cong H_i(M \otimes Q_\bullet).$$

Proof. (Sketch) The proof goes by building the total complex $\mathrm{Tot}(P_\bullet \otimes Q_\bullet)$ given by $(P_\bullet \otimes Q_\bullet)_n = \sum_{i+j=n} P_i \otimes_R Q_j$ and differential d given by $d(x,y) = d_i^P(x) \otimes y + (-1)^i x \otimes d_i^Q(y)$ for each $x \in P_i$ and $y \in Q_j$ *(Exercise, check that this is indeed a differential).* Then one shows that the homology of this complex coincides with both the homology of $P_\bullet \otimes N$ and the homology of $M \otimes Q_\bullet$. For the proof of this I refer to [Wei94, Section 2.7]. □

In other words, Tor is commutative: $\mathrm{Tor}_i^R(M,N) = \mathrm{Tor}_i^R(N,M)$. It can be computed either from a projective resolution of M (then applying $(-) \otimes_R N$ and taking homology) or from a projective resolution of N (then applying $M \otimes_R (-)$ and taking homology).

Remark 5.3.4. *(Functoriality of Tor)* Let $f : M_1 \longrightarrow M_2$ be a homomorphism of R-modules. If N is an R-module and $Q_\bullet$ is a projective resolution of N, then f induces a map of complexes $f \otimes \mathrm{id} : M_1 \otimes Q_\bullet \longrightarrow M_2 \otimes Q_\bullet$. Hence, $f \otimes \mathrm{id}$ (and thus f) induces a map in homology

$$f_* : \mathrm{Tor}_i^R(M_1, N) = H_i(M_1 \otimes Q_\bullet) \longrightarrow H_i(M_2 \otimes Q_\bullet) = \mathrm{Tor}_i^R(M_2, N).$$

Plus, notice that if $g : M_2 \longrightarrow M_3$ is another homomorphism of R-modules, then $(gf)_* = g_* f_*$ (it follows from $(gf) \otimes \mathrm{id} = (g \otimes \mathrm{id})(f \otimes \mathrm{id})$). Thus $\mathrm{Tor}_i^R(-, N)$ is a functor in the category of R-modules.

Exercise: Convince yourself of the following: if $x \in R$ and $f : M \longrightarrow M$ is "multiplication by x" $(m \longmapsto xm)$, then the map $f_* : \mathrm{Tor}_i^R(M,N) \longrightarrow \mathrm{Tor}_i^R(M,N)$ that f induces at the level of Tor is also the "multiplication by x" map.

Remark 5.3.5. *(Finite generation)* Suppose R is Noetherian and M is a finitely generated R-module. Then one can pick a free resolution $F_\bullet$ of M where each F_i is a free R-module of finite rank.

Indeed, as M is finitely generated, we can pick a finitely generated free R-module F_0 and a surjective map $f_0 : F_0 \longrightarrow M$. As F_0 is a Noetherian R-module, $K_0 = \ker f_0$ is also a finitely generated R-module. Hence we can pick a finitely generated free R-module F_1 and a surjective map $f_1' : F_1 \longrightarrow K_0$. The composition of f_1 with the inclusion of K_0 in F_0 gives a map $f_1 : F_1 \longrightarrow F_0$ whose image is K_0. Now, as F_1 is a Noetherian R-module, $K_1 = \ker f_1$ is also a finitely generated R-module, and we can continue on with this process, choosing successively finitely generated free R-modules $F_2, F_3, \ldots$ such that

$$F_\bullet : \cdots \xrightarrow{f_3} F_2 \xrightarrow{f_2} F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} M \longrightarrow 0$$

is a free resolution of M. Suppose now N is another finitely generated R-module. $\mathrm{Tor}_i^R(M,N)$ can be computed as the i-th homology module of the complex

$$F_\bullet \otimes N : \cdots \xrightarrow{f_3 \otimes \mathrm{id}} F_2 \otimes_R N \xrightarrow{f_2 \otimes \mathrm{id}} F_1 \otimes_R N \xrightarrow{f_1 \otimes \mathrm{id}} F_0 \otimes_R N \longrightarrow 0 \ .$$

We see that each $F_i \otimes_R N \cong N^{\mathrm{rank} F_i}$ is a finitely generated R-module. Thus, $\mathrm{Tor}_i^R(M,N)$, being isomorphic to a quotient of a submodule of $F_i \otimes_R N$, is also finitely generated.

We conclude: R Noetherian and M, N finitely generated $\Longrightarrow \mathrm{Tor}_i^R(M,N)$ finitely generated for all $i \geq 0$.

Example 5.3.6. Given $n > 1$, let's compute $\mathrm{Tor}_i^{\mathbb{Z}}(\mathbb{Z}/(n), M)$ for a $\mathbb{Z}$-module M. We begin by observing that $F_\bullet : 0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \longrightarrow 0$ is a free resolution of $\mathbb{Z}/n\mathbb{Z}$. Hence we can compute $\mathrm{Tor}_i^{\mathbb{Z}}(\mathbb{Z}/(n), M)$ from the homology of $F_\bullet \otimes M : 0 \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}} M \xrightarrow{(\cdot n) \otimes \mathrm{id}} \mathbb{Z} \otimes_{\mathbb{Z}} M \longrightarrow 0$. But under the isomorphism $\mathbb{Z} \otimes_{\mathbb{Z}} M \cong M$ this complex becomes $0 \longrightarrow M \xrightarrow{\cdot n} M \longrightarrow 0$. Thus $\mathrm{Tor}_0^{\mathbb{Z}}(\mathbb{Z}/(n), M) = M/nM$, $\mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/(n), M) = (0 :_M n)$ and $\mathrm{Tor}_i^{\mathbb{Z}}(\mathbb{Z}/(n), M) = 0$ for all $i \geq 2$.

A powerful tool that can be used to compute Tor indirectly is the long exact sequence in Tor associated to a short exact sequence of R-modules.

Theorem 5.3.7. (Long exact sequence in Tor) *Suppose*

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 0$$

is a short exact sequence of R-modules. Then for every R-module N we have a long exact sequence

$$\cdots \longrightarrow \mathrm{Tor}_i^R(A,N) \longrightarrow \mathrm{Tor}_i^R(B,N) \longrightarrow \mathrm{Tor}_i^R(C,N) \longrightarrow \mathrm{Tor}_{i-1}^R(A,N) \longrightarrow \cdots$$

$$\cdots \longrightarrow \mathrm{Tor}_1^R(B,N) \longrightarrow \mathrm{Tor}_1^R(C,N) \longrightarrow A \otimes_R N \longrightarrow B \otimes_R N \longrightarrow C \otimes_R N \longrightarrow 0$$

Proof. We of course want to resort to Theorem 5.1.5. To set it up, we need to use the following:

Lemma 5.3.8. (Horseshoe lemma) *Let $P_\bullet$ be a projective resolution of A and $Q_\bullet$ a projective resolution of C. Then there exists a projective resolution $F_\bullet$ of B, together with maps of complexes f and g, liftings of i and p respectively, such that*

$$0 \longrightarrow P_\bullet \xrightarrow{f} F_\bullet \xrightarrow{g} Q_\bullet \longrightarrow 0$$

is a short exact sequence of complexes.

Proof. (Small sketch) $F_\bullet$ will be constructed so that $F_n = P_n \oplus Q_n$; f will be defined by the embeddings of P_n in F_n and g will be defined by the projections of F_n onto Q_n. From this it is already clear that the desired sequence of complexes is exact. It remains to build a differential on $F_\bullet$ that makes $F_\bullet$ a projective resolution of B and that makes f and g liftings of i and p (which still requires some work). □

We now claim that

$$0 \longrightarrow P_\bullet \otimes N \xrightarrow{f\otimes \mathrm{id}} F_\bullet \otimes N \xrightarrow{g\otimes \mathrm{id}} Q_\bullet \otimes N \longrightarrow 0$$

is a short exact sequence of complexes. Indeed, this easy to observe from the fact that, as we have seen, $F_\bullet$ can be constructed so that $F_n = P_n \oplus Q_n$. Now we can use Theorem 5.1.5 on this short exact sequence of complexes, giving us the desired long exact sequence in Tor. □

The Ext functor:

To construct the Ext functors, we will do something similar to the construction of the Tor functors. We will just use Hom instead of tensor product.

Let M and N be R-modules. Let

$$P_\bullet : \cdots \xrightarrow{f_3} P_2 \xrightarrow{f_2} P_1 \xrightarrow{f_1} P_0 \longrightarrow 0$$

be a projective resolution of M and

$$E^\bullet : 0 \longrightarrow E_0 \xrightarrow{g_1} E_1 \xrightarrow{g_2} E_2 \xrightarrow{g_3} \cdots$$

be an injective resolution of N. Define $\mathrm{Hom}(P_\bullet, N)$ and $\mathrm{Hom}(M, E^\bullet)$ as the complexes

$$\mathrm{Hom}(P_\bullet, N) : 0 \longrightarrow \mathrm{Hom}_R(P_0,N) \xrightarrow{f_1'} \mathrm{Hom}_R(P_1,N) \xrightarrow{f_2'} \mathrm{Hom}_R(P_2,N) \xrightarrow{f_3'} \cdots$$

and

$$\mathrm{Hom}(M, E^\bullet) : 0 \longrightarrow \mathrm{Hom}_R(M,E_0) \xrightarrow{g_1'} \mathrm{Hom}_R(M,E_1) \xrightarrow{g_2'} \mathrm{Hom}_R(M,E_2) \xrightarrow{g_3'} \cdots,$$

where f_i' and g_i' denote the maps induced by f_i and g_i.

We are interested in the cohomology of these complexes. First of all, by arguments analogous to the ones we used in Remark 5.3.2, we see that $H^i(\mathrm{Hom}(P_\bullet, N))$ does not depend on the choice of projective resolution $P_\bullet$ of M. Also, $H^i(\mathrm{Hom}(M, E^\bullet))$ does not depend on the choice of injective resolution $E^\bullet$ of N. It also turns out that these cohomology modules can be computed from either complex.

Theorem 5.3.9. (and definition) (Balancing Ext) *Let M and N be R-modules, $P_\bullet$ a projective resolution of M and $E^\bullet$ an injective resolution of N. Then for all $i \geq 0$ we have*

$$H^i(\mathrm{Hom}(P_\bullet, N)) \cong H^i(\mathrm{Hom}(M, E^\bullet)).$$

These modules are denoted

$$\mathrm{Ext}^i_R(M, N).$$

The following properties of Ext are left as an exercise. They essentially follow by arguments similar to the ones used in the treatment of Tor.

1. $\mathrm{Ext}^0_R(M, N) = \mathrm{Hom}_R(M, N)$ (follows from the left exactness of Hom).
2. If P is projective then $\mathrm{Ext}^i_R(P, N) = 0$ for all $i > 0$ and all N.
3. If E is injective then $\mathrm{Ext}^i_R(M, E) = 0$ for all $i > 0$ and all M.
4. $\mathrm{Ext}^i_R(M_1 \oplus M_2, N) \cong \mathrm{Ext}^i_R(M_1, N) \oplus \mathrm{Ext}^i_R(M_2, N)$.
5. $\mathrm{Ext}^i_R(M, N_1 \oplus N_2) \cong \mathrm{Ext}^i_R(M, N_1) \oplus \mathrm{Ext}^i_R(M, N_2)$.
6. $\mathrm{Ann}(M) + \mathrm{Ann}(N) \subseteq \mathrm{Ann}\,\mathrm{Ext}^i_R(M, N)$ for all $i \geq 0$.
7. For each $i \geq 0$, $\mathrm{Ext}^i_R(-, N)$ is a contravariant functor and $\mathrm{Ext}^i_R(M, -)$ is a covariant functor.
8. If R is Noetherian and M and N are finitely generated, then $\mathrm{Ext}^i_R(M, N)$ is finitely generated for all $i \geq 0$.

For the case of Ext, a short exact sequence induces two long exact sequences. The proof of the following result is similar to that of Theorem 5.3.7.

Theorem 5.3.10. (Long exact sequences in Ext) *Suppose*

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 0$$

is a short exact sequence of R-modules. Then for every R-module N we have a long exact sequence

$$0 \longrightarrow \mathrm{Hom}_R(C, N) \longrightarrow \mathrm{Hom}_R(B, N) \longrightarrow \mathrm{Hom}_R(A, N) \longrightarrow \mathrm{Ext}^1_R(C, N) \longrightarrow \mathrm{Ext}^1_R(B, N) \longrightarrow \cdots$$

$$\cdots \longrightarrow \mathrm{Ext}^i_R(C, N) \longrightarrow \mathrm{Ext}^i_R(B, N) \longrightarrow \mathrm{Ext}^i_R(A, N) \longrightarrow \mathrm{Ext}^{i+1}_R(C, N) \longrightarrow \cdots .$$

Also, for every R-module M we have a long exact sequence

$$0 \longrightarrow \mathrm{Hom}_R(M, A) \longrightarrow \mathrm{Hom}_R(M, B) \longrightarrow \mathrm{Hom}_R(M, C) \longrightarrow \mathrm{Ext}^1_R(M, A) \longrightarrow \mathrm{Ext}^1_R(M, B) \longrightarrow \cdots$$

$$\cdots \longrightarrow \mathrm{Ext}^i_R(M, A) \longrightarrow \mathrm{Ext}^i_R(M, B) \longrightarrow \mathrm{Ext}^i_R(M, C) \longrightarrow \mathrm{Ext}^{i+1}_R(M, A) \longrightarrow \cdots .$$

Exercise 5.3.11. Show the following:

1. P is projective $\iff$ $\mathrm{Ext}^i_R(P, N) = 0$ for all $i > 0$ and all N $\iff$ $\mathrm{Ext}^1_R(P, N) = 0$ for all N.
2. E is injective $\iff$ $\mathrm{Ext}^i_R(M, E) = 0$ for all $i > 0$ and all M $\iff$ $\mathrm{Ext}^1_R(M, E) = 0$ for all M.

Example 5.3.12. Let $R = k[x]$, where k is a field. Let's compute $\mathrm{Ext}^i_R(k, R)$. We start by observing that a free resolution of k is $F_\bullet : 0 \longrightarrow R \xrightarrow{\cdot x} R \longrightarrow 0$. Thus $\mathrm{Ext}^i_R(k, R)$ can be computed as the cohomology of $\mathrm{Hom}_R(F_\bullet, R) : 0 \longrightarrow \mathrm{Hom}_R(R, R) \xrightarrow{(\cdot x)'} \mathrm{Hom}_R(R, R) \longrightarrow 0$. Under the homomorphism $\mathrm{Hom}_R(R, R) \cong R$, this complex becomes $0 \longrightarrow R \xrightarrow{\cdot x} R \longrightarrow 0$. Thus $\mathrm{Ext}^0_R(k, R) = (0 : x)$ (which equals $\mathrm{Hom}_R(k, R)$, as we expected), $\mathrm{Ext}^1_R(k, R) = R/(x) \cong k$ and $\mathrm{Ext}^i_R(k, R) = 0$ for all $i > 1$.

Notice that $\mathrm{Ext}^1_R(R, k) = 0$ because R is a free (hence projective) R-module. Thus in this example we have $\mathrm{Ext}^1_R(k, R) \neq \mathrm{Ext}^1_R(R, k)$, showing that Ext is not commutative, unlike Tor.

5.4 Minimal free resolutions

Let R be a Noetherian ring and M a finitely generated R-module. We saw in Remark 5.3.5 how one can always build a free resolution of an R-module M. Pick generators $m_1, \dots, m_{r_0}$ of M, let $F_0 = R^{r_0}$ and define $f_0 : F_0 \longrightarrow M$ by $f_0(a_1, \dots, a_{r_0}) = a_1 m_1 + \cdots + a_{r_0} m_{r_0}$. Then pick generators $x_1, \dots, x_{r_1}$ of $\ker f_0$, let $F_1 = R^{r_1}$ and define $f_1 : F_1 \longrightarrow F_0$ by $f_0(b_1, \dots, b_{r_1}) = b_1 x_1 + \cdots + b_{r_1} x_{r_1}$. Keep this process going and you obtain a free resolution

$$F_\bullet : \cdots \xrightarrow{f_3} F_2 \xrightarrow{f_2} F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} M \longrightarrow 0$$

of M (denoted here in its augmented form).

The local case:

If $(R, \mathfrak{m})$ is also local, then we can be more precise in this process of building a free resolution: instead of just picking random generators, we can at each step pick *minimal* generators of $\ker f_i$. A resolution built in this way will be called a minimal free resolution of M.

Example 5.4.1. Let $R = k[\![x, y, z]\!]$ and $M = R/(xy, xz, yz)$. Let's build a minimal free resolution $F_\bullet$ of M.

M is cyclic (generated by $1 + (xy, xz, yz)$), So

$$R \xrightarrow{f_0} M \longrightarrow 0$$

is the first step in a minimal free resolution of M, with f_0 sending the generator of R to $1 + (xy, xz, yz)$. We have $\ker f_0 = (xy, xz, yz)$, which is minimally generated by $\{xy, xz, yz\}$, hence the next step in the minimal free resolution is a map $f_1 : R^3 \longrightarrow R$ sending a basis $\{e_1, e_2, e_3\}$ of R^3 to $\{xy, xz, yz\}$.

$$R^3 \xrightarrow{[xy\ xz\ yz]} R \longrightarrow M \longrightarrow 0$$

Next we determine $\ker f_1$ and a minimal set of generators for it. $\ker f_1$ consists of the elements $(u, v, w) \in R^3$ such that $uxy + vxz + wyz = 0$. We see that u, v and w must be multiples of z, y and x, respectively. Write $u = u'z$, $v = v'y$ and $w = w'x$. Then $(u, v, w) \in \ker f_1$ if and only if $u' + v' + w' = 0$. From this we see that a minimal set of generators of $\ker f_1$ is $\{(z, -y, 0), (0, y, -x)\}$. Thus, the next step in the minimal free resolution of M is a map $f_2 : R^2 \longrightarrow R^3$ sending a basis $\{e_1', e_2'\}$ of R^2 to $\{(z, -y, 0), (0, y, -x)\}$.

$$R^2 \xrightarrow{\begin{bmatrix} z & 0 \\ -y & y \\ 0 & -x \end{bmatrix}} R^3 \xrightarrow{[xy\ xz\ yz]} R \longrightarrow M \longrightarrow 0$$

We now observe that $\ker f_2 = 0$, so that this process stops here. A minimal free resolution of $M = R/(xy, xz, yz)$, as an R-module, is thus

$$0 \longrightarrow R^2 \xrightarrow{\begin{bmatrix} z & 0 \\ -y & y \\ 0 & -x \end{bmatrix}} R^3 \xrightarrow{[xy\ xz\ yz]} R \longrightarrow M \longrightarrow 0\ .$$

Remark 5.4.2. Suppose

$$F_\bullet : \cdots \xrightarrow{f_3} F_2 \xrightarrow{f_2} F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} M \longrightarrow 0$$

is a free resolution of M built by choosing at each step minimal generators of $\ker f_i$. Let's look at the piece

$$F_{i+1} \xrightarrow{f_{i+1}} F_i \xrightarrow{f_i} F_{i-1}$$

with $i \geq 0$ (set $F_{-1} = M$). We claim that $\operatorname{im} f_{i+1} \subseteq \mathfrak{m} F_i$. Indeed, fix a basis $\{e_1, \dots, e_r\}$ of F_i. Then, by minimality of the resolution, $\{f_i(e_1), \dots, f_i(e_r)\}$ is a minimal system of generators of $\ker f_{i-1} = \operatorname{im} f_i$. Given $b \in F_{i+1}$, write $f_{i+1}(b) = (a_1, \dots, a_r)$ (in the basis $\{e_1, \dots, e_r\}$). Since $f_i f_{i+1} = 0$, we have $a_1 f_i(e_1) + \cdots + a_r f_i(e_r) = 0$. Now, because $\{f_i(e_1), \dots, f_i(e_r)\}$ is a minimal system of generators of $\operatorname{im} f_i$, we must have $a_j \in \mathfrak{m}$ for all j (by Proposition 1.3.7). We conclude that $\operatorname{im} f_{i+1} \subseteq \mathfrak{m} F_i$.

This is actually the property that characterizes minimal free resolutions. We now define them formally.

Definition 5.4.3. Let $(R, \mathfrak{m})$ be a Noetherian local ring. A complex

$$\cdots \longrightarrow F_{i+1} \xrightarrow{f_{i+1}} F_i \xrightarrow{f_i} F_{i-1} \longrightarrow \cdots$$

is said to be *minimal* if $\operatorname{im} f_i \subseteq \mathfrak{m}F_{i-1}$ for all i. A free resolution

$$F_\bullet : \cdots \xrightarrow{f_3} F_2 \xrightarrow{f_2} F_1 \xrightarrow{f_1} F_0 \longrightarrow 0$$

of a finitely generated R-module M is said to be *a minimal free resolution of* M if it is minimal as a complex.

Proposition 5.4.4. *Let $(R, \mathfrak{m})$ be a Noetherian local ring and M a finitely generated R-module. A free resolution*

$$F_\bullet : \cdots \xrightarrow{f_3} F_2 \xrightarrow{f_2} F_1 \xrightarrow{f_1} F_0 \longrightarrow 0$$

of M is minimal (i.e., $\operatorname{im} f_i \subseteq \mathfrak{m}F_{i-1}$ for all i) if and only if for each i we have that f_i sends a basis of F_i onto a minimal set of generators of $\ker f_{i-1}$.

Proof. We have seen the "if" part in Remark 5.4.2. The proof of the "only if" part is very similar. □

Up to isomorphism, minimal free resolutions are unique (i.e., the choice of minimal generators at each step does not affect the resolution). This is the content of the following theorem. I refer to [Pee10, Theorem 7.5] for the proof. In [Pee10] the proof is done in the graded case, but it is totally similar in the local case. A complex is said to be *trivial* if it is a direct sum of complexes of the form $\cdots \longrightarrow 0 \longrightarrow R \xrightarrow{\text{id}} R \longrightarrow 0 \longrightarrow \cdots$.

Theorem 5.4.5. *Let $(R, \mathfrak{m})$ be a Noetherian local ring, M a finitely generated R-module and $F_\bullet$ a minimal free resolution of M. Then any free resolution of M is isomorphic to a direct sum of $F_\bullet$ with a trivial complex. In particular, the minimal free resolution $F_\bullet$ is unique up to isomorphism.*

Consequently, we can talk about *the* minimal free resolution of a finitely generated module M over a Noetherian local ring. To understand M, we can study its minimal free resolution, as it contains a large amount of information about the module. In particular, it allows us to associate several homological invariants to M, the following being the most important.

Definition 5.4.6. Let $(R, \mathfrak{m})$ be a Noetherian local ring, M a finitely generated R-module and

$$F_\bullet : \cdots \xrightarrow{f_3} F_2 \xrightarrow{f_2} F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} M \longrightarrow 0$$

a minimal free resolution of M.

For each $i \geq 1$, the module $\Omega_i(M) := \operatorname{im} f_i = \ker f_{i-1}$ is called the i-th *syzygy* module of M.

For each $i \geq 0$, the i-th *Betti number* of M is $\beta_i^R(M) = \operatorname{rank}(F_i)$.

The *projective dimension* of M is $\operatorname{pd}_R(M) = \sup\{i \geq 0 : F_i \neq 0\} = \sup\{i \geq 0 : \beta_i^R(M) \neq 0\}$.

Remark 5.4.7. The first syzygy of M should be interpreted as the "module of relations" between the generators of M. Indeed, let $\{e_1, ..., e_r\}$ be a basis of F_0 (here $r = \beta_0^R(M)$). $\{f_0(e_1), \ldots, f_0(e_r)\}$ is a minimal set of generators of M and any element in $\Omega_1(M) = \operatorname{im} f_1 = \ker f_0$ correspondes to a tuple $(a_1, \ldots, a_r) \in F_0$ such that $a_1 f_0(e_1) + \cdots + a_r f_0(e_r)$ i.e., corresponds to a *relation* among the generators of M. In sum, $\beta_0^R(M)$ measures the number of minimal generators of M (i.e., $\beta_0^R(M) = \mu(M)$), while $\Omega_1(M)$ tells us what are the relations among the generators. In turn, the map f_0 in the resolution tells exactly what are the minimal generators.

$\beta_1(M)$ equals the number of minimal generators of $\ker f_0 = \Omega_1(M)$. In other words, it measures the number of minimal relations among the generators of M. Picking a minimal set of generators of $\Omega_1(M)$ and looking at the relations among those generators gives us the module $\Omega_2(M)$. So we interpret $\Omega_2(M)$ as the "module of relations among the relations of the generators of M".

In sum, $\beta_0^R(M)$ = number of minimal generators, $\beta_1^R(M)$ = number of minimal relations, $\beta_2^R(M)$ = number of minimal relations among the relations, etc...

Example 5.4.8. 1. Let's revisit Example 5.4.1. We have computed the minimal free resolution of $M = R/(xy, xz, yz)$ over $R = k[\![x, y, z]\!]$. From it, we see that $\beta_0^R(M) = 1$, $\beta_1^R(M) = 3$, $\beta_2^R(M) = 2$ and $\beta_i^R(M) = 0$ for $i \geq 3$. Thus we conclude that M has projective dimension 2. Also, the first syzygy module of M is $\Omega_1(M) = (xy, xz, yz)$, while the second syzygy module is $\Omega_2(M) = R(z, -y, 0) + R(0, y, -x)$.

2. Let's now revisit Example 5.2.13. We have that a minimal free resolution of $M = k[X]/(X^2)$ over the local ring $R = k[X]/(X^3)$ is

$$\cdots \xrightarrow{\cdot X} R \xrightarrow{\cdot X^2} R \xrightarrow{\cdot X} R \xrightarrow{\cdot X^2} R \longrightarrow 0 \ .$$

Thus in this case M has infinite projective dimension over R. We have $\beta_i(M) = 1$ for all $i \geq 0$. The i-th syzygy module of M is (X^2) for i odd and (X) for i even.

The Betti numbers can actually be computed by looking at the right Tor or Ext modules.

Proposition 5.4.9. *Let $(R, \mathfrak{m})$ be a Noetherian local ring, $k = R/\mathfrak{m}$ and M a finitely generated R-module. Then for all $i \geq 0$ we have that*

$$\beta_i^R(M) = \dim_k \operatorname{Tor}_i^R(M, k) = \dim_k \operatorname{Ext}_R^i(M, k).$$

Proof. Let

$$F_\bullet : \cdots \xrightarrow{f_3} F_2 \xrightarrow{f_2} F_1 \xrightarrow{f_1} F_0 \longrightarrow 0$$

be a minimal free resolution of M. We need to show that $\operatorname{rank} F_i = \dim_k \operatorname{Tor}_i^R(M, k) = \dim_k \operatorname{Ext}_R^i(M, k)$. In the case of $\operatorname{Tor}_i^R(M, k)$, it is computed as the i-th homology module of $F_\bullet \otimes R/\mathfrak{m}$. Since $F_i \otimes_R (R/\mathfrak{m}) \cong F_i/\mathfrak{m}F_i$, the complex $F_\bullet \otimes R/\mathfrak{m}$ equals

$$F_\bullet \otimes R/\mathfrak{m} : \cdots \xrightarrow{\overline{f_3}} F_2/\mathfrak{m}F_2 \xrightarrow{\overline{f_2}} F_1/\mathfrak{m}F_1 \xrightarrow{\overline{f_1}} F_0/\mathfrak{m}F_0 \longrightarrow 0$$

where each $\overline{f_i}$ is given by $\overline{f_i}(x + \mathfrak{m}F_i) = f_i(x) + \mathfrak{m}F_{i-1}$. But since $F_\bullet$ is minimal (i.e, $\operatorname{im} f_i \subseteq \mathfrak{m}F_{i-1}$), we see that $\overline{f_i} = 0$ for all i. Thus $\operatorname{Tor}_i^R(M, k) = H_i(F_\bullet \otimes R) = F_i/\mathfrak{m}F_i$. Now, if $r_i = \operatorname{rank}(F_i)$, we have $F_i = R^{r_i}$, so that $F_i/\mathfrak{m}F_i \cong F_i \otimes_R R/\mathfrak{m} = R^{r_i} \otimes_R k \cong k^{r_i}$. We conclude that $\dim_k \operatorname{Tor}_i^R(M, k) = \dim_k k^{r_i} = r_i = \operatorname{rank}(F_i)$. The proof that $\operatorname{rank} F_i = \dim_k \operatorname{Ext}_R^i(M, k)$ is similar. □

The graded case:

Suppose now that R is a Noetherian $\mathbb{N}$-graded ring with $R_0 = k$ a field (so that R is isomorphic to a quotient of the polynomial ring $k[x_1, \ldots, x_n]$ for some n). R is $*$-local with unique maximal homogeneous ideal $\mathfrak{m} = R_+$. Notice that $\mathfrak{m}$ is not only maximal among the homogeneous ideals of R, but is in fact itself a maximal ideal of R. In this setting we are interested in complexes that are graded.

Definition 5.4.10. A complex of R-modules

$$C_\bullet : \cdots \longrightarrow C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \longrightarrow \cdots$$

is said to be *graded* if each C_n is a graded R-module and each map d_n is degree preserving (so that $d_n((C_n)_i) \subseteq (C_{n-1})_i)$ for all n and all i. Notice that the homology modules $H_n(C_\bullet)$ of such a complex will also be graded R-modules, with the grading induced by the grading on C_n.

We are interested in graded free resolutions of graded R-modules, i.e., free resolutions which are graded as complexes. Moreover, since we have a well defined concept of minimal homogeneous generating sets of finitely generated graded R-modules, we are actually able to build graded free resolutions in a minimal way. The following definition will be useful in their construction.

Definition 5.4.11. Let M be a graded R-module. Given $d \in \mathbb{Z}$ we define $M(d)$ to be the graded module obtained by shifting M to the right d steps, i.e., $M(d)$ is given by $M(d)_i = M_{i+d}$ for all $i \in \mathbb{Z}$

In particular, elements of degree 0 in $M(-d)$ correspond to elements of degree d in M. Thus $R(-d)$ stands for the free R-module generated by an element of degree d and $\bigoplus_{j=1}^r R(-d_j)$ stands for the free R-module with a basis $\{e_1, \ldots, e_r\}$ with $\deg(e_j) = d_j$.

Let M be a finitely generated $\mathbb{Z}$-graded R-module. We can build a graded minimal free resolution of M following the same process we used in the local case; here, in the graded case, we just need to pick minimal homogeneous sets of generators at each step.

Pick homogeneous generators $g_1, \dots, g_{\beta_0}$ of M, each g_j of degree $d_{0,j}$. If we simply define $f_0' : R^{\beta_0} \longrightarrow M$ by $f_0'(a_1, \dots, a_{\beta_0}) = a_1 g_1 + \cdots + a_{\beta_0} g_{\beta_0}$, then f_0' is not a degree-preserving map, as it sends the j-th element of the canonical basis of R^{β_0} (which has degree 1) to g_j, which has degree $d_{0,j}$. Instead, we should consider $F_0 = \bigoplus_{j=1}^{\beta_0} R(-d_{0,j})$. The j-th summand of F_0 is generated by a basis element e_j of degree $d_{0,j}$ and the assigment $e_j \mapsto g_j$ defines a surjective degree-preserving map $f_0 : F_0 \longrightarrow M$.

Now, $\ker f_0$ is also a finitely generated graded R-module. Pick homogeneous generators $h_1, \dots, h_{\beta_1}$ of $\ker f_0$, each h_j of degree $d_{1,j}$. Let $F_1 = \bigoplus_{j=1}^{\beta_1} R(-d_{1,j})$ and define $f_1 : F_1 \longrightarrow F_0$ by sending each generator of degree $d_{1,j}$ to h_j. Then $F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} M \longrightarrow 0$ is exact, with the maps being degree preserving. We can keep this going, producing a graded free resolution of M:

$$\cdots \longrightarrow \bigoplus_{j=1}^{\beta_2} R(-d_{2,j}) \xrightarrow{f_2} \bigoplus_{j=1}^{\beta_1} R(-d_{1,j}) \xrightarrow{f_1} \bigoplus_{j=1}^{\beta_0} R(-d_{0,j}) \xrightarrow{f_0} M \longrightarrow 0 \ .$$

A graded free resolution obtained in this way is called a *minimal graded free resolution* of M. Similar to what we saw in the local case, minimal graded free resolutions are unique up to isomorphism and are characterized by every entry in the matrix of each f_i belonging to $\mathfrak{m}$ (the maximal homogeneous ideal of R).

The numbers $\beta_i = \beta_i^R(M)$ are called the *total Betti numbers* of M. They are uniquely determined by M since $\beta_i^R(M) = \dim_k \operatorname{Tor}_i^R(M,k) = \dim_k \operatorname{Ext}_R^i(M,k)$ (the proof is the same as in the local case). The i-th *syzygy* module of M, with $i \geq 1$ is defined as the image of the map f_i in the minimal graded free resolution of M and the *projective dimension* of M is also defined identicaly as in Definition 5.4.6.

In the graded case there is more information contained in the minimal graded free resolution of M, as we can keep track of the degrees of the minimal homogeneous generators of the syzygies of M. In each module $\bigoplus_{t=1}^{\beta_i} R(-d_{i,t})$, we can group together the free summands which have generators in the same degree, rewriting it as $\bigoplus_{j \geq 0} R(-j)^{\beta_{i,j}}$, where $\beta_{i,j}$ is the number of times j appears as one of the $d_{i,t}$. Thus we can rewrite the minimal graded free resolution of M as

$$\cdots \longrightarrow \bigoplus_{j \geq 0} R(-j)^{\beta_{2,j}} \xrightarrow{f_2} \bigoplus_{j \geq 0} R(-j)^{\beta_{1,j}} \xrightarrow{f_1} \bigoplus_{j \geq 0} R(-j)^{\beta_{0,j}} \xrightarrow{f_0} M \longrightarrow 0 \ .$$

The numbers $\beta_{i,j} = \beta_{i,j}^R(M)$ are called the *graded Betti numbers of* M. It is easy to see, adapting the proof of Proposition 5.4.9, that

$$\beta_{i,j}^R(M) = \dim_k \operatorname{Tor}_i^R(M,k)_j = \dim_k \operatorname{Ext}_R^i(M,k)_{-j}.$$

Remark 5.4.12. If M and N are graded R-modules, then $\operatorname{Tor}_i^R(M,N)$ and $\operatorname{Ext}_R^i(M,N)$ are also graded R-modules. Indeed, letting $F_\bullet$ be a graded free resolution of M, we have that $\operatorname{Tor}_i^R(M,N) = H_i(F_\bullet \otimes N)$. But $F_\bullet \otimes N$ is also a graded complex as each $F_i \otimes_R N$ has a grading given by $(F_i \otimes_R N)_j = \sum_{a+b=j} (F_i)_a \otimes_k N_b$. Thus, $\operatorname{Tor}_i^R(M,N)$, being a graded quotient of a graded submodule of $F_i \otimes_R N$, is also graded.

We also have that $\operatorname{Hom}_R(M,N)$ is graded, its piece of degree j being given by $\operatorname{Hom}_R^j(M,N)$, the set of homogeneous R-homomorphisms from M to N of degree j. As $\operatorname{Ext}_R^i(M,N) = H^i(\operatorname{Hom}_R(F_\bullet, N))$, this is also a graded R-module.

Notice that $\beta_{0,j}^R(M)$ equals how many generators of degree j are in a minimal set of homogeneous generators of M. In turn, $\beta_{1,j}^R(M)$ equals how many minimal relations of degree j are among the minimal homogeneous generators of M.

Proposition 5.4.13. *Suppose M is generated in non-negative degrees. If $\beta_{i,j}^R(M) \neq 0$ then $i \leq j$.*

Proof. By induction on i. For $i = 0$ it holds true since M has no minimal homogeneous generator of negative degree, by assumption. Suppose now the result holds for i, so that $\beta_{i,j}^R(M) = 0$ for all $j < i$.

Suppose $\beta_{i+1,j}^R(M) \neq 0$. Then $F_{i+1} = \bigoplus_{j \geq 0} R(-j)^{\beta_{i+1,j}}$ has a canonical basis element e of degree j. As f_{i+1} is degree preserving, we have $j = \deg(e) = \deg(f_{i+1}(e))$. Let $\{g_1, \dots, g_{\beta_i}\}$ be the homogeneous canonical basis of F_i. As $\operatorname{im} f_{i+1} \subseteq \mathfrak{m} F_i$ we see that $f_{i+1}(e)$ can be written as $b_1 g_1 + \cdots + b_{\beta_i} g_{\beta_i}$ with all b_j in $\mathfrak{m}$, i.e., of positive degree. By the induction hypothesis, F_i has no minimal generators of degree $< i$, so that $\deg(g_j) \geq i$ for all j. We conclude that $f_{i+1}(e)$ has degree $\geq i+1$, as we wanted to show. $\square$

In the scenario of this proposition, the only graded Betti numbers which can be nonzero are the Betti numbers $\beta^R_{i,i}(M), \beta^R_{i,i+1}(M), \beta^R_{i,i+2}(M), \ldots$. It is then common to organize these in a table as follows:

$\beta(M)$	0	1	2	$\cdots$
0	$\beta_{00}(M)$	$\beta_{11}(M)$	$\beta_{22}(M)$	
1	$\beta_{01}(M)$	$\beta_{12}(M)$	$\beta_{23}(M)$	
2	$\beta_{02}(M)$	$\beta_{13}(M)$	$\beta_{24}(M)$	
$\vdots$				$\ddots$

The convention is that the entry in column i and row j is the graded Betti number $\beta^R_{i,i+j}(M)$ (not $\beta^R_{i,j}(M)$). The table built in this way is called the *Betti table of* M. Notice that the i-th column sum $\sum_{j\geq 0}\beta^R_{i,i+j}(M)$ of this table equals the total Betti number $\beta^R_i(M)$.

Example 5.4.14. $R = k[x,y,z]$, with k a field. Let's compute the minimal graded free resolution $F_\bullet$ of $M = R/(x^2, xy, y^3)$ over R. As in Example 5.4.1, we will have $F_0 = R$, with $f_0 : R \longrightarrow M$ being given by $f_0(r) = r + (x^2, xy, y^3)$. A minimal homogeneous set of generators $\ker f_0 = (x^2, xy, y^3)$ is $\{x^2, xy, y^3\}$, its elements having degrees 2,2 and 3. Therefore, for the next step in the minimal graded free resolution we should pick $F_1 = R(-2)^2 \oplus R(-3)$. Denoting by e_1, e_2, e_3 the generators of F_1, we define $f_1 : F_1 \longrightarrow F_0$ by $f_1(e_1) = x^2$, $f_1(e_2) = xy$ and $f_1(e_3) = y^3$.

$$R(-2)^2 \oplus R(-3) \xrightarrow{\left[x^2\ xy\ y^3\right]} R \longrightarrow M \longrightarrow 0$$

Next we determine minimal homogeneous generators of $\ker f_1$. For this we need to solve $px^2 + qxy + ry^3 = 0$ with $p, q, r \in R$. We see that p must be divisible by y. Writting $p = p'y$ we get $p'x^2 + qx + ry^2$. Now we see that r must be divisible by x. Writting $r = r'x$ we obtain $p'x + q + r'y^2 = 0$, i.e., $q = -p'x - r'y^2$. Therefore, we see that all the solutions (p, q, r) are generated by the solutions corresponding to $(p', r') = (1, 0)$ and $(p', r') = (0, 1)$. Thus $\ker f_1$ is minimally generated by $(y, -x, 0)$ and $(0, -y^2, x)$. Observe that $(y, -x, 0) = ye_1 - xe_2$ has degree 3, while $(0, -y^2, x) = -y^2e_2 + xe_3$ has degree 4. Thus the next step in the minimal graded free resolution of M is a map $f_2 : R(-3) \oplus R(-4) \longrightarrow F_1$ sending the first basis element to $(y, -x, 0)$ and the second to $(0, -y^2, x)$. We easily see that $\ker f_2 = 0$, so that the minimal graded free resolution of $R/(x^2, xy, y^3)$ is

$$0 \longrightarrow R(-3) \oplus R(-4) \xrightarrow{\begin{bmatrix} y & 0 \\ -x & -y^2 \\ 0 & x \end{bmatrix}} R(-2)^2 \oplus R(-3) \xrightarrow{\left[x^2\ xy\ y^3\right]} R \longrightarrow M \longrightarrow 0$$

and the Betti table of $R/(x^2, xy, y^3)$ is

	0	1	2
0	1		
1		2	1
2		1	1

where we simply omit the entries that are zero.

Example 5.4.15. If we let $R = k[x,y,z]$ (instead of $k[\![x,y,z]\!]$) in Example 5.4.1, we see that a minimal graded free resolution of $M = R/(xy, xz, yz)$ over R is

$$0 \longrightarrow R(-3)^2 \xrightarrow{\begin{bmatrix} z & 0 \\ -y & y \\ 0 & -x \end{bmatrix}} R(-2)^3 \xrightarrow{\left[xy\ xz\ yz\right]} R \longrightarrow M \longrightarrow 0\ .$$

Example 5.4.16. Revisiting Example 5.2.13, we see that a minimal graded free resolution of $M = k[X]/(X^2)$ over the graded ring $R = k[X]/(X^3)$ is

$$\cdots \xrightarrow{\cdot X^2} R(-6) \xrightarrow{\cdot X} R(-5) \xrightarrow{\cdot X^2} R(-3) \xrightarrow{\cdot X} R(-2) \xrightarrow{\cdot X^2} R \longrightarrow 0\ .$$

It is not a coincidence that the resolutions in Examples 5.4.1 and 5.4.14 are finite. We will later see that this is always the case for minimal free resolutions of finitely generated modules over $k[\![x_1, \ldots, x_n]\!]$ and for minimal graded free resolutions of finitely generated graded modules over $k[x_1, \ldots, x_n]$.

6 Regular sequences

In this section we will define regular sequences and the invariant *depth*. The depth of a module is perhaps, after dimension, the most important invariant we can associate to it and it is what will later allow us to define Cohen-Macaulay rings.

6.1 Regular sequences

Definition 6.1.1. Let R be a ring and M an R-module. We say that an element $a \in R$ is *M-regular* if $ax = 0$, with $x \in M$, implies $x = 0$. *(So, yes, "regular" is just another name for "nonzerodivisor". From here on we will drop the term "nonzerodivisor" and start using the name "regular".)*

A sequence $a_1, \dots, a_n$ of elements in R is said to be an *M-regular sequence* if it satisfies the following two conditions:

(1) a_1 is M-regular and a_i is $M/(a_1M + \cdots + a_{i-1}M)$-regular for all $i = 2, \dots, n$.

(2) $M/(a_1M + \cdots + a_nM) \neq 0$.

If $a_1, \dots, a_n$ only satisfies (1), then it is said to be a *weak M-sequence*.

If a sequence is R-regular, we may simply say it is a *regular* sequence.

Theorem 6.1.2. *Let R be a ring and M an R-module. If $a_1, \dots, a_n$ is an M-regular sequence, then so is $a_1^{e_1}, \dots, a_n^{e_n}$ for any $e_1, \dots, e_n \geq 1$.*

Proof. [Mat86, Theorem 16.1]. □

Example 6.1.3. (1) $x_1, \dots, x_n$ is a regular sequence in $k[x_1, \dots, x_n]$.

(2) xy, xz is not a regular sequence in $k[x, y, z]$ since xz is not $k[x, y, z]/(xy)$-regular. Indeed, y is nonzero in $k[x, y, z]/(xy)$ and $(xz)y$ is zero in $k[x, y, z]/(xy)$.

In fact, the more general statement holds here: a sequence $f, g \in k[x_1, \dots, x_n]$ is $k[x_1, \dots, x_n]$-regular if and only if $\gcd(f, g) = 1$ and $(f, g) \neq k[x_1, \dots, x_n]$.

(3) Let k be a field and $R = k[x, y, z]$. Then $x, (x-1)y, (x-1)z$ is an R-regular sequence. This follows from the fact that $(x-1)y = -y$ and $(x-1)z = -z$ in $R/(x)$ plus the fact that $x, -y, -z$ is R-regular.

However, the permutation $(x-1)y, (x-1)z, x$ is not R-regular. Indeed, the piece $(x-1)y, (x-1)z$ is not R-regular by a similar argument to (2).

Notice that $(x-1)y, (x-1)z, x$ is not formed by homogeneous elements. We will later see that permutations of homogeneous regular sequences in $\mathbb{N}$-graded Noetherian rings are also regular. The same will happen for regular sequences in Noetherian local rings.

Regular sequences do produce ideals with the maximal possible height.

Theorem 6.1.4. *Let R be a Noetherian ring and $x_1, \dots, x_n$ be an R-regular sequence. Then $\operatorname{ht}(x_1, \dots, x_n) = n$. Moreover, every minimal prime of $(x_1, \dots, x_n)$ has height n.*

Proof. By induction on n. Suppose $n = 1$. As x_1 is a nonzerodivisor on R, x_1 is not in any associated prime of R. In particular, x_1 is not in any minimal prime of R. Thus $\operatorname{ht}(x_1) \geq 1$. On the other hand, by Krull's height theorem, we have $\operatorname{ht}(x_1) \leq 1$.

Suppose now that the theorem is valid for n and suppose $x_1, \dots, x_n, x_{n+1}$ is R-regular. Then $\operatorname{ht}(x_1, \dots, x_n) = n$ and, by the $n = 1$ case, $\operatorname{ht}(x_1, \dots, x_n, x_{n+1})/(x_1, \dots, x_n) = 1$. This implies $\operatorname{ht}(x_1, \dots, x_n, x_{n+1}) \geq n + 1$. Again, the opposite inequality follows from Krull's height theorem.

We have proved that $\operatorname{ht}(x_1, \dots, x_n) = n$, thus every minimal prime of $(x_1, \dots, x_n)$ has height at least n. But again, Krull's height theorem says more: every minimal prime of $(x_1, \dots, x_n)$ must have height at most n. □

Remark 6.1.5. In Cohen-Macaulay rings (something we will define later) a stronger statement holds: in these rings a sequence $x_1, \dots, x_n$ is R-regular if and only if $\operatorname{ht}(x_1, \dots, x_n) = n$.

An M-regular element x is in a sense the "nicest" kind of element one can have. For instance, it allows us to make use of the short exact sequence $0 \longrightarrow M \xrightarrow{\cdot x} M \longrightarrow M/xM \longrightarrow 0$. We now see that regular sequences are also good at preserving exactness of complexes.

Proposition 6.1.6. *Let R be a ring and*

$$N_\bullet : N_2 \xrightarrow{\varphi_2} N_1 \xrightarrow{\varphi_1} N_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

an exact sequence of R-modules. Let $\underline{x} = x_1, \ldots, x_n$ be a weak M-sequence. Then the induced sequence

$$N_\bullet \otimes R/(\underline{x}) : N_2/\underline{x}N_2 \xrightarrow{\overline{\varphi}_2} N_1/\underline{x}N_1 \xrightarrow{\overline{\varphi}_1} N_0/\underline{x}N_0 \xrightarrow{\overline{\varphi}_0} M/\underline{x}M \longrightarrow 0$$

is also exact.

Proof. By induction it is enough to prove it for when $\underline{x}$ consists of a single weak M-regular element x. Also, by the right-exactness of the tensor product, it is enough to prove exactness at N_1/xN_1. Let $y + xN_1$ be in $\ker \overline{\varphi}_1$. Then $\varphi_1(y) \in xN_0$. Write $\varphi_1(y) = xz$ with $z \in N_0$. Then $x\varphi_0(z) = \varphi_0(\varphi_1(y)) = 0$. As x is weakly M-regular, we conclude that $\varphi_0(z) = 0$. The exactness of $N_\bullet$ gives $z = \varphi_1(y')$ for some $y' \in N_1$. Then we have that $\varphi_1(y) = x\varphi_1(y')$, i.e., $y - xy' \in \ker \varphi_1 = \operatorname{im} \varphi_2$. Hence $y \in \operatorname{im} \varphi_2 + xN_1$. This gives $y + xN_1 \in \operatorname{im} \overline{\varphi}_2$, as desired. □

Proposition 6.1.7. *Let R be a ring and*

$$N_\bullet : \cdots \xrightarrow{\varphi_4} N_3 \xrightarrow{\varphi_3} N_2 \xrightarrow{\varphi_2} N_1 \xrightarrow{\varphi_1} N_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

an exact sequence of R-modules. Let $\underline{x} = x_1, \ldots, x_n$ be a weak M-sequence and a weak N_i-sequence for all $i \geq 0$. Then $N_\bullet \otimes R/(\underline{x})$ is also exact.

Proof. Again by induction it is enough to assume that $\underline{x}$ consists of a single element x. Since x is regular on M and N_i for all $i \geq 0$, x is also regular on $\operatorname{im} \varphi_i$ for all $i \geq 0$. The result now follows by applying Proposition 6.1.6 to the exact sequences $N_{i+2} \xrightarrow{\varphi_{i+2}} N_{i+1} \xrightarrow{\varphi_{i+1}} N_i \xrightarrow{\varphi_i} \operatorname{im} \varphi_i \longrightarrow 0$ for all $i \geq 0$. □

Corollary 6.1.8. *Let R be a Noetherian local ring $(R, \mathfrak{m})$ (resp. a Noetherian $\mathbb{N}$-graded ring with R_0 a field). Let M be a finitely generated R-module (resp. a graded R-module) and*

$$F_\bullet : \cdots \xrightarrow{f_4} F_3 \xrightarrow{f_3} F_2 \xrightarrow{f_2} F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} M \longrightarrow 0$$

a minimal free resolution of M (resp. a minimal graded free resolution of M). Let $\underline{x} = x_1, \ldots, x_n$ be a sequence of elements in $\mathfrak{m}$ (resp. a sequence of homogeneous elements of positive degree) which is both M-regular and R-regular. Then

$$F_\bullet \otimes R/(\underline{x}) : \cdots \xrightarrow{\overline{f}_4} F_3/\underline{x}F_3 \xrightarrow{\overline{f}_3} F_2/\underline{x}F_2 \xrightarrow{\overline{f}_2} F_1/\underline{x}F_1 \xrightarrow{\overline{f}_1} F_0/\underline{x}F_0 \xrightarrow{\overline{f}_0} M/\underline{x}M \longrightarrow 0$$

is a minimal free resolution of $M/\underline{x}M$ (resp. a minimal graded free resolution of $M/\underline{x}M$) over $R/\underline{x}R$. Consequently,

$$pd_R(M) = pd_{R/\underline{x}R}(M/\underline{x}M).$$

Proof. As $\underline{x}$ is R-regular and each F_i is a free R-module, $\underline{x}$ is F_i-regular for all $i \geq 0$. Plus, $F_i/\underline{x}F_i$ are also free $R/\underline{x}R$-modules of the same rank as F_i. Thus Proposition 6.1.7 guarantees that $F_\bullet \otimes R/(\underline{x})$ is a free (resp. graded free) resolution of $M/\underline{x}M$. In fact, one easily checks that $F_\bullet \otimes R/(\underline{x})$ is also minimal, using Proposition 5.4.4 (resp. the graded version of Proposition 5.4.4). The last statement of the corollary follows from this. □

6.2 Depth

Definition 6.2.1. *(maximal regular sequences)* Let I be an ideal in a Noetherian ring R and M an R-module. An M-regular sequence $x_1, \dots, x_n$ is said to be *maximal inside* I if $x_1, \dots, x_n \in I$ and if $x_1, \dots, x_n, x_{n+1}$ is not M-regular for any extra $x_{n+1} \in I$.

Suppose M is a finitely generated R-module and $IM \neq M$. Here is a process for constructing a maximal M-regular sequence inside I. First we must pick an element $x_1 \in I$ which is a nonzerodivisor of M. Since the set of nonzerodivisors of M is $R \setminus \bigcup_{P \in \mathrm{Ass}(M)} P$, this can be done if $I \not\subseteq \bigcup_{P \in \mathrm{Ass}(M)} P$, i.e. if $I \not\subseteq P$ for every $P \in \mathrm{Ass}(M)$ (by prime avoidance). If this is the case, pick $x_1 \in I$ such that $x_1 \notin P$ for every $P \in \mathrm{Ass}(M)$. Then x_1 is M-regular. Now consider $M_1 = M/x_1M$. By the same argument, if $I \not\subseteq \bigcup_{P \in \mathrm{Ass}(M_1)} P$, then one can pick $x_2 \in I$ which is M_1-regular. Keeping this process going, we obtain elements $x_1, x_2, \dots$ with $x_1M \subsetneq (x_1, x_2)M \subsetneq (x_1, x_2, x_3)M \subsetneq \cdots$ such that $x_1, \dots, x_i$ is M-regular for every i. As M is a Noetherian R-module, this process must end at some step n. Then $x_1, \dots, x_n$ is a maximal M-regular sequence inside I.

Definition 6.2.2. *(grade and depth)* Let I be an ideal in a Noetherian ring R and M an R-module. The *I-depth* of M is the maximal length of a maximal M-regular sequence inside I. This number is denoted $\mathrm{depth}_I(M)$.

The *grade* of an ideal I, denoted $\mathrm{grade}(I)$, equals the length of a maximal R-regular sequence inside I. In other words, $\mathrm{grade}(I) = \mathrm{depth}_I(R)$.

When $(R, \mathfrak{m})$ is local, the *depth* of M is defined as $\mathrm{depth}(M) := \mathrm{depth}_{\mathfrak{m}}(M)$.

Remark 6.2.3. If $x_1, \dots, x_n$ is an R-regular sequence inside I, then, by Theorem 6.1.4 we have that $n = \mathrm{ht}(x_1, \dots, x_n) \leq \mathrm{ht}(I)$. Thus $\mathrm{grade}(I) \leq \mathrm{ht}(I)$. In particular, if $(R, \mathfrak{m})$ is local, we obtain $\mathrm{depth}(R) \leq \mathrm{ht}(\mathfrak{m}) = \dim(R)$.

If k is a field and $R = k[\![x_1, \dots, x_n]\!]$ then, as $x_1, \dots, x_n$ is an R-regular sequence of length n and $\dim(R) = n$, we conclude that $\mathrm{depth}(R) = n$.

Apriori, it could be that there exist maximal M-regular sequences inside I of different lengths. We will now see that that is not the case: if R is Noetherian and M is finitely generated, then all maximal M-regular sequences inside I will have the same length $\mathrm{depth}_I(M)$. Plus, we will see that there is a homological characterization of this invariant in terms of vanishing and nonvanishing of certain Ext modules.

Lemma 6.2.4. *Let R be a Noetherian ring, I an ideal of R and M a finitely generated R-module. Then I contains an M-regular element if and only if* $\mathrm{Hom}_R(R/I, M) = 0$.

Proof. $(\Rightarrow)$: Suppose $a \in I$ is M-regular. Given a map $f \in \mathrm{Hom}_R(R/I, M)$ we then have $0 = f(a + I) = af(1 + I)$. As a in M-regular this implies $f(1 + I) = 0$. Thus $f = 0$.

$(\Leftarrow)$: Suppose I consists of zerodivisors of M. i.e., $I \subseteq \mathcal{Z}(M) = \bigcup_{P \in \mathrm{Ass}_R(M)} P$. By prime avoidance there exists $P \in \mathrm{Ass}_R(M)$ such that $I \subseteq P$. As $P \in \mathrm{Ass}_R(M)$, there is an inclusion $0 \neq R/P \subseteq M$. But there is also a surjection $R/I \longrightarrow R/P$. The composition of these two maps yields a nonzero element in $\mathrm{Hom}_R(R/I, M)$. □

Lemma 6.2.5. *Let R be a ring, I an ideal and M an R-module. Let $\underline{x} = x_1, \dots, x_n$ be an M-regular sequence inside I. Then*

$$\mathrm{Ext}^n_R(R/I, M) \cong \mathrm{Hom}_R(R/I, M/\underline{x}M).$$

Proof. By induction on n. The vacuous case $n = 0$ simply corresponds to $\mathrm{Ext}^0_R(R/I, M) \cong \mathrm{Hom}_R(R/I, M)$, which is trivialy true. Suppose now the result is valid for $n - 1$. Let $\underline{x}' = x_1, \dots, x_{n-1}$. Thus we know $\mathrm{Ext}^{n-1}_R(R/I, M) \cong \mathrm{Hom}_R(R/I, M/\underline{x}'M)$. But $\mathrm{Hom}_R(R/I, M/\underline{x}'M) = 0$, by Lemma 6.2.4, since x_n is an $(M/\underline{x}'M)$-regular element in I. From the short exact sequence

$$0 \longrightarrow M \xrightarrow{\cdot x_1} M \longrightarrow M/x_1M \longrightarrow 0$$

we extract the following piece of the associated long exact sequence in Ext:

$$0 = \mathrm{Ext}^{n-1}_R(R/I, M) \longrightarrow \mathrm{Ext}^{n-1}_R(R/I, M/x_1M) \xrightarrow{\partial} \mathrm{Ext}^n_R(R/I, M) \xrightarrow{\cdot x_1} \mathrm{Ext}^n_R(R/I, M) \ .$$

Since $x_1 \in I$ and I annihilates $\mathrm{Ext}^n_R(R/I, M)$, the multiplication by x_1 in this sequence is just the zero map. We conclude that ∂ is an isomorphism, so that $\mathrm{Ext}^n_R(R/I, M) \cong \mathrm{Ext}^{n-1}_R(R/I, M/x_1M)$. But $x_2, \dots, x_n$ is an (M/x_1M)-regular sequence inside I, so that by the case $n - 1$ we have $\mathrm{Ext}^{n-1}_R(R/I, M/x_1M) \cong \mathrm{Hom}_R(R/I, M/\underline{x}M)$. This concludes the proof. □

Theorem 6.2.6. *Let R be a Noetherian ring, M a finitely generated R-module and I an ideal of R such that $M \neq IM$. Then*

$$\operatorname{depth}_I(M) = \min\{i : \operatorname{Ext}^i_R(R/I, M) \neq 0\}.$$

Furthermore, all maximal M-regular sequences inside I have the same length $\operatorname{depth}_I(M)$.

Proof. Let $x_1, \ldots, x_n$ be a maximal M-regular sequence inside I. Then, for each $i = 0, \ldots, n-1$ we have

$$\operatorname{Ext}^i_R(R/I, M) \cong \operatorname{Hom}_R(R/I, M/(x_1, \ldots, x_i)M) = 0$$

by Lemmas 6.2.4 and 6.2.5, since I contains an $(M/(x_1, \ldots, x_i)M)$-regular element x_{i+1}. On the other hand, $\operatorname{Ext}^n_R(R/I, M) \cong \operatorname{Hom}_R(R/I, M/(x_1, \ldots, x_n)M) \neq 0$ by Lemma 6.2.4 and by the maximality of the sequence $x_1, \ldots, x_n$. This shows that $n = \min\{i : \operatorname{Ext}^i_R(R/I, M) \neq 0\}$. □

Remark 6.2.7. In the context of Theorem 6.2.6, suppose instead that $M = IM$. Then we claim that $\operatorname{Ext}^i_R(R/I, M) = 0$ for all i. To see this, first we observe that Nakayama gives us the existence of an element $r \in 1 + I$ such that $r \in \operatorname{Ann}(M)$. Thus $I + \operatorname{Ann}(M) = R$. But $I + \operatorname{Ann}(M) \subseteq \operatorname{Ann} \operatorname{Ext}^i_R(R/I, M)$ for every i. Hence we must have $\operatorname{Ext}^i_R(R/I, M) = 0$ for all i. Conversely, if $\operatorname{Ext}^i_R(R/I, M) = 0$ for all i, then Theorem 6.2.6 gives us $\operatorname{depth}_I(M) = \infty$. But then we must have $M = IM$, otherwise we would be able to construct a finite maximal M-regular sequence inside I, by the construction explained at the beginning of this section. This would yield $\operatorname{depth}_I(M) < \infty$, by the proof of Theorem 6.2.6. Therefore, we set $\operatorname{depth}_I(M) = \infty$ if $M = IM$.

Remark 6.2.8. In particular, for a Noetherian local ring $(R, \mathfrak{m}, k)$ and a finitely generated R-module M we have the following identity: $\operatorname{depth}(M) = \min\{i : \operatorname{Ext}^i_R(k, M) \neq 0\}$.

We now mention a few results that are useful for computing depth of modules.

Proposition 6.2.9. *Let R be a Noetherian ring, I an ideal and $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ a short exact sequence of finitely generated R-modules. Then*

$$\operatorname{depth}_I(B) \geq \min\{\operatorname{depth}_I(A), \operatorname{depth}_I(C)\},$$

$$\operatorname{depth}_I(A) \geq \min\{\operatorname{depth}_I(B), \operatorname{depth}_I(C) + 1\},$$

$$\operatorname{depth}_I(C) \geq \min\{\operatorname{depth}_I(B), \operatorname{depth}_I(A) - 1\}.$$

Proof. The short exact sequence induces a long exact sequence in Ext:

$$\longrightarrow \operatorname{Ext}^{i-1}_R(R/I, C) \longrightarrow \operatorname{Ext}^i_R(R/I, A) \longrightarrow \operatorname{Ext}^i_R(R/I, B) \longrightarrow \operatorname{Ext}^i_R(R/I, C) \longrightarrow \operatorname{Ext}^{i+1}_R(R/I, A) \longrightarrow$$

Therefore, if $\operatorname{Ext}^i_R(R/I, A)$ and $\operatorname{Ext}^i_R(R/I, C)$ both vanish, then $\operatorname{Ext}^i_R(R/I, B)$ must also vanish. This observation, together with Theorem 6.2.6, gives the first inequality. The remaining inequalities follow by a totally analogous argument. □

Exercise 6.2.10. Let R be a Noetherian ring, M a finitely generated R-module and $x_1, \ldots, x_n$ an M-regular sequence. If $P \in \operatorname{Supp}(M)$ contains $x_1, \ldots, x_n$, then $x_1/1, \ldots, x_n/1 \in R_P$ is an M_P-regular sequence.

Proposition 6.2.11. *Let R be a Noetherian ring, I, J ideals of R and M a finitely generated R-module. Then*

(i) $\operatorname{depth}_I(M) = \inf\{\operatorname{depth} M_P : P \in V(I) \cap \operatorname{Supp}(M)\}$.

(ii) $\operatorname{depth}_I(M) = \operatorname{depth}_{\sqrt{I}}(M)$.

(iii) $\operatorname{depth}_{I \cap J}(M) = \min\{\operatorname{depth}_I(M), \operatorname{depth}_J(M)\}$.

(iv) If $\underline{x} = x_1, \ldots, x_n$ is an M-regular sequence inside I, then $\operatorname{depth}_{I/(\underline{x})}(M/(\underline{x})M) = \operatorname{depth}_I(M/(\underline{x})M) = \operatorname{depth}_I(M) - n$.

Proof. (i) It is clear that $\operatorname{depth}_I(M) \leq \operatorname{depth}_P(M) \leq \operatorname{depth} M_P$ for $P \in V(I) \cap \operatorname{Supp}(M)$, the last equality following from exercise 6.2.10. Suppose $I \neq IM$ and choose a maximal M-regular sequence $\underline{x}$ inside I. Since I consists of zerodivisors of $M/(\underline{x})M$, there exists $P \in \operatorname{Ass}(M/(\underline{x})M)$ such that $I \subseteq P$. But also $PR_P \in \operatorname{Ass}_{R_P}((M/(\underline{x})M)_P) = \operatorname{Ass}_{R_P}(M_P/(\underline{x})M_P)$. Hence PR_P consists of zerodivisors of $M_P/(\underline{x})M_P$, which shows $\operatorname{depth} M_P \leq \operatorname{depth}_I(M)$.

In the case $\operatorname{depth}_I(M) = \infty$, we have $M = IM$. But then it is easy to see that $M_P = (PR_P)M_P$ for all $P \in V(I)$, which yields $\operatorname{depth} M_P = \infty$ for all $P \in V(I)$.

(ii) Follows from (i) and from $V(I) = V(\sqrt{I})$.

(iii) Follows from (i) and from $V(I \cap J) = V(I) \cup V(J)$.

(iv) Let $\overline{(-)}$ denote modulo $\underline{x}$. It is easy to see that $y_1, \ldots, y_s \in I$ form a $\overline{M}$-regular sequence if and only if $\overline{y_1}, \ldots, \overline{y_s}$ form a $\overline{M}$-regular sequence. This shows the first equality. The second follows from Theorem 6.2.6. Also, one sees that $IM = M \Leftrightarrow I\overline{M} = \overline{M} \Leftrightarrow \overline{IM} = \overline{M}$, which takes care of the case $\operatorname{depth}_I(M) = \infty$. □

Proposition 6.2.12. *Let $(R, \mathfrak{m})$ be a Noetherian local ring and $M \neq 0$ a finitely generated R-module. Then every M-regular sequence is part of a system of parameters of M. Hence*

$$\operatorname{depth} M \leq \dim M.$$

Proof. It is enough to prove that every M-regular element x is a parameter of M, i.e., $\dim(M/xM) = \dim(M) - 1$. Indeed, if x is M-regular, then x avoids all associated primes of M. In particular, it avoids all minimal primes of $\operatorname{Supp}(M)$ (remember Theorem 2.3.12). Therefore $\dim(M/xM) \leq \dim(M) - 1$. On the other hand, let $s = \dim(M/xM)$ and let $y_1, \ldots, y_s$ be a system of parameters of M/xM. Then $M/(x, y_1, \ldots, y_s)M$ has dimension zero. Therefore, $s + 1 \geq \delta(M) = \dim(M)$. From this we get $\dim(M/xM) \geq \dim(M) - 1$. □

In fact, this can be a bit refined.

Proposition 6.2.13. *Let $(R, \mathfrak{m})$ be a Noetherian local ring and $M \neq 0$ a finitely generated R-module. Then $\operatorname{depth} M \leq \dim R/P$ for all $P \in \operatorname{Ass}(M)$.*

Proof. Here I refer you to [BH98, Proposition 1.2.13]. □

6.3 The Koszul complex

Here we introduce the most important complex in Commutative Algebra. It is a complex which can be associated to any sequence of elements and whose exactness is directly connected to the invariant depth.

Definition 6.3.1. Let $x_1, \ldots, x_n$ be elements in a ring R. We define the *Koszul complex* of $x_1, \ldots, x_n$, denoted $K_\bullet(x_1, \ldots, x_n)$, to be the complex given by

$$K_\bullet : 0 \longrightarrow K_n \xrightarrow{d_n} \cdots \xrightarrow{d_3} K_2 \xrightarrow{d_2} K_1 \xrightarrow{d_1} K_0 \longrightarrow 0$$

where:

(1) K_p is the free R-module of rank $\binom{n}{p}$ for each $0 \leq p \leq n$.

Let $\{e_{i_1 \cdots i_p} : 1 \leq i_1 < \cdots < i_p \leq n\}$ denote the basis of K_p for each $p \geq 1$.

(2) The differential $d_p : K_p \longrightarrow K_{p-1}$ is given by

$$d_p(e_{i_1 \cdots i_p}) = \sum_{r=1}^{p} (-1)^{r-1} x_{i_r} e_{i_1 \cdots \widehat{i_r} \cdots i_p}$$

for each $p \geq 2$, where $\widehat{i_r}$ means we omit i_r. For $p = 1$ set $d_1(e_r) = x_r$.

For an R-module M, the *Koszul complex of $x_1, \ldots, x_n$ with coefficients in M* is

$$K_\bullet(x_1, \ldots, x_n; M) = K_\bullet(x_1, \ldots, x_n) \otimes_R M.$$

So, instead of the modules in the complex being $R^{\binom{n}{p}}$, they become $M^{\binom{n}{p}}$.

Exercise 6.3.2. Check that the Koszul complex is indeed a complex.

Notice that $K_\bullet(x_1, \ldots, x_n)$ is a finite complex which is invariant up to reordering of the elements $x_1, \ldots, x_n$.

Example 6.3.3. Here is what the Koszul complex of $x_1, \dots, x_n$ looks like for:

$n = 1$:

$$0 \longrightarrow R \xrightarrow{\cdot x_1} R \longrightarrow 0 \ .$$

$n = 2$:

$$0 \longrightarrow R \xrightarrow{\left[\begin{smallmatrix} -x_2 \\ x_1 \end{smallmatrix}\right]} R^2 \xrightarrow{[x_1 \ x_2]} R \longrightarrow 0 \ .$$

$n = 3$:

$$0 \longrightarrow R \xrightarrow{\left[\begin{smallmatrix} x_3 \\ -x_2 \\ x_1 \end{smallmatrix}\right]} R^3 \xrightarrow{\left[\begin{smallmatrix} -x_2 & -x_3 & 0 \\ x_1 & 0 & -x_3 \\ 0 & x_1 & x_2 \end{smallmatrix}\right]} R^3 \xrightarrow{[x_1 \ x_2 \ x_3]} R \longrightarrow 0 \ .$$

Observe that x_1 is a regular element if and only if $K_\bullet(x_1)$ is an exact complex. It is also easy to see that if x_1, x_2 is a regular sequence, then $K_\bullet(x_1, x_2)$ is exact. Our next step is in fact to show that, in the local or graded cases, a sequence is regular if and only if its Koszul complex is exact. Moreover, even when the Koszul complex is not exact, it is useful for detecting the length of a maximal regular sequence inside $(x_1, \dots, x_n)$.

Definition 6.3.4. If $P_\bullet, Q_\bullet$ are two complexes of R-modules, their tensor product is the complex $P_\bullet \otimes_R Q_\bullet$ given by $(P_\bullet \otimes Q_\bullet)_n = \sum_{i+j=n} P_i \otimes_R Q_j$ and differential d given by $d_n(x, y) = d_i^P(x) \otimes y + (-1)^i x \otimes d_j^Q(y)$ for each $x \in P_i$ and $y \in Q_j$ with $i + j = n$.

Exercise 6.3.5. (1) If $P_\bullet, Q_\bullet$ are two complexes or R-modules, check that their tensor product $P_\bullet \otimes_R Q_\bullet$ is in fact a complex.

(2) If $x_1, \dots, x_n$ is a sequence of elements in R. Check that $K_\bullet(x_1, \dots, x_n) = K_\bullet(x_1, \dots, x_{n-1}) \otimes_R K_\bullet(x_n)$.

Lemma 6.3.6. *Let $C_\bullet$ be a complex of R-modules. Let $x \in R$ and denote $C_\bullet(x) = C_\bullet \otimes_R K_\bullet(x)$. Then there is an exact sequence of complexes*

$$0 \longrightarrow C_\bullet \longrightarrow C_\bullet(x) \longrightarrow C_\bullet[-1] \longrightarrow 0$$

where $C_\bullet[-1]$ is given by $C_\bullet[-1]_p = C_{p-1}$ and differential $d_{C_\bullet[-1]} = d_{C_\bullet}$. The long exact sequence in homology associated to this short exact sequence is

$$\cdots \longrightarrow H_p(C_\bullet) \longrightarrow H_p(C_\bullet(x)) \longrightarrow H_{p-1}(C_\bullet) \xrightarrow{\cdot(-1)^{p-1}x} H_{p-1}(C_\bullet) \longrightarrow \cdots$$

and we have $xH_p(C_\bullet(x)) = 0$ for all p.

Proof. Since $K_\bullet(x)$ is just $0 \longrightarrow R \xrightarrow{\cdot x} R \longrightarrow 0$, we see that each module $C_\bullet(x)_p$ of $C_\bullet(x)$ can be identified with $C_p \oplus C_{p-1}$. With this identification, the differential of $C_\bullet(x)$ is given by $d(a, b) = (d(a) + (-1)^{p-1}xb, d(b))$. The short exact sequence of complexes follows from this.

Notice also that $H_p(C_\bullet[-1]) = H_{p-1}(C_\bullet)$. We claim that the connecting homomorphism $H_{p-1}(C_\bullet) \longrightarrow H_{p-1}(C_\bullet)$ is given by multiplication by $(-1)^{p-1}x$. Suppose we are given $b \in C_{p-1}$ such that $d(b) = 0$. b comes from $(0, b) \in C_p \oplus C_{p-1}$. We see that $d(0, b) = ((-1)^{p-1}xb, 0)$, which is the image of $(-1)^{p-1}xb \in C_{p-1}$ by the inclusion $C_{p-1} \longrightarrow C_{p-1} \oplus C_{p-2}$. This proves the claim.

We now prove the last statement of the lemma. Take $\overline{z} \in H_p(C_\bullet(x))$, represented by $z = (a, b) \in \ker d_p$. Then $0 = d_p(a, b)$ gives $d(b) = 0$ and $d(a) = (-1)^p xb$. But then we see that $xz = (xa, xb) = d_{p+1}(0, (-1)^p a) \in \operatorname{im} d_{p+1}$. So xz is zero in $H_p(C_\bullet(x))$. □

The homology modules of the Koszul complex actually deserve a special name and notation.

Definition 6.3.7. Let $x_1, \dots, x_n$ be elements in a ring R and M be an R-module. The p-th homology module of the Koszul complex $K_\bullet(x_1, \dots, x_n; M)$ is denoted $H_p(x_1, \dots, x_n; M)$ and is called the *p-th Koszul homology module of $x_1, \dots, x_n$ with respect to M*.

Remark 6.3.8. Notice that we always have $H_0(x_1, \dots, x_n; M) = M/(x_1, \dots, x_n)M$ and $H_n(x_1, \dots, x_n; M) = \{m \in M : x_i m = 0 \text{ for all } i = 1, \dots, n\} = \{m \in M : Im = 0\}$, where $I = (x_1, \dots, x_n)$.

The following is an immediate consequence of Lemma 6.3.6 and the fact that $K_\bullet(x_1, \dots, x_n; M) \cong K_\bullet(x_1) \otimes_R \cdots \otimes_R K_\bullet(x_n) \otimes_R M$.

Proposition 6.3.9. *Let $x_1, \dots, x_n$ be elements in a ring R and M an R-module. Denote $I = (x_1, \dots, x_n)$. Then*

$$IH_p(x_1, \dots, x_n; M) = 0$$

for all p. Plus, there is a long exact sequence of the form

$$\cdots \longrightarrow H_p(x_1, \dots, x_{n-1}; M) \longrightarrow H_p(x_1, \dots, x_n; M) \longrightarrow H_{p-1}(x_1, \dots, x_{n-1}; M) \xrightarrow{\pm x_n} H_{p-1}(x_1, \dots, x_{n-1}; M)$$

$$\longrightarrow H_{p-1}(x_1, \dots, x_n; M) \longrightarrow \cdots$$

Theorem 6.3.10. *Let M be an R-module and $x_1, \dots, x_n$ an M-regular sequence. Then*

$$H_p(x_1, \dots, x_n; M) = 0 \text{ for all } p > 0 \text{ and } H_0(x_1, \dots, x_n; M) = M/(x_1, \dots, x_n)M.$$

Proof. By induction on n, the result being obvious for $n = 1$. Suppose $n > 1$. If $p > 1$, Proposition 6.3.9 gives us an exact sequence

$$0 = H_p(x_1, \dots, x_{n-1}; M) \longrightarrow H_p(x_1, \dots, x_n; M) \longrightarrow H_{p-1}(x_1, \dots, x_{n-1}; M) = 0 \ .$$

From it we conclude $H_p(x_1, \dots, x_n; M) = 0$ for all $p > 1$. On the other hand, for $p = 1$ we have an exact sequence

$$0 = H_1(x_1, \dots, x_{n-1}; M) \longrightarrow H_1(x_1, \dots, x_n; M) \longrightarrow H_0(x_1, \dots, x_{n-1}; M) \xrightarrow{\cdot \pm x_n} H_0(x_1, \dots, x_{n-1}; M)$$

i.e., an exact sequence

$$0 \longrightarrow H_1(x_1, \dots, x_n; M) \longrightarrow M/(x_1, \dots, x_{n-1})M \xrightarrow{\cdot \pm x_n} M/(x_1, \dots, x_{n-1})M \ .$$

But as x_n is $M/(x_1, \dots, x_{n-1})M$-regular, this multiplication by $\pm x_n$ map is injective. Thus we obtain the remaining identity $H_1(x_1, \dots, x_n; M) = 0$. □

Remark 6.3.11. Theorem 6.3.10 is saying that if $x_1, \dots, x_n$ is an M-regular sequence, then $K_\bullet(x_1, \dots, x_n; M)$ is a free resolution of $M/(x_1, \dots, x_n)M$. If in addition $(R, \mathfrak{m})$ is local and $x_1, \dots, x_n \in \mathfrak{m}$, then the Koszul complex is in fact a minimal free resolution of $M/(x_1, \dots, x_n)M$, since all the entries in the matrices representing the maps in the Koszul complex are of the form $\pm x_i$, and therefore are in $\mathfrak{m}$.

We now see that the converse of Theorem 6.3.10 holds in a stronger form if we are in the appropriate local or graded cases.

Theorem 6.3.12. *Suppose we are in one of the two following situations:*

(1) $(R, \mathfrak{m})$ is a Noetherian local ring, M is a finitely generated R-module and $x_1, \dots, x_n$ is a sequence of elements in $\mathfrak{m}$.

(2) R is a Noetherian $\mathbb{N}$-graded ring, M is an $\mathbb{N}$-graded R-module and $x_1, \dots, x_n$ is a sequence formed by elements of R of positive degree.

Then $x_1, \dots, x_n$ is an M-regular sequence if and only if $M \neq 0$ and $H_1(x_1, \dots, x_n; M) = 0$.

Proof. The "if" part is Theorem 6.3.10. We prove the "only if " part by induction on n, the case $n = 1$ being trivial. So assume that $M \neq 0$ and that $H_1(x_1, \dots, x_n; M) = 0$. First of all observe that $M/(x_1, \dots, x_n)M \neq 0$ otherwise by Nakayama we would get $M = 0$. By Proposition 6.3.9 we have an exact sequence

$$H_1(x_1, \dots, x_{n-1}; M) \xrightarrow{\cdot \pm x_n} H_1(x_1, \dots, x_{n-1}; M) \longrightarrow H_1(x_1, \dots, x_n; M) = 0 \ ,$$

giving us $H_1(x_1, \dots, x_{n-1}; M) = x_n H_1(x_1, \dots, x_{n-1}; M)$. But $H_1(x_1, \dots, x_{n-1}; M)$, being a quotient of a submodule of the finitely generated R-module M^{n-1}, is finitely generated. Hence, by Nakayama's lemma (the local or graded version) we conclude that $H_1(x_1, \dots, x_{n-1}; M) = 0$. The induction hypothesis now gives us that $x_1, \dots, x_{n-1}$ is an M-regular sequence. Finally, using the exact sequence

$$0 = H_1(x_1, \dots, x_n; M) \longrightarrow M/(x_1, \dots, x_{n-1})M \xrightarrow{\cdot \pm x_n} M/(x_1, \dots, x_{n-1})M$$

(which we already used at the end of the proof of Theorem 6.3.10) we obtain that x_n is $M/(x_1, \dots, x_{n-1})M$-regular. □

Lemma 6.3.13. *Let*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be a short exact sequence of R-modules. If $\underline{x} = x_1, \dots, x_n$ is a sequence of elements in R, then there is a long exact sequence in Koszul homology

$$\cdots \longrightarrow H_1(\underline{x}; B) \longrightarrow H_1(\underline{x}; C) \longrightarrow H_0(\underline{x}; A) \longrightarrow H_0(\underline{x}; B) \longrightarrow H_0(\underline{x}; C) \longrightarrow 0 \ .$$

Proof. Let $K_\bullet = K_\bullet(\underline{x})$. The result follows from the fact that

$$0 \longrightarrow K_\bullet \otimes_R A \xrightarrow{\mathrm{id}\otimes f} K_\bullet \otimes_R B \xrightarrow{\mathrm{id}\otimes g} K_\bullet \otimes_R C \longrightarrow 0$$

is a short exact sequence of complexes. This is because $K_\bullet$ is a complex of free modules. As each module K_p in $K_\bullet$ is free we have that

$$0 \longrightarrow K_p \otimes_R A \xrightarrow{\mathrm{id}\otimes f} K_p \otimes_R B \xrightarrow{\mathrm{id}\otimes g} K_p \otimes_R C \longrightarrow 0$$

is exact for every p. □

The following result is commonly referred to as the "depth sensitivity" of the Koszul complex.

Theorem 6.3.14. *Let R be a Noetherian ring, M a finitely generated R-module and $I = (x_1, \dots, x_n)$ an ideal of R such that $M \neq IM$. Let*

$$q = \max\{p : H_p(x_1, \dots, x_n; M) \neq 0\}.$$

Then

$$\mathrm{depth}_I(M) = n - q.$$

Proof. Let $s = \mathrm{depth}_I(M)$. The proof is by induction on s. Let $y_1, \dots, y_s$ be a maximal M-regular sequence inside I.

Suppose $s = 0$. Then I consists of zerodivisors of M, so $I \subseteq \bigcup_{P \in \mathrm{Ass}(M)} P$. By prime avoidance there exists $P \in \mathrm{Ass}(M)$ such that $I \subseteq P$. Let $z \in M$ be a nonzero element such that $P = \mathrm{Ann}(z)$. Then $Iz = 0$. Notice that $H_n(x_1, \dots, x_n; M) = \{m \in M : x_i m = 0 \text{ for all } i = 1, \dots, n\} = \{m \in M : Im = 0\}$. Then we get that $z \in H_n(x_1, \dots, x_n; M)$ and thus $H_n(x_1, \dots, x_n; M) \neq 0$. We conclude that $q = n$.

Suppose now $s \geq 1$. Using Lemma 6.3.13 on the short exact sequence

$$0 \longrightarrow M \xrightarrow{\cdot x_1} M \longrightarrow M/x_1M \longrightarrow 0$$

we extract an exact sequence

$$H_p(\underline{x}; M) \xrightarrow{\cdot x_1} H_p(\underline{x}; M) \longrightarrow H_p(\underline{x}; M/x_1M) \longrightarrow H_{p-1}(\underline{x}; M) \xrightarrow{\cdot x_1} H_{p-1}(\underline{x}; M)$$

for every p. But since I annihilates $H_p(\underline{x}; M)$ for every p, by Proposition 6.3.9, we have in particular that $x_1 H_p(\underline{x}; M) = 0$ for all p. Hence we actually have a short exact sequence

$$0 \longrightarrow H_p(\underline{x}; M) \longrightarrow H_p(\underline{x}; M/x_1M) \longrightarrow H_{p-1}(\underline{x}; M) \longrightarrow 0$$

for every p. Since $H_q(\underline{x}; M) \neq 0$, we obtain $H_{q+1}(\underline{x}; M/x_1M) \neq 0$. Also, since $H_p(\underline{x}; M) = 0$ for all $p > q$, we obtain $H_p(\underline{x}; M/x_1M) = 0$ for all $p > q + 1$. Since $\mathrm{depth}_I(M/x_1M) = s - 1$, the induction hypothesis now gives

$$s - 1 = \mathrm{depth}_I(M/x_1M) = n - (q + 1).$$

This becomes $s = n - q$, which is what we wanted to show. □

In other words, in the situation of Theorem 6.3.14, $\mathrm{depth}_I(M)$ coincides with the number of zeros in the sequence $H_n(x_1, \dots, x_n; M), H_{n-1}(x_1, \dots, x_n; M), \dots, H_1(x_1, \dots, x_n; M)$, counting from the left.

References

[AM69] M. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Company, 1969.

[BH98] W. Bruns and J. Herzog. *Cohen-Macaulay Rings*. Vol. 39. Cambridge University Press, 1998.

[Mat86] H. Matsumura. *Commutative ring theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1986.

[Pee10] I. Peeva. *Graded syzygies*. Vol. 14. Springer Science & Business Media, 2010.

[Wei94] C. Weibel. *An introduction to homological algebra*. Vol. 38. Cambridge University Press, 1994.