Homological Algebra

Irena Swanson
Graz, Fall 2018

The goal of these lectures is to introduce homological algebra to the students whose commutative algebra background consists mostly of the material in Atiyah-MacDonald [1]. Homological algebra is a rich area and can be studied quite generally; in the first few lectures I tried to be quite general, using groups or left modules over not necessarily commutative rings, but in these notes and also in most of the lectures, the subject matter was mostly modules over commutative rings. Much in these notes is from the course I took from Craig Huneke in 1989, and I added much other material.

All rings are commutative with identity.

This is work in progress. I am still adding, subtracting, modifying, correcting errors. Any comments and corrections are welcome.

The first version of these notes was used at University Roma Tre between March and May 2010, where my stay was funded by INDAM through Professor Stefania Gabelli. A much corrected version is used in Graz, Austria in the fall of 2018, where I am spending a semester on the Fulbright–NAWI Fellowship. I thank Amr Al Maktry, Lukas Andritsch, Charles Beil, Victor Fadinger, Sophie Frisch, Ana Garcia Elsener, Jordan McMahon, Sarah Nakato, Arnur Nigmetov and Daniel Windisch for all the comments that helped improve these notes.

Table of contents:

1 Overview, background, and definitions

1. What is a complex? A **complex** is a collection of groups (or left modules) and homomorphisms, usually written in the following way:

$$\cdots \to M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \to \cdots,$$

where the M_i are groups (or left modules), the d_i are group (or left module) homomorphisms, and for all i, $d_i \circ d_{i+1} = 0$. Rather than write out the whole complex, we will typically abbreviate it as $C_\bullet$, $M_\bullet$ or $(M_\bullet, d_\bullet)$, et cetera, where the dot differentiates the complex from a module, and $d_\bullet$ denotes the collection of all the d_i. This $d_\bullet$ is called the **differential** of the complex.

A complex is **bounded below** if $M_i = 0$ for all sufficiently small (negative) i; a complex is **bounded above** if $M_i = 0$ for all sufficiently large (positive) i; a complex is **bounded** if $M_i = 0$ for all sufficiently large $|i|$. For complexes bounded below we abbreviate "$0 \to 0 \to 0 \to \cdots$" to one zero module, and similarly for complexes bounded above.

A complex is **exact at the ith place** if $\ker(d_i) = \mathrm{im}(d_{i+1})$. A complex is **exact** if it is exact at all places.

A complex is **free** (resp. **flat**, **projective**, **injective**) if all the M_i are free (resp. flat, projective, injective). (Flat modules are defined in Definition 2.3, projective modules in Section 5 and injective modules in Section 24.)

An **exact sequence** or a **long exact sequence** is another name for an exact complex. An exact sequence is a **short exact sequence** if it is of the form

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0.$$

For any R-modules M and N we have a short exact sequence $0 \to M \to M \oplus N \to N \to 0$, with the maps being $m \mapsto (m, 0)$ and $(m, n) \mapsto n$. Such a sequence is called a **split exact sequence** (it splits in a trivial way). But under what conditions does a short exact sequence $0 \to M \to K \to N \to 0$ split? When can we conclude that $K \cong M \oplus N$ (and more)? We will prove that the sequence splits if N is projective or if $\mathrm{Ext}^1_R(M, N) = 0$. See also Exercise 1.8.

Remark 1.1 Every long exact sequence

$$\cdots \to M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \to \cdots$$

decomposes into short exact sequences

$$\begin{array}{ccccccccccc}
 & & & & 0 & \to & \ker d_{i-1} & \to & M_{i-1} \to \operatorname{im} d_{i-1} \to 0 \\
 & & & & & & \| & & \\
 & & 0 & \to \ker d_i & \to & M_i & \to & \operatorname{im} d_i & \to & 0 \\
 & & & \| & & & & & \\
0 \to \ker d_{i+1} \to M_{i+1} & \to & \operatorname{im} d_{i+1} & \to & 0, & & & &
\end{array}$$

et cetera.

We will often write only parts of complexes, such as for example $M_3 \to M_2 \to M_1 \to 0$, and we will say that such a (fragment of a) complex is exact if there is exactness at a module that has both an incoming and an outgoing map.

2. Homology of a complex $C_\bullet$. The **nth homology group (or module)** is

$$H_n(C_\bullet) = \frac{\ker d_n}{\operatorname{im} d_{n+1}}.$$

3. Cocomplexes. A complex might be naturally numbered in the opposite order:

$$C^\bullet : \qquad \cdots \to M^{i-1} \xrightarrow{d^{i-1}} M^i \xrightarrow{d^i} M^{i+1} \to \cdots,$$

in which case we index the groups (or modules) and the homomorphisms with superscripts rather than the subscripts, and we call it a **co-complex**. The nth **cohomology module** of such a co-complex $C^\bullet$ is

$$H^n(C^\bullet) = \frac{\ker d^n}{\operatorname{im} d^{n-1}}.$$

If $(C^\bullet, d^\bullet)$ is a co-complex, then

$$\cdots \to C^{-2} \xrightarrow{d^{-2}} C^{-1} \xrightarrow{d^{-1}} C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^1} C^2 \xrightarrow{d^2} C^3 \to \cdots$$

After renaming $D_n = C^{-n}$ and $e_n = d^{-n}$ we convert the co-complex into the complex:

$$\cdots \to D_2 \xrightarrow{e_2} D_1 \xrightarrow{e_1} D_0 \xrightarrow{e_0} D_{-1} \xrightarrow{e_{-1}} D_{-2} \xrightarrow{e_{-2}} D_{-3} \to \cdots$$

The naming can be even shifted: $F_n = C^{-n+2}$ and $g_n = d^{-n+2}$ converts the co-complex into the following complex:

$$\cdots \to D_2(=E^0) \xrightarrow{e_2(=d^0)} D_1(=E^1) \xrightarrow{e_1} D_0 \xrightarrow{e_0} D_{-1} \xrightarrow{e_{-1}} D_{-2} \xrightarrow{e_{-2}} D_{-3} \to \cdots$$

Similarly, any complex can be converted into a co-complex, possibly with shifting. There are reasons for using both complexes and co-complexes (keep reading).

4. Free and projective resolutions.

Definition 1.2 *A (left) R-module F is* **free** *if it is a direct sum of copies of R. If $F = \oplus_{i \in I} Ra_i$ and $Ra_i \cong R$ for all i, then we call the set $\{a_i : i \in I\}$ a* **basis** *of F.*

Facts 1.3

(1) If X is a basis of F and M is a (left) R-module, then for any function $f : X \to M$ there exists a unique R-module homomorphism $\tilde{f} : F \to M$ that extends f.

(2) Every R-module is a homomorphic image of a free module.

Definition 1.4 *Let M be an R-module. A* **free** *(resp.* **projective***)* **resolution** *of M is a complex*

$$\cdots \to F_{i+1} \xrightarrow{d_{i+1}} F_i \xrightarrow{d_i} F_{i-1} \to \cdots \to F_1 \xrightarrow{d_1} F_0 \to 0,$$

where the F_i are free (resp. projective) modules over R (definition of projective modules is in Section 5) and where

$$\cdots \to F_{i+1} \xrightarrow{d_{i+1}} F_i \xrightarrow{d_i} F_{i-1} \to \cdots \longrightarrow F_1 \xrightarrow{d_1} F_0 \to M \to 0$$

is exact.

Free, projective, flat resolutions are not uniquely determined, in the sense that the free modules and the homomorphisms are not uniquely defined, not even up to isomorphisms.

Sometimes, mostly in order to save writing time, $\cdots \to F_{i+1} \to F_i \to F_{i-1} \to \cdots \to F_1 \to F_0 \to M \to 0$ is also called a free (resp. projective) resolution of M.

5. Construction of free resolutions. We use the fact that every module is a homomorphic image of a free module. Thus we may take F_0 to be a free module that maps onto M, and we have non-isomorphic choices there; we then take F_1 to be a free module that maps onto the kernel of $F_0 \to M$, giving an exact complex $F_1 \to F_0 \to M \to 0$; after which we may take F_2 to be a free module that maps onto the kernel of $F_1 \to F_0$, et cetera.

Example 1.5 Let R be the polynomial ring $k[x,y,z]$ in variables x,y,z over a field k. Let I be the ideal (x^3, y^3, xyz) in R. We will construct a free resolution of I in a slow way. One point of this example is to see that it is possible to construct resolutions methodically, at least for monomial ideals, and another point is that the explicit construction of resolutions takes effort. (One of the goals of the course is to get properties of free resolutions theoretically without necessarily constructing them, but seeing at least one construction is good as well.) By definition we see that the free R-module R^3 maps onto I via the map $d_0 : R^3 \to R$ defined by the 1×3 matrix $[x^3\ y^3\ xyz]$. The following elements are in the kernel of d_0:

$$\begin{bmatrix} y^3 \\ -x^3 \\ 0 \end{bmatrix}, \begin{bmatrix} yz \\ 0 \\ -x^2 \end{bmatrix}, \begin{bmatrix} 0 \\ xz \\ -y^2 \end{bmatrix}.$$

We next prove that the kernel of d_0 is generated by these three vectors. So let $[f\ g\ h]^T$ be an arbitrary element of the kernel. Write $h = h_0 + h_1x^2$, where $h_0 \in R$ has degree in x at most 1 and where $h_1 \in R$. Then

$$\begin{bmatrix} f \\ g \\ h \end{bmatrix} + h_1 \begin{bmatrix} yz \\ 0 \\ -x^2 \end{bmatrix} = \begin{bmatrix} f - h_1yz \\ g \\ h_0 \end{bmatrix}.$$

The sum of elements in the kernel is also in the kernel. If we can prove that this last element is in the module generated by the three vectors, then so is $[f\ g\ h]^T$. So we may assume that h has x-degree at most 1. Similarly, by adding a specific multiple of $[0\ xz\ -y^2]$ we may assume without loss of generality that h has simultaneously y-degree at most 1. Write $g = g_0 + g_1x + g_2x^2 + g_3x^3$, where $g_0, g_1, g_2 \in k[y,z]$ and $g_3 \in R$. By the definition of the kernel, $fx^3 + gy^3 + hxyz = 0$. We trace in this equation the monomials that are multiples of x^3 and we thus get that $f = g_3y^3$. Then

$$\begin{bmatrix} f \\ g \\ h \end{bmatrix} - g_3 \begin{bmatrix} y^3 \\ -x^3 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ g_0 + g_1x + g_2x^2 \\ h \end{bmatrix}.$$

It suffices to prove that any element in $\ker d_0$ that is of the form $(0, g, h)$ is in the R-module generated by the three vectors. By the assumption $gy^3 + hxyz = 0$, so that $gy^2 + hxz = 0$, so h must be a multiple of y^2, i.e., $h = ry^2$ for some $r \in R$, and then $g = -rxz$. Thus $(0, g, h) = -r(0, xz, -y^2)$, which proves that the kernel of d_0 is generated by the three vectors. So, we have constructed the following part of a free resolution of I:

$$R^3 \xrightarrow{\begin{bmatrix} y^3 & yz & 0 \\ -x^3 & 0 & xz \\ 0 & -x^2 & -y^2 \end{bmatrix}} R^3 \xrightarrow{[x^3\quad y^3\quad xyz]} R \to 0.$$

It is easy to see that $[z \ \ -y^2 \ x^2]$ is in the kernel of the 3×3 matrix, and a similar proof as for the kernel of d_0 shows that the following is a complete free resolution:

$$0 \to R \xrightarrow{\begin{bmatrix} z \\ -y^2 \\ x^2 \end{bmatrix}} R^3 \xrightarrow{\begin{bmatrix} y^3 & yz & 0 \\ -x^3 & 0 & xz \\ 0 & -x^2 & -y^2 \end{bmatrix}} R^3 \xrightarrow{[\,x^3 \quad y^3 \quad xyz\,]} R \to 0.$$

This was quite a calculation, and using elementary algebra! We will learn in the course to construct free resolutions of many ideals with more powerful theory. However, it is true that for some ideals the construction of free resolutions means detailed work as we did in this example.

6. Minimal free resolutions Let R be a Noetherian ring and M a finitely generated R-module. A **minimal free resolution** of M is a free resolution of M in which at each step the free module is chosen with a minimal possible number of generators. By the Noetherian properties all F_i are finitely generated free R-modules:

$$\cdots \to R^{b_2} \to R^{b_1} \to R^{b_0} \to M \to 0.$$

So b_0 is the cardinality of the smallest generating set of M, b_1 is the cardinality of the smallest number of the generating set of the kernel of $R^{b_0} \to M$, b_{i+1} is the cardinality of the smallest number of the generating set of the kernel of $R^{b_i} \to R^{b_{i-1}}$. The number b_i is called the **ith Betti number** of M. (See Exercise 6.9 to see that these are well-defined.)

When R is a Noetherian local ring with maximal ideal $\mathfrak{m}$, then the free resolution is minimal if and only if $b_0 = \dim_{R/\mathfrak{m}}(M/\mathfrak{m}M)$ and all the maps $F_i \to F_{i-1}$ have the range in $\mathfrak{m}F_{i-1}$. (See Proposition 6.8.)

In the case where R is a polynomial ring $k[x_1, \ldots, x_n]$ in variables $x_1, \ldots, x_n$ over a field k and M is a finitely generated R-module generated by homogeneous elements, then all the maps in a resolution can be taken to be homogeneous, and this is true also for a minimal resolution. Such a homogeneous resolution is minimal if and only if all the maps $F_i \to F_{i-1}$ have the range in $(x_1, \ldots, x_n)F_{i-1}$. (See Exercise 6.9.)

In the homogeneous case we may make a finer partition of the b_i, as follows. We already know that M is minimally generated by b_0 homogeneous elements, but the set of such b_0 elements is the union of sets of b_{0j} elements of degree j. So we write R^{b_0} more finely as $\oplus_j R^{b_{0j}}[-j]$, where $[-j]$ indicates a shift in the grading. An element of degree n in $R^{b_{0j}}[-j]$ is an element of degree $n-j$ in $R^{b_{0j}}$. With this shift, the natural map $\oplus_j R^{b_{0j}}[-j] \to M$ even has degree 0. i.e., the chosen homogeneous basis elements of $R^{b_{0j}}[-j]$ map to the homogeneous generators of M of degree j. Once we have rewritten R^{b_i} with the finer grading, then a minimal homogeneous generating set of the kernel can be also partitioned into its degrees, so that we can rewrite each R^{b_i} as $\oplus_j R^{b_{ij}}[-j]$. For example, the following is a resolution of the homogeneous $k[x,y,z]$-module $M = R/(x^2, xy, yz^2, y^4)$:

$$0 \to R[-7] \xrightarrow{\begin{bmatrix} 0 \\ y^3 \\ -z^2 \\ x \end{bmatrix}} \begin{matrix} R[-3] \\ \oplus \\ R[-4] \\ \oplus \\ R[-5] \\ \oplus \\ R[-6] \end{matrix} \xrightarrow{\begin{bmatrix} -y & 0 & 0 & 0 \\ x & -z^2 & -y^4 & 0 \\ 0 & x & 0 & -y^2 \\ 0 & 0 & x & z^2 \end{bmatrix}} \begin{matrix} R[-2]^2 \\ \oplus \\ R[-3] \\ \oplus \\ R[-4] \end{matrix} \xrightarrow{\begin{bmatrix} x^2 & xy & yz^2 & y^4 \end{bmatrix}} R \to 0.$$

Note that the columns of matrices correspond to homogeneous relations; and even though say the third column in the big matrix has non-zero entries $-y^3$ and x, it is homogeneous, as $-y^3$ is multiplying xy of degree 2 and x is multiplying y^4 of degree 4, so the relation is homogeneous of degree $3+2 = 1+4$, which accounts for the summand $R[-5]$. A symbolic computer algebra program, such as Macaulay 2, would record these b_{ij} in the following Betti diagram:

	0	1	2	3
0 :	1			
1 :		2	1	
2 :		1	1	
3 :		1	1	
4 :			1	1

A non-zero entry m in row i and column j denotes that R^{b_j} has m copies of $R[-i-j]$. The i is subtracted as at least that much of a shift is expected. Note that the zeroes are simply left blank in the diagram. There are other notions related to these fined-tuned Betti numbers: Hilbert functions, Castelnuovo-Mumford regularity, etc.

A resolution is called **pure** if each R_{b_i} is concentrated in one degree, i.e., if for each i, $b_i = b_{ij}$ for some j. There is recent work of Eisenbud and Schreyer (and Weyman, Floystad, Boij, Söderberg), that the Betti diagram of any finitely generated Cohen–Macaulay module is a positive linear combinations (with coefficients in $\mathbb{Q}_+$) of Betti diagrams of finitely many modules with pure resolutions. This is one of the more exciting recent results in commutative algebra and algebraic geometry. As a consequence it has that the multiplicity conjecture of Huneke and Srinivasan holds, and also proves the convexity of a fan naturally associated to the Young lattice.

7. Injective resolutions. Let M be an R-module. An **injective resolution** of M is a co-complex

$$0 \to I^0 \to I^1 \to I^2 \to I^3 \to \cdots,$$

where the I^n are injective modules over R (definition of injective modules is in Section 24) and where

$$0 \to M \to I^0 \to I^1 \to I^2 \to I^3 \to \cdots$$

is exact. We sometimes call the latter exact co-complex an injective resolution. Injective resolutions are not uniquely determined.

8. Commutative diagrams. In addition to complexes we will be drawing commutative diagrams.

Definition 1.6 *A* **commutative diagram** *of groups (resp. R-modules) is any directed graph whose vertices are groups (resp. modules) and whose directed edges are homomorphisms with the extra condition for any vertices A and B, the composition of homomorphisms starting from vertex A and ending at vertex B is independent of the path from A to B.*

We will define projective and injective modules in terms of commutative diagrams. (See Sections 5 and 24.) The commutativity of a diagram is often marked by saying so or also by using the symbol $\circlearrowleft$ inside the region surrounded by any two paths that yield the same composition.

9. Where do complexes arise.

(1) We have seen free resolutions, with and without the module that they are resolving. We will develop projective and injective resolutions later.

(2) **Chain complexes:** A **simplicial complex** (the word "complex" in "simplicial complex" is not a homological term) is a finite collection of points, finite line segments, solid triangles, solid tetrahedra... in a finite-dimensional real space with the proviso that the intersection of any such parts is either empty or it is a subface of each intersectand (subfaces of a line segment are the two endpoints, subfaces of triangles are its three edges and its three corner points, ...). I give a more precise definition of an abstraction of this where again the word "complex" is not homological: an **abstract simplicial complex** is collection Δ of subsets of a finite set X with the proviso that for any $A \in \Delta$ and any $B \subseteq A$, B is also in Δ. The points, line segments, solid triangles, solid tetrahedra in the simplicial complex are geometric realizations of abstract simplicial complexes. (A **simplex** is the (abstract) simplicial complex consisting of all subsets of a finite set.) From any abstract simplicial complex Δ we define a complex over a field k or over $\mathbb{Z}$ in the homological sense as follows. The module C_s is a free module whose basis consists of elements of Δ of cardinality $s+1$. To define the maps $C_s \to C_{s-1}$ we need to choose appropriate signs, and it is easiest if we do so by ordering all the elements of X appearing in Δ. So say that these are $a_1, \ldots, a_d$. Then $\delta_s : C_s \to C_{s-1}$ is defined for $1 \le i_0 < i_1 < \cdots < i_s \le d$ as follows:

$$\delta_s([a_{i_0}, \ldots, a_{i_s}]) = \sum_{j=0}^{s} (-1)^j [a_{i_0}, \ldots, \widehat{a_{i_j}}, \ldots, a_{i_s}],$$

where the hat over an element means the omission. Then

$$\delta_{s-1} \circ \delta_s([a_{i_0}, \ldots, a_{i_s}]) = \sum_{j=0}^{s} (-1)^j \left(\sum_{l=0}^{j} (-1)^l [a_{i_0}, \ldots, \widehat{a_{i_l}}, \ldots, \widehat{a_{i_j}}, \ldots, a_{i_s}] \right.$$
$$\left. + \sum_{l=j+1}^{s} (-1)^{l-1} [a_{i_0}, \ldots, \widehat{a_{i_j}}, \ldots, \widehat{a_{i_l}}, \ldots, a_{i_s}] \right),$$

and for any $p < q$ between 1 and $s+1$, the coefficient of $[a_{i_0}, \ldots, \widehat{a_{i_p}}, \ldots, \widehat{a_{i_q}}, \ldots, a_{i_s}]$ in this expression is $(-1)^{q+p} + (-1)^{p+q-1} = 0$. Thus (C_s, δ_s) is a complex. It is called the **chain complex**. The chain complex also includes C_{-1} corresponding to the empty set, and often that is omitted to get the **reduced homology**. Then the rank of $H_0(C_\bullet)$ is the number of connected components of Δ, and the ranks of higher homology modules also have geometric meanings (describe).

(3) Chain complexes with similarly defined maps also arise in **singular homology** of CW complexes: starting with a topological space X, we let $C_s(X)$ be the free abelian group (or a module over a ring R) generated by singular n-simplices on X (i.e., continuous functions from the standard n-simplex to X).

(4) **Topological data analysis:** Let X be a finite subset of a metric space. For any real number $\alpha \geq 0$ the **Vietoris-Rips** complex of X with parameter α is the abstract simplicial complex on X with elements being all subsets of X of diameter at most α. The **Čech complex** of X with parameter α is the abstract simplicial complex with elements being all subsets A of X for which $\cap_{x \in A} B(x, \alpha)$ is not empty. The chain complexes and their homologies arising from the Vietoris-Rips and Čech complexes are used to infer certain features of possibly complex data. My source for topological data analysis is [3].*

(5) Let $R = k[x_1, \ldots, x_n]$ be a polynomial ring in variables $x_1, \ldots, x_n$ over a field k. Let $m_1, \ldots, m_d$ be monomials in R. The **Taylor complex** of $m_1, \ldots, m_d$ is the complex whose sth module C_s is the free module whose basis consists of subsets of $\{m_1, \ldots, m_d\}$ of cardinality s and for which $\delta_s : C_s \to C_{s-1}$ is defined on the summand corresponding to the subset $\{m_{i_1}, \ldots, m_{i_s}\}$ with $i_1 < i_2 < \cdots < i_s$ as

$$\delta_s([m_{i_1}, \ldots, m_{i_s}]) = \sum_{j=1}^{s} (-1)^{j-1} \frac{\operatorname{lcm}\{m_{i_1}, \ldots, m_{i_s}\}}{\operatorname{lcm}\{m_{i_1}, \ldots, \widehat{m_{i_j}}, \ldots, m_{i_s}\}} [m_{i_1}, \ldots, \widehat{m_{i_j}}, \ldots, m_{i_s}].$$

The proof that (C_s, δ_s) is a complex is similar to the proof for chain complexes. What is true is that Taylor complexes are free resolutions of $R/(m_1, \ldots, m_d)$. This

* Leopold Vietoris was born in Bad Radkersberg, which is now in Austria, in 1891, and he died in Innsbruck, Austria, in the year 2002 at the age of 110 years and 309 days. He stopped skiing at age 80 and he stopped climbing mountains at age 90. His last mathematical paper was published at age 103.

was proved by Diana Taylor in her Ph.D. thesis in 1965. She never published a paper, but her thesis is widely cited. See Exercise 7.8 for more on these complexes.

(6) Let $x_1, \dots, x_d$ be elements of R and M an R-module. Define C_s to be the direct sum of copies of M, one copy for each subset of $\{x_1, \dots, x_d\}$ of cardinality s. On the summand of C_s corresponding to the subset $\{x_{i_1}, \dots, x_{i_s}\}$ with $i_1 < i_2 < \cdots < i_s$, the map $\delta_s : C_s \to C_{s-1}$ is defined as

$$\delta_s(m[x_{i_1}, \dots, x_{i_s}]) = m \sum_{j=1}^{s} (-1)^{j-1} x_{i_j} [x_{i_1}, \dots, \widehat{x_{i_j}}, \dots, x_{i_s}].$$

The proof that (C_s, δ_s) is a complex is similar to the proof for chain complexes. This complex is called the **Koszul complex** of M with respect to $x_1, \dots, x_d$. More on Koszul complexes is on pages 19, in Exercise 4.11, Section 4, Proposition 12.5.

(7) If M is a smooth manifold, let $\Omega^s(M)$ be the real vector space of differential s-forms. Let $\delta^s : \Omega^s(M) \to \Omega^{s+1}(M)$ be the exterior derivative with the plus/minus signs just as in chain complexes. This gives rise to a co-complex whose cohomology is called **de Rham cohomology** of M.

(8) Let M be an R-module and $x_1, \dots, x_d$ elements of R whose product is not nilpotent. We define

$$C^s = \oplus_{1 \le i_1 < i_2 < \cdots < i_s \le d} M_{x_{i_1} \cdot x_{i_2} \cdots x_{i_s}}.$$

The summands of C_s are localizations of M at the multiplicatively closed sets generated by products of the listed elements. We define $\delta^s : C^s \to C^{s+1}$ as follows. For any $m \in M_{x_{i_1} \cdot x_{i_2} \cdots x_{i_s}}$ we define the component of $\delta^s(m)$ in $M_{x_j x_{i_1} \cdot x_{i_2} \cdots x_{i_s}}$ to be 0 if $j \in \{i_1, \dots, i_s\}$, and otherwise equal to the image of m times the sign of the insertion of j into the ordered set $\{i_1, \dots, i_s\}$. This makes (C^s, δ^s) a bounded co-complex, called the **Čech co-complex** of M with respect to $x_1, \dots, x_d$. The cohomology of this complex is called the Čech cohomology.

10. Exactness criteria. Here are a few general criteria for exactness, starting with fairly vague ones:

(1) from theoretical aspects;

(2) after a concrete computation, possibly via Gröbner bases;

(3) Buchsbaum–Eisenbud criterion (see Theorem 29.6);

(4) knowledge of special complexes and their properties, such as Koszul complexes, the Hilbert-Burch complex (see Exercise 1.10)...;

(5) and a more concrete tool/answer: the Snake Lemma. A proof requires some diagram chasing, which is left to the reader.

Lemma 1.7 (Snake Lemma) *Assume that the rows in the following commutative diagram are exact:*

$$\begin{tikzcd}
 & A \arrow[r, "a"] \arrow[d, "\alpha"] \arrow[dr, phantom, "\circlearrowleft"] & B \arrow[r, "b"] \arrow[d, "\beta"] \arrow[dr, phantom, "\circlearrowleft"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A' \arrow[r, "a'"] & B' \arrow[r, "b'"] & C'. &
\end{tikzcd}$$

Then

$$\ker\alpha \to \ker\beta \to \ker\gamma \xrightarrow{\Delta} \operatorname{coker}\alpha \to \operatorname{coker}\beta \to \operatorname{coker}\gamma$$

is exact, where the first two maps are the restrictions of a and b, respectively, the last two maps are the natural maps induced by a' and b', respectively, and the middle map Δ is the so-called **connecting homomorphism**.

In addition, if a is injective, so is $\ker\alpha \to \ker\beta$; and if b' is surjective, so is $\operatorname{coker}\beta \to \operatorname{coker}\gamma$.

The connecting homomorphism is defined as follows. Let $x \in \ker\gamma$. Since b is surjective, there exists $y \in B$ such that $x = b(y)$. Since the diagram commutes, $b' \circ \beta(y) = \gamma \circ b(y) = \gamma(x) = 0$, so that $\beta(y) \in \ker b' = \operatorname{im} a'$. Thus $\gamma(y) = a'(z)$ for some $z \in A'$. Then we define $\Delta(x)$ as the image of z in $\operatorname{coker}\alpha$. The reader should verify that this is a well-defined map.

Thus if a is injective, b' is surjective, and α and γ are isomorphisms, then β is an isomorphism as well.

11. Why study homological algebra? This is very brief, as I hope that the rest of the course justifies the study of this material. Exactness and non-exactness of certain complexes yields information on whether a ring in question is regular, Cohen–Macaulay, Gorenstein, what is the depth of a particular ideal, what its dimensions (Krull, projective, injective, etc.) are, and so on. While one has other tools to determine such non-singularity properties, homological algebra is often an excellent, convenient, and sometimes the best tool.

Exercise 1.8 Let $0 \to M_1 \xrightarrow{g} M_2 \xrightarrow{h} M_3 \to 0$ be a short exact sequence of R-modules. Consider the following conditions:

(1) There exists an R-module homomorphism $f : M_3 \to M_2$ such that $h \circ f = \mathrm{id}_{M_3}$.

(2) There exists an R-module homomorphism $e : M_2 \to M_1$ such that $e \circ g = \mathrm{id}_{M_1}$.

(3) $M_2 \cong M_3 \oplus M_1$.

Prove that (1) implies (3) and that (2) implies (3).

Exercise 1.9 Let R be a domain and I a non-zero ideal such that for some $n, m \in \mathbb{N}_0$, $R^n \cong R^m \oplus I$. The goal is to prove that I is free.

(1) Use linear algebra and localization to prove that $m + 1 = n$.

(2) Let $0 \to R^{n-1} \xrightarrow{A} R^n \to I \to 0$ be a short exact sequence. (Why does it exist?) Let d_j be $(-1)^j$ times the determinant of the submatrix of A obtained by deleting the jth row. Let d be the transpose of the vector $[d_1, \ldots, d_n]$. Prove that $Ad = 0$.

(3) Define a map g from I to the ideal generated by all the d_i sending the image of a basis vector of R^n to d_j. Prove that g is a well-defined homomorphism.

(4) Prove that $I \cong (d_1, \ldots, d_n)$.

(5) Prove that $(d_1, \ldots, d_n) = R$. (Hint: tensor the short exact sequence with R modulo some maximal ideal of R.)

Exercise 1.10 The Hilbert–Burch Theorem. Let R be a commutative Noetherian ring. Let A be an $n \times (n-1)$ matrix with entries in R and let d_j be the determinant of the matrix obtained from A by deleting the jth row. Suppose that the ideal $(d_1, \ldots, d_n)$ contains a non-zerodivisor. Let I be the cokernel of the matrix A. Prove that $I = t(d_1, \ldots, d_n)$ for some non-zerodivisor $t \in R$.

2 Complexes and functors

1. Functors. What underlies much of homological algebra are the functors. In our context, a **functor** $\mathcal{F}$ is a function from the category of groups or R-modules to a similar category, so that for each object M in the domain category, $\mathcal{F}(M)$ is an object in the codomain category, for each morphism in the domain category, $\mathcal{F}(f)$ is a morphism in the codomain category, $\mathcal{F}(\mathrm{id}_M) = \mathrm{id}_{\mathcal{F}(M)}$ for all M in the domain category, and such that one additional condition is satisfied. This condition is different for covariant and contravariant functors. We say that $\mathcal{F}$ is **covariant** if for all $f : M \to N$, $\mathcal{F}(f) : \mathcal{F}(M) \to \mathcal{F}(N)$ and if for all $g : N \to P$, $\mathcal{F}(g \circ f) = \mathcal{F}(f) \circ \mathcal{F}(g)$. We say that $\mathcal{F}$ is **contravariant** if for all $f : M \to N$, $\mathcal{F}(f) : \mathcal{F}(N) \to \mathcal{F}(M)$ and if for all $g : N \to P$ we have $\mathcal{F}(f \circ g) = \mathcal{F}(g) \circ \mathcal{F}(f)$.

Objects in all our categories will be algebraic structures such as modules over a fixed ring R, and all morphisms are R-module homomorphisms. For any two objects M and N in such a category, the set $\mathrm{Hom}(M, N)$ of all morphisms from M to N is an R-module. All our functors will be **additive**, in the sense that for all objects M, N, if $\mathcal{F}$ is covariant, then the map $\mathrm{Hom}(M, N) \to \mathrm{Hom}(\mathcal{F}(M), \mathcal{F}(N))$ is an additive homomorphism, and if $\mathcal{F}$ is contravariant, then the map $\mathrm{Hom}(M, N) \to \mathrm{Hom}(\mathcal{F}(N), \mathcal{F}(M))$ is an additive homomorphism. In particular, for such $\mathcal{F}$, $\mathcal{F}$ takes the zero homomorphism to the zero homomorphism.

The following are easy from the definitions:

Lemma 2.1 *A functor takes isomorphisms to isomorphisms. An additive functor takes complexes to complexes.* □

2. Examples of functors. Let $(C_\bullet, d_\bullet) = \cdots \to C_n \xrightarrow{d_n} C_{n-1} \xrightarrow{d_{n-1}} C_{n-2} \to \cdots$ be a complex of R-modules.

(1) **Identity functor:** The result is $(C_\bullet, d_\bullet)$.

(2) **Localization** at a multiplicatively closed subset W of R is a functor. The resulting complex is

$$W^{-1}C_\bullet = \cdots \to W^{-1}C_n \xrightarrow{W^{-1}d_n} W^{-1}C_{n-1} \xrightarrow{W^{-1}d_{n-1}} W^{-1}C_{n-2} \to \cdots$$

is a complex because the localization of a zero map is still zero. If $C_\bullet$ is exact at the nth place, so is $W^{-1}C_\bullet$. When W consists of units only, then localization at W is the same as the identity functor.

(3) If M is an R-module, then the **tensor product** $\_ \otimes_R M$ is a functor. (A review of tensor products can be found in Appendix A.)

$$C_\bullet \otimes_R M: \qquad \cdots \to C_n \otimes_R M \xrightarrow{d_n \otimes \mathrm{id}} C_{n-1} \otimes_R M \xrightarrow{d_{n-1} \otimes \mathrm{id}} C_{n-2} \otimes_R M \to \cdots.$$

Localization is a special case of tensor products.

(4) If M is an R-module, then **Hom from M**, denoted $\mathrm{Hom}_R(M, \_)$, is a functor. The resulting $\mathrm{Hom}_R(M, C_\bullet)$ is as follows:

$$\cdots \to \mathrm{Hom}(M, C_n) \xrightarrow{\mathrm{Hom}(M,d_n)} \mathrm{Hom}_R(M, C_{n-1}) \xrightarrow{\mathrm{Hom}(M,d_{n-1})} \mathrm{Hom}_R(M, C_{n-2}) \to \cdots,$$

where $\mathrm{Hom}(M, d_n) = d_n \circ \_$.

(5) If M is an R-module, then **Hom into M**, denoted $\mathrm{Hom}_R(\_, M)$, is a contravariant functor. The resulting $\mathrm{Hom}_R(C_\bullet, M)$ is as follows:

$$\cdots \to \mathrm{Hom}(C_{n-1}, M) \xrightarrow{\mathrm{Hom}(d_n,M)} \mathrm{Hom}_R(C_n, M) \xrightarrow{\mathrm{Hom}(d_{n+1},M)} \mathrm{Hom}_R(C_{n+1}, M) \to \cdots,$$

where $\mathrm{Hom}(d_n, M) = \_ \circ d_n$.

(6) Let J be an ideal in R. For any R-module M, define the **global sections on M with support in J** to be $\Gamma_J(M) = \{m \in M : J^n m = 0 \text{ for some positive integer } n\}$. Then Γ_J is a covariant functor with the induced maps being the restriction maps, and

$$\Gamma_J(C_\bullet) = \qquad \cdots \to \Gamma_J(C_n) \to \Gamma_J(C_{n-1}) \to \Gamma_J(C_{n-2}) \to \cdots.$$

If $C_\bullet$ is an injective resolution of an R-module M, then $C_\bullet$ and $\Gamma_J(C_\bullet)$ are cocomplexes (despite writing "$C_\bullet$"), and the cohomologies of $\Gamma_J(C_\bullet)$ are the **local cohomology** modules of M with support in J.

Definition 2.2 *If $\mathcal{F}$ is covariant functor, we say that it is* **left-exact** *if $0 \to \mathcal{F}(A) \to \mathcal{F}(B) \to \mathcal{F}(C)$ is exact for every short exact sequence $0 \to A \to B \to C \to 0$, and we say that it is* **right-exact** *if $\mathcal{F}(A) \to \mathcal{F}(B) \to \mathcal{F}(C) \to 0$ is exact for every short exact sequence $0 \to A \to B \to C \to 0$.*

If $\mathcal{F}$ is contravariant functor, we say that it is **left-exact** *if $0 \to \mathcal{F}(C) \to \mathcal{F}(B) \to \mathcal{F}(A)$ is exact for every short exact sequence $0 \to A \to B \to C \to 0$, and we say that it is* **right-exact** *if $\mathcal{F}(C) \to \mathcal{F}(B) \to \mathcal{F}(A) \to 0$ is exact for every short exact sequence $0 \to A \to B \to C \to 0$.*

Definition 2.3 *An R-module M is* **flat** *if $M \otimes_R \_$ is exact.*

By Exercise 2.6, M is flat if and only if $f \otimes \mathrm{id}_M$ is injective for every injective f. It is straightforward to prove that free modules and localizations of flat modules are flat. (A localization of a free R-module need not be a free R-module.)

Exercise 2.4 Alternative formulations of exactness of functors:

i) Prove that a covariant functor $\mathcal{F}$ is left-exact if and only if $0 \to \mathcal{F}(A) \to \mathcal{F}(B) \to \mathcal{F}(C)$ is exact for every exact complex $0 \to A \to B \to C$.

ii) Prove that a covariant functor $\mathcal{F}$ is right-exact if and only if $\mathcal{F}(A) \to \mathcal{F}(B) \to \mathcal{F}(C) \to 0$ is exact for every exact complex $A \to B \to C \to 0$.

iii) Prove that a contravariant functor $\mathcal{F}$ is left-exact if and only if $0 \to \mathcal{F}(C) \to \mathcal{F}(B) \to \mathcal{F}(A)$ is exact for every exact complex $A \to B \to C \to 0$.

iv) Prove that a contravariant functor $\mathcal{F}$ is right-exact if and only if $\mathcal{F}(C) \to \mathcal{F}(B) \to \mathcal{F}(A) \to 0$ is exact for every exact complex $0 \to A \to B \to C$.

Exercise 2.5 Prove that M is flat if and only if $\_ \otimes_R M$ is exact.

Exercise 2.6 Let R be a ring and M a left R-module.

(1) Prove that $\mathrm{Hom}_R(M, \_)$ and $\mathrm{Hom}_R(\_, M)$ are left-exact.

(2) Prove that $M \otimes_R \_$ and $\_ \otimes_R M$ are right-exact.

(3) Determine the exactness properties of $\Gamma_J(\_)$.

3 General manipulations of complexes

We saw in the previous section some manipulations of complexes with functors. This section contains some further manipulations.

Let $C_\bullet = (C_\bullet, d_\bullet) = \cdots C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \to \cdots$ be a complex.

1. Shifting: For any complex $C_\bullet$ and any $m \in \mathbb{Z}$ we denote by $C_\bullet[m]$ the complex whose nth module is $C[m]_n = C_{n+m}$ and whose nth map $C[m]_n \to C[m]_{n-1}$ is the map d_{n+m}.

2. Taking homology: From a complex $C_\bullet$ we can form the homology complex $H(C_\bullet)$, where the nth module is $H_n(C_\bullet)$, and all the complex maps are zero (which we may think of as the maps induced by the original complex maps). These complexes are not very interesting on their own, but the homology modules of one complex interact with homology modules in other complexes, and that is where homological algebra gets interesting.

Below are some established homology names; much more about these homology modules appears in the rest of the notes.

(1) **Tor:** If M and N are R-modules, and if $F_\bullet$ is a projective resolution of M, then $\mathrm{Tor}_n^R(M,N) = H_n(F_\bullet \otimes N)$. It takes some work to prove that $\mathrm{Tor}_n^R(M,N) \cong \mathrm{Tor}_n^R(N,M)$, or in other words, that if $G_\bullet$ is a projective resolution of N, then $\mathrm{Tor}_n^R(M,N) \cong H_n(M \otimes G_\bullet)$. (See Section 8.)

(2) **Ext:** If M and N are R-modules, and if $F_\bullet$ is a projective resolution of M, then $\mathrm{Ext}_R^n(M,N) = H^n(\mathrm{Hom}_R(F_\bullet, N))$. It takes some work to prove that $\mathrm{Ext}_R^n(M,N) \cong H^n(\mathrm{Hom}_R(M, I^\bullet))$, where $I^\bullet$ is an injective resolution of N. (See Section 20.)

(3) **Local cohomology:** If M is an R-module and J is an ideal in R, then the nth local cohomology of M with respect to J is $H_J^n(M) = H^n(\Gamma_J(I))$, where $I^\bullet$ is an injective resolution of M. (This may be expanded in a future section.)

3. Tensor product of complexes: Let $K_\bullet = \cdots \to K_n \xrightarrow{e_n} K_{n-1} \xrightarrow{e_{n-1}} K_{n-2} \to \cdots$ be another complex of R-modules. We can form a tensor product of the two complexes, which can be considered as a **bicomplex**, as follows:

$$\begin{array}{ccccccc}
\downarrow & & \downarrow & & \downarrow & & \\
C_n \otimes K_m & \to & C_{n-1} \otimes K_m & \to & C_{n-2} \otimes K_m & \to \\
\downarrow & & \downarrow & & \downarrow & & \\
C_n \otimes K_{m-1} & \to & C_{n-1} \otimes K_{m-1} & \to & C_{n-2} \otimes K_{m-1} & \to \\
\downarrow & & \downarrow & & \downarrow & &
\end{array}$$

where the vertical and horizontal maps are the naturally induced maps, where the horizontal maps are as expected $d_\bullet \otimes \mathrm{id}$ and where the vertical maps are **signed** by the degrees in $C_\bullet$, meaning that the map $C_n \otimes K_m \to C_n \otimes K_{m-1}$ is $(-1)^n \mathrm{id}_{C_n} \otimes e_m$. (Think of this latter map as the differential – on $K_\bullet$ – crossing n components on the left, and each n changes the sign.) Note that this bicomplex is a complex along all vertical and along all horizontal strands.

However, this bicomplex has a complex structure called the **total complex** as follows: the nth module is $G_n = \sum_i C_i \otimes K_{n-i}$, and the map $g_n : G_n \to G_{n-1}$ is defined on the summand $C_i \otimes K_{n-i}$ as $d_i \otimes \mathrm{id}_{K_{n-i}} + (-1)^i \mathrm{id}_{C_i} \otimes e_{n-i}$, where the first summand has image in $C_{i-1} \otimes K_{n-i}$ and the second has image in $C_i \otimes K_{n-i-1}$. This new construction is a complex:

$$\begin{aligned} g_{n-1} \circ g_n|_{C_i \otimes K_{n-i}} &= g_{n-1}(d_i \otimes \mathrm{id}_{K_{n-i}} + (-1)^i \mathrm{id}_{C_i} \otimes e_{n-i}) \\ &= d_{i-1} \circ d_i \otimes \mathrm{id}_{K_{n-i}} + (-1)^{i-1} d_i \otimes e_{n-i} \\ &\quad + (-1)^i d_i \otimes e_{n-i} + (-1)^i (-1)^i \mathrm{id}_{C_i} \otimes e_{n-i-1} \circ e_{n-i} \\ &= 0. \end{aligned}$$

4. Direct sum of complexes: If $K_\bullet = \cdots \to K_n \xrightarrow{e_n} K_{n-1} \xrightarrow{e_{n-1}} K_{n-2} \to \cdots$ is another complex of R-modules, then the nth module of the direct sum $C_\bullet \oplus K_\bullet$ is $C_n \oplus K_n$ and the nth map is (d_n, e_n). (We saw in the section starting on page 8 and we will see in Section 4, Theorem 7.4 (and other places: HERE: list) **more meaningful** maps on the direct sum of complexes.)

Definition 3.1 *A* **map of complexes** *is a function $f_\bullet : C_\bullet \to C_\bullet{}'$, where $(C_\bullet, d)$ and $(C_\bullet{}', d')$ are complexes, where $f_\bullet$ restricted to C_n is denoted f_n, where f_n maps to C'_n, and such that for all n, $d'_n \circ f_n = f_{n-1} \circ d_n$. We can draw this as a commutative diagram:*

$$\begin{array}{ccccccc} \cdots \to & C_{n+1} & \xrightarrow{d_{n+1}} & C_n & \xrightarrow{d_n} & C_{n-1} & \to \cdots \\ & \downarrow f_{n+1} & & \downarrow f_n & & \downarrow f_{n-1} & \\ \cdots \to & C'_{n+1} & \xrightarrow{d'_{n+1}} & C'_n & \xrightarrow{d'_n} & C'_{n-1} & \to \cdots \end{array}$$

It is clear that the kernel and the image of a map of complexes are naturally complexes. Thus we can talk about **(exact) complexes of complexes**, and in particular about **short exact sequences of complexes**, and the following is straightforward:

Remark 3.2 Let $f_\bullet : C_\bullet \to C_\bullet{}'$ be a map of complexes. Then we get the **induced map** $f_* : H(C_\bullet) \to H(C_\bullet{}')$ of complexes.

Examples of short exact sequences of complexes are constructed in Theorem 4.2, in Theorem 7.4, ...

Theorem 3.3 (**Short exact sequence of complexes yields a long exact sequence on homology**) *Let $0 \to C_\bullet{}' \xrightarrow{f_\bullet} C_\bullet \xrightarrow{g_\bullet} C_\bullet{}'' \to 0$ be a short exact sequence of complexes. Then we have a long exact sequence on homology:*

$$\cdots \to H_{n+1}(C_\bullet{}'') \xrightarrow{\Delta_{n+1}} H_n(C_\bullet{}') \xrightarrow{f} H_n(C_\bullet) \xrightarrow{g} H_n(C_\bullet{}'') \xrightarrow{\Delta_n} H_{n-1}(C_\bullet{}') \xrightarrow{f} H_{n-1}(C_\bullet) \to \cdots$$

where the arrows denoted by f and g are only induced by $f_\bullet$ and $g_\bullet$, and the Δ maps are the connecting homomorphisms as in Lemma 1.7.

Proof. By assumption the following are commutative diagrams with exact rows for all n:

$$\begin{array}{ccccccc} 0 \to & C'_n & \xrightarrow{f_n} & C_n & \xrightarrow{g_n} & C''_n & \to 0 \\ & \downarrow d'_n & & \downarrow d_n & & \downarrow d''_n & \\ 0 \to & C'_{n-1} & \xrightarrow{f_{n-1}} & C_{n-1} & \xrightarrow{g_{n-1}} & C''_{n-1} & \to 0. \end{array}$$

Consider the naturally commuting diagram:

$$\begin{array}{ccccccc} & \operatorname{coker} d'_{n+1} & \xrightarrow{f_{n+1}} & \operatorname{coker} d_{n+1} & \xrightarrow{g_{n+1}} & \operatorname{coker} d''_{n+1} & \to 0 \\ & \downarrow d'_n & & \downarrow d_n & & \downarrow d''_n & \\ 0 \to & \ker d'_{n-1} & \xrightarrow{f_{n-1}} & \ker d_{n-1} & \xrightarrow{g_{n-1}} & \ker d''_{n-1}. & \end{array}$$

By the Snake Lemma (Lemma 1.7) the rows are exact for all n. Another application of Lemma 1.7 yields exactly a part of the desired sequence. One still has to verify that the induced map f on $H_n(C_\bullet{}') \to H_n(C_\bullet)$ obtained from the cokernel row is identical to the induced map f on $H_n(C_\bullet{}') \to H_n(C_\bullet)$ when constructed via the kernel row, but this is just what "induced by f" is. Thus the constructed part of the sequence can be extended into the desired full long exact sequence. $\square$

The following is now immediate:

Corollary 3.4 *Let $0 \to C_\bullet{}' \to C_\bullet \to C_\bullet{}'' \to 0$ be a short exact sequence of complexes. If two of the modules have zero homology, so does the third.* $\square$

Corollary 3.5 *If $f_\bullet$ is a map of complexes that is an isomorphism, then the induced f_* is an isomorphism on homology.*

Proof. We can make $f_\bullet$ part of a short exact sequence of complexes with the other map being 0. Since the zero map of complexes induces the zero map on homologies, the conclusion follows from the long exact sequence in Theorem 3.3. $\square$

Definition 3.6 *A map $f_\bullet : C_\bullet \to C_\bullet{}'$ (of degree 0) of complexes is* **null-homotopic** *if for all n there exist maps $s_n : C_n \to C'_{n+1}$ such that $f_n = d'_{n+1} \circ s_n + s_{n-1} \circ d_n$. Maps $f_\bullet, g_\bullet : C_\bullet \to C_\bullet{}'$ are* **homotopic** *if $f_\bullet - g_\bullet$ is null-homotopic.*

The diagram for $f_\bullet$ being null-homotopic is as follows:

$$\begin{tikzcd} \cdots \arrow[r] & C_{n+1} \arrow[r, "d_{n+1}"] \arrow[d, "f_{n+1}"] & C_n \arrow[r, "d_n"] \arrow[d, "f_n"] \arrow[dl, "s_n"'] & C_{n-1} \arrow[r, "d_{n-1}"] \arrow[d, "f_{n-1}"] \arrow[dl, "s_{n-1}"'] & C_{n-2} \arrow[r, "d_{n-2}"] \arrow[d, "f_{n-2}"] \arrow[dl, "s_{n-2}"'] & \cdots \\ \cdots \arrow[r] & C'_{n+1} \arrow[r, "d'_{n+1}"] & C'_n \arrow[r, "d'_n"] & C'_{n-1} \arrow[r, "d'_{n-1}"] & C'_{n-2} \arrow[r, "d'_{n-2}"] & \cdots \end{tikzcd}$$

Proposition 3.7 *If $f_\bullet$ and $g_\bullet$ are homotopic, then $f_* = g_*$ (recall Remark 3.2).*

Proof. By assumption there exist maps $s_n : C_n \to C'_{n+1}$ such that for all n, $f_n - g_n = d'_{n+1} \circ s_n + s_{n-1} \circ d_n$. If $z \in \ker d_n$, then $f_n(z) - g_n(z) = d'_{n+1} \circ s_n(z)$ is zero in $H_n(C_\bullet{}')$.$\square$

The following is straightforward from the definitions (and no proof is provided here):

Proposition 3.8 *If $f_\bullet$ and $g_\bullet$ are homotopic, so are*

(1) $f_\bullet \otimes \mathrm{id}_M$ *and* $g_\bullet \otimes \mathrm{id}_M$*;*

(2) $\mathrm{Hom}_R(M, f_\bullet)$ *and* $\mathrm{Hom}_R(M, g_\bullet)$*;*

(3) $\mathrm{Hom}_R(f_\bullet, M)$ *and* $\mathrm{Hom}_R(g_\bullet, M)$*;*

Exercise 3.9 Prove that $H_n(C_\bullet \oplus D_\bullet) = H_n(C_\bullet) \oplus H_n(D_\bullet)$.

Exercise 3.10 **(Splitting off of exact summands.)** Let $(R, \mathfrak{m})$ be a Noetherian local ring and $(C_\bullet, d_\bullet)$ a bounded complex of finitely generated free R-modules. Prove that there exist an exact complex $(F_\bullet, f_\bullet)$ and a complex $(E_\bullet, e_\bullet)$ such that for all n, the image of e_n is in $\mathfrak{m}E_{n-1}$ (a minimal complex) and such that $(C_\bullet, d_\bullet) \cong (F_\bullet, f_\bullet) \oplus (E_\bullet, e_\bullet)$. Thus $H_n(C_\bullet) \cong H_n(E_\bullet)$. (Hint: Say that there exists n such that $d_n(C_n) \not\subseteq C_{n-1}$. If we think of d_n as a matrix, then some entry of d_n is not in $\mathfrak{m}$, i.e., it is a unit in R. Let $\varphi : C_{n-1} \to C_{n-1}$ and $\psi : C_n \to C_n$ be R-module isomorphisms such that $\varphi \circ d_n \circ \psi$ is a matrix with entry 1 on the diagonal and zeros elsewhere in its row and column. (This is simply performing row and column reductions.) Set

$$d'_k = \begin{cases} \psi^{-1} \circ d_{n+1}, & \text{if } k = n+1, \\ \varphi \circ d_{n+1} \circ \psi, & \text{if } k = n, \\ d_{n-1} \circ \varphi^{-1}, & \text{if } k = n-1, \\ d_k, & \text{otherwise.} \end{cases}$$

Prove that $(C_\bullet, d_\bullet{}')$ is a complex isomorphic to $(C_\bullet, d_\bullet)$, and the advantage is that in d'_n an obvious exact $0 \to R \xrightarrow{1} R \to 0$ can be split off.)

4 Koszul complexes

Definition 4.1 *Let R be a ring, M a left R-module, and $x \in R$. The* **Koszul complex** *of x and M is*

$$K_\bullet(x;M): \qquad \begin{array}{ccccccc} 0 & \to & M & \xrightarrow{x} & M & \to & 0 \\ & & \uparrow & & \uparrow & & \\ & & 1 & & 0 & & \end{array}$$

where the map labeled x is multiplication by x and where the numbers under M are there only to note which copy of M is considered to be in which numerical place in the complex.

For $x_1, \ldots, x_d \in R$ and an R-module M, the **Koszul complex** *$K_\bullet(x_1, \ldots, x_d; M)$ of $x_1, \ldots, x_d$ and M is the total complex of $K_\bullet(x_1, \ldots, x_{d-1}; M) \otimes K_\bullet(x_d; R)$, defined inductively. It is straightforward to see that $K_\bullet(x_1, \ldots, x_d; M) \cong K_\bullet(x_1, \ldots, x_d; R) \otimes_R M \cong K_\bullet(x_1; M) \otimes K_\bullet(x_2, \ldots, x_d; R)$, et cetera.*

Let's write down $K_\bullet(x_1, x_2; M)$ explicitly. From

$$\begin{pmatrix} 0 & \to & \underset{1}{M} & \xrightarrow{x_1} & \underset{0}{M} & \to & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & \to & \underset{1}{R} & \xrightarrow{x_2} & \underset{0}{R} & \to & 0 \end{pmatrix}$$

we get the total complex (as on page 16)

$$0 \to \underset{1 \quad 1}{M \otimes R} \xrightarrow{\begin{bmatrix} -x_2 \\ x_1 \end{bmatrix}} \underset{1 \quad 0}{M \otimes R} \oplus \underset{0 \quad 1}{M \otimes R} \xrightarrow{\begin{bmatrix} x_1 & x_2 \end{bmatrix}} \underset{0 \quad 0}{M \otimes R} \to 0$$

(Really we do not need to write the numerical subscripts, but it helps the first time in the construction.) This complex is exact at the second place if and only if the ideal (x_1, x_2) contains a non-zerodivisor on M; it is exact in the middle (in the first place) if and only if every equation of the form $ax_1 = bx_2$ with $a, b \in M$ has the property that there exists $c \in M$ with $a = x_2 c$ and $b = x_1 c$. (So x_1, x_2 is a regular sequence on M, see Definition 4.6).

The reader may verify that the following is $K_\bullet(x_1, x_2, x_3; R)$:

$$0 \to R \xrightarrow{\begin{bmatrix} x_3 \\ -x_2 \\ x_1 \end{bmatrix}} R^3 \xrightarrow{\begin{bmatrix} -x_2 & -x_3 & 0 \\ x_1 & 0 & -x_3 \\ 0 & x_1 & x_2 \end{bmatrix}} R^3 \xrightarrow{\begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix}} R \to 0.$$

We next construct the Koszul complex in another way. The first result below is more general.

Theorem 4.2 *Let R be a commutative ring. Let $C_\bullet$ be a complex over R and let $K_\bullet = K_\bullet(x; R)$ be the Koszul complex of $x \in R$. Then there exists a short exact sequence of complexes*

$$0 \to C_\bullet \to C_\bullet \otimes K_\bullet \to C_\bullet[-1] \to 0,$$

where for each n, the map $C_n \to (C_n \otimes R) \oplus (C_{n-1} \otimes R) \cong C_n \oplus C_{n-1}$ takes a to $(a, 0)$, the map $C_n \oplus C_{n-1} \to (C_\bullet[-1])_n = C_{n-1}$ takes (a, b) to b, and the **differential** *$\delta_\bullet$ on $C_\bullet \otimes K_\bullet$ is $\delta_n(a, b) = (d_n(a) + (-1)^n xb, d_{n-1}(b))$.*

Proof. It is straightforward to check that the horizontal levels of $0 \to C_\bullet \to C_\bullet \otimes K_\bullet \to C_\bullet[-1] \to 0$ are short exact sequences of modules and that $\delta_\bullet$ makes all the necessary maps commute. □

Corollary 4.3 *With hypotheses as in Theorem 4.2, we get a long exact sequence*

$$\cdots \xrightarrow{x} H_{n+1}(C_\bullet) \to H_{n+1}(C_\bullet \otimes K_\bullet) \to H_n(C_\bullet) \xrightarrow{x} H_n(C_\bullet) \to H_n(C_\bullet \otimes K_\bullet) \to H_{n-1}(C_\bullet) \xrightarrow{x} \cdots$$

Proof. First of all, $H_n(C_\bullet) = H_{n+1}(C_\bullet[-1])$, so that the long exact sequence above is a consequence of the Theorem 4.2 and of Theorem 3.3. Furthermore, we need to go through the proof of the previous proposition, of Theorem 3.3, and of the Snake Lemma Lemma 1.7, to verify that the connecting homomorphisms are indeed multiplications by x (actually by $(-1)^n x$ on $H_n(C_\bullet)$.). □

The long exact sequence in the corollary breaks into short exact sequences:

$$0 \to \frac{H_i(C_\bullet)}{xH_i(C_\bullet)} \to H_i(C_\bullet \otimes K_\bullet) \to \operatorname{ann}_{H_{i-1}(C_\bullet)}(x) \to 0 \tag{4.4}$$

for all i, where $\operatorname{ann}_M(N)$ denotes the set of all elements of M that annihilate N. In particular, if $C_\bullet$ is the Koszul complex $K_\bullet(x_1, \ldots, x_{n-1}; M)$, then $C_\bullet \otimes K_\bullet(x_n; R)$ is the Koszul complex $K_\bullet(x_1, \ldots, x_n; M)$. This gives an inductive construction of Koszul complexes. The short exact sequences are then:

$$0 \to \frac{H_i(K_\bullet(x_1, \ldots, x_{n-1}; M))}{xH_i(K_\bullet(x_1, \ldots, x_{n-1}; M))} \to H_i(K_\bullet(x_1, \ldots, x_n; M)) \to \operatorname{ann}_{H_{i-1}(K_\bullet(x_1, \ldots, x_{n-1}; M))}(x) \to 0$$

for all i.

Lemma 4.5 *Let M be an R-module and let $x_1, \ldots, x_n$ be elements of R. Then $H_0(K_\bullet(x_1, \ldots, x_n; M)) = M/(x_1, \ldots, x_n)M$.*

Proof. When $n = 1$, the lemma follows easily from the form of the Koszul complex. For $n > 1$, we use the short exact sequences in Equation (4.4) with $i = 0$. Since $K_\bullet(x_1, \ldots, x_{n-1}; M)$ has zero module in degree -1, $H_0(K_\bullet(x_1, \ldots, x_n; M))$ equals $H_0(K_\bullet(x_1, \ldots, x_{n-1}; M))/x_n H_0(K_\bullet(x_1, \ldots, x_{n-1}; M))$, which by induction on n is as stated. □

Definition 4.6 *We say that* $x_1, \ldots, x_n \in R$ *is a* **regular sequence** *on a module* M, *or a* **M-regular sequence** *if* $(x_1, \ldots, x_n)M \neq M$ *and if for all* $i = 1, \ldots, n$, x_i *is a non-zerodivisor on* $M/(x_1, \ldots, x_{i-1})M$. *We say that* $x_1, \ldots, x_n \in R$ *is a* **regular sequence** *if it is a regular sequence on the* R*-module* R.

Whether an element is a non-zerodivisor can be expressed with the **colon** notation, using the symbol ":". So far we have used the colon for grammatical reasons, for naming complexes, for specifying elements of a set, and for defining functions. Another mathematical notation for ":" is with division. Namely, $5 : 3$ is that number which when multiplied by 3 produces 5. Similarly, given some appropriately compatible algebraic structures A, B, C, we define

$$A :_B C$$

as the set of all those elements in B which when multiplied by any element in C produce an element of A. With this notation, saying that $x_1, \ldots, x_n$ is a regular sequence on M is saying that for all $i = 1, \ldots, n$,

$$(x_1, \ldots, x_{i-1})M :_M x_i = (x_1, \ldots, x_{i-1})M.$$

One can also express this with annihilators, namely that for all $i = 1, \ldots, n$,

$$\operatorname{ann}_{\frac{M}{(x_1,\ldots,x_{i-1})M}} x_i = 0_{\frac{M}{(x_1,\ldots,x_{i-1})M}} :_{\frac{M}{(x_1,\ldots,x_{i-1})M}} x_i = 0_{\frac{M}{(x_1,\ldots,x_{i-1})M}}.$$

(0_A is the zero submodule of the module A.)

The following result is a partial exactness criterion for the left end of a Koszul complex.

Theorem 4.7 (Depth sensitivity of the Koszul complex) *Let* M *be an* R*-module and let* $x_1, \ldots, x_n \in R$ *satisfy* $(x_1, \ldots, x_n)M \neq M$. *Suppose that for some* $d \leq n$, $x_1, \ldots, x_d$ *is a regular sequence on* M. *Then*

$$H_i(K_\bullet(x_1, \ldots, x_n; M)) = \begin{cases} 0, & \text{for all } i > n - d; \\ \frac{(x_1,\ldots,x_d)M :_M (x_1,\ldots,x_n)}{(x_1,\ldots,x_d)M}, & \text{for } i = n - d. \end{cases}$$

In particular, if $x_1, \ldots, x_n$ *is a regular sequence on* R, *then* $K_\bullet(x_1, \ldots, x_n; R)$ *is a free resolution of* $R/(x_1, \ldots, x_n)$.

Proof. When $n = 1$, the explicit form of the Koszul complex $K_\bullet(x_1, M)$ shows that $H_1(K_\bullet(x_1, M)) = \operatorname{ann}_M(x_1) = 0_M :_M x_1$ and that $H_0(K_\bullet(x_1, M)) = M/x_1M$. If $d = 1$, then x_1 is a non-zerodivisor on M so that $H_1(K_\bullet(x_1, M)) = 0_M :_M x_1 = 0$, which proves the theorem in this case. If instead $d = 0$, then $H_1(K_\bullet(x_1, M)) = 0_M :_M x_1 = \frac{0_M :_M (x_1)}{0_M}$, which finishes the proof of the theorem in the case $n = 1$.

Now let $n > 1$. By induction on n we have that $H_i(K_\bullet(x_1, \ldots, x_{n-1}; M)) = 0$ for $i > n - 1 - \min\{n-1, d\}$, and that

$$H_{n-1-\min\{n-1,d\}}(K_\bullet(x_1, \ldots, x_{n-1}; M)) = \frac{(x_1, \ldots, x_{\min\{n-1,d\}})M :_M (x_1, \ldots, x_{n-1})}{(x_1, \ldots, x_{\min\{n-1,d\}})M}.$$

By the short exact sequences in Equation (4.4) then $H_i(K_\bullet(x_1,\dots,x_n;M)) = 0$ for $i > n - \min\{n-1,d\}$, and

$$\begin{aligned}
H_{n-\min\{n-1,d\}}(K_\bullet(x_1,\dots,x_n;M)) &= \operatorname{ann}_{H_{n-1-\min\{n-1,d\}}(K_\bullet(x_1,\dots,x_{n-1};M))} x_d \\
&= 0_{\left(\frac{(x_1,\dots,x_{\min\{n-1,d\}})M :_M (x_1,\dots,x_{n-1})}{(x_1,\dots,x_{\min\{n-1,d\}})M}\right)} : x_n \\
&= \frac{(x_1,\dots,x_{\min\{n-1,d\}})M :_M (x_1,\dots,x_{n-1},x_n)}{(x_1,\dots,x_{\min\{n-1,d\}})M}.
\end{aligned}$$

First suppose that $n-1 \ge d$. The we just proved that $H_i(K_\bullet(x_1,\dots,x_n;M)) = 0$ for $i > n-d$ and that

$$H_{n-d}(K_\bullet(x_1,\dots,x_n;M)) = \frac{(x_1,\dots,x_d)M :_M (x_1,\dots,x_{n-1},x_n)}{(x_1,\dots,x_d)M},$$

as desired.

Now suppose that $n-1 < d$. Then $x_1,\dots,x_n$ is a regular sequence, and the above proves that $H_i(K_\bullet(x_1,\dots,x_n;M)) = 0$ for $i > 1$, that $H_1(K_\bullet(x_1,\dots,x_n;M)) = \frac{(x_1,\dots,x_{n-1})M :_M (x_1,\dots,x_n)}{(x_1,\dots,x_{n-1})M} = 0$, and by Lemma 4.5 we know that $H_0(K_\bullet(x_1,\dots,x_n;M))$ is as desired. □

Theorem 4.8 (Depth sensitivity of the Koszul complex) *Let R be a Noetherian ring, let M be a finitely generated R-module, and let $x_1,\dots,x_n \in R$ satisfy $(x_1,\dots,x_n)M \neq M$. Then the largest length of a regular sequence on M contained in the ideal $(x_1,\dots,x_n)$ equals*

$$\max\{r : H_i(K_\bullet(x_1,\dots,x_n;M)) = 0 \text{ for all } i > n-r\}.$$

Proof. We state the proof in stages, and the details of the stages are left for the reader.

(1) For any permutation π on $\{1,\dots,n\}$, $K_\bullet(x_1,\dots,x_n;M)$ is naturally isomorphic to $K_\bullet(x_{\pi(1)},\dots,x_{\pi(n)};M)$, so that all homologies of the two complexes are isomorphic.

(2) Let $y_1 = x_1$, $y_2 = ux_2 + rx_1$, where u is a unit in R and r is an arbitrary element of R. Make an explicit isomorphism of complexes $K_\bullet(x_1,x_2;M)$ and $K_\bullet(y_1,y_2;M)$.

(3) Suppose that $f_\bullet : C_\bullet \to D_\bullet$ is an isomorphism of complexes. Prove that for any $x \in R$, the map $f_\bullet \otimes \mathrm{id}_{K_\bullet(x;R)}$ induces a map of complexes $C_\bullet \otimes K_\bullet(x;R) \to D_\bullet \otimes K_\bullet(x;R)$ that is an isomorphism.

(4) Suppose that for some $d < n$, $x_1,\dots,x_d$ is a regular sequence on M. Suppose that $(x_{d+1},\dots,x_n)$ contains a non-zerodivisor on $M/(x_1,\dots,x_d)M$. Since M is finitely generated over a Noetherian ring, this is equivalent to $(x_{d+1},\dots,x_n)$ not being contained in any of the finitely many associated primes of $M/(x_1,\dots,x_d)M$. Thus by the strengthened form of Prime Avoidance (Exercise 4.15) there exists an element of the form $x_n + \sum_{i=d+1}^{n-1} r_i x_i$ for some $r_i \in R$ that is a non-zerodivisor on $M/(x_1,\dots,x_d)M$.

(5) Use (2) and (3) to replace x_{n-1} and x_n with x_{n-1} and $x_n + r_{n-1}x_{n-1}$ in the Koszul sequence without changing the Koszul homology. Use (1) to switch the new x_{n-1} and x_n. Then use (2) and (3) to replace the new x_{n-2} and x_{n-1} with x_{n-2} and $x_{n-1} + r_{n-2}x_{n-2}$ in the Koszul sequence. Continue until you get that $x_1, \ldots, x_{d+1}$ is a regular sequence without a change in the Koszul homology.

(6) Repeat the steps increasing d until $(x_{d+1}, \ldots, x_n)$ is contained in an associated prime of $M/(x_1, \ldots, x_d)M$.

(7) Use the depth sensitivity of the previous theorem. □

There is yet another way of constructing Koszul complexes, but first we need a few definitions.

If M is an R-module, we define the **n-fold tensor product** $M^{\otimes n}$ **of** M as follows: $M^{\otimes 1} = M$, $M^{\otimes 2} = M \otimes M$, and in general for $n \geq 1$, $M^{\otimes (n+1)} = M^{\otimes n} \otimes M$. It is sensible to define $M^{\otimes 0} = R$.

We define the **nth exterior power of a module** M to be

$$\wedge^n M = \frac{M^{\otimes n}}{\langle m_1 \otimes \cdots \otimes m_n : m_1, \ldots, m_n \in M, m_i = m_j \text{ for some } i \neq j \rangle}.$$

Image of an element $m_1 \otimes \cdots \otimes m_n \in M^{\otimes n}$ in $\wedge^n M$ is written as $m_1 \wedge \cdots \wedge m_n$. Since $0 = (m_1 + m_2) \wedge (m_1 + m_2) = m_1 \wedge m_1 + m_1 \wedge m_2 + m_2 \wedge m_1 + m_2 \wedge m_2 = m_1 \wedge m_2 + m_2 \wedge m_1$, we get that for all $m_1, m_2 \in M$, $m_1 \wedge m_2 = -m_2 \wedge m_1$. Because of this it is easy to verify that if $e_1, \ldots, e_m$ form a basis of R^m, then $\wedge^n R^m$ is generated by $B_{nm} = \{e_{i_1} \wedge \cdots \wedge e_{i_n} : 1 \leq i_1 < i_2 < \cdots < e_{i_n} \leq m\}$. If $m = 1$ or $m = n$, clearly B_{nm} is a basis for $\wedge^n R^m$, and it is a basis for all m, n by induction on m. This proves that $\wedge^n R^m \cong R^{\binom{m}{n}}$.

For any elements $x_1, \ldots, x_d \in R$ we can now define a complex

$$\begin{aligned} &G_\bullet(x_1, \ldots, x_d; R) = \\ &\qquad 0 \to \wedge^d R^d \to \wedge^{d-1} R^d \to \wedge^{d-2} R^d \to \cdots \to \wedge^2 R^d \to \wedge^1 R^d \to \wedge^0 R^d \to 0, \end{aligned}$$

where the map $\wedge^n R^d \to \wedge^{n-1} R^d$ takes the basis element $e_{i_1} \wedge \cdots \wedge e_{i_n}$ to $\sum_{j=1}^n (-1)^{j+1} x_j\, e_{i_1} \wedge \cdots \wedge \widehat{e_{i_j}} \wedge \cdots \wedge e_{i_n}$.

Exercise 4.9 Verify the following:

(1) $G_\bullet(x; R) = K(x; R)$.

(2) $G_\bullet(x_1, \ldots, x_{d-1}; R) \otimes_R G_\bullet(x_d; R) \cong G_\bullet(x_1, \ldots, x_d; R)$.

(3) Verify that $G_\bullet(x_1, \ldots, x_d; R)$ is a complex and that it equals $K_\bullet(x_1, \ldots, x_d; R)$.

Exercise 4.10 Think through Theorem 4.7 without the assumption $(x_1, \ldots, x_n)M \neq M$.

Exercise 4.11 Let R be a commutative ring, let M be an R-module, and let $x_1, \ldots, x_n \in R$. Prove that $H_n(K_\bullet(x_1, \ldots, x_n; M)) = \operatorname{ann}_M(x_1, \ldots, x_n)$.

Exercise 4.12 Let R be a commutative ring, $x_1, \ldots, x_n \in R$, and M an R-module. Prove that $(x_1, \ldots, x_n)$ annihilates each $H_i(K_\bullet(x_1, \ldots, x_n; M))$.

Exercise 4.13 (Depth sensitivity of Koszul complexes) Let $I = (x_1, \ldots, x_n) = (y_1, \ldots, y_m)$ be an ideal in R. Let M be a finitely generated R-module. Suppose that $H_i(K_\bullet(x_1, \ldots, x_n; M)) = 0$ for $i = n, n-1, \ldots, n-l+1$. Prove that $H_i(K_\bullet(y_1, \ldots, y_m; M)) = 0$ for $i = m, m-1, \ldots, m-l+1$.

Exercise 4.14 Let $f : (A_\bullet, d_\bullet) \to (B_\bullet, e_\bullet)$ be a map of complexes. The **mapping cone** of f is the complex $(B_\bullet \oplus A_\bullet[-1], \delta_\bullet)$ with $\delta_n : B_n \oplus A_{n-1} \to B_{n-1} \oplus A_{n-2}$ defined as $\delta_n(b, a) = ((-1)^n f(a) + e_n(b), d_{n-1}(a))$.

i) Prove that $0 \to B_\bullet \to A_\bullet[-1] \oplus B_\bullet \to A_\bullet[-1] \to 0$ is a short exact sequence of complexes.

ii) Prove that the construction in Theorem 4.2 is essentially a mapping cone construction.

Exercise 4.15 (Prime Avoidance) Let I be an ideal contained in the union $\cup_{i=1}^n P_n$, where $P_1, \ldots, P_n$ are prime ideals. Prove that I is contained in one of the P_i. Strengthened form: if I is contained in the Jacobson radical of I and all the P_i except possibly one are prime ideals, then there exists a minimal generator y of I that is not contained in any P_i. (The **Jacobson radical** is the intersection of all the maximal ideals.) Another strengthened form: Assume that $I = (x_1, \ldots, x_m)$. Prove that there exists $r \in (x_2, \ldots, x_m)$ such that $x_1 + r$ is not in any P_i.

5 Projective modules

A motivation behind projective modules are certain good properties of free modules. Even though we typically construct (simpler) free resolutions when we are speaking of more general projective resolutions, we cannot restrict our attention to free modules only as we cannot guarantee that all direct summands of free modules are free (see Fact 5.5 (1) and Exercise 5.20).

Proposition 5.1 *Let F, M and N be (left) R-modules. Suppose that F is free, that $f : M \to N$ is surjective, and that $g : F \to N$. Then there exists $h : F \to M$ such that $f \circ h = g$. This is often drawn as follows:*

$$\begin{tikzcd} & F \arrow[dl, dashed, "\exists h"'] \arrow[d, "g"] \arrow[dl, phantom, "\circlearrowleft", shift right=3ex] & \\ M \arrow[r, "f"] & N \arrow[r] & 0 \end{tikzcd}$$

Proof. Let X be a basis of F. For all $x \in X$, let $m_x \in M$ such that $f(m_x) = g(x)$. By the property of free modules there exists a unique R-module homomorphism $h : F \to M$ extending the function $x \mapsto m_x$, and the rest is easy. $\square$

Definition 5.2 *A (left) R-module P is* **projective** *if whenever $f : M \to N$ is a surjective (left) module homomorphism and $g : P \to N$ is a homomorphism, we have*

$$\begin{tikzcd} & P \arrow[dl, dashed, "\exists h"'] \arrow[d, "g"] \\ M \arrow[r, "f"] \arrow[ur, phantom, "\circlearrowleft" near end] & N \arrow[r] & 0 \end{tikzcd}$$

The following is an immediate corollary of Proposition 5.1:

Corollary 5.3 *Free modules are projective.* $\square$

Theorem 5.4 *The following are equivalent for a left R-module P:*

(1) P is projective.

(2) $\mathrm{Hom}_R(P, \_)$ is exact.

(3) For any R-module M and any surjective $f : M \to P$ there exists $h : P \to M$ such that $f \circ h = \mathrm{id}_P$.

(4) For any R-module M and any surjective $f : M \to P$ we have $M \cong P \oplus \ker f$.

(5) There exists a free R-module F such that $F \cong P \oplus Q$ for some left R-module Q. (Note that by the equivalences, this Q is necessarily projective.)

(6) Given a single free R-module G with $G \overset{g}{\twoheadrightarrow} P$, there is $k : P \to G$ such that $g \circ k = \mathrm{id}_P$.

(7) Given a single free R-module G with $G \overset{g}{\twoheadrightarrow} P$, $\mathrm{Hom}_R(P, G) \xrightarrow{g \circ \_} \mathrm{Hom}_R(P, P)$ is onto.

Proof. By Exercise 2.6, the covariant functor $\mathrm{Hom}_R(P, \_)$ is left-exact. So condition (2) is equivalent to saying that $\mathrm{Hom}_R(P, M) \xrightarrow{\_ \circ f} \mathrm{Hom}_R(P, N)$ is onto whenever $f : M \to N$ is onto. But this is equivalent to P being projective. Thus (1) $\Leftrightarrow$ (2).

(1) $\Rightarrow$ (3) follows from the definition of projective modules and from the commutative diagram

$$\begin{tikzcd} & P \arrow[dl, dashed] \arrow[d] \\ M \arrow[r] \arrow[ur, phantom, "\circlearrowleft" near end] & P \arrow[r] & 0 \end{tikzcd}$$

where the vertical map is the identity map.

(3) $\Rightarrow$ (4): We start with a short exact sequence $0 \to \ker f \to M \overset{f}{\twoheadrightarrow} P \to 0$. Define $\varphi : P \oplus \ker f \to M$ by $\varphi(a, b) = h(a) + b$. This is a module homomorphism. The kernel of φ

consists of all those (a,b) for which $h(a)+b=0$. For such (a,b), $a=f\circ h(a)=f(-b)=0$ since $b\in\ker f$, so that $a=0$ and hence $b=-h(a)=0$, so that $\ker(\varphi)=0$. If $m\in M$, then $f\circ h\circ f(m)=f(m)$, so that $m-h\circ f(m)\in\ker f$, whence $m=h(f(m))+(m-h\circ f(m))\in \operatorname{im}\varphi$. This proves that φ is an isomorphism.

(4) ⇒ (5): Let F be a free R-module mapping onto P. Then (5) follows immediately from (4).

(5) ⇒ (1): We start with the following diagram, with the horizontal row exact:

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

Let $F\cong P\oplus Q$ be free. Then by Proposition 5.1, the following diagram commutes:

$$\begin{tikzcd} & F\cong P\oplus Q \arrow[d] \arrow[ddl, dashed, "\tilde{h}"'] & \\ & P \arrow[d] & \\ M \arrow[r] & N \arrow[r] & 0 \end{tikzcd}$$

Now define the map $h:P\to M$ to be $h(p)=\tilde{h}(p,0)$. It is then straightforward to show that the P-M-N triangle commutes as well. Thus P is projective.

Thus (1) through (5) are equivalent.

Clearly (7) implies (6). Assume (6). If $f:P\to P$ and $g\circ k=\mathrm{id}_P$, then $g\circ(k\circ f)=f$, which proves (7). Thus (6) and (7) are equivalent.

Clearly (3) implies (6). Assume (6). The proof of (3) implying (4) shows that P is a direct summand of G, and the proof of (5) implying (1) shows that P is projective. This finishes the proof of the theorem. □

Facts 5.5

(1) Not every projective module is free. For example, if $R=R_1\oplus R_2$, where R_1,R_2 are non-trivial rings, then $R_1\oplus 0$ is a projective R-module which is not free.

(2) If R is a Dedekind domain that is not a principal ideal domain, then any non-principal ideal is a non-free projective R-module. An example of this is the ideal $(1+\sqrt{-5},2)$ in the ring $R=\mathbb{Z}[\sqrt{-5}]$.

(3) Every projective module is flat. It is straightforward to show that free modules are flat. But P and Q are flat if and only if $P\oplus Q$ is flat, which proves that every direct summand of a free module is flat, whence every projective module is flat.

(4) Not every flat module is projective. For example, $\mathbb{Q}$ is flat over $\mathbb{Z}$, but if it were projective, it would be a direct summand of a free $\mathbb{Z}$-module F. In that case, $1=\sum_i n_ie_i$ for some finite sum with $n_i\in\mathbb{Z}$ and for some basis $\{e_i:i\}$ of F. Then

for any positive integer m, $\frac{1}{m} = \sum_i a_i e_i$ for a finite sum with $a_i \in \mathbb{Z}$, and then by the uniqueness of representations of elements of a free module, $n_i = ma_i$ for all i, so that each n_i is a multiple of every positive integer, which is impossible.

(5) Every projective module over a principal ideal domain is free. For finitely generated modules this is the structure theorem, and the general result is due to Kaplansky [5].

(6) If R is a commutative Noetherian local ring, then any finitely generated projective R-module is free. Proof: Let P be a finitely generated R-module, and let n be its minimal number of generators. Then we have a short exact sequence $0 \to K \to R^n \to P \to 0$. Let $\mathfrak{m}$ be the maximal ideal of R. Since P is projective, $R^n \cong K \oplus P$, and so $(\frac{R}{\mathfrak{m}})^n \cong \frac{K}{\mathfrak{m}K} \oplus \frac{P}{\mathfrak{m}P}$ are vector spaces over $R/\mathfrak{m}$. By dimension count, $\frac{K}{\mathfrak{m}K}$ has dimension 0, and since K is finitely generated, by Nakayama's lemma $K = 0$.

(7) Kaplansky [5] proved that every projective module over a commutative Noetherian local ring is free.

(8) Quillen [8] and Suslin [10] proved independently that every finitely generated projective module over a polynomial ring over a field is free.

Lemma 5.6 *Let $0 \to C_\bullet' \to C_\bullet \to C_\bullet'' \to 0$ be a short exact sequence of complexes. If all modules in $C_\bullet'$ and $C_\bullet''$ are projective, so are all the modules in $C_\bullet$.*

Proof. Since C_n'' is projective, we know that $C_n \cong C_n' \oplus C_n''$. Since both C_n' and C_n'' are projective, so is C_n. □

Definition 5.7 *An R-module P is* **finitely presented** *if it is finitely generated and the kernel of the surjection of some finitely generated free module onto M is finitely generated.*

Proposition 5.8 *Let R be a commutative ring and let P be a finitely presented R-module. Then P is projective if and only if P_Q is projective for all $Q \in \operatorname{Spec} R$, and this holds if and only if P_M is projective for all $M \in \operatorname{Max} R$.*

Proof. P is projective if and only if $\operatorname{Hom}_R(P, R^n) \to \operatorname{Hom}_R(P, P)$ is onto. But this map is onto if and only if it is onto after localization either at all prime ideals or at all maximal ideals. Namely, P is projective if and only if $(\operatorname{Hom}_R(P, R^n))_Q \to (\operatorname{Hom}_R(P, P))_Q$ is onto for all prime/maximal ideals Q in R.

It remains to prove that for any R-module M, for any finitely presented R-module P and for any multiplicatively closed set W in R, $W^{-1}(\operatorname{Hom}_R(P, M)) \cong \operatorname{Hom}_{W^{-1}R}(W^{-1}P, W^{-1}M)$. There is a natural map

$$\varphi : W^{-1}(\operatorname{Hom}_R(P, M)) \to \operatorname{Hom}_{W^{-1}R}(W^{-1}P, W^{-1}M).$$

Namely, an arbitrary element in $W^{-1}(\operatorname{Hom}_R(P, M))$ is of the form $\frac{g}{w}$ for some $w \in W$ and $g \in \operatorname{Hom}_R(P, M)$. Then $\varphi\left(\frac{g}{w}\right)$ takes the element $\frac{p}{u}$ from $W^{-1}P$ to $\frac{g(p)}{wu}$ in $W^{-1}M$. It is straightforward to prove that φ is well-defined, it is in $\mathrm{Hom}_{W^{-1}R}(W^{-1}P, W^{-1}M)$ and it is injective.

We now use that P is finitely presented. This means that there exists a surjective map $p : R^n \to P$ whose kernel is finitely generated. Let $g \in \mathrm{Hom}_{W^{-1}R}(W^{-1}P, W^{-1}M)$. It remains to prove that g is in the image of φ. Let $\{e_1, \ldots, e_n\}$ be a basis of R^n. For each $i = 1, \ldots, n$ let $m_i \in M$ and $w_i \in W$ such that $g\left(\frac{e_i + \ker p}{1}\right) = \frac{m_i}{w_i}$. Let $\{z_1, \ldots, z_s\}$ be a generating set of $\ker p$. Since $g(\frac{z_i + \ker p}{1}) = 0$ in $W^{-1}M$, there exists $u_i \in W$ such that $u_i g(\frac{z_i + \ker p}{1})$ is an element of N and as such it is zero. Set $w = w_1 \cdots w_n u_1 \cdots u_s \in W$. Define an R-module homomorphism $G : R^n \to M$ with $G(e_i) = \frac{w}{w_i} m_i \in M$. In particular, G restricted to $\ker p$ is zero, so that there is a natural R-module homomorphism

$$\overline{G} : M = \frac{R^n}{\ker p} \to M$$

with $\overline{G}(e_i + \ker p) = \frac{w}{w_i} m_i$. Then $\frac{\overline{G}}{w} \in W^{-1} \mathrm{Hom}_R(P, M)$ and by definition $\varphi\left(\frac{\overline{G}}{w}\right) = g$. □

Remark 5.9 In the proof above the finite presentation is necessary. Let $R = k[x_1, x_2, \ldots]$ be a polynomial ring in infinitely many variables $x_1, x_2, \ldots$ over a field k. Let $P = R\langle< x_n^{-n} : n \in \mathbb{N}^+\rangle$, $M = R\langle< x_n^{-n-1} : n \in \mathbb{N}^+\rangle$, and W the multiplicatively closed subset of R of all monomials. Then $W^{-1}R = W^{-1}P = W^{-1}M$, and there exists an element $g \in \mathrm{Hom}_{W^{-1}R}(W^{-1}P, W^{-1}M)$ with $g(\frac{x_n^{-n}}{1}) = \frac{x^{-n-1}}{1}$. If there exist $G \in \mathrm{Hom}_R(P, M)$ and $w \in W$ such that $\varphi \frac{G}{w}$ equals g, then $G(1) = x_n^n G(x_n^{-n}) = x_n^n w x_n^{-n-1} = w x_n^{-1}$. But $G(1)$ is independent of x_n, so that w must be a multiple of x_n. Since there are infinitely many n, this is impossible. (HERE: find a finitely generated but not finitely presented example.)

Definition 5.10 *An R-module P is* **stably free** *if there exist free R-modules F_1 and F_2 such that $P \oplus F_1 \cong F_2$.*

Clearly every stably free module is projective. Serre proved [9] that every stably free module over a polynomial ring over a field is free. There is a way of generating stably free modules:

Proposition 5.11 *Let $a_1, \ldots, a_n$ be elements of a ring R that generate the whole ring. Let $f : R \to R^n$ be the map $f(x) = (xa_1, \ldots, xa_n)$. Then the cokernel of f is stably free.*

Proof. Let P be the cokernel of f. We can write $\sum r_i a_i = 1$ for some $r_1, \ldots, r_n \in R$. If $xa_i = 0$ for all i, then $x \cdot 1 = 0$ as well. This proves that f is injective. Thus $0 \to R \xrightarrow{f} R^n \to P \to 0$ is a short exact sequence. We define $g : R^n \to R$ as $g(x_1, \ldots, x_n) = \sum_i r_i x_i$. Then for all $x \in R$, $g \circ f(x) = g(xa_1, \ldots, xa_n) = \sum_i r_i x a_i = x \sum_i r_i a_i = x$, so that $g \circ f = \mathrm{id}_R$. Thus by Exercise 1.8, $R^n \cong P \oplus R$. □

(It is hard to prove that there exist non-free stably free P as in the proposition.)

Proposition 5.12 *Let R be a commutative domain. Let I be an ideal in R such that $R^m \oplus I \cong R^n$ for some m, n. Then I is free and isomorphic to R^{n-m}.*

Proof. If $I = 0$, necessarily $n = m$, and $R^{n-m} = 0$. Now assume that I is non-zero. The proof of this case is already worked out step by step in Exercise 1.9. For fun we give here another proof, which is shorter but involves more machinery. By localization at $R \setminus \{0\}$ we know that $n - m = 1$. We apply $\wedge^n$:

$$\begin{aligned} R &\cong \wedge^n R^n \cong \wedge^n (R^{n-1} \oplus I) \\ &\cong \oplus_{i=0}^{n} ((\wedge^i R^{n-1}) \otimes (\wedge^{n-i} I)) \quad \text{(interpret $\otimes$ appropriately)} \\ &\cong ((\wedge^{n-1} R^{n-1}) \otimes (\wedge^1 I)) \oplus ((\wedge^n R^{n-1}) \otimes (\wedge^0 I)) \\ &\qquad\qquad \text{(since I has rank 1 and higher exterior powers vanish)} \\ &\cong (R \otimes I) \oplus (0 \otimes R) \cong I. \end{aligned}$$

□

Exercise 5.13 (Base change) Let R be a ring, S an R-algebra, and P a projective R-module. Prove that $P \otimes_R S$ is a projective S-module.

Exercise 5.14 If P is a finitely generated projective module over a ring R, show that $\mathrm{Hom}_R(P, R)$ is a projective R-module.

Exercise 5.15 If P and Q are projective R-modules, prove that $P \otimes_R Q$ is a projective R-module.

Exercise 5.16 (An alternate proof of Proposition 5.8.) Let P be a finitely presented module over a commutative ring R. Let W be a multiplicatively closed set in R. Prove that $W^{-1}(\mathrm{Hom}_R(P, \_)) \cong \mathrm{Hom}_{W^{-1}R}(W^{-1}P, W^{-1}(\_))$.

Exercise 5.17 Let r, n be positive integers and let r divide n. Prove that the $(\mathbb{Z}/n\mathbb{Z})$-module $r(\mathbb{Z}/n\mathbb{Z})$ is projective if and only if $\gcd(r, n/r) = 1$. Prove that $2(\mathbb{Z}/4\mathbb{Z})$ is not a projective module over $\mathbb{Z}/4\mathbb{Z}$. Prove that $2(\mathbb{Z}/6\mathbb{Z})$ is projective over $\mathbb{Z}/6\mathbb{Z}$ but is not free.

Exercise 5.18 Let D be a Dedekind domain. Prove that every ideal in D is a projective D-module.

Exercise 5.19 Let R be a commutative Noetherian domain in which every ideal is a projective R-module. Prove that R is a Dedekind domain.

Exercise 5.20 Find a Dedekind domain D that is not a principal ideal domain. Let I be a non-principal ideal in D.

i) Prove that I is projective and not free.

ii) Prove that I is not a direct summand of D.

iii) Prove that I is a direct summand of a finitely generated free D-module.

6 Projective, flat, free resolutions

Now that we know what free, flat, and projective modules are, the definition of free and projective resolutions given on page 4 makes sense. (A flat resolution has the obvious definition.)

Remarks 6.1

(1) Every module has a free resolution, thus a projective and a flat resolution.

(2) Every finitely generated module over a principal ideal domain R has a resolution of the form

$$0 \to F_1 \to F_0 \to M \to 0,$$

where F_1 and F_0 are free over R (and possibly 0). Namely, by the structure theorem $M \cong R^n \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$ for some non-zero non-units $a_1, \ldots, a_m$, whence we may take $F_0 = R^{n+m}$ and $F_1 = R^m$.

(3) Let M be the $\mathbb{Z}$-module $\mathbb{Z}^5/\langle(0,3,5,1,0),(4,0,3,2,0)\rangle$. We will build the resolution of M as a $\mathbb{Z}$-module as above explicitly. Then if e_1, e_2, e_3, e_4, e_5 form the standard basis of $\mathbb{Z}^5$, in M we have $e_4 = -3e_2 - 5e_3$, so that M is isomorphic to $\mathbb{Z}^4/\langle(4,-4,-13,0)\rangle$. But then by changing the standard basis $\{e_1, e_2, e_3, e_4\}$ of $\mathbb{Z}^4$ to $\{e_1 - 3e_3, e_2, e_3, e_4\}$, we have $4e_1 - 4e_2 - 13e_3 = 4(e_1 - 3e_3) - 4e_2 - e_3$, so that M can also be represented as $\mathbb{Z}^4/\langle(4,-4,-1,0)\rangle$, but this is easily seen to be isomorphic to $\mathbb{Z}^3$. Thus $F_0 = \mathbb{Z}^3$ and $F_1 = 0$.

(4) Verify that for $M = \mathbb{Z}^5/\langle(0,3,5,1,0),(4,0,4,2,0)\rangle$, $F_0 = \mathbb{Z}^4$ and $F_1 = \mathbb{Z}$.

(5) **General fact** that was used in parts (2) and (3) as well as in many future parts in these notes: Suppose that $f : A \to B$ is an R-module homomorphism, α is an automorphism on A and β an automorphism on B. Then

$$\beta \circ f \circ \alpha^{-1} : \alpha(A) \to \beta(B)$$

has the same information as f in the sense that the two homomorphisms have isomorphic kernels, isomorphic images and isomorphic cokernels. In (2) and (3) this was applied with α corresponding to column reduction and β corresponding to row reduction of the matrix.

(6) Let $R = \frac{k[x,y]}{(xy)}$, where k is a field and x and y are variables over k. Let $M = R/(x)$. Verify that

$$\cdots \xrightarrow{x} R \xrightarrow{y} R \xrightarrow{x} R \xrightarrow{y} R \xrightarrow{x} R \to M \to 0$$

is a free resolution that does not stop in finitely many steps.

(7) Let $R = \mathbb{Z}[\sqrt{-5}]$. Then R is a Dedekind domain that is not a principal ideal domain. In particular, $I = (1 + \sqrt{-5}, 2)$ is a non-principal ideal in R. By the exercises in the previous section, I is projective but not free. Then

$$0 \to I \to I \to 0$$

is a projective resolution of I. A free resolution is necessarily longer. The following is a start of a free resolution:

$$\underset{2}{R^2} \xrightarrow{\begin{bmatrix} 2 & 1+\sqrt{-5} \\ 1-\sqrt{-5} & 3 \end{bmatrix}} \underset{1}{R^2} \xrightarrow{\begin{bmatrix} 1-\sqrt{-5} & -2 \\ -3 & 1+\sqrt{-5} \end{bmatrix}} \underset{0}{R^2} \xrightarrow{\begin{bmatrix} 1+\sqrt{-5} & 2 \end{bmatrix}} I \to 0.$$

This can be verified with basic arithmetic. One can further verify that the kernel of the last map is also two-generated, and that the kernel at the next step is two-generated as well. In fact, for all $n \geq 1$, the following repeat in a free resolution of I over R:

$$\underset{\text{2n+2}}{R^2} \xrightarrow{\begin{bmatrix} 2 & 1+\sqrt{-5} \\ 1-\sqrt{-5} & 3 \end{bmatrix}} \underset{\text{2n+1}}{R^2} \xrightarrow{\begin{bmatrix} -3 & 1+\sqrt{-5} \\ 1-\sqrt{-5} & -3 \end{bmatrix}} \underset{\text{2n}}{R^2}$$

Write I as a direct summand of R^2. Can we shorten this?

Definition 6.2 *An R-module M is said to have* **finite projective dimension** *if there exists a projective resolution $0 \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to 0$ of M. The least such n for a given M is called the* **projective dimension of** *M, and is denoted $\mathrm{pd}_R(M)$.*

Examples 6.3

(1) $\mathrm{pd}_R(M) = 0$ if and only if M is projective.

(2) The resolutions in Remarks 6.1 (3) and (4) show that

$$\mathrm{pd}_{\mathbb{Z}}(\mathbb{Z}^5/\langle(0,3,5,1,0),(4,0,3,2,0)\rangle) = 0$$

and

$$\mathrm{pd}_{\mathbb{Z}}(\mathbb{Z}^5/\langle(0,3,5,1,0),(4,0,4,2,0)\rangle) \leq 1,$$

and since $\mathbb{Z}^5/\langle(0,3,5,1,0),(4,0,4,2,0)\rangle$ is not free, its projective dimension is necessarily 1 (and not 0).

(3) The R-resolution of $R/(x)$ in Remarks 6.1 (6) indicates that $R/(x)$ does not have finite projective dimension over R. Well – how can we be sure of this? Just because we found one resolution that does not terminate? We postpone this discussion to the end of the section.

Theorem 6.4 (Schanuel's lemma) *Let R be a ring. Suppose that $0 \to K_1 \to P_1 \to M \to 0$ and $0 \to K_2 \to P_2 \to M \to 0$ are exact sequences of R-modules, and that P_1 and P_2 are projective. Then $K_1 \oplus P_2 \cong K_2 \oplus P_1$.*

Proof. We write the two short exact sequences as follows:

$$\begin{array}{ccccccc} 0 \to & K_1 & \overset{i_1}{\to} & P_1 & \overset{\alpha_1}{\to} & M & \to 0 \\ & & & & & \downarrow\beta & \\ 0 \to & K_2 & \overset{i_2}{\to} & P_2 & \overset{\alpha_2}{\to} & M & \to 0 \end{array}$$

where β is any isomorphism, and in particular it could be the identity map on M. Since P_1 is projective and since α_2 is surjective, there exists $p : P_1 \to P_2$ that makes the following diagram commute:

$$\begin{array}{ccccccc} 0 \to & K_1 & \overset{i_1}{\to} & P_1 & \overset{\alpha_1}{\to} & M & \to 0 \\ & & & \downarrow p & & \downarrow\beta & \\ 0 \to & K_2 & \overset{i_2}{\to} & P_2 & \overset{\alpha_2}{\to} & M & \to 0 \end{array}$$

Now let $x \in K_1$. Then $\alpha_2 \circ p \circ i_1(x) = \beta \circ \alpha_1 \circ i_1(x) = 0$, so that $p \circ i_1(x) \in \ker \alpha_2 = \operatorname{im} i_2$, whence $p \circ i_1(x) = i_2(y)$ for a unique y. Define $\kappa : K_1 \to K_2$ by $x \mapsto y$. It is easy to verify that κ is an R-module homomorphism and that

$$\begin{array}{ccccccc} 0 \to & K_1 & \overset{i_1}{\to} & P_1 & \overset{\alpha_1}{\to} & M & \to 0 \\ & \downarrow\kappa & & \downarrow p & & \downarrow\beta & \\ 0 \to & K_2 & \overset{i_2}{\to} & P_2 & \overset{\alpha_2}{\to} & M & \to 0 \end{array}$$

commutes.

Define $\varphi : K_1 \to K_2 \oplus P_1$ by $\varphi(x) = (\kappa(x), i_1(x))$. This is an injective R-module homomorphism.

Define $\psi : K_2 \oplus P_1 \to P_2$ by $\psi(a, b) = i_2(a) - p(b)$. This is an R-module homomorphism, and $\psi \circ \varphi(x) = \psi(\kappa(x), i_1(x)) = i_2 \circ \kappa(x) - p \circ i_1(x)$, which is 0 since the displayed diagram commutes. Let $(a, b) \in \ker \psi$. Then $i_2(a) = p(b)$, so that $0 = \alpha_2 \circ i_2(a) = \alpha_2 \circ p(b) = \beta \circ \alpha_1(b)$. Since β is an isomorphism, $\alpha_1(b) = 0$, so that $b = i_1(x)$ for some $x \in K_1$. But then $i_2(a) = p(b) = p \circ i_1(x) = i_2 \circ \kappa(x)$, whence by injectivity of i_2, $a = \kappa(x)$. It follows that the arbitrary element (a, b) in the kernel of ψ equals $(\kappa(x), i_1(x))$, which is in the image of φ. Thus $\ker \psi = \operatorname{im} \varphi$. If $z \in P_2$, then $\alpha_2(z) = \beta \circ \alpha_1(y)$ for some $y \in P_1$, so that $\alpha_2(z) = \alpha_2 \circ p(y)$, whence $z - p(y) \in \ker \alpha_2 = \operatorname{im} i_2$, whence $z = (z - p(y)) - p(-y) \in \operatorname{im} \psi$, so that ψ is surjective.

We just proved that $0 \to K_1 \to K_2 \oplus P_1 \to P_2 \to 0$ is exact, which by Theorem 5.4 proves the theorem. $\square$

Theorem 6.5 (Generalized Schanuel's lemma) *Let R be a ring. Suppose that $0 \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to M \to 0$ and $0 \to Q_n \to Q_{n-1} \to \cdots \to Q_1 \to Q_0 \to M \to 0$ are exact sequences of R-modules, and that the P_i and Q_i are projective for all $i < n$. Let $P_{odd} = \oplus_{i\ odd} P_i$, $P_{even} = \oplus_{i\ even} P_i$, $Q_{odd} = \oplus_{i\ odd} Q_i$, $Q_{even} = \oplus_{i\ even} Q_i$.*

$$Q_{even} \oplus P_{odd} \cong Q_{odd} \oplus P_{even}.$$

Proof. We only sketch the proof by induction on n, the base case having been proved in Theorem 6.4. The two sequences can be split into the following four exact sequences:

$$\begin{array}{ll} 0 \to P_n \to P_{n-1} \to P'_{n-1} \to 0, & 0 \to P'_{n-1} \to P_{n-2} \to \cdots \to P_1 \to P_0 \to M \to 0, \\ 0 \to Q_n \to Q_{n-1} \to Q'_{n-1} \to 0, & 0 \to Q'_{n-1} \to Q_{n-2} \to \cdots \to Q_1 \to Q_0 \to M \to 0. \end{array}$$

Let $\widetilde{P}_s$ be the direct sum of all P_i with $i < n-1$ such that $n-1-i$ is even, let $\widetilde{P}_d$ be the direct sum of all P_i with $i < n-1$ such that $n-1-i$ is odd, and we similarly define $\widetilde{Q}_s$ and $\widetilde{Q}_d$. Then by induction, $P'_{n-1} \oplus \widetilde{P}_s \oplus \widetilde{Q}_d \cong Q'_{n-1} \oplus \widetilde{Q}_s \oplus \widetilde{P}_d$. The two short exact sequences in the display above can each be converted trivially to the following short exact sequences:

$$\begin{array}{l} 0 \to P_n \to P_{n-1} \oplus \widetilde{P}_s \oplus \widetilde{Q}_d \to P'_{n-1} \oplus \widetilde{P}_s \oplus \widetilde{Q}_d \to 0, \\ 0 \to Q_n \to Q_{n-1} \oplus \widetilde{Q}_s \oplus \widetilde{P}_d \to Q'_{n-1} \oplus \widetilde{Q}_s \oplus \widetilde{P}_d \to 0. \end{array}$$

The generalized version of Schanuel's lemma now follows from the one given in Theorem 6.4 — at least by the proof in which we allow the extreme right modules to not necessarily be identical but only isomorphic. The details on evenness and oddness of subscripts is left to the reader. $\square$

Proposition 6.6 *Let M be an R-module with finite projective dimension n. Let $(F_\bullet, d_\bullet)$ be any projective resolution of M. Then $F_n \neq 0$ and*

$$0 \to \ker(d_{n-1}) \to F_{n-1} \xrightarrow{d_{n-1}} F_{n-2} \to \cdots \to F_1 \to F_0 \to M \to 0$$

is a projective resolution of M.

Furthermore, for any $m \geq n-1$ the kernel of $d_m : F_m \to F_{m-1}$ is projective.

Proof. If $F_n = 0$ then the projective dimension of M would be strictly smaller than n. Thus $F_n \neq 0$.

By assumption there exists a projective resolution $0 \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to M \to 0$. By the generalized Schanuel's lemma (Theorem 6.5) the direct sum of $\ker(d_m)$ and some projective R-module is isomorphic to another projective R-module. Since the direct sum of projective modules is projective and a direct summand of a projective module is projective, it follows that $\ker(d_m)$ is projective. In particular, $\ker(d_{n-1})$ is projective. $\square$

Theorem 6.7 (Minimal free resolutions over Noetherian local rings) *Let R be a Noetherian local ring, and let M be a finitely generated R-module with finite projective dimension n. Let $(P_\bullet, d_\bullet)$ be any projective resolution of M. Define b_0 to be the minimal number of generators of M. Then $R^{b_0} \to M \to 0$ is exact and starts a free resolution of M over R. Suppose that we have constructed recursively an exact complex $R^{b_i} \to R^{b_{i-1}} \to \cdots \to R^{b_1} \to R^{b_0} \to M \to 0$ where $b_0, \ldots, b_i$ are non-negative integers. Define b_{i+1} to be the minimal number of generators of the kernel of $R^{b_i} \to R^{b_{i-1}}$. We extend the complex by one step to the left and keep exactness.*

Then $b_n \neq 0$ and $b_{n+1} = 0$. In other words, a projective resolution of minimal length may be obtained by constructing a free resolution in which at each step we take the minimal possible number of generators of the free modules.

Proof. By the Noetherian property all b_i are integers. By Proposition 6.6, $b_n \neq 0$ and the kernel of $R^{b_{n-1}} \to R^{b_{n-2}}$ is projective. All projective modules over a Noetherian local ring are free by Fact 5.5 (6). Thus we can write the kernel as R^b, and necessarily the unique number b is the minimal number and $b_{n+1} = 0$. $\square$

Proposition 6.8 *Let $(R, \mathfrak{m})$ be a Noetherian local ring, let M be a finitely generated R-module and let $\cdots \to R^{b_i} \to R^{b_{i-1}} \to \cdots \to R^{b_1} \to R^{b_0} \to M \to 0$ be a free resolution of M. The following are equivalent:*

(1) The resolution is minimal.

(2) For all $i \geq 1$, the image of R^{b_i} is in $\mathfrak{m}R^{b_{i-1}}$.

Proof. (1) implies (2): If the image of R^{b_i} is not in $\mathfrak{m}R^{b_{i-1}}$, then without loss of generality $(1, 0, \ldots, 0) \in R^{b_i}$ does not map to $\mathfrak{m}R^{b_{i-1}}$, and by changing a basis on $R^{b_{i-1}}$ we may assume that $(1, 0, \ldots, 0) \in R^{b_i}$ maps to $(1, 0, \ldots, 0) \in R^{b_{i-1}}$. But then $(1, 0, \ldots, 0) \in R^{b_{i-1}}$ maps to 0 in the complex, so this basis element of $R^{b_{i-1}}$ is redundant in the resolution. Thus b_{i-1} was not chosen minimal so that the resolution is not minimal.

(2) implies (1): Suppose that some b_i is not minimal. Then after a change of basis on R^{b_i} we may assume that elements $e_1 = (1, 0, \ldots, 0)$ and $c = (0, c_1, \ldots, c_{b_i})$ in R^{b_i} map to the same element via d_i. But then $(1, -c_1, \ldots, -c_n)$ is in the image of $d_{i+1} : R^{b_{i+1}} \to R^{b_i}$, which contradicts (2). $\square$

Exercise 6.9 Let R be a polynomial ring in finitely many variables over a field. Let M be a graded finitely generated R-module. We will prove later (see Theorem 9.4) that every finitely generated R-module has finite projective dimension. Let $\cdots \to R^{b_i} \to R^{b_{i-1}} \to \cdots \to R^{b_1} \to R^{b_0} \to M \to 0$ be exact, with all maps homogeneous, and with b_0 chosen smallest possible, after which b_1 is chosen smallest possible, etc. Prove that all the entries of the matrices of the maps $R^{b_i} \to R^{b_{i-1}}$ have positive degree and may be chosen to be homogeneous. Prove that if $n = \mathrm{pd}_R(M)$ then $b_{n+1} = 0$ and $b_n \neq 0$.

Exercise 6.10 Prove that $\mathrm{pd}_R(M_1 \oplus M_2) = \sup\{\mathrm{pd}_R(M_1), \mathrm{pd}_R(M_2)\}$.

Exercise 6.11 Let R be either a Noetherian local ring or a polynomial ring over a field. Let M be a finitely generated R-module that is graded in case R is a polynomial ring. Let $F_\bullet$ be a free resolution of M, and let $G_\bullet$ be a minimal free resolution of M. Prove that there exists an exact complex $H_\bullet$ such that $F_\bullet \cong G_\bullet \oplus H_\bullet$ (isomorphism of maps of complexes). In particular, if $G_\bullet$ is minimal, this proves that $F_\bullet \cong G_\bullet$.

Exercise 6.12 Prove that $\mathrm{pd}_R(R/(x)) = \infty$ where R and x are as in Remarks 6.1 (6).

Exercise 6.13 Let R be a commutative ring. Let $0 \to M_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to M \to 0$ be an exact sequence of R-modules, where all P_i are projective. Prove that $\mathrm{pd}_R(M) \le n$ if and only if M_n is projective. Prove that if $\mathrm{pd}_R(M) \ge n$, then $\mathrm{pd}_R(M) = \mathrm{pd}(M_n) + n$.

Exercise 6.14 Let R be a commutative Noetherian ring and M a finitely generated R-module.

i) Prove that there exists a projective resolution of M in which all modules are finitely generated.

ii) Prove that if M has finite projective dimension n then there exists a projective resolution of M of length n in which all modules are finitely generated.

Exercise 6.15 What should the projective dimension of the zero R-module be?

i) Justify defining the projective dimension of the zero module to be 0.

ii) Justify defining the projective dimension of the zero module to be -1.

iii) Justify defining the projective dimension of the zero module to be $-\infty$.

iv) What is your conclusion/preference?

7 Manipulating projective resolutions

The following is a workhorse of projective resolutions.

Theorem 7.1 (Comparison Theorem) *Let $P_\bullet$: $\cdots \to P_2 \to P_1 \to P_0 \to M \to 0$ be a complex with all P_i projective. Let $C_\bullet$: $\cdots \to C_2 \to C_1 \to C_0 \to N \to 0$ be an exact complex. Then for any $f \in \mathrm{Hom}_R(M, N)$ there exists a map of complexes $f_\bullet : P_\bullet \to C_\bullet$ that extends f, i.e., that $f_{-1} = f$. Moreover, any two such liftings $f_\bullet$ are homotopic.*

Proof. Let the map $P_i \to P_{i-1}$ be denoted d_i, and let the map $C_i \to C_{i-1}$ be denoted δ_i. Since P_0 is projective, we get the following commutative diagram:

$$\begin{tikzcd}
 & P_0 \arrow[d, "d_0"] \arrow[ddl, dashed, "f_0"'] & \\
 & M \arrow[d, "f"] \arrow[dl, phantom, "\circlearrowleft"] & \\
C_0 \arrow[r, "\delta_0"] & N \arrow[r] & 0
\end{tikzcd}$$

which means that we have constructed $f_\bullet$ up to $n = 0$. Suppose that we have constructed $f_\bullet$ up to some $n \geq 0$. Then $\delta_n \circ f_n \circ d_{n+1} = f_{n-1} \circ d_n \circ d_{n+1} = 0$, so that $\operatorname{im}(f_n \circ d_{n+1}) \in \ker \delta_n = \operatorname{im} \delta_{n+1}$. But then we get the following commutative diagram, with the horizontal row exact:

$$\begin{tikzcd}
 & P_{n+1} \arrow[d, "f_n \circ d_{n+1}"] \arrow[dl, dashed, "f_{n+1}"'] \arrow[dl, phantom, "\circlearrowleft"] & \\
C_{n+1} \arrow[r, "\delta_{n+1}"] & \operatorname{im} \delta_{n+1} \arrow[r] & 0
\end{tikzcd}$$

This allows us to construct $f_\bullet$ up to another step, and thus by induction it proves the existence of $f_\bullet$.

Now suppose that $f_\bullet$ and $g_\bullet$ are both maps of complexes that extend $f : M \to N$. Define $s_{-1} : M \to C_0$ to be the zero map (we really cannot hope for it to be anything else as we do not have control over M and C_0). Note that $\delta_0 \circ (f_0 - g_0) = \delta_0 \circ f_0 - \delta_0 \circ g_0 = f \circ \delta_0 - f \circ \delta_0 = 0$, so that we get $s_0 : P_0 \to C_1$ by the following commutative diagram:

$$\begin{tikzcd}
 & P_0 \arrow[d, "f_0 - g_0"] \arrow[dl, dashed, "s_0"'] \arrow[dl, phantom, "\circlearrowleft"] & \\
C_1 \arrow[r, "\delta_1"] & \operatorname{im} \delta_1 \arrow[r] & 0
\end{tikzcd}$$

This now has built s_{-1}, s_0 with the desired properties for a homotopy relation between $f_\bullet$ and $g_\bullet$. Suppose that we have built such $s_{-1}, s_0, s_1, \ldots, s_n$ with the desired relations. Then $\delta_{n+1} \circ (f_{n+1} - g_{n+1} - s_n \circ d_{n+1}) = \delta_{n+1} \circ (f_{n+1} - g_{n+1}) - \delta_{n+1} \circ s_n \circ d_{n+1} = (f_n - g_n) \circ d_{n+1} - \delta_{n+1} \circ s_n \circ d_{n+1} = (f_n - g_n - \delta_{n+1} \circ s_n) \circ d_{n+1} = s_{n-1} \circ d_n \circ d_{n+1} = 0$, so that $\operatorname{im}(f_{n+1} - g_{n+1} - s_n \circ d_{n+1}) \subseteq \ker \delta_{n+1} = \operatorname{im} \delta_{n+2}$. But then we get the commutative diagram below,

$$\begin{tikzcd}
 & P_{n+1} \arrow[d, "f_{n+1} - g_{n+1} - s_n \circ d_{n+1}"] \arrow[dl, dashed, "s_{n+1}"'] \arrow[dl, phantom, "\circlearrowleft"] & \\
C_{n+2} \arrow[r, "\delta_{n+2}"] & \operatorname{im} \delta_{n+2} \arrow[r] & 0
\end{tikzcd}$$

which gives exactly the map s_{n+1} with the desired property for building a homotopy between $f_\bullet$ and $g_\bullet$. This proves the theorem. $\square$

Proposition 7.2 *Let $P_\bullet$ be a projective resolution of M, let $Q_\bullet$ be a projective resolution of N, and let $f \in \mathrm{Hom}_R(M, N)$. Then there exists a map of complexes $f_\bullet : P_\bullet \to Q_\bullet$ such that*

$$\begin{array}{ccc} P_\bullet & \to & M & \to 0 \\ \downarrow f_\bullet & & \downarrow f & \\ Q_\bullet & \to & N & \to 0 \end{array}$$

commutes. Furthermore, any two such $f_\bullet$ are homotopic.

Proof. This is just an application of the Comparison Theorem (Theorem 7.1). □

Corollary 7.3 *Let $P_\bullet$ and $Q_\bullet$ be projective resolutions of M. Then for any additive functor $\mathcal{F}$ (i.e., a functor which preserves the addition), the homologies of $\mathcal{F}(P_\bullet)$ and of $\mathcal{F}(Q_\bullet)$ are isomorphic.*

Proof. By Proposition 7.2 there exists $f_\bullet : P_\bullet \to Q_\bullet$ that extends id_M, and there exists $g_\bullet : Q_\bullet \to P_\bullet$ that extends id_M. Thus $f_\bullet \circ g_\bullet : Q_\bullet \to Q_\bullet$ extends id_M, but so does the identity map on $Q_\bullet$. Thus by the Comparison Theorem (Theorem 7.1), $f_\bullet \circ g_\bullet$ and id are homotopic, whence so are $\mathcal{F}(f_\bullet \circ g_\bullet)$ and $\mathcal{F}(\mathrm{id})$. Thus by Proposition 3.7, the map $(\mathcal{F}(f_\bullet \circ g_\bullet))_*$ induced on the homology of $\mathcal{F}(Q_\bullet)$ is the identity map. If $\mathcal{F}$ is covariant, this says that $(\mathcal{F}(f_\bullet))_* \circ (\mathcal{F}(g_\bullet))_*$ is identity, whence $(\mathcal{F}(f_\bullet))_*$ is surjective and $(\mathcal{F}(g_\bullet))_*$ is injective. Similarly, by looking at the other composition, we get that $(\mathcal{F}(g_\bullet))_*$ is surjective and $(\mathcal{F}(f_\bullet))_*$ is injective. Thus $(\mathcal{F}(f_\bullet))_*$ is an isomorphism, which proves the corollary in case $\mathcal{F}$ is covariant. The argument for contravariant functors is similar. □

Theorem 7.4 *Let ${C_\bullet}'$ be a projective resolution of M' and let ${C_\bullet}''$ be a projective resolution of M''. Suppose that $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ is a short exact sequence. Then there exists a projective resolution $C_\bullet$ such that*

$$\begin{array}{ccccccc} 0 \to & {C_\bullet}' & \xrightarrow{i_\bullet} & C_\bullet & \xrightarrow{p_\bullet} & {C_\bullet}'' & \to 0 \\ & \downarrow d_0' & & \downarrow d_0 & & \downarrow d_0'' & \\ 0 \to & M' & \xrightarrow{i} & M & \xrightarrow{p} & M'' & \to 0 \end{array}$$

is a commutative diagram, in which the top row is a short exact sequence of complexes.

Proof. Define $C_n = C_n' \oplus C_n''$, with the horizontal maps in the short exact sequence $0 \to C_n' \xrightarrow{i_n} C_n \xrightarrow{p_n} C_n'' \to 0$ the obvious maps. This gives the modules of $C_\bullet$. We have to work harder to construct the differential maps on $C_\bullet$.

Note that

$$\cdots \to C_1' \xrightarrow{d_1'} C_0' \xrightarrow{i \circ d_0'} M \xrightarrow{p} M'' \to 0$$

is exact at all C_i' and at M'', and it is also exact at M because $\ker(p) = \mathrm{image}(i) = \mathrm{image}(i \circ d_0')$ because d_0' is surjective. Thus by the Comparison Theorem (Theorem 7.1), there exist maps $t_0 : C''_0 \to M$ and $t_n : C''_n \to C'_{n-1}$ for $n \geq 1$ that make the following diagram commute.

$$\begin{array}{ccccccccc}
\cdots \to & C''_2 & \stackrel{d''_2}{\to} & C''_1 & \stackrel{d''_1}{\to} & C''_0 & \stackrel{d''_0}{\to} & M'' & \to 0 \\
& \downarrow t_2 & & \downarrow t_1 & & \downarrow t_0 & & \| & \\
\cdots \to & C'_1 & \stackrel{d'_1}{\to} & C'_0 & \stackrel{i \circ d'_0}{\to} & M & \stackrel{p}{\to} & M'' & \to 0
\end{array}$$

Define $d_0 : C_0 \to M$ as $d_0(a, b) = i \circ d'_0(a) + t_0(b)$, and $d_n : C_n \to C_{n-1}$ as $d_n(a, b) = (d'_n(a) + (-1)^n t_n(b), d''_n(b))$ for $n \geq 1$.

Then $(C_\bullet, d_\bullet)$ is a complex:

$$\begin{aligned}
d_0 \circ d_1(a, b) &= d_0(d'_1(a) - t_1(b), d''_1(b)) \\
&= i \circ d'_0(d'_1(a) - t_1(b)) + t_0 \circ d''_1(b) \\
&= -i \circ d'_0 \circ t_1(b) + t_0 \circ d''_1(b) \\
&= 0, \\
d_{n-1} \circ d_n(a, b) &= d_{n-1}(d'_n(a) + (-1)^n t_n(b), d''_n(b)) \\
&= (d'_{n-1}(d'_n(a) + (-1)^n t_n(b)) + (-1)^{n-1} t_{n-1} \circ d''_n(b), d''_{n-1} \circ d''_n(b)) \\
&= ((-1)^n d'_{n-1} \circ t_n(b) + (-1)^{n-1} t_{n-1} \circ d''_n(b), 0) \\
&= (0, 0).
\end{aligned}$$

Certainly $C_\bullet$ is a complex of projective modules.

The diagram in the statement of the theorem commutes, i.e., we do have maps of complexes:

$$\begin{aligned}
d_0 \circ i_1(a) &= d_0(a, 0) = i \circ d'_0(a), \\
p \circ d_0(a, b) &= p(i \circ d'_0(a) + t_0(b)) = p \circ t_0(b) = d''_0 \circ p_0(a, b), \\
d_n \circ i_n(a) &= d_n(a, 0) = (d'_n(a), 0) = i_{n-1} \circ d'_n(a), \\
d''_n \circ p_n(a, b) &= d''_n(b) = p_n \circ d_n(a, b).
\end{aligned}$$

If we take any two adjacent rows of the diagram in the statement of the theorem, the rows are exact and the diagram commutes. In particular, if we take rows 0 and -1, the Snake Lemma (Lemma 1.7) says that $d_0 : C_0 \to M$ is surjective because d'_0 and d''_0 are surjective. Let $(a, b) \in \ker d_0$. Then $i \circ d'_0(a) + t_0(b) = 0$. Thus $0 = p(0) = p \circ t_0(b) = d''_0(b)$, which means that there exists $b'' \in C''_0$ such that $b = d''_0(b'')$. It follows that $0 = i \circ d'_0(a) + t_0(b) = i \circ d'_0(a) + t_0 \circ d''_0(b'') = i \circ d'_0(a) + i \circ d'_0 \circ t_1(b'')$. Since i is injective, then $d'_0(a + t_1(b'')) = 0$, and since $C_\bullet{}'$ is exact, there exists $a' \in C'_1$ such that $d'_1(a') = a + t_1(b'')$. Hence $(a, b) = d_1(a', b'')$, whic proves exactness of $(C_\bullet, d_\bullet)$ at the zeroeth spot. We next prove that $(C_\bullet, d_\bullet)$ is exact at the nth spot for $n \geq 1$. Let $(a, b) \in \ker d_n$. Then $d'_n(a) + (-1)^n t_n(b) = 0$ and $d''_n(b) = 0$. Since $C_\bullet{}''$ is exact there exists $b'' \in C''_{n-1}$ such that $b = d''_{n+1}(b'')$. Thus $0 = d'_n(a) + (-1)^n t_n \circ d''_{n+1}(b'') = d'_n(a) + (-1)^n d'_n \circ t_{n+1}(b'')$. Since $C_\bullet{}'$ is exact, there exists $a' \in C'_{n_1}$ such that $d'_{n+1}(a') = a + (-1)^n t_{n+1}(b'')$. Hence $(a, b) = d_{n+1}(a', b'')$. Thus $C_\bullet$ is a projective resolution of M. $\square$

Exercise 7.5 Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules. Prove that $\mathrm{pd}_R(M) \le \sup\{\mathrm{pd}_R(M'), \mathrm{pd}_R(M'')\}$. If $\mathrm{pd}_R(M) < \sup\{\mathrm{pd}_R(M'), \mathrm{pd}_R(M'')\}$, prove that $\mathrm{pd}_R(M'') = \mathrm{pd}_R(M') + 1$.

Exercise 7.6 Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules. Prove that if any two of the modules have finite projective dimension, so does the third.

Exercise 7.7 Let R be a Noetherian ring and M a finitely generated R-module. Prove that $\mathrm{pd}_R(M) = \sup\{\mathrm{pd}_{R_p}(M_p) : p \in \operatorname{Spec} R\}$.

Exercise 7.8 (This is taken from [6].) Let R be a polynomial ring in finitely many variables over a field, let $m_1, \ldots, m_n$ be monomials in R, and let $I = (m_1, \ldots, m_n)$. Let $J = (m_1, \ldots, m_{n-1})$. Let $(C_\bullet, d_\bullet)$ be a free resolution of $R/(J : m_r)$ and let $(K_\bullet, e_\bullet)$ be a free resolution of R/J. By the Comparison Theorem (Theorem 7.1), the injective R-module homomorphism $R/(J : m_n) \to R/J$ given by multiplication by m_n induces a map of complexes $f_\bullet : C_\bullet \to K_\bullet$.

(1) Prove that the mapping cone of $f_\bullet$ is a free resolution of R/I. (Mapping cone construction is in Exercise 4.14.)
(2) Suppose that $C_\bullet$ and $K_\bullet$ are Taylor resolutions. (The definition of the Taylor complex of a monomial ideal is on page 9.) Prove that the mapping cone is a Taylor resolution of R/I.
(3) Prove that the Taylor complex of a monomial ideal is always exact.

8 Tor

Let M, N be R-modules, and let $P_\bullet : \quad \cdots \to P_2 \to P_1 \to P_0 \to 0$ be a projective resolution of M. We define

$$\operatorname{Tor}_n^R(M, N) = H_n(P_\bullet \otimes_R N).$$

With all the general manipulations of complexes we can fairly quickly develop some main properties of Tor:

1. Independence of the resolution. The definition of $\operatorname{Tor}_n^R(M, \_)$ is independent of the projective resolution $P_\bullet$ of M. This follows from Corollary 7.3.

2. Tor has no terms of negative degree. $\operatorname{Tor}_n^R(M, \_) = 0$ if $n < 0$. This follows as $P_\bullet$ has zero modules in all the negative positions.

3. Tor_0. $\operatorname{Tor}_0^R(M, N) \cong M \otimes_R N$. Proof: By assumption $P_1 \to P_0 \to M \to 0$ is exact, and as $\_ \otimes_R N$ is right-exact, $P_1 \otimes_R N \to P_0 \otimes_R N \to M \otimes_R N \to 0$ is exact as well. Thus $\operatorname{Tor}_0^R(M, N) = H_0(P_\bullet \otimes_R N) = (P_0 \otimes_R N)/\operatorname{im}(P_1 \otimes_R N) \cong M \otimes_R N$.

4. What if M is projective? If M is projective, then $\operatorname{Tor}_n^R(M, N) = 0$ for all $n \ge 1$. This is clear as in that case we may take $P_0 = M$ and all other P_n to be 0.

5. What if N is flat? If N is flat, then $\operatorname{Tor}_n^R(M,N)=0$ for all $n\geq 1$. This follows as $P_{n+1}\to P_n\to P_{n-1}$ is exact, and so as N is flat, $P_{n+1}\otimes N\to P_n\otimes N\to P_{n-1}\otimes N$ is exact as well, giving that the nth homology of $P_\bullet\otimes N$ is 0 if $n>0$.

6. Tor on short exact sequences. If $0\to M'\to M\to M''\to 0$ is a short exact sequence of modules, then for any module N there is a long exact sequence

$$\cdots\to\operatorname{Tor}_{n+1}^R(M'',N)\to\operatorname{Tor}_n^R(M',N)\to\operatorname{Tor}_n^R(M,N)\to\operatorname{Tor}_n^R(M'',N)\to\operatorname{Tor}_{n-1}^R(M',N)\to\cdots.$$

The proof goes as follows. Let $P_\bullet{}'$ be a projective resolution of M', and let $P_\bullet{}''$ be a projective resolution of M''. Then by Theorem 7.4 there exists a projective resolution $P_\bullet$ of M such that

$$\begin{array}{ccccccc}
0\to & P_\bullet{}' & \to & P_\bullet & \to & P_\bullet{}'' & \to 0\\
 & \downarrow & & \downarrow & & \downarrow & \\
0\to & M' & \to & M & \to & M'' & \to 0
\end{array}$$

is a commutative diagram in which the rows are exact. In particular, we have a short exact sequence $0\to P_\bullet{}'\to P_\bullet\to P_\bullet{}''\to 0$, and since this is a split exact sequence, it follows that $0\to P_\bullet{}'\otimes N\to P_\bullet\otimes N\to P_\bullet{}''\otimes N\to 0$ is still a short exact sequence of complexes. The rest follows from Theorem 3.3.

7. Tor and annihilators. For any M,N and n, $\operatorname{ann}M+\operatorname{ann}N\subseteq\operatorname{ann}\operatorname{Tor}_n^R(M,N)$. Proof: Since $\operatorname{Tor}_n^R(M,N)$ is a quotient of a submodule of $P_n\times N$, it is clear that $\operatorname{ann}N$ annihilates all Tors. Now let $x\in\operatorname{ann}M$. Then multiplication by x on M, which is the same as multiplication by 0 on M, has two lifts μ_x and μ_0 on $P_\bullet$ (multiplication by x and multiplication by 0, respectively). By the Comparison Theorem (Theorem 7.1), the two maps μ_x and μ_0 are homotopic. Thus $\mu_x\otimes\mathrm{id}_N$ and 0 are homotopic on $P_\bullet\otimes N$, whence by Proposition 3.7, $(\mu_x\otimes\mathrm{id}_N)_*=0$. But $(\mu_x\otimes\mathrm{id}_N)_*$ is simply multiplication by x, which says that multiplication by x on $\operatorname{Tor}_n^R(M,N)$ is 0. This proves that indeed $\operatorname{ann}M+\operatorname{ann}N\subseteq\operatorname{ann}\operatorname{Tor}_n^R(M,N)$.

8. Tor on syzygies. Let $0\to M_n\to P_{n-1}\to\cdots\to P_1\to P_0\to M\to 0$ be an exact sequence with all P_i projective. Such M_n is called an **nth syzygy of** M. Then for all $i\geq 1$, $\operatorname{Tor}_i^R(M_n,N)\cong\operatorname{Tor}_{i+n}^R(M,N)$. This follows from the definition of Tor (and from the independence on the projective resolution). In particular, if $\operatorname{pd}_R(M)<n$, then $\operatorname{Tor}_{i+n}^R(M,N)=0$ and M_n is projective by Proposition 6.6, so that $\operatorname{Tor}_i^R(M_n,N)=0$ for all $i\geq 1$. (If $\operatorname{pd}_R(M)\geq n$, then $\operatorname{pd}_R(M_n)=\operatorname{pd}_R(M)-n$; the isomorphism on Tors of M_n and M holds for all $i\geq 1$.)

9. Tor for finitely generated modules over Noetherian rings. If R is Noetherian and M and N are finitely generated R-modules, then $\operatorname{Tor}_n^R(M,N)$ is a finitely generated R-module for all n. To prove this, we may choose $P_\bullet$ such that all P_n are finitely generated (since submodules of finitely generated modules are finitely generated). Then $P_n\otimes N$ is finitely generated, whence so is $\operatorname{Tor}_n^R(M,N)$.

Note that we do not yet have symmetric results for M and N in $\operatorname{Tor}_n^R(M,N)$.

Theorem 8.1 *Let R be a commutative ring and let M and N be R-modules. Then for all n, $\mathrm{Tor}_n^R(M,N) \cong \mathrm{Tor}_n^R(N,M)$.*

Proof. Let $P_\bullet$ be a projective resolution of M and let $Q_\bullet$ be a projective resolution of N. We temporarily introduce another construction: $\overline{\mathrm{Tor}}_n^R(M,N) = H_n(M \otimes_R Q_\bullet)$. The goal is to prove that $\mathrm{Tor}_n^R(M,N) \cong \overline{\mathrm{Tor}}_n^R(M,N)$ (for which we do not need a commutative ring).

It is clear that the properties 1.–9. listed above hold in the analogous symmetric formulation for $\overline{\mathrm{Tor}}$. In particular, it follows that $\mathrm{Tor}_n^R(M,N) \cong \overline{\mathrm{Tor}}_n^R(M,N)$ for all $n \le 0$.

Let M_1, N_1 be defined so that $0 \to M_1 \to P_0 \to M \to 0$ and $0 \to N_1 \to Q_0 \to N \to 0$ are exact. We tensor these two complexes into a commutative diagram as below:

$$
\begin{tikzcd}
 & & & \overline{\mathrm{Tor}}_1^R(M,Q_0)=0 \arrow[d] & \\
 & & 0 \arrow[d] & \overline{\mathrm{Tor}}_1^R(M,N) \arrow[d] & \\
 & M_1\otimes N_1 \arrow[r] \arrow[d, "\alpha"] & P_0\otimes N_1 \arrow[r] \arrow[d, "\beta"] & M\otimes N_1 \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & M_1\otimes Q_0 \arrow[r] \arrow[d] & P_0\otimes Q_0 \arrow[r] \arrow[d] & M\otimes Q_0 \arrow[r] \arrow[d] & 0 \\
 & M_1\otimes N \arrow[r] \arrow[d] & P_0\otimes N \arrow[r] \arrow[d] & M\otimes N \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}
$$

By right-exactness of the tensor product and properties 1.–9., the rows and the columns in the diagram are exact. By the Snake Lemma (Lemma 1.7), $\ker\beta \to \ker\gamma \to \operatorname{coker}\alpha \to \operatorname{coker}\beta \to \operatorname{coker}\gamma \to 0$ is exact, or in other words,

$$0 \to \overline{\mathrm{Tor}}_1^R(M,N) \to M_1\otimes N \to P_0 \otimes N \to M\otimes N \to 0$$

is exact. The maps between the tensor products above are the natural maps. Property (6) of Tor in this section says that

$$0 = \mathrm{Tor}_1^R(P_0,N) \to \mathrm{Tor}_1^R(M,N) \to M_1\otimes N \to P_0\otimes N \to M\otimes N \to 0$$

is exact with the natural maps on the tensor products. This proves that for all R-modules M and N, $\mathrm{Tor}_1^R(M,N) = \overline{\mathrm{Tor}}_1^R(M,N)$. For later usage I label this result (I1).

But the big commutative diagram above shows even more if we fill it up a bit more in the upper left corner to get the following exact rows and exact columns in the commutative diagram:

$$
\begin{tikzcd}
 & & \overline{\mathrm{Tor}}_1^R(M_1,Q_0)=0 \arrow[d] & \\
 & & \overline{\mathrm{Tor}}_1^R(M_1,N) \arrow[d] & 0 \arrow[d] \\
\mathrm{Tor}_1^R(P_0,N_1)=0 \arrow[r] & \mathrm{Tor}_1^R(M,N_1) \arrow[r] & M_1\otimes N_1 \arrow[r, "f"] \arrow[d, "\alpha"] & P_0\otimes N_1 \arrow[d, "\beta"] \\
 & 0 \arrow[r] & M_1\otimes Q_0 \arrow[r, "g"] & P_0\otimes Q_0
\end{tikzcd}
$$

From this diagram we see that $\overline{\mathrm{Tor}}_1^R(M_1, N)$ is the kernel of α, and since g is injective, $\overline{\mathrm{Tor}}_1^R(M_1, N)$ is the kernel of $g \circ \alpha = \beta \circ f$. But $\mathrm{Tor}_1^R(M, N_1)$ is the kernel of f and hence of $\beta \circ f$, which proves that $\overline{\mathrm{Tor}}_1^R(M_1, N) \cong \mathrm{Tor}_1^R(M, N_1)$. For later usage I label this result (I2).

So far we have proved that for all M, N, $\overline{\mathrm{Tor}}_1^R(M, N) \cong \mathrm{Tor}_1^R(M, N)$, and that for any first syzygy M_1 of M and any first syzygy N_1 of N, $\overline{\mathrm{Tor}}_1^R(M_1, N) \cong \mathrm{Tor}_1^R(M, N_1)$.

Now let $M_n = \ker(P_{n-1} \to P_{n-2})$ and $N_n = \ker(Q_{n-1} \to Q_{n-2})$. Then by what we just proved and by 1.–9. and their analogous symmetric versions, for all $n \geq 2$,

$$\begin{aligned}
\overline{\mathrm{Tor}}_n^R(M, N) &\cong \overline{\mathrm{Tor}}_1^R(M, N_{n-1}) \text{ (by Property 8. } \overline{\mathrm{Tor}} \text{ on syzygies)} \\
&\cong \mathrm{Tor}_1^R(M, N_{n-1}) \text{ (by (I1))} \\
&\cong \overline{\mathrm{Tor}}_1^R(M_1, N_{n-2}) \text{ (by (I2))} \\
&\cong \mathrm{Tor}_1^R(M_1, N_{n-2}) \text{ (by (I1))} \\
&\cong \overline{\mathrm{Tor}}_1^R(M_2, N_{n-3}) \text{ (by (I2) if } n > 3) \\
&\cong \mathrm{Tor}_1^R(M_2, N_{n-3}) \text{ (by (I1))} \\
&\cong \cdots \\
&\cong \mathrm{Tor}_1^R(M_{n-2}, N_1) \text{ (by repetition of the steps)} \\
&\cong \overline{\mathrm{Tor}}_1^R(M_{n-1}, N) \text{ (by (I2))} \\
&\cong \mathrm{Tor}_1^R(M_{n-1}, N) \text{ (by (I1))} \\
&\cong \mathrm{Tor}_n^R(M, N) \text{ (by Property 8. Tor on syzygies).}
\end{aligned}$$ □

Now the following are easy corollaries:

Corollary 8.2 *If M is flat, then $\mathrm{Tor}_n^R(M, \_) = 0$ for all $n \geq 1$.* □

Corollary 8.3 *Let $0 \to N' \to N \to N'' \to 0$ be a short exact sequence of modules. Then there exists a long exact sequence*

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

Proof. Combine... □

Corollary 8.4 *Let $0 \to M_n \to L_{n-1} \to \cdots \to L_1 \to L_0 \to M \to 0$ be an exact sequence, where each L_i is a flat module. Then for all $i \geq 1$, $\mathrm{Tor}_i^R(M_n, N) \cong \mathrm{Tor}_{i+n}^R(M, N)$.*

Proof. If $n = 1$, then we get a long exact sequence

$$\cdots \to \mathrm{Tor}_{m+1}^R(L_0, N) \to \mathrm{Tor}_{m+1}^R(M, N) \to \mathrm{Tor}_{m+1}^R(M_1, N) \to \mathrm{Tor}_m^R(L_0, N) \to \cdots$$

By Property 5. of Tor, the two outside modules are zero for $m \geq 1$, so that $\mathrm{Tor}_{m+1}^R(M, N) \cong \mathrm{Tor}_{m+1}^R(M_1, N)$. For higher n, the conclusion follows by induction on n and the split of $0 \to M_n \to L_{n-1} \to \cdots \to L_1 \to L_0 \to M \to 0$ into exact sequences $0 \to M_{n-1} \to L_{n-2} \to \cdots \to L_1 \to L_0 \to M \to 0$ and $0 \to M_n \to L_{n-1} \to M_{n-1} \to 0$. □

Proposition 8.5 *Let I and J be ideals in a commutative ring R. Then* $\mathrm{Tor}_1(R/I, R/J) \cong \frac{I \cap J}{IJ}$ *and for all $i \geq 1$,* $\mathrm{Tor}_{i+1}(R/I, R/J) \cong \mathrm{Tor}_i(I, R/J)$.

Proof. The short exact sequence $0 \to I \to R \to R/I \to 0$ yields the long exact sequence

$$\cdots \to \mathrm{Tor}_1^R\left(R, \frac{R}{J}\right) \to \mathrm{Tor}_1^R\left(\frac{R}{I}, \frac{R}{J}\right) \to \mathrm{Tor}_0^R\left(I, \frac{R}{J}\right) \to \mathrm{Tor}_0^R\left(R, \frac{R}{J}\right) \to \mathrm{Tor}_0^R\left(\frac{R}{I}, \frac{R}{J}\right) \to 0.$$

In other words, the following is exact:

$$0 \to \mathrm{Tor}_1^R(R/I, R/J) \to I/JI \to R/J \to R/(I+J) \to 0.$$

But the kernel of $I/JI \to R/J$ equals $(I \cap J)/IJ$.

The last part follows from Property 6. Tor on syzygies. □

Note that the proof does not require knowing a projective resolution of R/I or of R/J.

Definition 8.6 *An R-module M is* **torsion** *if for every $x \in M$ there exists a non-zerodivisor $r \in R$ (possibly a unit) such that $rx = 0$. A module M is* **torsion-free** *if no non-zero element in M is annihilated by any non-zerodivisor in R.*

The following may justify the name "Tor".

Theorem 8.7 (Tor and torsion) *Let M and N be modules over a commutative domain R. Then for all $i \geq 1$, $\mathrm{Tor}_i^R(M, N)$ is torsion.*

Proof. First suppose that N is torsion. For any R-module P an arbitrary element of $P \otimes_R N$ is of the form $\sum_{j=1}^s p_j \otimes n_j$ for $p_1, \ldots, p_s \in P$ and $n_1, \ldots, n_s \in N$. Since N is torsion there exists a non-zerodivisor r_i in R such that $r_i n_i = 0$. Then $r = r_1 \cdots r_s$ is a non-zerodivisor in R and $r \sum_{j=1}^s p_j \otimes n_j = 0$. Thus $P \otimes_R N$ is torsion. In particular, $P_i \otimes N$ is torsion for all i, whence $\mathrm{Tor}_i^R(M, N)$ is torsion.

Now suppose that N is torsion-free. Let K be the field of fractions of R. Then the natural map $N \to N \otimes K$ is an injection. Furthermore, $N \otimes K$ is a flat R-module (as it is a vector space over K), and $(N \otimes K)/N$ is torsion. Then the short exact sequence $0 \to N \to N \otimes K \to (N \otimes K)/N \to 0$ yields via Theorem 8.1 and Corollary 8.4 that for all $i \geq 1$,

$$\mathrm{Tor}_i^R(M, N) \cong \mathrm{Tor}_i^R(N, M) \cong \mathrm{Tor}_{i+1}^R(N \otimes K/N, M) \cong \mathrm{Tor}_{i+1}^R(M, N \otimes K/N),$$

which is torsion by the first part.

If N is arbitrary, we take N' to be the submodule generated by all the non-zero elements that are annihilated by some non-zero element of R. In other words, N' is the torsion submodule of N. It is straightforward to prove that $N'' = N/N'$ is torsion-free. Then the long exact sequence on homology obtained from the short exact sequence $0 \to N' \to N \to N'' \to 0$ gives that for all $i \geq 1$,

$$\mathrm{Tor}_i^R(M, N') \xrightarrow{f} \mathrm{Tor}_i^R(M, N) \xrightarrow{g} \mathrm{Tor}_i^R(M, N/N')$$

is exact. By previous work we know that the two outside modules are torsion. Let $x \in \operatorname{Tor}_i^R(M, N)$. Then there exists a non-zerodivisor $r \in R$ such that $g(rx) = rg(x) = 0$. Thus there exists $y \in \operatorname{Tor}_i^R(M, N')$ such that $f(y) = rx$. But for some non-zerodivisor s in R we have that $sy = 0$, so that the non-zerodivisor sr multiplies x to $srx = sf(y) = f(sy) = 0$. Since x was arbitrary, this proves that $\operatorname{Tor}_i^R(M, N)$ is torsion. $\square$

Exercise 8.8 Let I and J be ideals in a commutative ring R such that $I + J = R$. Use the previous exercise to discuss the Chinese Remainder Theorem in terms of short exact sequences.

Exercise 8.9 Let $(R, \mathfrak{m})$ be a Noetherian local ring, and let $\cdots F_n \to F_{n-1} \to \cdots \to F_1 \to F_0 \to M \to 0$ be a minimal free resolution of M. By Proposition 6.8 we know that each F_n has finite rank. Prove that $\operatorname{rank} F_n = \dim_{R/\mathfrak{m}} \operatorname{Tor}_n^R(M, R/\mathfrak{m})$.

Exercise 8.10 (This is relevant for the assumptions in Theorem 8.7.) Find a Noetherian commutative ring R with identity and an R-module N such that $N \otimes_R K$ is not flat over R, where K is the total ring of fractions of R (K is the localization of R at the multiplicatively closed set consisting of all non-zerodivisors of R).

9 Regular rings, part I

Theorem 9.1 (Auslander and Buchsbaum) *Let $(R, \mathfrak{m})$ be a Noetherian local ring and n a non-negative integer. The following statements are equivalent:*

(1) $\operatorname{pd}_R(R/\mathfrak{m}) \le n$.
(2) $\operatorname{pd}_R(M) \le n$ *for all finitely generated R-modules M.*
(3) $\operatorname{Tor}_i^R(M, R/\mathfrak{m}) = 0$ *for all $i > n$ and all finitely generated R-modules M.*

Proof. Trivially (2) implies (1) and (3). Also, (1) implies (3) since $\operatorname{Tor}_i^R(M, R/\mathfrak{m}) \cong \operatorname{Tor}_i^R(R/\mathfrak{m}, M)$.

Now let M be a finitely generated R-module. Let $P_\bullet$ be its minimal free resolution as in Theorem 6.7. By Proposition 6.8, the image of $P_i \to P_{i-1}$ for $i \ge 1$ is in $\mathfrak{m}P_{i-1}$. Thus all the maps in $P_\bullet \otimes R/\mathfrak{m}$ are 0, so that $\operatorname{Tor}_i^R(M, R/\mathfrak{m}) = P_i/\mathfrak{m}P_i$. If we assume (3), then $P_i/\mathfrak{m}P_i = 0$ for all $i > n$, and since P_i is finitely generated it follows by Nakayama's lemma that $P_i = 0$ for $i > n$. Thus $\operatorname{pd}_R(M) \le n$. Thus (3) implies (2). $\square$

Definition 9.2 *A Noetherian local ring $(R, \mathfrak{m})$ is* **regular** *if* $\operatorname{pd}_R(R/\mathfrak{m}) < \infty$.

Theorem 9.3 *Let $(R, \mathfrak{m})$ be a regular local ring, using Definition 9.2. Then for any prime ideal P in R, R_P is regular (under the same definition).*

Proof. By Theorem 9.1, R/P has a finite projective resolution. Since a localization of a projective resolution is a projective resolution, we get that $(R/P)_P = R_P/PR_P$ has finite projective dimension. Hence by Theorem 9.1, since PR_P is the unique maximal ideal of R_P, R_P is regular. $\square$

Theorem 9.4 (**The (almost) Hilbert Syzygy Theorem**) *Let R be a polynomial ring in finitely many variables over a field k. Then every finitely generated R-module has finite projective dimension.*

(What makes this result an **almost** Hilbert Syzygy Theorem is that it does not assert that the projective dimension is at most the number of variables. That part is proved in Theorem 13.6.)

Proof. We know that the variables form a regular sequence in R. Thus by Theorem 4.7, the Koszul complex gives a free resolution of the field. Thus the projective dimension of the field over R is at most the number n of variables. The same proof as that in Theorem 9.1 shows that every finitely generated graded module has projective dimension at most n.

Now let M be an arbitrary finitely generated R-module (not necessarily graded). Let $R^{b_1} \xrightarrow{\alpha} R^{b_0} \to M \to 0$ be exact. Here, α is a $b_0 \times b_1$ matrix with entries in R. Let d be the largest degree of any entry of α. Introduce a new variable t over R, and homogenize each entry of α with t to make it of degree d. (For example, the homogenization of $x^2+xy^4-3xz^2$ to degree 5 is $x^2t^3+xy^4-3xz^2t^2$, and the homogenization to degree 6 is $x^2t^4+xy^4t-3xz^2t^3$.) Let $S = R[t]$, and let $\widehat{\alpha}$ be the resulting matrix with entries in S. Let $\widehat{M}$ be the cokernel of $\widehat{\alpha}$. Then $\widehat{M}$ is a graded finitely generated module over S, so that by the established graded part, there exists a free resolution $F_\bullet$ of $\widehat{M}$ over S of length at most $n+1$. Certainly $1-t$ is a non-zerodivisor on S, and $0 \to S \xrightarrow{1-t} S \to 0)$ is a resolution of $S/(1-t)S = R$ over S. Thus for all $i \geq 0$, $H_i(F_\bullet \otimes_S (S/(1-t)S)) = \mathrm{Tor}_i^S(\widehat{M}, S/(1-t)S) = H_i(0 \to \widehat{M} \xrightarrow{1-t} \widehat{M} \to 0)$. Since $\widehat{M}$ is graded, the non-homogeneous element $1-t$ is a non-zerodivisor on $\widehat{M}$, so that for all $i \neq 0$, $H_i(F_\bullet \otimes_S (S/(1-t)S)) = 0$. Hence $F_\bullet \otimes_S (S/(1-t)S)$ is a free R-resolution of $H_0(0 \to \widehat{M} \xrightarrow{1-t} \widehat{M} \to 0) = \widehat{M}/(1-t)\widehat{M}$, which is the cokernel of $\widehat{\alpha} \otimes_S (S/(1-t)S) = \alpha$, so it is M. This proves that M has finite projective dimension over R. (In fact, it has projective dimension at most n by the Auslander-Buchsbaum formula, see Theorem 13.6.) $\square$

It is time to connect projective dimensions of modules to the Krull dimension and to more classical ring-theoretic properties. Krull dimension is reviewed in Section 10.

Definition 9.5 *A Noetherian local ring $(R, \mathfrak{m})$ is* **regular** *if the minimal number of generators of $\mathfrak{m}$ is the same as the Krull dimension of R.*

It turns out that the two definitions Definition 9.2 and Definition 9.5 of regularity coincide. We will prove this later in Section 14. Naturally, the homological definition came on the scene much later. It is difficult (or even impossible) to prove that a localization of a regular local ring (regular in the sense above) at a prime ideal is regular, whereas with the homological definition of regularity we proved it very easily in Theorem 9.3.

Exercise 9.6 Let $(R, \mathfrak{m})$ be a Noetherian local ring and let M be a finitely generated R-module. Prove that $\mathrm{pd}_R(M) = \sup\{n : \mathrm{Tor}_n^R(M, R/\mathfrak{m}) \neq 0\}$.

10 Review of Krull dimension

Definition 10.1 *We say that $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ is a* **chain of prime ideals** *if $P_0, \ldots, P_n$ are prime ideals. We also say that this chain has* **length n**, *and that the chain* **starts** *with P_0 and* **ends** *with P_n. The chain is* **saturated** *if for all $i = 1, \ldots, n$ there is no prime ideal strictly between P_{i-1} and P_i.*

An example of a saturated chain of prime ideals is $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \cdots \subsetneq (X_1, \ldots, X_n)$ in $k[X_1, \ldots, X_n]$, where k is a field and $X_1, \ldots, X_n$ are variables. It is clear that this is a chain of prime ideals, and to see that it is saturated between $(X_1, \ldots, X_{i-1})$ and $(X_1, \ldots, X_i)$, we may pass to the quotient ring modulo $(X_1, \ldots, X_{i-1})$ and localize at $(X_1, \ldots, X_i)$, so that we are verifying whether a localization of $k(X_{i+1}, \ldots, X_n)[X_i]$ has any prime ideals between (0) and (X_i). But since this ring is a principal ideal domain, we know that there are no intermediate prime ideals.

In rings arising in algebraic geometry and number theory, namely in commutative rings that are finitely generated as algebras over fields or over the ring of integers, whenever $P \subseteq Q$ are prime ideals, the length of any two saturated chains of prime ideals that start with P and end with Q are the same. Rings with this property are called **catenary**. See Remark 15.4 for a proof that indeed these rings are catenary.

Definition 10.2 *The* **height (or codimension)** *of a prime ideal P is the supremum of all the lengths of chains of prime ideals that end with P. The* **height (or codimension)** *of an arbitrary ideal I is the infimum of all the heights of prime ideals that contain I. The height of an ideal I is denoted as $\mathrm{ht}(I)$.*

The **(Krull) dimension** *of a ring R, denoted $\dim R$, is the supremum of all the heights of prime ideals in R.*

Let R be a commutative ring and let M be an R-module. The **(Krull) dimension** *of M is $\dim(R/\mathrm{ann}(M))$.*

If $I = R$, i.e., when I is not contained in any prime ideal of R, then the infimum is taken over an empty set of integers, so that $\mathrm{ht}(I) = \infty$. For proper ideals the height is either a non-negative integer or ∞. We prove in Corollary 10.4 that in a Noetherian ring every proper ideal has finite height.

The Krull dimension of a field is 0, the Krull dimension of a principal ideal domain that is not a field is 1. It is proved in Atiyah-MacDonald [1] that if R is commutative Noetherian, then for any variable X over R, $\dim R[X] = \dim R + 1$. In particular, $\dim k[X_1, \ldots, X_n] = n$, if k is a field and $X_1, \ldots, X_n$ are variables over k. Note that the Krull dimension of $k[X]/(X^2)$ is 0, but that the k-vector space dimension is 2.

Theorem 10.3 (Krull Principal Ideal Theorem, or Krull's Height Theorem) *Let R be a Noetherian ring, let $x_1, \dots, x_n \in R$, and let P be a prime ideal in R minimal over $(x_1, \dots, x_n)$. Then $\operatorname{ht} P \le n$.*

Proof. Height of a prime ideal does not change after localization at it, so we may assume without loss of generality that P is the unique maximal ideal in R.

The case $n = 0$ is trivial, then P is minimal over the ideal generated by the empty set, i.e., P is minimal over (0), so P is a minimal prime ideal and no prime ideal is strictly contained in it, so that $\operatorname{ht} P = 0$.

Next we prove the case $n = 1$. Let Q be a prime ideal strictly contained in P. We want to prove that Q is a minimal prime ideal. Since P is minimal over (x_1), it follows that $R/(x_1)$ has only one prime ideal, so that $R/(x_1)$ is Artinian. It follows that the descending sequence

$$Q + (x_1) \supseteq Q^2 R_Q \cap R + (x_1) \supseteq Q^3 R_Q \cap R + (x_1) \supseteq \cdots$$

stabilizes somewhere, so there exists n such that $Q^{n+1} R_Q \cap R + (x_1) = Q^n R_Q \cap R + (x_1)$. Thus $Q^n R_Q \cap R \subseteq (Q^{n+1} R_Q \cap R + (x_1)) \cap Q^n R_Q \cap R = Q^{n+1} R_Q \cap R + (x_1) \cap Q^n R_Q \cap R$. Since $Q^n R_Q$ is primary in R_Q,* it follows that $Q^n R_Q \cap R$ is primary in R. Since x_1 is not in Q, x_1 is a non-zerodivisor modulo the Q-primary ideal $Q^n R_Q \cap R$, so that $(x_1) \cap Q^n R_Q \cap R = x_1(Q^n R_Q \cap R)$. Hence $Q^n R_Q \cap R \subseteq Q^{n+1} R_Q \cap R + x_1(Q^n R_Q \cap R)$, and even equality holds. Thus by Nakayama's lemma, $Q^n R_Q \cap R = Q^{n+1} R_Q \cap R$, so that $Q^n R_Q = Q^{n+1} R_Q$, and so by Nakayama's lemma again, $Q^n R_Q = 0$. This says that in the Noetherian local ring R_Q the maximal ideal is nilpotent, so that R_Q is Artinian and $Q R_Q$ has height 0. This proves the case $n = 1$.

Now let $n \ge 2$. Let $P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_n \subsetneq P = P_{n+1}$ be a chain of prime ideals. If $x_1 \in P_0$, then P/P_0 is minimal over the ideal $(x_2, \dots, x_n)(R/P_0)$, so that by induction on n, $\operatorname{ht}(P/P_0) \le n - 1$, which contradicts the existence of the chain above. So $x_1 \notin P_0$. Let i be the smallest integer such that $x_1 \in P_{i+1} \setminus P_i$. We just proved that $i \in \{0, \dots, n\}$. Suppose that $i > 0$. Then in the Noetherian local domain $R_{P_{i+1}}/P_{i-1}R_{P_{i+1}}$, the maximal ideal has height at least 2 and it contains the non-zero image of x_1. Let Q be a prime ideal in this domain that is minimal over the image of (x_1). By the case $n = 1$, the height of Q is at most 1, and since Q cannot be the minimal prime ideal as it contains a non-zero element, it follows that the height of Q is 1. Thus Q is not the maximal ideal in this ring and it lifts to R to a prime ideal strictly between P_{i-1} and P_{i+1} that contains x_1. So by possibly replacing P_i with Q, we may assume that $x_1 \in P_i$, and by repetition of this argument, we may assume that $x_1 \in P_1$. The prime ideal P/P_1 is minimal over $(x_2, \dots, x_n)(R/P_1)$, so that by induction on n, $\operatorname{ht}(P/P_1) \le n - 1$, which gives a contradiction to the existence of the long chain of prime ideals. $\square$

* A review of primary modules is in Section 12.

Corollary 10.4 *Every ideal in a Noetherian ring has finite height.*

Proof. Let I be an ideal. Since the ring is Noetherian, I is finitely generated, say by n elements. By Theorem 10.3 the height of every prime ideal minimal over I is at most n, so that the height of I is at most n. $\square$

Thus every Noetherian local ring is finite-dimensional, but there exist Noetherian rings that are not finite-dimensional.

Theorem 10.5 (A converse of the Krull Principal Ideal Theorem) *Let R be a Noetherian ring, and let P be a prime ideal in R of height n. Then there exist $x_1, \ldots, x_n \in P$ such that P is minimal over $(x_1, \ldots, x_n)$.*

More precisely, for all i we take x_{i+1} to be an element of P that is not contained in any prime ideal minimal over the ideal $(x_1, \ldots, x_i)$ of height i.

Proof. If the height of P is 0, there is nothing to do, as P is minimal over the ideal generated by the empty set.

Now suppose that $n > 0$. We determine $x_1, \ldots, x_n$ recursively. Suppose that we have constructed $x_1, \ldots, x_i \in P$ with $i < n$ and that $(x_1, \ldots, x_i)$ has height i. When $i = 0$, then $(x_1, \ldots, x_i) = (0)$ certainly has height 0. By primary decomposition there are only finitely many primes minimal over $(x_1, \ldots, x_i)$, and they all have height i. By Prime Avoidance there exists $x_{i+1} \in P$ that avoids all these finitely many primes. Necessarily $(x_1, \ldots, x_{i+1})$ has height strictly bigger than i, and by the Krull Principal Ideal Theorem it must have height exactly equal to $i+1$. We stop when we construct n elements in this way. Necessarily by height considerations P is minimal over $(x_1, \ldots, x_n)$. $\square$

Definition 10.6 *In a Noetherian local ring $(R, \mathfrak{m})$ any sequence of* $\dim R$ *elements that generate an $\mathfrak{m}$-primary ideal is called a* **system of parameters***.*

There are typically infinitely many systems of parameters in a Noetherian local ring, but by definition they all have the same length. The following is immediate from Theorem 10.5:

Corollary 10.7 *Let $(R, \mathfrak{m})$ be a Noetherian local ring of dimension n. For $i = 0, \ldots, n-1$ let x_{i+1} be an element of $\mathfrak{m}$ that is not contained in any prime ideal minimal over $(x_1, \ldots, x_i)$. Then $x_1, \ldots, x_n$ is a system of parameters.* $\square$

Proposition 10.8 *Let $(R, \mathfrak{m})$ be a Noetherian local ring and let M be a finitely generated non-zero R-module. The following integers are the same:*

(1) *The Krull dimension $\dim(M)$ of M.*

(2) *The smallest integer n for which there exist $y_1, \ldots, y_n$ in $\mathfrak{m}$ with $(y_1, \ldots, y_n) + \operatorname{ann} M$ being $\mathfrak{m}$-primary.*

(3) *The smallest integer l for which there exist $z_1, \ldots, z_l$ in $\mathfrak{m}$ with $M/(z_1, \ldots, z_l)M$ being of finite length.*

Proof. The non-zero assumption says that $\operatorname{ann}(M) \subseteq \mathfrak{m}$. The dimension of M is the dimension of $R/\operatorname{ann}(M)$, which equals the height of $\mathfrak{m}/\operatorname{ann}(M)$ and so it is finite. Let $d = \dim(M)$.

By Theorem 10.5 there exist $x_1, \ldots, x_d \in \mathfrak{m}$ such that $\mathfrak{m}/\operatorname{ann}(M)$ is minimal over $((x_1, \ldots, x_d) + \operatorname{ann}(M))/\operatorname{ann}(M)$. Thus $\mathfrak{m}$ is minimal over $(x_1, \ldots, x_d) + \operatorname{ann}(M)$ and since $\mathfrak{m}$ is the only prime ideal containing $(x_1, \ldots, x_d) + \operatorname{ann}(M)$, necessarily $(x_1, \ldots, x_d) + \operatorname{ann}(M)$ is $\mathfrak{m}$-primary. Thus finite collections of elements as in (2) exist and $n \leq d$ by minimality of n.

Assume that $(y_1, \ldots, y_n) + \operatorname{ann}(M)$ is $\mathfrak{m}$-primary. Then there exists a positive integer e such that $\mathfrak{m}^e \subseteq (y_1, \ldots, y_n) + \operatorname{ann}(M)$. Set $F_i = \mathfrak{m}^i(M/(y_1, \ldots, y_n)M)$. This gives the finite filtration

$$0 = F_e \subseteq F_{e-1} \subseteq F_{e-2} \subseteq \cdots \subseteq F_1 \subseteq F_0 = M/(y_1, \ldots, y_n)M.$$

For each i, the ith quotient F_i/F_{i+1} of consecutive modules is an $(R/\mathfrak{m})$-module and its $(R/\mathfrak{m})$-vector space dimension at most the number of generators of $\mathfrak{m}^i$ times the number of generators of M. Thus the length of F_0 is finite, so that finite collections of elements as in (3) exist and $l \leq n$ by minimality of l.

Now assume that $M' = M/(z_1, \ldots, z_l)M$ has finite length. Let P be a prime ideal minimal over $(z_1, \ldots, z_l) + \operatorname{ann}(M)$. If P does not contain the annihilator of M' then $M'_P = 0$, i.e., $M_P \subseteq (z_1, \ldots, z_l)M_P$. Since the z_i are in the maximal ideal of R_P and since M_P is finitely generated, by Nakayama's lemma we have that $M_P = 0$. But this contradicts that P contains $\operatorname{ann}(M)$. So necessarily P contains the annihilator of M'. Since $\operatorname{ann}(M')$ contains $(z_1, \ldots, z_l) + \operatorname{ann}(M)$ it follows that the radicals of the two ideals are identical. By assumption $\operatorname{ann}(M')$ contains a power of the maximal ideal so that $\mathfrak{m}$ is the only prime ideal containing $\operatorname{ann}(M')$ and hence it is the only prime ideal containing $(z_1, \ldots, z_l) + \operatorname{ann}(M)$. Thus by Theorem 10.3, $d = \dim(M) = \operatorname{ht}(R/\operatorname{ann}(M)) \leq l$.

This proves that $d \geq n \geq l \geq d$ so that all the numbers are the same. □

Proposition 10.9 *Let $(R, \mathfrak{m})$ be a Noetherian local ring and let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of finitely generated R-modules. Then*

(1) $\dim M \leq \max\{\dim M', \dim M''\}$,

(2) $\dim M', \dim M'' \leq \dim M$.

(3) $\dim M = \max\{\dim M', \dim M''\}$,

Proof. Let $n = \max\{\dim M', \dim M''\}$. By Prime Avoidance and Theorem 10.5, we may choose $x_1, \ldots, x_n \in \mathfrak{m}$ so that $(x_1, \ldots, x_n) + \operatorname{ann} M'$ and $(x_1, \ldots, x_n) + \operatorname{ann} M''$ are $\mathfrak{m}$-primary. In the sequel $\underline{x}$ stands for $x_1, \ldots, x_n$. This means that the modules $M'/(\underline{x})M'$ and $M''/(\underline{x})M''$ have Krull dimension 0, i.e., they have finite length. By the right-exactness of the tensor product, tensoring with $R/(\underline{x})$ yields the following exact complex:

$$M'/(\underline{x})M' \to M/(\underline{x})M \to M''/(\underline{x})M'' \to 0.$$

Thus the middle module $M/(\underline{x})M$ also has finite length, so that $\dim M \leq n$ by Proposition 10.8. This proves (1).

Now let $n = \dim M$. By Proposition 10.8 there exist $x_1, \ldots, x_n \in \mathfrak{m}$ so that $(\underline{x}) + \operatorname{ann} M$ is $\mathfrak{m}$-primary. Then $M/(\underline{x})M$ has finite length, and so necessarily $M''/(\underline{x})M''$ has finite length. Thus again by Proposition 10.8 the dimension of M'' is at most n, i.e., $\dim M'' \leq \dim M$. The long exact sequence on Tor from the given short exact sequence gives that

$$\operatorname{Tor}_1^R(M'', R/(\underline{x})) \to M'/(\underline{x})M' \to M/(\underline{x})M \to M''/(\underline{x})M'' \to 0$$

is exact. Set $I = (\underline{x}) + \operatorname{ann} M''$. We have that $I \subseteq \operatorname{ann} \operatorname{Tor}_1^R(M'', R/(\underline{x}))$ by Property 7. of Tor. Clearly $\operatorname{ann}(M)$ is contained in $\operatorname{ann}(M'')$ so that I contains the $\mathfrak{m}$-primary ideal $(\underline{x}) + \operatorname{ann} M$. Thus I is either R or an $\mathfrak{m}$-primary ideal. In any case, the finitely generated R-module $\operatorname{Tor}_1^R(M'', R/(\underline{x}))$ is a finitely generated module over the finite-length ring R/I, so that $\operatorname{Tor}_1^R(M'', R/(\underline{x}))$ has finite length. The long exact sequence then gives that $M'/(\underline{x})M'$ also has finite length, and so by Proposition 10.8 $\dim M' \leq n$. This finishes the proof of (2).

(1) and (2) combine to give (3). □

Exercise 10.10 Let $(R, \mathfrak{m})$ be a Noetherian local ring and let M be a finitely generated R-module of positive dimension. Let $x \in \mathfrak{m}$ not be in any prime ideal minimal over $\operatorname{ann}(M)$. Prove that $\dim(M/xM) = \dim M - 1$. (Hint: Use Theorem 10.5.)

Exercise 10.11 Let $(R, \mathfrak{m})$ be a Noetherian local ring and let M be a finitely generated R-module of dimension d. Let $x_1, \ldots, x_n \in \mathfrak{m}$. Prove that $M/(x_1, \ldots, x_n)M$ has dimension at least $d - n$.

Exercise 10.12 Let $P' \subseteq P$ be prime ideals in a Noetherian ring with at least one intermediate prime ideal. Prove that there exist infinitely many prime ideals between P' and P. (Hint: Adapt the proof of Theorem 10.3.)

Exercise 10.13 Let (R, m) be a Noetherian local ring of dimension d. Suppose that $m = (x_1, \ldots, x_d)$.

(1) Prove that R is a field if $d = 0$.

(2) Prove that R is a principal ideal domain if $d = 1$.

Exercise 10.14 Find an example of a Noetherian ring of infinite Krull dimension.

11 Primary decomposition of modules

This section contains a quick review of the theory of primary decompositions in case R is Noetherian and M is a finitely generated module over R. The proofs are straightforward and mostly omitted.

(1) A submodule N of M is said to be **primary** if $N \neq M$ and whenever $r \in R$, $m \in M \setminus N$, and $rm \in N$, then there exists a positive integer n such that $r^n M \subseteq N$. In other words, N is primary in M if and only if for any $r \in R$, whenever multiplication by r on M/N is not injective, then multiplication by r is nilpotent on M/N.

(2) If $N \subseteq M$ is a primary submodule, then $\sqrt{N :_R M}$ is a prime ideal. In this case N is also called P**-primary**, where $P = \sqrt{N :_R M}$. Then also $N :_R M$ is a P-primary ideal.

(3) The intersection of any finite set of P-primary submodules of M is P-primary.

(4) If $N \subseteq M$ is a P-primary submodule, then for any $r \in R$,

$$N :_M r = \begin{cases} N, & \text{if } r \notin P; \\ M, & \text{if } r \in N :_R M; \\ \text{a } P\text{-primary submodule of } M & \\ \qquad \text{strictly containing } N, & \text{if } r \in P \setminus (N :_R M), \end{cases}$$

and for any $m \in M$,

$$N :_R m = \begin{cases} R, & \text{if } m \in N; \\ \text{a } P\text{-primary ideal containing } N :_R M, & \text{if } m \notin N. \end{cases}$$

Moreover, there exists $m \in M$ such that $N : m = P$.

(5) By the Noetherian conditions every proper submodule $N \subsetneq M$ can be written as a finite intersection of primary submodules of M. Such an intersection is called a **primary decomposition** of N in M.

(6) By (3) we may re-write an arbitrary primary decomposition of N as an intersection of primary modules that are primary for distinct prime ideals. If in addition we remove any redundant intersectands, the decomposition is called **minimal** or **irredundant**.

(7) The set of prime ideals P such that a P-primary submodule appears in an irredundant primary decomposition of $N \subseteq M$ is uniquely determined. Such prime ideals are called **associated primes** of N, and their set is denoted $\text{Ass}_R(M/N)$.

(8) In this set-up $\text{Ass}_R(M/N)$ is a finite set.

(9) If $N = \cap_i N_i$ is an (irredundant) primary decomposition of N in M, then $0 = \cap_i (N_i/N)$ is an (irredundant) primary decomposition of 0 in M/N. The set of associated primes of N in M is the set of associated primes of 0 in M/N.

(10) $\operatorname{Ass}_R(M)$ equals the set of prime ideals P of R such that $P = 0_M :_R f$ for some $f \in M$.

(11) The elements of $\operatorname{Ass}_R(M)$ that are minimal with respect to inclusion are called the **minimal primes** of M. The set of minimal primes of M is denoted $\operatorname{Min}(M)$.

(12) If U is a multiplicatively closed subset of R and $N \subseteq M$ is P-primary and $U \cap P = \emptyset$, then $U^{-1}N$ is $U^{-1}P$-primary in $U^{-1}M$.

(13) $\operatorname{Min}(M) = \operatorname{Min}(R/\operatorname{ann}(M))$. Proof: Let P be a prime ideal in R. Minimality is preserved after localization, so we may assume that R is Noetherian local with maximal ideal P. If $P \in \operatorname{Min}(M)$ (and it is the maximal ideal of the ring), then the zero submodule of M is P-primary, so that $P = \sqrt{0 :_R M} = \sqrt{\operatorname{ann}_R(M)}$ and $P \in \operatorname{Min}(R/\operatorname{ann}(M))$. If $P \in \operatorname{Min}(R/\operatorname{ann}(M))$ (and it is the maximal ideal of the ring), then P is the only prime ideal containing $\operatorname{ann}_R(M) = 0 :_R M$, so that 0 is the P-primary submodule of M. Thus $\operatorname{Ass}(M) = \{P\}$, and so $P \in \operatorname{Min}(M)$. $\square$

(14) For any $P \in \operatorname{Min} M$, the P-primary component of 0 in M is $\ker(M \to M_P)$. This is uniquely determined. The embedded components are not uniquely determined.

(15) The set of zero divisors on M/N equals $\displaystyle\bigcup_{P \in \operatorname{Ass}(M/N)} P$.

Proof of (5): Let T be the collection of proper submodules of M that cannot be written as a finite intersection of primary submodules. If T is empty, we are done. If T is not empty, since M is Noetherian there exists a maximal element N in T. Then $N \subsetneq M$. By assumption N is not primary. Thus there exist $r \in R$ and $m \in M \setminus N$ such that $rm \in N$ and $r^n M \not\subseteq N$ for all n. The ascending chain $N \subseteq N :_M r \subseteq N :_M r^2 \subseteq N :_M r^3 \subseteq \cdots$. of R-submodules of M must stabilize. By assumption on r the stable value $N' = N :_M r^n$ is a proper submodule of M that properly contains N. Let $N'' = N + r^n M$. Certainly $N \subseteq N' \cap N''$. Let $x \in N' \cap N''$. Then $x = y + r^n z$ for some $y \in N$ and $z \in M$ and $r^n x = r^n y + r^{2n} z \in N$. Since $y \in N$ it follows that $z \in N :_M r^{2n} = N :_M r^n$, so that $x = y + r^n z \in N$. This proves that $N = N' \cap N''$. But both N' and N'' properly contain N, so that by the maximality of N in T the two modules can be written as finite intersections of primary submodules. But then N is such a finite intersection as well. $\square$

12 Regular sequences

Recall Definition 4.6: $x_1, \ldots, x_n \in R$ is a **regular sequence** on a module M if $(x_1, \ldots, x_n)M \neq M$ and if for all $i = 0, \ldots, n-1$, x_{i+1} is a non-zerodivisor on $M/(x_1, \ldots, x_i)M$. We say that this is an M-regular sequence and that it has **length n**.

Saying that x_{i+1} is a non-zerodivisor on $M/(x_1, \ldots, x_i)M$ is that same as saying that $(x_1, \ldots, x_i)M :_M x_{i+1} = (x_1, \ldots, x_i)M$.

If the regular sequence $x_1, \ldots, x_n$ is contained in the Jacobson radical of a Noetherian ring, the order is irrelevant (see Proposition 12.7), but in general the order of the elements in the sequence matters. The standard example is the regular sequence $x, (x-1)y, (x-1)z$ in the polynomial ring $k[x, y, z]$ over a field k; the permutation $(x-1)y, (x-1)z, x$ is not a regular sequence.

Definition 12.1 *Let R be a commutative ring, M an R-module and I an ideal in R. The* **I-depth** *of M is the supremum of the lengths of sequences of elements in I that form regular sequences on M. We denote it by* $\operatorname{depth}_I(M)$. *If (R, m) is local, the* **depth** *of M is the m-depth of M.*

Proposition 12.2 (How to construct a regular sequence) *Let R be a Noetherian ring, let I be an ideal in R, and let M be a finitely generated R-module. Then a regular sequence $x_1, \ldots, x_n \in I$ on M can be constructed as follows: If I is contained in some prime ideal associated to M, then all regular sequences in I on M have length 0, and there is nothing to construct. Othewise, we first choose $x_1 \in I$ that is not in any prime ideal associated to M. We can do this by Prime Avoidance. If I is contained in some prime ideal associated to $M/(x_1)M$, then we stop at x_1, otherwise we may by Prime Avoidance choose $x_2 \in I$ that is not contained in any prime ideal associated to $M/(x_1)M$. If I is contained in some prime ideal associated to $M/(x_1, x_2)M$, then we stop at x_1, x_2, otherwise we may by Prime Avoidance choose $x_3 \in I$ that is not contained in any prime ideal associated to $M/(x_1, x_2)M$. And we continue in this way.*

Clearly this procedure constructs some regular sequence. It terminates in Noetherian modules because if $x_1, x_2, \ldots, x_n \in I$ is a regular sequence on M, then for all $i < n$, $(x_1, \ldots, x_i)M \subsetneq (x_1, \ldots, x_{i+1})M$.

Proposition 12.3 *Let R be a Noetherian ring and M a finitely generated R-module. Let $x_1, x_2, \ldots, x_n \in I$ be a regular sequence on M. Then for all $i < n$, x_{i+1} is not contained in any prime ideal minimal over $(x_1, \ldots, x_i) + \operatorname{ann}(M)$ and $\operatorname{ht}((x_1, \ldots, x_i) + \operatorname{ann}(M)) < \operatorname{ht}((x_1, \ldots, x_{i+1}) + \operatorname{ann}(M))$.*

Proof. Suppose that x_{i+1} is contained in a prime ideal P which is minimal over $(x_1, \ldots, x_i) + \operatorname{ann}(M)$. The minimality of P over $(x_1, \ldots, x_i) + \operatorname{ann}(M)$ means that there exist $s \in R \setminus P$ and a positive integer m such that $sP^m \subseteq (x_1, \ldots, x_i) + \operatorname{ann}(M)$. Thus

$sx_{i+1}^m M \subseteq (x_1, \ldots, x_i)M$ and so $sM \subseteq (x_1, \ldots, x_i)M$. Then after localizing at P and using Nakayama's lemma we get that $M_P = 0$, so that there exists $t \in R \setminus P$ such that $tM = 0$. But then $t \in \operatorname{ann}(M) \subseteq P$, which is a contradiction.

The second part of the conclusion follows from the first part. $\square$

Corollary 12.4 *For any Noetherian ring R, for any proper ideal I, and any finitely generated R-module M, $\operatorname{depth}_I(M) \le \dim M, \operatorname{ht}(I/\operatorname{ann}(M)) \le \operatorname{ht}(I)$. All these numbers are finite.* $\square$

By Theorem 10.5 every regular sequence in a maximal ideal of a Noetherian local ring can be extended to a system of parameters.

What is not clear yet that all choices of $x_1, \ldots, x_n$ of maximal length have the same length. We give a proof of this fact in Proposition 12.9. Another proof is given using Ext in Proposition 26.6.

We can detect existence of some regular sequences via Koszul complexes, say by Theorem 4.8 or by the following:

Proposition 12.5 *Let R be a Noetherian ring, let M be a finitely generated R-module, and let $x_1, \ldots, x_n$ be contained in the Jacobson radical of R. If $H_i(K_\bullet(x_1, \ldots, x_n; M) = 0$ for $i = n, n-1, \ldots, n-l+1$, then there exist $y_1, \ldots, y_n \in R$ such that $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$ and $y_1, \ldots, y_l$ is a regular sequence on M.*

Proof. If $l = 0$, there is nothing to prove. So we may assume that $l > 0$. Then by Exercise 4.11, $0 = H_n(K_\bullet(x_1, \ldots, x_n; M)) = \operatorname{ann}_M(x_1, \ldots, x_n)$. If $(x_1, \ldots, x_n)$ is contained in a prime ideal P associated to M, then $(x_1, \ldots, x_n) \subseteq P = \sqrt{0_M :_R f}$ for some $f \in M$, so that $f \in \operatorname{ann}_M(x_1, \ldots, x_n) = 0$, which means that $P = \sqrt{0_M :_R f} = R$, which is a contradiction. Thus $(x_1, \ldots, x_n)$ is not contained in any prime ideal associated to M. By the strengthened form of Prime Avoidance (Exercise 4.15) there exists an element y_1 that is in a minimal generating set of $(x_1, \ldots, x_n)$ and not in any associated prime of M. Thus $\operatorname{ann}_M(y_1) = 0$, i.e., y_1 is a non-zerodivisor on M. Thus there exist $y_2, \ldots, y_n \in (x_1, \ldots, x_n)$ such that $(y_1, y_2, \ldots, y_n) = (x_1, \ldots, x_n)$. If $l = 1$, we are done. Otherwise, the short exact sequence $0 \to M \xrightarrow{y_1} M \to M/y_1M \to 0$ tensored with the complex $K_\bullet(y_2, \ldots, y_n; R)$ of free modules yields the short exact sequence of complexes

$$0 \to K_\bullet(y_2, \ldots, y_n; M) \xrightarrow{y_1} K_\bullet(y_2, \ldots, y_n; M) \to K_\bullet(y_2, \ldots, y_n; M/y_1M) \to 0.$$

By Equation (4.4), $H_i(K_\bullet(y_2, \ldots, y_n; M))/y_1 H_i(K_\bullet(y_2, \ldots, y_n; M)) = 0$ for all $i = n, n-1, \ldots, n-l+1$. Thus by Nakayama's lemma, $H_i(K_\bullet(y_2, \ldots, y_n; M)) = 0$. By the long exact sequence obtained from the displayed short exact sequence we get that $H_i(K_\bullet(y_2, \ldots, y_n; M/y_1M)) = 0$ for all $i = n, n-1, \ldots, n-l$. Thus by induction there exist $z_2, \ldots, z_n$ such that $(z_2, \ldots, z_n) = (y_2, \ldots, y_n)$ and such that $z_2, \ldots, z_l$ is a regular sequence on M/y_1M. Hence $y_1, z_2, \ldots z_n$ are the desired elements. $\square$

Lemma 12.6 *Whenever x, y is a regular sequence on M and y is a non-zerodivisor on M, then y, x is a regular sequence on M.*

Proof. Suppose $xm = yn$ for some $m, n \in M$. Since x, y is a regular sequence on M there exists $p \in M$ such that $n = xp$. But then $xm = yn = xyp$ and since x is a non-zerodivisor on M it follows that $m = yp$. This proves that x is a non-zerodivisor on M/yM, and so by assumption y, x is a regular sequence on M. $\square$

Proposition 12.7 *Let $x_1, \ldots, x_n$ be in the Jacobson radical of a Noetherian ring. Suppose that $x_1, \ldots, x_n$ is a regular sequence on a finitely generated R-module M. Then for any permutation $\pi \in S_n$ and for any positive integers $m_1, \ldots, m_n$, $x_{\pi(1)}^{m_1}, \ldots, x_{\pi(n)}^{m_n}$ is a regular sequence on M.*

Proof. There are two issues here: we may permute the elements $x_1, \ldots, x_n$, and we may take them to different powers. To prove that the permutation works, it suffices to prove the case of permuting two consecutive elements, i.e., it suffices to prove that if x, y is a regular sequence on M, so is y, x. By Lemma 12.6 it suffices to prove that y is a non-zerodivisor on M. If $ym = 0$ for some $m \in M$, then $ym \in xM$, so by assumption $m \in xM$. Write $m = xm_1$ for some $m_1 \in M$. Then $0 = ym = yxm_1$, and since x is a non-zerodivisor on M, $ym_1 = 0$. By repeating this process, we get that $m_1 \in xM$ whence $m \in x^2M$, and similarly $m \in x^kM$ for all $k \geq 1$. Thus $m \in \cap x^kM$. Since x is in the Jacobson radical it follows that this intersection is 0. This proves that y, x is a regular sequence on M, and so more generally, that $x_{\pi(1)}, \ldots, x_{\pi(n)}$ is a regular sequence on M.

It remains to prove that $x_1^{m_1}, \ldots, x_n^{m_n}$ is a regular sequence on M. Since x_n is a non-zerodivisor on $M/(x_1, \ldots, x_{n-1})M$, so is $x_n^{m_n}$, so that $x_1, \ldots, x_{n-1}, x_n^{m_n}$ is a regular sequence on M. Hence by the previous paragraph, $x_n^{m_n}, x_1, \ldots, x_{n-1}$ is a regular sequence, and by induction we may raise $x_1, \ldots, x_{n-1}$ to various powers and still preserve the regular sequence property, whence by the previous paragraph $x_{\pi(1)}^{m_1}, \ldots, x_{\pi(n)}^{m_n}$ is a regular sequence on M. $\square$

Proposition 12.8 *Let R be a Noetherian ring, let I be an ideal in R, and let M be a finitely generated R-module of depth k. Let $x_1, \ldots, x_k \in I$ be a maximal regular sequence on M. Then there exists $w \in M \setminus (x_1, \ldots, x_k)M$ such that $Iw \subseteq (x_1, \ldots, x_k)M$.*

In particular, if $I = \mathfrak{m}$ is the unique maximal ideal in R, then the following hold.

(1) $\mathfrak{m}$ is associated to $M/(x_1, \ldots, x_k)M$,

(2) There exists $w \in M/(x_1, \ldots, x_k)M$ such that $\mathfrak{m} = \operatorname{ann}(w)$,

(3) There exists an injection $R/\mathfrak{m} \to M/(x_1, \ldots, x_k)M$ (taking 1 to w from part (2)).

Proof. For all parts we may pass to $R/(x_1, \ldots, x_k)$ and $M/(x_1, \ldots, x_k)M$ and assume that $k = 0$.

The assumption on I-depth zero implies that I is contained in an associated prime ideal P of M. Thus there exists $w \in M$ such that $P = 0_M : w$. Hence $w \neq 0$ and $Iw \subseteq Pw = 0$. This proves the first part.

Now assume that $I = \mathfrak{m}$ is the unique maximal ideal in R. If the (finite) set of associated primes of M does not include $\mathfrak{m}$, then by Prime Avoidance we can find $x_{k+1} \in \mathfrak{m}$ which is a non-zerodivisor on M, which contradicts the definition of depth of M being 0. Thus $\mathfrak{m}$ is associated to M, proving (1). This means that there exists a non-zero element $y \in M$ such that $\mathfrak{m} = 0_M : y$. Thus part (2) follows, and (3) is as indicated. □

Proposition 12.9 *Let I be an ideal in a Noetherian ring R and M a finitely generated R-module such that $IM \neq M$. Then all maximal regular sequences on M contained in I have the same length.*

Proof. Let $x_1, \ldots, x_n \in I$ and $y_1, \ldots, y_m \in I$ be maximal regular sequences on M. Without loss of generality $n \leq m$. If $n = 0$, this says that I consists of zerodivisors on M, so that $m = 0$ as well.

Suppose that $n = 1$. Then I consists of zerodivisors on M/x_1M. By Proposition 12.8 there exists $w \in M \setminus x_1M$ such that $Iw \subseteq x_1M$. Thus $y_1w = x_1w'$ for some $w' \in M$. If $w' \in y_1M$, then $y_1w = x_1w' \in x_1y_1M$, so that $w \in x_1M$, which is not the case. So necessarily $w' \notin y_1M$. Also, $Ix_1w' = Iy_1w = y_1Iw \subseteq y_1x_1M$, so that $Iw' \subseteq y_1M$. Thus $w' \notin y_1M$ and I consists of zerodivisors on M/y_1M. Thus $m = 1$ as well.

Now suppose that $n > 1$ and that $m > n$. Then there exists $c \in I$ that is not contained in any associated primes of M, $M/(x_1)M$, $M/(x_1, x_2)M$, …, $M/(x_1, \ldots, x_{n-1})M$, $M/(y_1)M$, $M/(y_1, y_2)M$, …, $M/(y_1, \ldots, y_n)M$. Then $x_1, \ldots, x_{n-1}, c$ and $y_1, \ldots, y_n, c$ are regular sequences on M. Since $x_1, \ldots, x_n$ is a maximal M-regular sequence in I, by possibly first passing to $M/(x_1, \ldots, x_{n-1})M$, the case $n = 1$ says that that $x_1, \ldots, x_{n-1}, c$ is also a maximal M-regular sequence in I. Thus by Lemma 12.6, $c, x_1, \ldots, x_{n-1}$ and $c, y_1, \ldots, y_n$ are regular sequences on M, and necessarily $c, x_1, \ldots, x_{n-1}$ is a maximal M-regular sequence in I. It follows that $x_1, \ldots, x_{n-1}$ and $y_1, \ldots, y_n$ are regular sequences on M/cM, with the first sequence maximal, and so by induction on n, $n \leq n - 1$, which gives a contradiction. Thus $m \leq n$, and by the minimality of n, $m = n$. □

Exercise 12.10 Prove that a prime ideal in a Noetherian ring minimal over an ideal generated by a regular sequence of length n has height exactly n.

Exercise 12.11 Prove that if $x \in I$ is a non-zerodivisor on M, then $\operatorname{depth}_I(M/xM) = \operatorname{depth}_I(M) - 1$.

Exercise 12.12 Prove that $\operatorname{depth}_I(M \oplus N) = \min\{\operatorname{depth}_I(M), \operatorname{depth}_I(N)\}$.

Exercise 12.13 Prove that $\operatorname{depth}_I(M) = \operatorname{depth}_{\sqrt{I}}(M)$.

Exercise 12.14 Let k be a field, x, y variables over k, $R = k[x, y]$ and $M = R/(xy)/$ Prove that $x - y \in R$ is a non-zerodivisor on M. Let $P = (x - y)$. Is $x - y \in R_P$ a regular sequence on M_P?

Exercise 12.15 Let R be a Noetherian commutative ring and let I be a proper ideal in R. Suppose that I is generated by a regular sequence. Prove that I/I^2 is a free (R/I)-module and that R/I has finite projective dimension over R. (See also Exercise 15.12.) (Hint: Koszul complex for the last part.)

13 Regular sequences and Tor

Proposition 13.1 *Let M and N be finitely generated modules over a Noetherian local ring (R, m), and suppose that M is non-zero and with finite projective dimension n and that $m \in \operatorname{Ass} N$. Then $\operatorname{Tor}_n^R(M, N) \neq 0$.*

Proof. Since $m \in \operatorname{Ass} N$, by Proposition 12.8 there exists a short exact sequence $0 \to R/m \to N \to L \to 0$. The relevant part of the induced long exact sequence on Tor is

$$\operatorname{Tor}_{n+1}^R(M, L) \to \operatorname{Tor}_n^R(M, R/m) \to \operatorname{Tor}_n^R(M, N).$$

Since M has projective dimension n, $\operatorname{Tor}_{n+1}^R(M, L) = 0$. By Exercise 9.6, $\operatorname{Tor}_n^R(M, R/m) \neq 0$. Hence $\operatorname{Tor}_n^R(M, N) \neq 0$. □

Corollary 13.2 *Let (R, m) be a Noetherian local ring, let M and N be finitely generated R-modules of finite projective dimension such that m is associated to both. Then $\operatorname{pd}_R(M) = \operatorname{pd}_R(N)$.*

Proof. Let $n = \operatorname{pd} M$ and let $n' = \operatorname{pd} N$. By Proposition 13.1, $\operatorname{Tor}_n^R(M, N) \neq 0$, so that $n' \geq n$. Since $\operatorname{Tor}_n^R(M, N) = \operatorname{Tor}_n^R(N, M)$, by symmetry we get also $n \geq n'$. □

In general the depth of a Noetherian local ring can be strictly smaller than the depth of some finitely generated module. For example, let $R = k[[x, y]]/(x^2, xy)$ and $M = R/(x)$. Then R is a Noetherian local ring of depth 0, but $y \in R$ is a non-zerodivisor on M, so that $\operatorname{depth} M \geq 1$. See the contrast with the proposition below:

Proposition 13.3 *Let (R, m) be a Noetherian local ring and let M be a non-zero finitely generated R-module of finite projective dimension. Then $\operatorname{depth} M \leq \operatorname{depth} R$.*

Proof. Suppose that $d = \min\{\operatorname{depth} R, \operatorname{depth} M\} = \operatorname{depth} R$. By Proposition 12.2, there exists a sequence $x_1, \ldots, x_d \in m$ that is regular on R and on M. By Theorem 4.7, $K_\bullet(x_1, \ldots, x_d; R)$ is a free resolution of $R/(x_1, \ldots, x_d)$, and $K_\bullet(x_1, \ldots, x_d; M) \to M/(x_1, \ldots, x_d)M \to 0$ is exact.

Let $n = \operatorname{pd}_R(M)$. By Proposition 12.8, m is associated to $R/(x_1, \ldots, x_d)$, and so by Proposition 13.1,

$$H_n(K_\bullet(x_1, \ldots, x_d; M)) = H_n(M \otimes K_\bullet(x_1, \ldots, x_d; R)) = \operatorname{Tor}_n^R(M, R/(x_1, \ldots, x_d))$$

is non-zero. Thus by exactness of $K_\bullet(x_1, \ldots, x_d; M)$ necessarily $n = 0$. But then M is a projective R-module, and hence it is free (by Fact 5.5 (6)), whence $\operatorname{depth} M = \operatorname{depth} R$. □

Proposition 13.4 *Let (R, m) be a Noetherian local ring, let M be a finitely generated R-module of projective dimension n, and let $x \in R$ be a non-zerodivisor on R.*

(1) *If x is a non-zerodivisor on M, then M/xM has projective dimension n over R/xR.*

(2) *Suppose that M is not free. Let F be any finitely generated free R-module mapping onto M and let K be the kernel of the surjection $F \to M$). Then K/xK has projective dimension $n-1$ over R/xR.*

Proof. Let $0 \to F_n \to F_{n-1} \to \cdots \xrightarrow{\alpha} F_1 \to F_0 \to M \to 0$ be exact, where all F_i are finitely generated projective and hence free over R (by Fact 5.5 (6)), and where for all $i > 0$, the map $F_{i+1} \to F_i$ has image in mF_i. Tensoring with $R/(x)$ gives the complex

$$0 \to \frac{F_n}{xF_n} \to \frac{F_{n-1}}{xF_{n-1}} \to \cdots \xrightarrow{\alpha} \frac{F_1}{xF_1} \to \frac{F_0}{xF_0} \to \frac{M}{xM} \to 0 \qquad (13.5)$$

which is exact at F_0/xF_0 and M/xM. The homology at the ith place for $i > 0$ is $\operatorname{Tor}_i^R(M, R/(x))$. Since $R/(x)$ has projective dimension 1, the homology is zero at places $i \geq 2$. The homology at the first place is

$$\operatorname{Tor}_1^R(M, R/(x)) = H_1(M \otimes (0 \to R \xrightarrow{x} R \to 0)) = H_1(0 \to M \xrightarrow{x} M \to 0) = (0 :_M x).$$

If x is a non-zerodivisor on M, then $\operatorname{Tor}_1^R(M, R/(x)) = 0$, so that the complex above is a free resolution of M/xM over R/xR. We could have chosen F_0 minimal as well, by assumption on the projective dimension of M and the minimality of the resolution of M, by Proposition 6.8 the resolution of M/xM in (13.5) is minimal as well, which means that the projective dimension of M/xM over R/xR is n.

For the second part we assume that $F_0 = F$ and is thus not necessarily of minimal rank. The resolution in (13.5) is still exact, and so is

$$0 \to \frac{F_n}{xF_n} \to \frac{F_{n-1}}{xF_{n-1}} \to \cdots \xrightarrow{\alpha} \frac{F_1}{xF_1} \to \frac{F_1}{xF_1 + \operatorname{im} \alpha} \to 0$$

is exact. But all the matrices representing the maps in this resolution have entries in $\mathfrak{m}$, so that this resolution is minimal. By construction of resolutions, $\frac{F_1}{\operatorname{im} \alpha} \cong K$, so that $\frac{F_1}{xF_1 + \operatorname{im} \alpha} \cong \frac{K}{xK}$. This proves that the projective dimension of K/xK over R/xR is $n-1$. $\square$

Theorem 13.6 (Auslander–Buchsbaum formula) *Let (R, m) be a Noetherian local ring, and let M be a finitely generated R-module of finite projective dimension. Then* $\operatorname{pd}_R(M) + \operatorname{depth} M = \operatorname{depth} R$.

Proof. Let $d = \operatorname{depth} R$. There exist $x_1, \ldots, x_d \in m$ that form a regular sequence on R. Then by Proposition 12.8, m is associated to $R/(x_1, \ldots, x_d)$. Since $R/(x_1, \ldots, x_d)$ has a minimal finite free resolution via the Koszul complex of length d, its projective dimension is d.

First suppose that $\operatorname{depth} M = 0$. Then by Proposition 12.8, m is associated to M, and so by Corollary 13.2, $\operatorname{depth} R = d = \operatorname{pd}(R/(x_1, \ldots, x_d)) = \operatorname{pd} M = \operatorname{pd} M + \operatorname{depth} M$.

Now suppose that $\operatorname{depth} M > 0$. By Proposition 13.3, $\operatorname{depth} R > 0$. Thus by Proposition 12.2, there exists $x \in m$ that is a non-zerodivisor on M and on R. By Proposition 13.4, M/xM has finite projective dimension over R/xR equal to $\operatorname{pd}_R M$. Also, M/xM has depth exactly one less than M, and $\operatorname{depth} R/(x) = \operatorname{depth} R - 1$, whence by induction on $\operatorname{depth} R$ we get:

$$\begin{aligned}\operatorname{depth} R &= \operatorname{depth}(R/xR) + 1 \\ &= \operatorname{pd}_{R/xR}(M/xM) + \operatorname{depth}(M/xM) + 1 \\ &= \operatorname{pd}_R(M) + \operatorname{depth}(M).\end{aligned}$$

□

Exercise 13.7 Go through this section and remove the finitely generated assumption wherever possible.

14 Regular rings, part II

Here we tie some loose ends from Section 9.

Proposition 14.1 *Let R be a Noetherian ring. Suppose that $(x_1, \ldots, x_d)$ is a prime ideal of height d that lies in the Jacobson radical. Then $(x_1, \ldots, x_{d-1})$ is a prime ideal strictly contained in $(x_1, \ldots, x_d)$.*

Proof. Let $P = (x_1, \ldots, x_d)$ and $J = (x_1, \ldots, x_{d-1})$. Let Q be a prime ideal minimal over J contained in P. By the Krull principal ideal theorem (Theorem 10.3), $Q \neq P$. Suppose that $Q \neq J$. Let $a \in Q$. Since $Q \subseteq P$, we can write $a = j_1 + a_1 x_d$ for some $j_1 \in J$ and some a_1 in R. Then $a_1 x_d \in Q$, and since $x_d \notin Q$, it follows that $a_1 \in Q$. Then we can write a_1 in a similar way as a, and an iteration of this gives that for all $n \geq 1$, $a = j_n + a_n x_d^n$ for some $j_n \in J$ and some a_n in R. Thus $a \in J + (x_d)^n$ for all n, so that since x_d is in the Jacobson radical we conclude that $a \in J$. This proves that $J = Q$ is a prime ideal strictly contained in P. □

Corollary 14.2 *Suppose that $(x_1, \ldots, x_d)$ is a prime ideal of height d contained in the Jacobson radical of a Noetherian ring. Then $x_1, \ldots x_d$ is a regular sequence in R.*

Proof. If $d = 0$, there is nothing to prove. If $d = 1$, then Proposition 14.1 says that (0) is a prime ideal and that x_1 is not in it and so x_1 is a regular sequence in R.

So we may assume that that $d > 1$. Set $J = (x_1, \ldots, x_{d-1})$ and $P = J + (x_d)$. Then P is prime by assumption and J is prime by Proposition 14.1. By the Krull principal ideal theorem (Theorem 10.3), the height of J is at most $d - 1$. If the height of J equals $d - 1$, then by induction on d we get that $x_1, \ldots, x_{d-1}$ is a regular sequence in R, and so by Proposition 14.1 we get that $x_1, \ldots, x_d$ is a regular sequence in R.

Thus we may suppose that $n = \operatorname{ht} J < d-1$. We will prove that this is impossible. We want to choose $y_1, \ldots, y_n \in J$ such that for all $i = 0, \ldots, n-1$, y_{i+1} avoids $P^2 + (y_1, \ldots, y_i)$ and all the prime ideals minimal over $(y_1, \ldots, y_i)$. The latter prime ideals do not contain J by assumption on the height (this part of the construction is as in Theorem 10.5). Suppose that $P^2 + (y_1, \ldots, y_i)$ contains J. Then $P = J + (x_d) \subseteq P^2 + (y_1, \ldots, y_i, x_d)$. Thus by Nakayama's Lemma $P \subseteq (y_1, \ldots, y_i, x_d)$. But the height of the latter ideal is by the Krull Principal Ideal theorem at most $i + 1 \le n < d - 1$ so it cannot contain P. Thus by Prime Avoidance we may choose $y_1, \ldots, y_n \in J$ as specified. By construction, $y_1, \ldots, y_n \in J$ are part of a minimal generating set of P and of J, and J is minimal over $(y_1, \ldots, y_n)$. By possibly modifying the generators of J we may assume that $y_i = x_i$ for all i. By minimality there exist a positive integer m and an element s not in J such that $sJ^m \subseteq (x_1, \ldots, x_n)$. Then for all positive integers e we have that $sJ^m \subseteq (x_1, \ldots, x_n, \ldots x_{d-2}, x_{d-1} + x_d^e)$. The latter ideal is prime strictly contained in P by Proposition 14.1. If this prime ideal contains J, then it contains x_{d-1} and hence also x_d, so it contains P, which contradicts Proposition 14.1. So necessarily $s \in \cap_e (x_1, \ldots, x_{d-2}, x_{d-1} + x_d^e) \subseteq \cap_e (J + (x_d^e)) = J$, which contradicts the assumption. $\square$

We now strengthen Theorem 9.1.

Theorem 14.3 (Auslander and Buchsbaum) *Let $(R, \mathfrak{m})$ be a Noetherian local ring. Then the following are equivalent:*

(1) $\operatorname{pd}_R(R/\mathfrak{m}) = \dim R$.
(2) $\operatorname{pd}_R(M) \le \dim R$ *for all finitely generated R-modules M.*
(3) $\operatorname{Tor}_i^R(M, R/\mathfrak{m}) = 0$ *for all $i > \dim R$ and all finitely generated R-modules M.*
(4) $\operatorname{pd}_R(R/\mathfrak{m})$ *is finite.*
(5) The projective dimension of every finitely generated R-module is finite.
(6) There exists an integer n such that $\operatorname{Tor}_i^R(M, R/\mathfrak{m}) = 0$ for all $i > n$ and all finitely generated R-modules M.
(7) The minimal number of generators of $\mathfrak{m}$ equals the dimension of R.
(8) Every minimal generating set of $\mathfrak{m}$ is a regular sequence.
(9) $\mathfrak{m}$ is generated by a regular sequence.

Proof. Theorem 9.1 says that (2) and (3) are equivalent, that (4) and (6) are equivalent, and that (4) implies (5). Clearly (1) and (2) imply (4) and (5) implies (4).

Assume (5). By the Auslander-Buchsbaum formula (Theorem 13.6), $\operatorname{depth} R = \operatorname{pd}_R(M) + \operatorname{depth}(M)$, and since $\operatorname{depth} R \le \dim R$, this proves (2). In particular, $\operatorname{pd}(R/\mathfrak{m}) \le \dim(R)$.

Thus (2) through (6) are equivalent, and (1) implies (4).

Now assume (2) through (6) and we prove below (1) and (7). Let $n = \operatorname{pd}_R(R/\mathfrak{m})$. By the Auslander-Buchsbaum formula, $n = \operatorname{depth}(R) \le \dim(R)$. If $n = 0$, then $R/\mathfrak{m}$ is a projective hence a free R-module (by Fact 5.5 (6)), whence $R = R/\mathfrak{m}$ is a field, so that (1) holds trivially and (7) holds vacuously. So we assume that $n > 0$. Since $\mathfrak{m}$ is the first syzygy of a minimal free resolution of $R/\mathfrak{m}$ over R, it follows that $\mathrm{pd}_R(\mathfrak{m}) = n-1$. But $\operatorname{depth}(R) = n > 0$, so by Prime Avoidance we can choose a non-zerodivisor $x \in \mathfrak{m}$ that avoids $\mathfrak{m}^2$. Since x is a non-zerodivisor on R and hence on $\mathfrak{m}$, it follows by Proposition 13.4 (1) that $\mathrm{pd}_{R/(x)}(\mathfrak{m}/x\mathfrak{m}) = n-1$. In the sequel we will use that $\dim(R/(x)) + 1 = \dim(R)$, which is a result of Exercise 10.10. Since $x \in \mathfrak{m} \setminus \mathfrak{m}^2$, it is part of a minimal generating set of $\mathfrak{m}$; let J be the ideal generated by the generators other than x in such a generating set. Then

$$\frac{\mathfrak{m}}{x\mathfrak{m}} = \frac{(x)+J}{x\mathfrak{m}} = \frac{(x)+J+x\mathfrak{m}}{x\mathfrak{m}} = \frac{(x)}{x\mathfrak{m}} + \frac{J+x\mathfrak{m}}{x\mathfrak{m}}.$$

The sum of the last two quoient modules is a direct sum because $(x) \cap J = x(J:x) \subseteq x\mathfrak{m}$. Furthermore, $R/\mathfrak{m} \cong (x)/x\mathfrak{m} \cong R/\mathfrak{m}$ and

$$\frac{J+x\mathfrak{m}}{x\mathfrak{m}} \cong \frac{J}{J\cap x\mathfrak{m}} = \frac{J}{J\cap (x) \cap x\mathfrak{m}} = \frac{J}{J\cap (x)} \cong \frac{J+(x)}{(x)} = \frac{\mathfrak{m}}{(x)}.$$

It follows that

$$\frac{\mathfrak{m}}{x\mathfrak{m}} \cong \frac{R}{\mathfrak{m}} \oplus \frac{\mathfrak{m}}{(x)}. \tag{14.4}$$

By Exercise 6.10, we conclude that $n-1$ is the maximum of the projective dimensions of $R/\mathfrak{m}$ and of $\mathfrak{m}/(x)$ over $R/(x)$. By induction on the depth of R, the projective dimension of $R/\mathfrak{m}$ over $R/(x)$ equals $\dim(R/(x))$. This says that $n-1 \geq \dim(R/(x))$, so that $n \geq \dim(R/(x)) + 1 = \dim(R)$. From before we know that $n \leq \dim(R)$, so that we just proved (1). Induction on the depth of the ring also says that $\mathfrak{m}/(x)$ is minimally generated by $\dim(R/(x))$ elements, so that $\mathfrak{m}$ is generated by at most $\dim(R/(x)) + 1 = \dim(R)$ elements, and so by the Krull principal ideal theorem (Theorem 10.3) we just proved (7).

Assume (7). By Nakayama's lemma every minimal generating set of $\mathfrak{m}$ has $\dim R = \operatorname{ht} \mathfrak{m}$ elements, so by Corollary 14.2 every minimal generating set of $\mathfrak{m}$ forms a regular sequence. This proves (8).

(8) implies (9) trivially, and (9) implies (1) via the Koszul resolution of the regular sequence generating $\mathfrak{m}$ (see Theorem 4.7). □

With this theorem we can now see that the Definitions 9.2 and 9.5 of regularity describe identical rings. More generally, we have a new definition:

Definition 14.5 *A Noetherian ring R is* **regular** *if for all maximal ideals $\mathfrak{m}$ in R, $R_\mathfrak{m}$ is regular (by either of the definitions 9.2 and/or 9.5).*

Corollary 14.6 *By Theorem 9.3, R is regular if and only if for all prime ideals P in R, R_P is regular.* □

Examples 14.7

(1) Every field is a regular ring.

(2) Every principal ideal domain and every Dedekind domain is regular. Every Noetherian valuation domain is regular.

(3) Every polynomial ring $k[x_1, \ldots, x_n]$ over a field is regular. Every power series ring $k[[x_1, \ldots, x_n]]$ in indeterminates over a field is regular.

(4) For every regular local ring R, Theorem 14.3 shows that $\operatorname{depth} R = \dim R$. Such rings are called Cohen–Macaulay. More on such rings is in Section 15.

(5) Let R be a regular ring. Let X be a variable over R. Then $R[X]$ is regular. Proof: Let M be a prime ideal in $R[X]$. It suffices to prove that $R[X]_M$ is regular. Let $\mathfrak{m} = M \cap R$. Then $R[X]_M$ is a localization of $R_{\mathfrak{m}}[X]$, so without loss of generality we may replace R with $R_{\mathfrak{m}}$ and thus assume that R is a regular local ring and that M contracts to the maximal ideal $\mathfrak{m}$ in R. Then, since $(R/\mathfrak{m})[X]$ is a principal ideal domain, M is either $\mathfrak{m}R[X]$ or $\mathfrak{m}R[X] + (f)$ for some monic polynomial f in X of positive degree. In the first case, $R[X]_M$ has dimension equal to R and the maximal ideal is generated by the generators of m, so that $R[X]_M$ is regular. In the second case, $R[X]_M$ has dimension equal to $\dim R + 1$ and $MR[X]_M$ is generated by one more element than m, which again proves that $R[X]_M$ is regular.

Question 14.8 Let R be a regular ring of finite (Krull) dimension. Is it true that every finitely generated R-module over R has finite projective dimension? Is it true that for any finitely generated R-module M, $\operatorname{pd}_R(M) \leq \dim R$.

Theorem 14.9 (**The Hilbert Syzygy Theorem**) *Let R be a polynomial ring in n variables over a field and let M be a finitely generated R-module. Then $\operatorname{pd}_R(M) \leq n$.*

Proof. Let $(F_\bullet, d_\bullet)$ be a projective resolution of M. We may assume that all F_i are finitely generated R-modules. If $\operatorname{pd}_R(M) > n$, then the kernel K of the map $d_{n-1} : F_{n-1} \to F_{n-2}$ is not projective. Since R is Noetherian and F_{n-1} is finitely generated, K is finitely presented. By Proposition 5.8 there exists a maximal ideal m in R such that K_m is not projective. But the height of m is n, so by Theorem 9.1 and Proposition 6.6 we get a contradiction. So necessarily $\operatorname{pd}_R(M) \leq n$. □

Remark 14.10 Quillen [8] and Suslin [10] proved independently that every finitely generated projective module over a polynomial ring over a field is free. We did not need this hard result in the proof.

Remark 14.11 There is a very useful criterion, called the **Jacobian criterion**, for determining the regularity of localizations of affine domains. Namely, let $R = k[X_1, \ldots, X_n]/(f_1, \ldots, f_m)$ be a finitely generated equidimensional ring over a field k. Say that its dimension is d. We first form the **Jacobian matrix** of R over k as the $m \times n$ matrix whose (i, j) entry is $\frac{\partial f_i}{\partial X_j}$ (where the derivatives of polynomials are taken as expected, even when k is not $\mathbb{R}$ or $\mathbb{C}$). Certainly this matrix depends on the presentation of R over k. The **Jacobian ideal** $J_{R/k}$ of R over k is the ideal in R generated by all the $(n-d) \times (n-d)$ minors of the Jacobian matrix. It takes some effort to prove that $J_{R/k}$ is independent of the presentation. The **Jacobian criterion** says that at least when k is perfect (say when k has characteristic 0 or if k is a finite field), for a prime ideal P in R, the Noetherian local ring R_P is regular if and only if $J_{R/k} \not\subseteq P$. The proof of this fact would take us too far away from homological algebra, so we won't go through it in class. If you are interested in seeing a proof, read for example Section 4 of Chapter 4 in [4] (and you will need to know the basics on integral closure from earlier in that book).

We apply this criterion to the domain $R = \mathbb{C}[x, y, z]/(xy - z^2)$. The Jacobian matrix is a 1×3 matrix $[y \quad x \quad -2z]$, so that $J_{R/k} = (xy - z^2, y, x, -2z)R = (x, y, z)$. The only prime ideal which contains $J_{R/k}$ is therefore (x, y, z). Hence by the Jacobian criterion $R_{(x,y,z)}$ is not regular, but all other proper localizations of R are regular. We can verify that a maximal regular sequence in $(x, y, z)R_{x,y,z}$ is x, y but that $(x, y, z)R_{x,y,z}$ is not generated by two elements.

The criterion proves that for every finitely generated affine equidimensional reduced ring over a perfect field, the set of all prime ideals at which the ring is not regular is a closed set in the Zariski topology. (Let R be a ring. For any subset S let $V(S)$ be the set of all prime ideals in R that contain S. It is easy to show that $V(S)$ equals $V(I)$ where I is the ideal generated by S. In the **Zariski topology** on the set of all prime ideals of R the closed sets are of the form $V(S)$ as S varies over subsets (or ideals) of R.)

Exercise 14.12 Prove that every regular local ring is a domain. Give examples of regular rings that are not domains.

Exercise 14.13 Let (R, m) be a Noetherian local ring. Let $x \in m$ be a non-zerodivisor on R such that $R/(x)$ is a regular local ring. Prove that R is regular.

Exercise 14.14 Let $R = \mathbb{C}[x^3, x^2y, xy^2, y^3]$. Determine all the prime ideals P for which R_P is regular. (Hint: first rewrite R as a quotient of a polynomial ring over $\mathbb{C}$, then use the Jacobian criterion.)

Exercise 14.15 Let R be a finitely generated $\mathbb{Z}$-algebra contained in a number field K.

i) Give an example of such an R that is not a regular ring.

(ii)* Let A be the integral closure of R in K. (So A is a **ring of integers**.) Prove that A is regular.

Exercise 14.16 Let $(R, \mathfrak{m})$ be a regular local ring. Prove that the m-adic completion of R is a regular local ring.

15 Cohen–Macaulay rings and modules

Recall that in a Noetherian local ring $(R, \mathfrak{m})$ any sequence of $\dim R$ elements that generate an $\mathfrak{m}$-primary ideal is called a **system of parameters**.

Definition 15.1 *A Noetherian local ring* $(R, \mathfrak{m})$ *is* **Cohen–Macaulay** *if* m *contains a regular sequence of length equal to the dimension of* R*, i.e., if some system of parameters in* R *is a regular sequence.*

More generally, a finitely generated R*-module* M *is* **Cohen–Macaulay** *if* $\operatorname{depth} M = \dim M$*.*

A Noetherian ring R *is* **Cohen–Macaulay** *if all of its localizations at maximal ideals are Cohen–Macaulay. A finitely generated* R*-module* M *over a Noetherian ring is* **Cohen–Macaulay** *if for all maximal ideals* $\mathfrak{m}$ *in* R*,* $M_{\mathfrak{m}}$ *is a Cohen–Macaulay* $R_{\mathfrak{m}}$*-module.*

The following are easy facts:

(1) Every regular ring is Cohen–Macaulay.

(2) $\mathbb{Z}$, principal ideal domains, fields, and polynomial and power series rings over fields are Cohen–Macaulay (they are even regular).

(3) Every 0-dimensional Noetherian ring is Cohen–Macaulay.

(4) Every 1-dimensional Noetherian domain is Cohen–Macaulay.

(5) Let $(R, \mathfrak{m})$ be a Noetherian local ring, let M be a Cohen–Macaulay R-module, and let $x_1, \ldots, x_n \in \mathfrak{m}$ form a (not necessarily maximal) regular sequence on M. Then $M/(x_1, \ldots, x_n)M$ is Cohen–Macaulay.

(6) Let x, y be variables over a field k. Then $k[x, y]/(x^2, xy)$ is not Cohen-Macaulay.

Theorem 15.2 *The following are equivalent for a finitely generated module* M *over a Noetherian local ring* $(R, \mathfrak{m})$*:*

(1) M *is Cohen–Macaulay.*

(2) Some system of parameters in $R/\operatorname{ann}(M)$ *forms a regular sequence on* M*.*

(3) Every system of parameters in $R/\operatorname{ann}(M)$ *forms a regular sequence on* M*.*

Proof. Clearly (1) is equivalent to (2), and (3) implies both (1) and (2). Now suppose that (1) and (2) hold. Let $d = \dim M$ and let $y_1, \ldots, y_d \in R$ such that $(y_1, \ldots, y_d) + \operatorname{ann}(M)$ is $\mathfrak{m}$-primary. We need to prove that $y_1, \ldots, y_d$ is a regular sequence on M. If $d = 0$, there is nothing to prove. If $d = 1$, then $R/\operatorname{ann}(M)$ has only finitely many primes: all the minimal primes and $\mathfrak{m}$. Since by assumption $\mathfrak{m}$ contains a non-zerodivisor, all zerodivisors live in the union of the set of all minimal primes. Since y_1 is a parameter in a one-dimensional ring, it is not in any minimal prime, so then it is not a zerodivisor. This proves the case

$d = 1$. Now let $d > 1$. Let $x_1, \ldots, x_d$ be a system of parameters in $R/\mathrm{ann}(M)$ that is a regular sequence on M. By construction of non-zerodivisors and parameters, since it is a matter of avoiding finitely many primes that do not contain $\mathfrak{m}$, there exists $c \in \mathfrak{m}$ such that $x_1, \ldots, x_{d-1}, c$ is a regular sequence on M and such that $(x_1, \ldots, x_{d-1}, c) + \mathrm{ann}(M)$ and $(y_1, \ldots, y_{d-1}, c) + \mathrm{ann}(M)$ are $\mathfrak{m}$-primary. By Proposition 12.7, $c, x_1, \ldots, x_{d-1}$ is a regular sequence on M. Since c is a non-zerodivisor, $\dim(M/cM) = \dim M - 1$ and $\mathrm{depth}(M/cM) = \mathrm{depth}\, M - 1$. Thus M/cM is Cohen–Macaulay. By induction on d, then $y_1, \ldots, y_{d-1}$ is a regular sequence on M/cM, so that $c, y_1, \ldots, y_{d-1}$ is a regular sequence on M. Again by Proposition 12.7, $y_1, \ldots, y_{d-1}, c$ is a regular sequence on M, and then by passing to $M/(y_1, \ldots, y_{d-1})M$ and the case $d = 1$, $y_1, \ldots, y_d$ is a regular sequence on M.□

Theorem 15.3 *Let $(R, \mathfrak{m})$ be a Cohen–Macaulay local ring and let P be a prime ideal in R. Then the following properties hold.*

(1) R_P is a Cohen–Macaulay local ring,

(2) $\mathrm{ht}\, P + \dim(R/P) = \dim R$.

(3) If $x_1, \ldots, x_n$ is any (not necessarily maximal) regular sequence, than any prime ideal associated to $(x_1, \ldots, x_n)$ is minimal over the ideal.

Proof. Certainly by the definition of dimension, we always have $\mathrm{ht}\, P + \dim(R/P) \le \dim R$. Let $n = \mathrm{ht}\, P$ and $d = \dim R$.

By Theorem 10.5 there exists a part of a system of parameters $x_1, \ldots, x_n \in P$ such that P is minimal over $(x_1, \ldots, x_n)$. These can be extended to a full system of parameters $x_1, \ldots, x_d$. By Theorem 15.2, $x_1, \ldots, x_d$ is a regular sequence. Thus P is minimal over the ideal generated by a regular sequence $x_1, \ldots, x_n$, whence PR_P is minimal over an ideal generated by a regular sequence, so that by definition, R_P is Cohen–Macaulay.

We next prove the dimension equality. More generally, we prove that $\mathrm{ht}\, Q = n$ and $\dim(R/Q) = n - d$ for any associated prime ideal Q of $R/(x_1, \ldots, x_n)$. If $n = d$, then $P = \mathfrak{m}$ and we are done. So suppose that $n < d$. Since Q contains a regular sequence of length n we get that $n \le \mathrm{depth}_Q(R) \le \mathrm{ht}\, Q$.

Claim: Q consists of zerodivisors on $R/(x_1, \ldots, x_{n+1})$. Proof: By assumption $Q \subseteq (x_1, \ldots, x_n) : s$ for some $s \notin (x_1, \ldots, x_n)$. Suppose for contradiction that Q is not contained in any prime ideal associated to $(x_1, \ldots, x_{n+1})$. This in particular means that $s \in (x_1, \ldots, x_{n+1})$. We can write $s = r_1 + s_1 x_{n+1}$ for some $r_1 \in (x_1, \ldots, x_n)$ and some $s_1 \in R$. Suppose that we have $s = r_e + s_e x_{n+1}^e$ for some $r_e \in (x_1, \ldots, x_n)$ and some $s_e \in R$. Then $Q \subseteq (x_1, \ldots, x_n) : s_e$ and so $s_e \in (x_1, \ldots, x_{n+1})$ and $s \in (x_1, \ldots, x_n, x_{n+1}^{e+1})$. But this ideal is in the Jacobson radical of R, so that $s \in \cap_e (x_1, \ldots, x_n, x_{n+1}^{e+1}) = (x_1, \ldots, x_n)$, which is a contradiction. This proves the claim.

Thus Q is contained in a prime ideal Q' associated to $R/(x_1, \ldots, x_{n+1})$. By induction on $d - n$, $\mathrm{ht}\, Q' = n + 1$ and $\dim(R/Q') = d - n - 1$. If $Q = Q'$, then Q contains x_{n+1}, but that contradicts the fact that x_{n+1} is a non-zerodivisor on $R/(x_1, \ldots, x_n)$. Thus Q is properly contained in Q' so that $\dim(R/Q) \ge \dim(R/Q') + 1 = d - n$. Also, $d =$

$(d-n)+n \le \dim(R/Q) + \operatorname{ht} Q \le \dim R = d$ forces equality throughout, so that $\operatorname{ht} Q = n$ and $\dim(R/Q) = d-n$. $\square$

Remark 15.4 A ring is called **catenary** if for any prime ideals $P \subseteq Q$, every saturated chain of prime ideals starting at P and ending at Q has the same length. We show next that Cohen–Macaulay rings are catenary. First of all, by the Noetherian property of Cohen–Macaulay rings every chain of prime ideals between P and Q is finite. By Theorem 15.3, $\operatorname{ht}(Q/P) = \operatorname{ht}((Q/P)_Q) = \dim(R_Q/P_Q) = \dim R_Q - \operatorname{ht} P_Q = \operatorname{ht} Q - \operatorname{ht} P$. Let P_1 be any prime ideal strictly between P and Q. Then similarly, $\operatorname{ht}(Q/P_1) = \operatorname{ht} Q - \operatorname{ht} P_1$, $\operatorname{ht}(P_1/P) = \operatorname{ht} P_1 - \operatorname{ht} P$, and so combining the chain of primes between P_1 and Q with the chain between P and P_1 gives a chain of length $\operatorname{ht}(Q/P_1) + \operatorname{ht}(P_1/P) = \operatorname{ht} Q - \operatorname{ht} P = \operatorname{ht}(Q/P)$, and this length is independent of P_1.

Theorem 15.5 (Hironaka) *Let $(R, \mathfrak{m}) \subseteq (S, \mathfrak{n})$ be Noetherian local rings. Suppose that R is regular and that S is module-finite over R. Then S is Cohen–Macaulay if and only if S is a free R-module.*

Proof. Let $d = \dim R$ and $(x_1, \ldots, x_d) = \mathfrak{m}$. Recall from [1] that $\dim R = \dim S$ and that $\mathfrak{n}$ is minimal over $\mathfrak{m}S$.

If S is free, then as an R-module, $\operatorname{depth}_{\mathfrak{m}} S = \operatorname{depth}_{\mathfrak{m}} R$, and $x_1, \ldots, x_d$ is a regular sequence on the R-module S. But then $x_1, \ldots, x_d$ is a regular sequence on the S-module S, so that $\operatorname{depth} S \ge d$. Hence $d \le \operatorname{depth} S \le \dim S = \dim R = d$, which says that S is Cohen–Macaulay.

Now assume that $\operatorname{depth} S = \dim S = d$. Then $x_1, \ldots, x_d$ is a system of parameters for R and hence also for S, so that by Theorem 15.2, $x_1, \ldots, x_d$ is a regular sequence on S. Thus $\operatorname{depth}_{\mathfrak{m}} S \ge d$. Since R is regular, the finitely generated R-module S has a finite projective dimension, so that by the Auslander-Buchsbaum formula (Theorem 13.6), $\operatorname{pd}_R(S) + \operatorname{depth}_R(S) = \operatorname{depth}_R(R) = d$. Thus $\operatorname{pd}_R(S) = 0$ and so S is a projective R-module. But since R is Noetherian local and S is finitely generated, S is a free R-module by Fact 5.5 (6)). $\square$

This theorem is useful for determining when an affine domain S (or other rings) is Cohen–Macaulay. Namely, we first find a Noether normalization R of S and suppose that we find that S is free over R. We want to conclude that S is Cohen-Macaulay. Let Q be a prime ideal in S. It suffices to prove that S_Q is Cohen-Macaulay. Set $P = Q \cap R$. Then R_P is a regular local ring, $R_P \to S_{R \setminus P}$ is free and module-finite, and $S_{R \setminus P}$ is a subring of S_Q. Note that the second paragraph of the proof of Theorem 15.5 does not require S to be local: it proves that $QS_{R\setminus P}$ contains a regular sequence of length at least d, and hence so does QS_Q, so that S_Q is Cohen-Macaulay.

Exercise 15.6 Give examples of Cohen–Macaulay rings that are not regular.

Exercise 15.7 Prove that $\mathbb{Q}[[x^2, x^3]]$ is Cohen–Macaulay but is not regular either by Definition 9.2 or by Definition 9.5.

Exercise 15.8 Prove that $\mathbb{Q}[x, y, u, v]/(x, y)(u, v)$ is not Cohen–Macaulay.

Exercise 15.9 Prove that a localization of a Cohen–Macaulay module is Cohen–Macaulay.

Exercise 15.10 Let R be a Cohen–Macaulay local ring. Prove that for any system of parameters $x_1, \ldots, x_d$, $R/(x_1, \ldots, x_d)$ has finite projective dimension.

Exercise 15.11 Let R be a Cohen–Macaulay ring. Prove that for any variables $X_1, \ldots, X_n$ over R, $R[X_1, \ldots, X_n]$ is Cohen–Macaulay. (If you get stuck, look at Examples 14.7.)

Exercise 15.12 (Ferrand, Vasconcelos) Let R be a Noetherian local commutative ring and let I be a proper ideal in R. Suppose that R is local, that I/I^2 is a free (R/I)-module and that R/I has finite projective dimension over R. Prove that I is generated by a regular sequence. (Compare with Exercise 12.15.)

16 Injective modules

Definition 16.1 *A (left) R-module E is* **injective** *if whenever $f : M \to N$ is an injective (left) module homomorphism and $g : M \to E$ is a homomorphism, there exists $h : N \to E$ such that $g = h \circ f$. In other words, we have the following commutative diagram:*

$$\begin{tikzcd}
& E & \\
0 \arrow[r] & M \arrow[u, "g"] \arrow[r, "f"] \arrow[ur, phantom, "\circlearrowleft"] & N \arrow[ul, dashed, "\exists h"']
\end{tikzcd}$$

At this point we can say that the zero module is injective over any ring, but it would be hard to pinpoint any other injective modules. Certainly $\mathbb{Z}$ is not injective, as the following diagram cannot be filled as in the definition of injective modules if n is an integer with $|n| > 1$:

$$\begin{tikzcd}
& \mathbb{Z} & \\
0 \arrow[r] & \mathbb{Z} \arrow[u, "id"] \arrow[r, "n"] & \mathbb{Z}
\end{tikzcd}$$

Theorem 16.2 **(Baer's criterion)** *E is an injective R-module if and only if for every ideal I in R, we have a commutative diagram (where $I \to R$ is the usual inclusion):*

$$\begin{tikzcd}
 & E & \\
0 \arrow[r] & I \arrow[u] \arrow[r] \arrow[ur, phantom, "\circlearrowleft"] & R \arrow[ul, dashed]
\end{tikzcd}$$

Proof. Clearly the definition using modules implies the ideal formulation. Now let's assume the ideal definition and assume that we have an injective module homomorphism $f : M \to N$ and a module homomorphism $g : M \to E$.

This paragraph proves that we may assume that f is the inclusion homomorphism. Since $f : M \to f(M)$ is a bijection, it has an inverse R-module homomorphism $\overline{f} : f(M) \to f$. We define $\overline{g} : f(M) \to E$ as $g \circ \overline{f}$. Then $\overline{g} \circ f = g$. Let $i : f(M) \to N$ be the inclusion. If we can prove that there exists $h : N \to E$ such that $h \circ i = \overline{g}$, then by abuse of notation of the codomain of f we have that $h \circ f = h \circ i \circ f = \overline{g} \circ f = g$, which finishes the proof. Thus we may assume that f is the inclusion homomorphism.

Let Λ be defined as the set of all pairs (H, h), where $M \subseteq H \subseteq N$, h is a homomorphism from H to E, and h restricted to M is g. Then Λ is not empty as it contains (M, g). We partially order Λ by imposing $(H, h) \le (L, l)$ if $H \subseteq L$ and l restricted to H equals h. Let $\{(H_i, h_i)\}$ be a chain in Λ. Note that $H = \cup H_i$ is an R-module contained in N, and that $h : H \to E$, defined by $h(x) = h_i(x)$ if $x \in H_i$, is a homomorphism. Clearly (H, h) is an upper bound on the chain. Thus by Zorn's lemma, Λ contains a maximal element (H, h). If $H = N$, we are done. If not, let $x \in N \setminus H$. Define $I = H :_R x$. This is an ideal of R. Define $\tilde{g} : I \to E$ by $\tilde{g}(i) = h(ix)$. This $\tilde{g}$ is a homomorphism, and by assumption, there exists $\tilde{h} : R \to E$ such that $\tilde{h}|_I = \tilde{g}$. Now we define $\varphi : H + Rx \to E$ by $\varphi(y+rx) = h(y)+\tilde{h}(r)$, where $y \in H$ and $r \in R$. This is well-defined, for if $y+rx = y'+r'x$, then $(r - r')x = y' - y \in H$, so that $r - r' \in I$ and

$$\tilde{h}(r) - \tilde{h}(r') = \tilde{h}(r - r') = \tilde{g}(r - r') = h((r - r')x) = h(y' - y) = h(y') - h(y).$$

But then (H, h) could not have been maximal in Λ, so that $H = N$. $\square$

Lemma 16.3

(1) A direct summand of an injective module is injective.

(2) A direct product of injective modules is injective.

(3) If the ring is Noetherian, then a direct sum of injective modules is injective.

Proof. The proofs of (1) and (2) are straightforward.

Proof of (3): Let R be a Noetherian ring and let E_α be injective modules, as α varies over an index set. Let I be an ideal in R, and let $f : I \to \oplus_\alpha E_\alpha$ be a homomorphism. Since R is Noetherian, I is finitely generated, say $I = (a_1, \ldots, a_n)$. Each $f(a_i)$ lies in a finite direct sum of the E_α, so that $\operatorname{im} f \in \oplus_{\alpha \in T} E_\alpha$ for some finite subset T. But then by (2), f can be extended to a homomorphism on all of R to this finite direct sum and hence to $\oplus_\alpha E_\alpha$. Hence since I was arbitrary, Baer's criterion (Theorem 16.2) says that $\oplus_\alpha E_\alpha$ is injective. $\square$

Compare the following to Theorem 5.4:

Theorem 16.4 *Let E be a left R-module. The following are equivalent:*

(1) E is an injective R-module.

(2) $\operatorname{Hom}_R(\_, E)$ is exact.

Proof. Let $f : M \to N$ be injective. By Exercise 2.6, $\operatorname{Hom}_R(\_, E)$ is left-exact for all E. It suffices to prove that E is injective if and only if $\operatorname{Hom}_R(N, E) \xrightarrow{\_\circ f} \operatorname{Hom}_R(M, E)$ is onto. But this is the definition of injective modules. $\square$

Proposition 16.5 (Base change – of sorts) *If E is an injective left R-module and S is an R-algebra, then $\operatorname{Hom}_R(S, E)$ is an injective left S-module.*

Proof. $\operatorname{Hom}_R(S, E)$ is a left S-module as follows: for $s \in S$ and $f \in \operatorname{Hom}_R(S, E)$, $sf \in \operatorname{Hom}_R(S, E)$ is that function which for all $t \in S$ gives $sf(t) = f(ts)$. With this definition, sf in $\operatorname{Hom}_R(S, E)$ as for any $r \in R$, $r(sf)(t) = rf(ts) = f(rts) = sf(rt)$, and additivity is easy to show. Clearly $\operatorname{Hom}_R(S, E)$ is closed under addition, and if $s, s' \in S$, then $(ss')f(r) = f(rss') = (s'f)(rs) = s(s'f)(r)$.

By tensor-hom adjointness, $\operatorname{Hom}_S(\_, \operatorname{Hom}_R(S, E)) \cong \operatorname{Hom}_R(\_ \otimes_S S, E) \cong \operatorname{Hom}_R(\_, E)$, which is exact as a functor of R-modules and hence as S-modules. Thus the proof is complete by Theorem 16.4. $\square$

Example 16.6 If E is an injective R-module and I is an ideal in R, then $\operatorname{Hom}_R(R/I, E) \cong \{e \in E : Ie = 0\} = (0_E : I)$ is an injective module over R/I.

Theorem 16.7 (Northcott, Injective envelopes and inverse polynomials, *J. London Math. Soc. (2)*, **8** (1974), 290–296.) *Let k be a field and $x_1, \ldots, x_n, X_1, \ldots, X_n$ variables over k and $R = k[x_1, \ldots, x_n]$. Let $E_p = k[[X_1^{-1}, \ldots, X_n^{-1}]]$, the power series ring over k. We make E_p into an R-module with R-multiplication on E_p induced by*

$$x_k X_1^{-i_1} \cdots X_n^{-i_n} = \begin{cases} X_1^{-i_1} \cdots X_{k-1}^{-i_{k-1}} X_k^{-i_k+1} \cdots X_{k+1}^{-i_{k+1}} \cdots X_n^{-i_n}, & \textit{if } i_k \geq 1; \\ 0, & \textit{otherwise.} \end{cases}$$

Then $E_p = \operatorname{Hom}_k(R, k)$ is an injective R-module. (Here, k is both a submodule and the quotient module $R/(x_1, \ldots, x_n)$ of R.)

Proof. The k-module $R/(x_1, \ldots, x_n) = k$ is an injective module, so by Proposition 16.5, $\operatorname{Hom}_k(R, k)$ is an injective R-module. Let $\varphi : \operatorname{Hom}_k(R, k) \to E_p$ be defined as

$$\varphi(f) = \sum_{a_i \geq 0} f(x_1^{a_1} \cdots x_n^{a_n}) X_1^{-a_1} \cdots X_n^{-a_n}.$$

This is clearly a bijection. We next prove that it is an R-module homomorphism. Additivity is clear. It remains to prove that for any $c \in k$ and any $b_i \geq 0$, $\varphi(cx_1^{b_1} \cdots x_n^{b_n} f) = cx_1^{b_1} \cdots x_n^{b_n} \varphi(f)$. But for any $r \in R$, $(cx_1^{b_1} \cdots x_n^{b_n} f)(r) = f(cx_1^{b_1} \cdots x_n^{b_n} r)$, so that

$$\begin{aligned}
\varphi(cx_1^{b_1} \cdots x_n^{b_n} f) &= \sum_{a_i \geq 0} f(cx_1^{b_1} \cdots x_n^{b_n} x_1^{a_1} \cdots x_n^{a_n}) X_1^{-a_1} \cdots X_n^{-a_n} \\
&= \sum_{a_i \geq 0} cx_1^{b_1} \cdots x_n^{b_n} f(x_1^{a_1+b_1} \cdots x_n^{a_n+b_n}) X_1^{-a_1-b_1} \cdots X_n^{-a_n-b_n} \\
&= cx_1^{b_1} \cdots x_n^{b_n} \sum_{a_i \geq b_i} f(x_1^{a_1} \cdots x_n^{a_n}) X_1^{-a_1} \cdots X_n^{-a_n} \\
&= cx_1^{b_1} \cdots x_n^{b_n} \sum_{a_i \geq 0} f(x_1^{a_1} \cdots x_n^{a_n}) X_1^{-a_1} \cdots X_n^{-a_n} \\
&= cx_1^{b_1} \cdots x_n^{b_n} \varphi(f).
\end{aligned}$$

□

Theorem 16.8 *Let k be a field and $x_1, \ldots, x_n, X_1, \ldots, X_n$ variables over k and $R = k[x_1, \ldots, x_n]$. Let $E = k[X_1^{-1}, \ldots, X_n^{-1}]$ be the polynomial ring over k. We make E into an R-module with R-multiplication on E induced by*

$$x_k X_1^{-i_1} \cdots X_n^{-i_n} = \begin{cases} X_1^{-i_1} \cdots X_{k-1}^{-i_{k-1}} X_k^{-i_k+1} X_{k+1}^{-i_{k+1}} \cdots X_n^{-i_n}, & \text{if } i_k \geq 1; \\ 0, & \text{otherwise.} \end{cases}$$

Then E is an injective R-module.

Proof. Let E_p be as in Theorem 16.7. Clearly E is an R-submodule of E_p. Let I be an ideal in R with an R-module homomorphism $g : I \to E$. Since E_p is an injective R-module, there exists $h_p : R \to E_p$ that when restricted to I equals g. This h_p is multiplication by $h_p(1) \in E_p$ with possibly infinitely many basis elements in the expansion. However, for all $a \in I$ we have $g(a) = h_p(a) = ah_p(1) \in E$, and so only finitely many summands of $h_p(1)$ are needed for a. Say $I = (a_1, \ldots, a_m)$. Let $e \in E$ use only finitely many summands of $h_p(1)$ such that for all $i = 1, \ldots, m$, $g(a_i) = a_i e$. Then we define $h : R \to E$ as multiplication by e. □

Exercise 16.9 Prove that a localization of an injective module over a Noetherian ring is injective. (Hint: Baer's criterion Theorem 16.2.)

Exercise 16.10 Let E be an injective R-module, and let $I_1, \ldots, I_n$ be ideals in R. Prove that

$$\operatorname{ann}_E(I_1 \cap \cdots \cap I_n) = \sum_i \operatorname{ann}_E(I_i).$$

(Hint: consider the injection $R/(I_1 \cap I_2) \to (R/I_1) \oplus (R/I_2)$.)

17 Divisible modules

Definition 17.1 *An R-module M is* **divisible** *if for every $a \in R$ that is a non-zerodivisor in R and for every $m \in M$ there exists $n \in M$ such that $m = an$.*

Examples 17.2

(1) Any vector space over a field is divisible.
(2) If R is a domain, its field of fractions is a divisible R-module.
(3) If M is divisible and N is a submodule, then M/N is divisible.
(4) Direct sums and products of divisible modules are divisible.

Proposition 17.3 *Injective modules are divisible.*

Proof. Let E be an injective module over R. Let $m \in E$ and let a be a non-zerodivisor in R. Then

$$\begin{tikzcd}
 & E & \\
0 \arrow[r] & R \arrow[u, "m"] \arrow[r, "a"] \arrow[ur, phantom, "\circlearrowleft"] & R \arrow[ul, dashed, "h"']
\end{tikzcd}$$

gives that $ah(1) = m$. □

Recall the definition of torsion-free modules Definition 8.6.

Proposition 17.4 *Any torsion-free and divisible module over a domain is injective.*

Proof. Let R be a domain and E a torsion-free and divisible module. Let I be an ideal in R, and let $g : I \to E$ be a homomorphism. If I is 0, we may take $h : R \to E$ to be the zero map, and so $h|_I = g$. Thus we may assume that I is a non-zero ideal. Let a be a non-zero element of I. Then a is a non-zerodivisor in R, so there exists $x \in E$ such that $g(a) = ax$. We define $h : R \to E$ be $h(r) = rx$ (multiplication by x). This is a homomorphism. If $i \in I$, then $h(i) = ix$. We claim that $g(i) = ix$. We know that $ag(i) = g(ai) = g(ia) = ig(a) = iax = aix$, and since E is torsion-free, $g(i) = ix$. □

Proposition 17.5 *A divisible module over a principal ideal domain is injective.*

Proof. By Baer's criterion (Theorem 16.2) we only need to verify that each homomorphism from an ideal (a) to the module can be extended to all of R. By this is the definition of divisible modules. □

Example 17.6 If R is a principal ideal domain with field of fractions K, then every quotient module of a direct sum of copies of K is an injective R-module. Namely, since R is principal ideal domain, by Lemma 16.3, any direct sum of injective modules is injective, so that a direct sum of copies of K is injective. Thus it is divisible by Proposition 17.3, and by Examples 17.2, every quotient module of a direct sum of copies of K is a divisible R-module. Thus by Proposition 17.5, it is also injective.

Theorem 17.7 *Every (left) module over a ring (with identity) embeds in an injective module.*

Proof. Let R be a ring and M an R-module.

First let $R = \mathbb{Z}$. We can write $M \cong (\oplus_\alpha \mathbb{Z})/H$ for some index set of α and for some submodule H of $\oplus_\alpha \mathbb{Z}$. Then $M \subseteq (\oplus_\alpha \mathbb{Q})/H$, and the latter is divisible, hence injective.

Now let R be any ring. We have a canonical map $\mathbb{Z} \to R$. Then M can be also considered as a $\mathbb{Z}$-module, and as such it is embedded in an injective $\mathbb{Z}$-module E_Z. By Proposition 16.5, $E = \operatorname{Hom}_{\mathbb{Z}}(R, E_Z)$ is a left injective R-module. Define $f : M \to E$ as multiplication μ_m by m, i.e., by $f(m)(r) = \mu_m(r) = rm$ (here, we use that M is a subset of E_Z). Then f is certainly additive, and it is an R-module homomorphism (refer to Proposition 16.5 for the R-module structure of E), as for any $s \in R$ and any $m \in M$, $f(sm)(r) = \mu_{sm}(r) = rsm = (s\mu_m)(r) = (sf)(r)$. Furthermore, f is injective, because if $rm = 0$ for all $r \in R$, then $m = 0$. Thus M embeds in E as an R-module. $\square$

We can now extend Theorem 16.4. (Compare to Theorem 5.4.)

Theorem 17.8 *Let E be a left R-module. The following are equivalent:*

(1) E is an injective R-module.

(2) $\operatorname{Hom}_R(\_, E)$ is exact.

(3) Whenever $f : E \to M$ is injective homomorphism, there exists $h : M \to E$ such that $h \circ f = \mathrm{id}_E$, and so $M \cong E \oplus \operatorname{coker} f$.

Proof. (1) and (2) are equivalent by Theorem 16.4.

Assume (2) and that $f : E \to M$ is injective. Then $\operatorname{Hom}_R(M, E) \xrightarrow{\_\circ f} \operatorname{Hom}_R(E, E)$ is surjective, so that there exists $h : M \to E$ so that $h \circ f = \mathrm{id}_E$. Thus by Exercise 1.8 we have that (2) implies (3).

Now assume (3). By Theorem 17.7 there exists an injective R-module I that contains E. By assumption E is a direct summand of an injective module, hence it is injective by Lemma 16.3. $\square$

Exercise 17.9 Let E be an injective module over a Noetherian ring R. Let f be a non-zerodivisor on R. Prove that the natural map $E \to E_f$ is surjective.

18 Injective resolutions

Theorem 17.7 says that every R-module M is a submodule of an injective module I^0. The cokernel of the inclusion $M \to I^0$ is an R-module which is a submodule of an injective module I^1. The cokernel of the map $I^0 \to I^1$ is a submodule of an injective module I^2, and so on. This builds an injective resolution as in the following definition:

Definition 18.1 *An* **injective resolution** *of an R-module M is a co-complex of injective modules*

$$0 \to I^0 \to I^1 \to I^2 \to \cdots$$

such that $0 \to M \to I^0 \to I^1 \to I^2 \to \cdots$ is exact. As noted before, and analogously with the projective resolutions, for expediency in writing, when no confusion can arise, $0 \to M \to I^0 \to I^1 \to I^2 \to \cdots$ is also sometimes called an **injective resolution** *of M.*

Example 18.2 Let R be a principal ideal domain, and let K be its field of fractions. Then $0 \to R \to K \to K/R \to 0$ is a finite injective resolution of R and for any $a \in R$, $0 \to R/aR \to K/aR \to K/R \to 0$ is a finite injective resolution of R/aR. If M is an R-module, we can write it as $\sum_i R/a_iR$ for i varying over some index set and some $a_i \in R$. Since R is principal ideal domain, by Lemma 16.3. $\sum_i K/a_iR$ is injective and $0 \to \sum_i R/a_iR \to \sum_i K/a_iR \to \sum_i K/R \to 0$ is a finite injective resolution of M.

Theorem 18.3 (Comparison Theorem for Injectives) *Let $C^\bullet : \quad 0 \to M \to C^0 \to C^1 \to C^2 \to \cdots$ be an exact co-complex, and let $I^\bullet : \quad 0 \to N \to I^0 \to I^1 \to I^2 \to \cdots$ be a co-complex with all I^i injective. Then for any $f \in \mathrm{Hom}_R(M,N)$ there exists a map of co-complexes $f^\bullet : C^\bullet \to I^\bullet$ that extends f, i.e., such that $f^\bullet$ in degree -1 equals f. (We write $f^{-1} = f$.) Moreover, any two such liftings $f^\bullet$ are homotopic.*

Proof. Let the co-complex maps on $C^\bullet$ be d^n, and those on $I^\bullet$ be δ^n.

Existence, via induction: certainly $f^0 : C^0 \to I^0$ is obtained via the diagram

$$\begin{tikzcd}
 & I^0 & \\
0 \arrow[r] & M \arrow[u, "\delta^{-1}\circ f"] \arrow[r, "d^{-1}"'] \arrow[ur, phantom, "\circlearrowleft"] & C^0 \arrow[ul, dashed, "f^0"']
\end{tikzcd}$$

Thus we have f^0 and $f^{-1} = f$.

Suppose that we have f^{n-1}, f^n. Then $\delta^n \circ f^n \circ d^{n-1} = \delta^n \circ \delta^{n-1} \circ f^{n-1} = 0$, so that $\delta^n \circ f^n$ restricted to $\mathrm{im}\, d^{n-1} = \ker d^n$ equals 0. Hence we get f^{n+1} making with $f^{n+1} \circ d^n = \delta^n \circ f^n$ via the following diagram:

$$
\begin{tikzcd}
 & I^{n+1} & \\
0 \arrow[r] & \frac{C^n}{\ker d^n} \arrow[u, "\delta^n \circ f^n"] \arrow[r, "d^n"] \arrow[ur, phantom, "\circlearrowleft"] & C^{n+1} \arrow[ul, dashed, "f^{n+1}"']
\end{tikzcd}
$$

In this way we construct a map of complexes $f^\bullet : C^\bullet \to I^\bullet$.

Now suppose that $f^\bullet$ and $g^\bullet$ are maps of complexes that extend $f : M \to N$. Let $h^\bullet = f^\bullet - g^\bullet$. Define $s^0 : C^0 \to N$ to be the zero map (we really cannot hope for it to be anything else). Note that $(h^0 - \delta^{-1} \circ s^0) \circ d^{-1} = h^0 \circ d^{-1} = \delta^{-1}) \circ h^{-1} = 0$, so that $h^0 - s^0 \circ d^{-1}$ restricted to $\operatorname{im} \delta^{-1} = \ker \delta^0$ is zero. Thus we have the diagram

$$
\begin{tikzcd}
 & I^0 & \\
0 \arrow[r] & \frac{C^0}{\ker \delta^0} \arrow[u] \arrow[r] \arrow[ur, phantom, "\circlearrowleft"] & C^2 \arrow[ul, dashed, "s^1"']
\end{tikzcd}
$$

We leave to the reader how to construct $s^2, s^3, \ldots$, and that this gives a homotopy. ☐

Corollary 18.4 *Let $I^\bullet$ and $J^\bullet$ be injective resolutions of M. Then there exists a map of complexes $f^\bullet : I^\bullet \to J^\bullet$ such that*

$$
\begin{array}{ccccc}
0 \to & M & \to & I^\bullet \\
 & \downarrow \mathrm{id}_M & & \downarrow f^\bullet \\
0 \to & M & \to & J^\bullet
\end{array}
$$

and any two such $f^\bullet$ are homotopic. ☐

The following has a proof similar to Corollary 7.3:

Corollary 18.5 *Let $I^\bullet$ and $J^\bullet$ be injective resolutions of M. Then for any additive functor $\mathcal{F}$, the homologies of $\mathcal{F}(I^\bullet)$ and of $\mathcal{F}(J^\bullet)$ are isomorphic.* ☐

The following has a proof similar to Theorem 7.4:

Proposition 18.6 *Let $I'^\bullet$ be an injective resolution of M' and let $I''^\bullet$ be an injective resolution of M''. Suppose that $0 \to M'^\bullet \to M^\bullet \to M''^\bullet \to 0$ is a short exact sequence. Then there exists an injective resolution $I^\bullet$ such that*

$$
\begin{array}{cccccccc}
0 \to & M' & \to & M & \to & M'' & \to 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
0 \to & I'^\bullet & \to & I^\bullet & \to & I''^\bullet & \to 0
\end{array}
$$

is a commutative diagram, in which the bottom row is a split short exact sequence of complexes. ☐

Proof. Let the maps in the short exact sequence be $i : M' \to M$ and $p : M \to M''$, and let the maps on $I'^\bullet$ be $\delta'^\bullet$, and the maps on $I''^\bullet$ be $\delta''^\bullet$. Consider the diagram in which the rows are exact:

$$\begin{array}{cccccccccccc} 0 \to & M' & \overset{i}{\to} & M & \overset{\delta''^{-1}\circ p}{\longrightarrow} & I''^0 & \overset{\delta''^0}{\to} & I''^1 & \overset{\delta''^1}{\to} & I''^2 & \to \cdots \\ & \downarrow \mathrm{id}_M & & & & & & & & & \\ 0 \to & M' & \overset{\delta'^{-1}}{\to} & I'^0 & \overset{\delta'^0}{\to} & I'^1 & \overset{\delta'^1}{\to} & I'^2 & \overset{\delta'^2}{\to} & I'^3 & \to \cdots \end{array}$$

By the Comparison Theorem for injectives (Theorem 18.3), there exist the maps as below that make all squares commute:

$$\begin{array}{cccccccccccc} 0 \to & M' & \overset{i}{\to} & M & \overset{\delta''^{-1}\circ p}{\longrightarrow} & I''^0 & \overset{\delta''^0}{\to} & I''^1 & \overset{\delta''^1}{\to} & I''^2 & \to \cdots \\ & \downarrow \mathrm{id}_M & & \downarrow f^0 & & \downarrow f^1 & & \downarrow f^2 & & \downarrow f^3 & \\ 0 \to & M' & \overset{\delta'^{-1}}{\to} & I'^0 & \overset{\delta'^0}{\to} & I'^1 & \overset{\delta'^1}{\to} & I'^2 & \overset{\delta'^2}{\to} & I'^3 & \to \cdots \end{array}$$

Now define $I^n = I'^n \oplus I''^n$, $\delta^{-1} : M \to I^0$ by $\delta^{-1}(m) = (-f^0(m), \delta''^{-1} \circ p(m))$, and $\delta^n : I^n \to I^{n+1}$ by $\delta^n(a, b) = (\delta'^n(b) + (-1)^n f^{n+1}(a), \delta''^n(a))$.

This works. Namely, let $m \in \ker \delta^{-1}$. Then $\delta''^{-1} \circ p(m) = 0$, so that $p(m) = 0$, whence $m = i(m')$ for some $m' \in M'$. Also, $0 = f^0(m) = f^0 \circ i(m') = \delta'^{-1}(m')$, so that $m' = 0$ and so $m = i(m') = 0$. So δ^{-1} is injective.

Exactness at I^0: $\delta^0 \circ \delta^{-1}(m) = \delta^0(-f^0(m), \delta''^{-1} \circ p(m)) = (-\delta'^0 \circ f^0(m) + f^1 \circ \delta''^{-1} \circ p(m), \delta''^0 \circ \delta''^{-1} \circ p(m)) = 0$, so that $\operatorname{im} \delta^{-1} \subseteq \ker \delta^0$. If $(a, b) \in \ker \delta^0$, then $\delta''^0(b) = 0$ and $\delta'^0(a) + f^1(b) = 0$. Thus $b = \delta''^{-1}(m'')$ for some $m \in M''$, and even $b = \delta''^{-1} \circ p(m)$ for some $m \in M$, and $\delta'^0(a) = -f^1(b) = -f^1 \circ \delta''^{-1} \circ p(m) = -\delta'^0 \circ f^0(m)$, whence $a + f^0(m) \in \ker \delta'^0 = \delta'^{-1}M'$, so that $a + f^0(m) = \delta'^{-1}m'$ for some $m' \in M$. Then $\delta^{-1}(m - i(m')) = (-f^0(m - i(m')), \delta''^{-1} \circ p(m + i(m'))) = (-f^0(m) + f^0 \circ i(m'), \delta''^{-1} \circ p(m)) = (-\delta'^{-1}m' + a + \delta'^{-1}(m'), b) = (a, b)$, which proves that $\operatorname{im} \delta^{-1} = \ker \delta^0$.

For $n \geq 0$, $\delta^{n+1} \circ \delta^n(a, b) = \delta^{n+1}(\delta'^n(b) + (-1)^n f^{n+1}(a), \delta''^n(a)) = (\delta'^{n+1} \circ (\delta'^n(b) + (-1)^n f^{n+1}(a) + (-1)^{n+1} f^{n+2} \circ \delta''^n(a), \delta''^{n+1} \circ \delta''^n(a))) = 0$. This proves that $\operatorname{im} \delta^n \subseteq \ker \delta^{n+1}$. Now let $(a, b) \in \ker \delta^{n+1}$. Then $\delta''^{n+1}(b) = 0$ and $\delta'^{n+1}(a) + (-1)^{n+1} f^{n+2}(b) = 0$. It follows that $b = \delta''^n(c)$ for some $c \in I''^n$. Then $\delta'^{n+1}(a) = (-1)^n f^{n+2} \circ \delta''^n(c) = (-1)^n \delta'^{n+1} \circ f^{n+1}(c)$, so that $a - (-1)^n f^{n+1}(c) \in \ker \delta'^{n+1} = \operatorname{im} \delta'^n$, whence $a - (-1)^n f^{n+1}(c) = \delta'^n(d)$ for some $d \in I'^n$. Thus

$$\delta^n(d, c) = (\delta'^n(d) + (-1)^n f^{n+1}(c), \delta''^n(c)) = (a - (-1)^n f^{n+1}(c) + (-1)^n f^{n+1}(c), b) = (a, b),$$

which proves that $\ker \delta^{n+1} = \operatorname{im} \delta^n$ for all $n \geq 0$.

We leave it to the reader to verify that this makes a short exact sequence of injective resolutions. $\square$

The following two Schanuel-lemma type results for injectives have proofs dual to those of Theorem 6.4 and Theorem 6.5:

Theorem 18.7 (Schanuel's lemma for injectives) *Let R be a ring. Suppose that $0 \to M \to I \to K \to 0$ and $0 \to M \to E \to L \to 0$ are exact sequences of R-modules, and that I and E are injective. Then $I \oplus L \cong E \oplus K$.* $\square$

Theorem 18.8 (Generalized Schanuel's lemma for injectives) *Let R be a ring. Suppose that $0 \to M \to I^0 \to I^1 \to \cdots \to I^{k-1} \to I^k \to K \to 0$ and $0 \to M \to E^0 \to E^1 \to \cdots \to E^{k-1} \to E^k \to L \to 0$ are exact sequences of R-modules, and that all the I^j and E^j are injective. Let $I_{odd} = \oplus_{i\ odd} I^i$, $I_{even} = \oplus_{i\ even} I^i$, $E_{odd} = \oplus_{i\ odd} E^i$, $E_{even} = \oplus_{i\ even} E^i$. Then*

(1) If k is even, $K \oplus E_{even} \oplus I_{odd} \cong L \oplus E_{odd} \oplus I_{even}$.

(2) If k is odd, $K \oplus E_{odd} \oplus I_{even} \cong L \oplus E_{even} \oplus I_{odd}$. $\square$

19 A definition of Ext using injective resolutions

Let M, N be R-modules, and let $I^\bullet : \quad 0 \to I^0 \to I^1 \to I^2 \cdots$ be an injective resolution of N. We define

$$\overline{\mathrm{Ext}}^n_R(M, N) = H^n(\mathrm{Hom}_R(M, I^\bullet)).$$

With the manipulations of injective resolutions in the previous section we can fairly quickly develop some main properties of Ext:

1. Independence of the resolution. The definition of $\overline{\mathrm{Ext}}^n_R(\_, N)$ is independent of the injective resolution $I^\bullet$ of N. This follows from Corollary 18.5.

2. Ext has no terms of negative degree. $\overline{\mathrm{Ext}}^n_R(\_, N) = 0$ if $n < 0$. This follows as $I^\bullet$ has zero modules in negative positions.

3. $\overline{\mathrm{Ext}}^0$. $\overline{\mathrm{Ext}}^0_R(M, N) \cong \mathrm{Hom}_R(M, N)$. Proof: By assumption $0 \to N \to I^0 \to I^1$ is exact, and as $\mathrm{Hom}(M, \_)$ is left-exact, $0 \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(I^0, N) \to \mathrm{Hom}_R(I^1, N)$ is exact as well. Thus $\overline{\mathrm{Ext}}^0_R(M, N) = H^0(\mathrm{Hom}_R(M, I^\bullet)) = \ker(\mathrm{Hom}_R(I^0, N) \to \mathrm{Hom}_R(I^1, N)) = \mathrm{Hom}_R(M, N)$.

4. What if M is projective? If M is projective, then $\overline{\mathrm{Ext}}^n_R(M, N) = 0$ for all $n \geq 1$. This follows as $I^{n-1} \to I^n \to I^{n+1}$ is exact, and so as M is projective, by Theorem 5.4, $\mathrm{Hom}_R(M, P_{n-1}) \to \mathrm{Hom}_R(M, P_n) \to \mathrm{Hom}_R(M, P_{n+1})$ is exact as well, giving that the nth cohomology of $\mathrm{Hom}_R(M, I^\bullet)$ is 0 if $n > 0$.

5. What if N is injective? If N is injective, then $\overline{\mathrm{Ext}}^n_R(M, N) = 0$ for all $n \geq 1$. This is clear as in that case we may take $I^0 = N$ and all other I^n to be 0.

6. Ext on short exact sequences. If $0 \to N' \to N \to N'' \to 0$ is a short exact sequence of modules, then for any module M, there is a long exact sequence

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

The proof goes as follows. Let $I'^\bullet$ be an injective resolution of N', and let $I''^\bullet$ be an injective resolution of N''. Then by Proposition 18.6 there exists an injective resolution $I^\bullet$ of N such that

$$\begin{array}{ccccccc} 0 \to & N' & \to & N & \to & N'' & \to 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 \to & I'^\bullet & \to & I^\bullet & \to & I''^\bullet & \to 0 \end{array}$$

is a commutative diagram in which the rows are exact. In particular, we have a short exact sequence $0 \to I'^\bullet \to I^\bullet \to I''^\bullet \to 0$, and since this is a split exact sequence, it follows that $0 \to \mathrm{Hom}_R(M, I''^\bullet) \to \mathrm{Hom}_R(M, I^\bullet) \to \mathrm{Hom}_R(M, I'^\bullet) \to 0$ is still a short exact sequence of complexes. The rest follows from Theorem 3.3.

Exercise 19.1 Let $0 \to I'^\bullet \to I^\bullet \to I''^\bullet \to 0$ be a short exact sequence of complexes. If all modules in $I'^\bullet$ and $I''^\bullet$ are injective, so are all the modules in $I^\bullet$.

Exercise 19.2 Let $x \in R$ and suppose that $0 \to N \xrightarrow{x} N \to N/xN \to 0$ is a short exact sequence. Prove that the maps $\mathrm{Ext}^n_R(M, N) \to \mathrm{Ext}^n_R(M, N)$ in the long exact sequence above are also multiplications by x.

Exercise 19.3 Prove that for any R-modules M and N, $\mathrm{ann}\, M + \mathrm{ann}\, N \subseteq \mathrm{ann}\, \overline{\mathrm{Ext}}^n_R(M, N)$.

Exercise 19.4 Let $0 \to N \to I^0 \to I^1 \to \cdots \to I^{n-1} \to N_n \to 0$ be exact, where all I^j are injective. Prove that for all $i \geq 1$, $\overline{\mathrm{Ext}}^i_R(M, N_n) \cong \overline{\mathrm{Ext}}^{i+n}_R(M, N)$.

20 A definition of Ext using projective resolutions

Let M, N be R-modules, and let $P_\bullet : \quad \cdots \to P_2 \to P_1 \to P_0 \to 0$ be a projective resolution of M. We define

$$\mathrm{Ext}^n_R(M, N) = H^n(\mathrm{Hom}_R(P_\bullet, N)).$$

With all the general manipulations of complexes we can fairly quickly develop some main properties of Ext:

1. Independence of the resolution. The definition of $\mathrm{Ext}^n_R(M, \_)$ is independent of the projective resolution $P_\bullet$ of M. This follows from Corollary 7.3.

2. Ext has no terms of negative degree. $\mathrm{Ext}^n_R(M, \_) = 0$ if $n < 0$. This follows as $P_\bullet$ has only zero modules in negative positions.

3. Ext^0. $\mathrm{Ext}^0_R(M, N) \cong \mathrm{Hom}_R(M, N)$. Proof: By assumption $P_1 \to P_0 \to M \to 0$ is exact, and as $\mathrm{Hom}(\_, N)$ is left-exact, $0 \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(P_0, N) \to \mathrm{Hom}_R(P_1, N)$ is exact as well. Thus $\mathrm{Ext}^0_R(M, N) = H^0(\mathrm{Hom}_R(P_\bullet, N)) = \ker(\mathrm{Hom}_R(P_0, N) \to \mathrm{Hom}_R(P_1, N)) = \mathrm{Hom}_R(M, N)$.

4. What if M is projective? If M is projective, then $\operatorname{Ext}_R^n(M,N) = 0$ for all $n \geq 1$. This is clear as in that case we may take $P_0 = M$ and all other P_n to be 0.

5. What if N is injective? If N is injective, then $\operatorname{Ext}_R^n(M,N) = 0$ for all $n \geq 1$. This follows as $P_{n+1} \to P_n \to P_{n-1}$ is exact, and so as N is injective, $\operatorname{Hom}_R(P_{n-1}, N) \to \operatorname{Hom}_R(P_n, N) \to \operatorname{Hom}_R(P_{n+1}, N)$ is exact as well, giving that the nth cohomology of $\operatorname{Hom}_R(P_\bullet, N)$ is 0 if $n > 0$.

6. Ext on short exact sequences. If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of modules, then for any module N, there is a long exact sequence

$$\cdots \to \operatorname{Ext}_R^{n-1}(M', N) \to \operatorname{Ext}_R^n(M'', N) \to \operatorname{Ext}_R^n(M, N) \to \operatorname{Ext}_R^n(M', N) \to \operatorname{Ext}_R^{n+1}(M'', N) \to \cdots.$$

The proof goes as follows. Let ${P_\bullet}'$ be a projective resolution of M', and let ${P_\bullet}''$ be a projective resolution of M''. Then by Theorem 7.4 there exists a projective resolution $P_\bullet$ of M such that

$$\begin{array}{ccccccc} 0 \to & {P_\bullet}' & \to & P_\bullet & \to & {P_\bullet}'' & \to 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 \to & M' & \to & M & \to & M'' & \to 0 \end{array}$$

is a commutative diagram in which the rows are exact and the top row is split-exact. It follows that $0 \to \operatorname{Hom}_R({P_\bullet}'', N) \to \operatorname{Hom}_R(P_\bullet, N) \to \operatorname{Hom}_R({P_\bullet}', N) \to 0$ is a short exact sequence of complexes. The rest follows from Theorem 3.3.

7. Ext and annihilators. For any M, N and n, $\operatorname{ann} M + \operatorname{ann} N \subseteq \operatorname{ann} \operatorname{Ext}_R^n(M,N)$. Proof: Since $\operatorname{Ext}_R^n(M,N)$ is a quotient of a submodule of $\operatorname{Hom}_R(P_n, N)$, it is clear that $\operatorname{ann} N$ annihilates all Exts. Now let $x \in \operatorname{ann} M$. Then multiplication by x on M, which is the same as multiplication by 0 on M, has two lifts μ_x and μ_0 on $P_\bullet$, and by the Comparison Theorem (Theorem 7.1), the two maps are homotopic. Thus $\operatorname{Hom}_R(\mu_x, N)$ and 0 are homotopic on $\operatorname{Hom}_R(P_\bullet, N)$, whence by Proposition 3.7, $\operatorname{Hom}_R(\mu_x, N)_* = 0$. In other words, multiplication by x on $\operatorname{Hom}_R(P_\bullet, N)$ is zero.

8. Ext on syzygies. Let M_n be an nth syzygy of M, i.e., $0 \to M_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to M \to 0$ is exact for some projective modules P_i. Then for all $i \geq 1$, $\operatorname{Ext}_R^i(M_n, N) \cong \operatorname{Ext}_R^{i+n}(M, N)$. This follows from the definition of Ext (and from the independence on the projective resolution).

9. Ext for finitely generated modules over Noetherian rings. If R is Noetherian and M and N are finitely generated R-modules, then $\operatorname{Ext}_R^n(M,N)$ is a finitely generated R-module for all n. To prove this, we may choose $P_\bullet$ such that all P_n are finitely generated (since submodules of finitely generated modules are finitely generated). Then $\operatorname{Hom}_R(P_n, N)$ is finitely generated, whence so is $\operatorname{Ext}_R^n(M,N)$.

Exercise 20.1 Let $x \in R$ and suppose that $0 \to M \xrightarrow{x} M \to M/xM \to 0$ is a short exact sequence. Prove that the maps $\operatorname{Ext}_R^n(M,N) \to \operatorname{Ext}_R^n(M,N)$ in the long exact sequence are also multiplications by x.

21 The two definitions of Ext are isomorphic

Theorem 21.1 *Let R be a commutative ring and let M and N be R-modules. Then for all n, $\mathrm{Ext}_n^R(M,N) \cong \overline{\mathrm{Ext}}_n^R(M,N)$.*

Proof. Let $P_\bullet$ be a projective resolution of M and let $I^\bullet$ be an injective resolution of N.

Let M_1, N_1 be defined so that $0 \to M_1 \to P_0 \to M \to 0$ and $0 \to N \to I^0 \to N_1 \to 0$ are exact. By applying Hom_R we get the following commutative diagram whose rows and columns are exact:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \mathrm{Hom}(M,N) & \to & \mathrm{Hom}(P_0,N) & \to & \mathrm{Hom}(M_1,N) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \mathrm{Hom}(M,I^0) & \to & \mathrm{Hom}(P_0,I^0) & \to & \mathrm{Hom}(M_1,I^0) & \to & 0 \\
 & & \downarrow\alpha & & \downarrow\beta & & \downarrow\gamma & & \\
0 & \to & \mathrm{Hom}(M,N_1) & \to & \mathrm{Hom}(P_0,N_1) & \to & \mathrm{Hom}(M_1,N_1) & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & \overline{\mathrm{Ext}}^1_R(M,N) & & 0 & & & & \\
 & & \downarrow & & & & & & \\
 & & \overline{\mathrm{Ext}}^1_R(M,I^0) = 0 & & & & & &
\end{array}$$

By the Snake Lemma (Lemma 1.7), $0 \to \ker\alpha \to \ker\beta \to \ker\gamma \to \operatorname{coker}\alpha \to \operatorname{coker}\beta$ is exact, or in other words,

$$0 \to \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(P_0,N) \to \mathrm{Hom}_R(M_1,N) \to \overline{\mathrm{Ext}}^1_R(M,N) \to 0$$

is exact. Note that the maps between the Hom modules above are the natural maps. But we also have that

$$0 \to \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(P_0,N) \to \mathrm{Hom}_R(M_1,N) \to \mathrm{Ext}^1_R(M,N) \to \mathrm{Ext}^1_R(P_0,N) = 0$$

is exact with the natural maps on the Hom modules, which proves that for all R-modules M and N, $\mathrm{Ext}^1_R(M,N) = \overline{\mathrm{Ext}}^1_R(M,N)$.

The commutative diagram shows even more, if we fill it up a bit more in the lower right corner to get the following exact rows and exact columns in the commutative diagram:

$$\begin{array}{ccccccc}
\mathrm{Hom}(P_0,I^0) & \xrightarrow{g} & \mathrm{Hom}(M_1,I^0) & \to & 0 & & \\
\downarrow\beta & & \downarrow\gamma & & & & \\
\mathrm{Hom}(P_0,N_1) & \xrightarrow{f} & \mathrm{Hom}(M_1,N_1) & \to & \mathrm{Ext}^1_R(M,N_1) & \to & \mathrm{Ext}^1_R(P_0,N_1) = 0 \\
\downarrow & & \downarrow & & & & \\
0 & & \overline{\mathrm{Ext}}^1_R(M_1,N) & & & & \\
 & & \downarrow & & & & \\
 & & \overline{\mathrm{Ext}}^1_R(M_1,I^0) = 0 & & & &
\end{array}$$

From this diagram we see that $\overline{\mathrm{Ext}}^1_R(M_1, N)$ is the cokernel of γ, and since g is injective, it is the cokernel of $\gamma \circ g = f \circ \beta$. But $\mathrm{Ext}^1_R(M, N_1)$ is the cokernel of f and hence of $f \circ \beta$, which proves that $\overline{\mathrm{Ext}}^1_R(M_1, N) \cong \mathrm{Ext}^1_R(M, N_1)$.

Thus, so far we proved that for all M, N, $\overline{\mathrm{Ext}}^1_R(M, N) \cong \mathrm{Ext}^1_R(M, N)$, and that for any first syzygy M_1 of M and any N_1 such that $0 \to N \to I^0 \to N_1 \to 0$ exact wth I^0 injective, $\overline{\mathrm{Ext}}^1_R(M_1, N) \cong \mathrm{Ext}^1_R(M, N_1)$.

Now let $M_n = \ker(P_{n-1} \to P_{n-2})$ and $N_n = \mathrm{coker}(I_{n-2} \to I_{n-1})$. Then by what we have proved in the previous two sections and above, for all $n \geq 2$,

$$\begin{aligned}
\overline{\mathrm{Ext}}^n_R(M, N) &\cong \overline{\mathrm{Ext}}^1_R(M, N_{n-1}) \\
&\cong \mathrm{Ext}^1_R(M, N_{n-1}) \\
&\cong \overline{\mathrm{Ext}}^1_R(M_1, N_{n-2}) \\
&\cong \mathrm{Ext}^1_R(M_2, N_{n-3}) \text{ (if } n \geq 3) \\
&\cong \cdots \\
&\cong \mathrm{Ext}^1_R(M_{n-2}, N_1) \\
&\cong \overline{\mathrm{Ext}}^1_R(M_{n-1}, N) \\
&\cong \mathrm{Ext}^1_R(M_{n-1}, N) \\
&\cong \mathrm{Ext}^n_R(M, N),
\end{aligned}$$

which finishes the proof of the theorem. □

22 Ext and extensions

Definition 22.1 *An* **extension** *e of groups or of left modules* **of M by N** *is an exact sequence $0 \to N \to K \to M \to 0$ for some group or left module K.*

Two extensions e and e' are **equivalent** *if there is a commutative diagram:*

$$\begin{array}{cccccccccc}
e: & 0 & \to & N & \to & K & \to & M & \to & 0 \\
 & & & \| & & \downarrow\cong & & \| & & \\
e': & 0 & \to & N & \to & K' & \to & M & \to & 0
\end{array}$$

An extension is **split** *if it is equivalent to*

$$0 \to N \xrightarrow{\mathrm{id}_N \oplus 0} N \oplus M \to M \to 0.$$

Let M and N be R-modules. For each extension $e: \quad 0 \to N \to K \to M \to 0$ of M by N consider

$$0 \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(K, N) \to \mathrm{Hom}_R(N, N) \xrightarrow{\delta} \mathrm{Ext}^1_R(M, N).$$

In particular, if $\mathrm{Ext}^1_R(M,N) = 0$, then the identity map on N is the image of a homomorphism from $K \to N$, i.e., id_N is the composition of $N \to K \to N$. Thus $\mathrm{Ext}^1_R(M,N) = 0$ implies that every extension of M by N splits.

In general, each e gives an element $\delta(\mathrm{id}_N)$. We will prove that the map $e \mapsto \delta(\mathrm{id}_N)$ from the equivalence class of extensions of M by N to $\mathrm{Ext}^1_R(M,N)$ is a bijection.

Lemma 22.2 *Let φ be the function that takes the equivalence classes of extensions of M by N to $\mathrm{Ext}^1_R(M,N)$ as above. Then φ is a well-defined bijection.*

Proof. First we prove that φ is well-defined. Let

$$\begin{array}{ccccccccc} e: & 0 & \to & N & \xrightarrow{i} & K & \xrightarrow{p} & M & \to & 0 \\ & & & \| & & \downarrow f & & \| & & \\ e': & 0 & \to & N & \xrightarrow{i'} & K' & \xrightarrow{p'} & M & \to & 0 \end{array}$$

where f is an isomorphism. From this we get

$$\begin{array}{ccccccc} 0 \to & \mathrm{Hom}_R(M,N) & \to & \mathrm{Hom}_R(K,N) & \to & \mathrm{Hom}_R(N,N) & \xrightarrow{\delta} & \mathrm{Ext}^1_R(M,N) \\ & \| & & \uparrow \_\circ f & & \| & & \| \\ 0 \to & \mathrm{Hom}_R(M,N) & \to & \mathrm{Hom}_R(K',N) & \to & \mathrm{Hom}_R(N,N) & \xrightarrow{\delta'} & \mathrm{Ext}^1_R(M,N) \end{array}$$

This shows that $\delta(\mathrm{id}_N) = \delta'(\mathrm{id}_N)$. Thus each equivalence class of extensions of M by N maps to the same element of $\mathrm{Ext}^1_R(M,N)$.

Next we prove that φ is surjective. Let $g \in \mathrm{Ext}^1_R(M,N)$. Let F be a projective R-module mapping onto M, and let C be the kernel. Then we have the short exact sequence $0 \to C \xrightarrow{\alpha} F \xrightarrow{\beta} M \to 0$, which gives the exact sequence

$$\to \mathrm{Hom}_R(C,N) \xrightarrow{\gamma} \mathrm{Ext}^1(M,N) \to \mathrm{Ext}^1_R(F,N) = 0,$$

so there exists $h \in \mathrm{Hom}_R(C,N)$ that maps to g via γ. Let

$$K = \frac{N \oplus F}{\{(h(c), -\alpha(c)) : c \in C\}}.$$

(This is a pushout). Let $i : N \to K$ and $k : F \to K$ be defined as $i(n) = (n,0)$ and $k(n) = (0,n)$. The map $i : N \to K$ is injective, because $(n,0) = (h(c), -\alpha(c)) \in N \oplus F$ means that $\alpha(c) = 0$, whence $c = 0$ and so $n = h(c) = 0$. The following diagram commutes:

$$\begin{array}{ccc} C & \xrightarrow{\alpha} & F \\ \downarrow h & & \downarrow k \\ N & \xrightarrow{i} & K \end{array}$$

We define $p : K \to M$ as $p(a,b) = \beta(b)$. This is a well-defined homomorphism because $p(h(c), -\alpha(c)) = \beta(-\alpha(c)) = 0$. Since β is surjective, so is p. The image of N in K is in the kernel of p, and if $(a,b) \in \ker p$, then $\beta(b) = 0$, so that $b = \alpha(c)$ for some $c \in C$, whence (a,b) in K equals $(a, \alpha(c)) = (a + h(c), 0)$, which is in the image of N. Thus $0 \to N \to K \to M \to 0$ is a short exact sequence. Furthermore, the following is a commutative diagram with exact rows:

$$\begin{array}{ccccccc}
0 \to & C & \xrightarrow{\alpha} & F & \xrightarrow{\beta} & M & \to 0 \\
 & \downarrow h & & \downarrow k & & \| & \\
0 \to & N & \xrightarrow{i} & K & \xrightarrow{p} & M & \to 0
\end{array}$$

From this diagram we get the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 \to & \mathrm{Hom}_R(M,N) & \to & \mathrm{Hom}_R(F,N) & \to & \mathrm{Hom}_R(C,N) & \xrightarrow{\gamma} & \mathrm{Ext}^1_R(M,N) \\
 & \| & & \uparrow _ \circ k & & \uparrow _ \circ h & & \| \\
0 \to & \mathrm{Hom}_R(M,N) & \to & \mathrm{Hom}_R(K,N) & \to & \mathrm{Hom}_R(N,N) & \xrightarrow{\delta} & \mathrm{Ext}^1_R(M,N)
\end{array}$$

which proves that $\varphi(0 \to C \xrightarrow{\alpha} F \xrightarrow{\beta} M \to 0) = \delta(\mathrm{id}_N) = \gamma(h) = g$.

It remains to prove that φ is injective. Suppose that φ takes both $0 \to N \to L \to M \to 0$ and $0 \to N \to L' \to M \to 0$ to the same element of $\mathrm{Ext}^1_R(M,N)$. Let δ, δ' be the corresponding maps $\mathrm{Hom}_R(N,N) \to \mathrm{Ext}^1_R(M,N)$ in the long exact sequences for the two short exact sequences such that $\delta(\mathrm{id}_N) = \delta'(\mathrm{id}_N)$. As in the proof of surjectivity we have a short exact sequence $0 \to C \xrightarrow{\alpha} F \xrightarrow{\beta} M \to 0$ with F projective. Since F is projective, there exists a commutative diagram with exact rows:

$$\begin{array}{ccccccc}
0 \to & C & \xrightarrow{\alpha} & F & \xrightarrow{\beta} & M & \to 0 \\
 & \downarrow h & & \downarrow l & & \| & \\
0 \to & N & \xrightarrow{i} & L & \xrightarrow{p} & M & \to 0
\end{array}$$

from which we get the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 \to & \mathrm{Hom}_R(M,N) & \to & \mathrm{Hom}_R(F,N) & \to & \mathrm{Hom}_R(C,N) & \xrightarrow{\gamma} & \mathrm{Ext}^1_R(M,N) \\
 & \| & & \uparrow _ \circ k & & \uparrow _ \circ h & & \| \\
0 \to & \mathrm{Hom}_R(M,N) & \to & \mathrm{Hom}_R(K,N) & \to & \mathrm{Hom}_R(N,N) & \xrightarrow{\delta} & \mathrm{Ext}^1_R(M,N)
\end{array}$$

We conclude that $\delta(\mathrm{id}_N) = \gamma(h)$. Similarly, $\delta'(\mathrm{id}_N) = \gamma(h')$, and so $\gamma(h) = \gamma(h')$. Since $\mathrm{Ext}^1_R(F,N) = 0$, it follows that γ is surjective, so there exists $f \in \mathrm{Hom}_R(F,N)$ such that $f \circ \alpha = h - h'$. Furthermore, L is the pushout of α and h and L' is the pushout of α and h', so each is uniquely determined up to isomorphism. We prove that the two pushouts are isomorphic to each other. Namely, we define

$$\psi : \frac{N \oplus F}{\{(h(c), -\alpha(c)) : c \in C\}} \to \frac{N \oplus F}{\{(h'(c), -\alpha(c)) : c \in C\}}$$

as $\psi(a,b) = (a - f(b), b)$. We leave it to the reader to verify that ψ is a well-defined isomorphism, and that this makes the two extensions with L and L' equivalent. $\square$

Definition 22.3 *Let $e : 0 \to N \xrightarrow{i} K \xrightarrow{p} M \to 0$ and $e' : 0 \to N \xrightarrow{i'} K' \xrightarrow{p'} M \to 0$ be extensions. Let $X = \{(x, x') \in K \oplus K' : p(x) = p'(x')\}$ (the pullback of p and p'). The diagonal $\Delta = \{(i(n), i'(n)) : n \in N\}$ is a submodule of X. The* **Baer sum** *of e and e' is the extension $0 \to N \xrightarrow{j} Y \xrightarrow{q} M \to 0$, where $Y = X/\Delta$, $j(n) = (i(n), 0) = (0, -i'(n))$, and $q(x, x') = p(x) = p'(x')$.*

Exercise 22.4 Prove that the Baer sum of two extensions of M by N is an extension of M by N.

Exercise 22.5 Let e, e', f, f' be extensions of M by N, that e, e' are equivalent and that f, f' are equivalent.

i) Prove that the Baer sum of e and f is equivalent to the Baer sum of e' and f'.

ii) If e is the split extension, prove that the Baer sum of e and f is equivalent to f.

We established the connection between $\mathrm{Ext}^1_R(M, N)$ and extensions of M by N above via $\mathrm{Hom}_R(\_, N)$. The connection can also be established via $\mathrm{Hom}_R(M, \_)$. The following description is only partial. Let M and N be R-modules. For each extension $e : \quad 0 \to N \to K \to M \to 0$ of M by N consider

$$\mathrm{Hom}_R(M, K) \to \mathrm{Hom}_R(M, M) \xrightarrow{\delta} \mathrm{Ext}^1_R(M, N).$$

Note that e gives an element $\delta(\mathrm{id}_M)$. This map from extensions to Ext is also a bijection.

23 Essential extensions

In this section we look more closely at the structure of injective modules.

Definition 23.1 *An inclusion $M \subseteq N$ of R-modules is said to be an* **essential extension** *if for every non-zero submodule K of N, $K \cap M$ is non-zero.*

Remarks 23.2

(1) If R is a domain and K its field of fractions, then $R \subseteq K$ is essential.

(2) If $M \subseteq L$ and $L \subseteq N$ are essential extensions of R-modules, then so is $M \subseteq N$.

(3) $M \subseteq N$ is essential if and only if for all non-zero $x \in N$ there exists $r \in R$ such that rx is a non-zero element of M.

(4) Let $M \subseteq L_\alpha \subseteq N$ be R-modules as α varies over some index set. If $M \subseteq L_\alpha$ is essential for all α, then $M \subseteq \cup L_\alpha$ is essential (whenever the union is a module). (Proof: previous part.)

(5) If $M \subseteq N$ is essential and S is a multiplicatively closed subset of R consisting of non-zerodivisors on M, then $S^{-1}M \subseteq S^{-1}N$ is essential over $S^{-1}R$.

Lemma 23.3 *Let $M \subseteq N$ be an inclusion of R-modules. Then there exists a module L between M and N such that $M \subseteq L$ is essential and such that L is a maximal submodule of N with this property.*

Proof. Zornify the set of all intermediate modules that are essential over M. The set is non-empty as it contains M. By the last part of Remarks 23.2, every chain has an upper bound. Thus by Zorn's lemma the existence conclusion follows. $\square$

Proposition 23.4 *An R-module E is injective if and only if there does not exist a proper essential extension of E.*

Proof. Suppose that E is injective and that $E \subsetneq N$ is an essential extension. By Theorem 16.4, $N \cong E \oplus M$ for some non-zero module M, whence no non-zero multiple of a non-zero element of M is in E, which gives a contradiction.

Now suppose that E has no proper essential extension. By Theorem 16.4 it suffices to prove that any injective homomorphism $f : E \to M$ splits. Without loss of generality f is not an isomorphism. By possibly replacing E with an isomorphic copy, we may assume that f is an inclusion. Let Λ be the set of all non-zero submodules K of M such that $K \cap E = 0$. By assumption that E contains no proper essential extension, Λ is not empty. We Zornify Λ, and (verify details) there exists a maximal element K in Λ. Since $K \cap E = 0$, we have that $K + E = K \oplus E \subseteq M$, and that E injects into M/K.

We claim that $E \to M/K$ is essential: otherwise there exists a non-zero submodule L/K of M/K such that $E \cap (L/K) = 0$. But then $E \cap L \subseteq E \cap K = 0$, whence by maximality of K, we have $L = K$.

But then by assumption $E = M/K$, i.e., $(E + K)/K = M/K$, so that $E + K = M$, so that $E \oplus K = M$, so E is a direct summand of M via inclusion. By Theorem 16.4, E is injective. $\square$

Now we strengthen Lemma 23.3 under an additional assumption:

Lemma 23.5 *Let $M \subseteq N$ be an inclusion of R-modules and suppose that N is injective. Then there exists a submodule L of N that is maximal with respect to the property that it is essential over M, and any such L is injective.*

Proof. By Lemma 23.3 there exists a submodule L of N that is maximal among essential extensions of M in N. Suppose for contradiction that L is not injective. Then by Proposition 23.4, L has a proper essential extension E (which is not necessarily a submodule of N). Since N is injective, by definition we have

$$\begin{tikzcd} & N & \\ 0 \arrow[r] & L \arrow[u] \arrow[r] & E \arrow[ul, dashed, "h"'] \arrow[l, phantom, shift left=4, "\circlearrowleft"] \end{tikzcd}$$

If $\ker h \neq 0$, then since $L \to E$ is essential, there exists a non-zero element $x \in L \cap \ker h$, which gives a contradiction to the commutative diagram since L embeds in N. Thus h is injective. Hence $M \subseteq L \subseteq E \subseteq N$. By transitivity of essential extensions (Remarks 23.2), E is an essential extension of M. Thus by the maximality of L in E, $L = E$. So L has no proper essential extensions, so by Proposition 23.4, L is injective. $\square$

Theorem 23.6 *Let M be an R-module. Then there exists an over-module that is injective and essential over M. Any two such over-modules are isomorphic.*

Proof. By Theorem 17.7 there exists an injective R-module containing M. By Lemma 23.5 then there exists an injective module that is an essential extension of M.

Suppose that E and E' are injective modules that are essential over M. Then

$$\begin{tikzcd} & E' & \\ 0 \arrow[r] & M \arrow[u] \arrow[r] \arrow[ur, phantom, "\circlearrowleft" near end] & E \arrow[ul, dashed, "h"'] \end{tikzcd}$$

and h has to be injective as E is essential over M and M embeds in E'. Since h and E are injective, E must be a direct summand of E', and since E' is essential over M, the complementary direct summand must be 0, so that $E' \cong E$. $\square$

Definition 23.7 *The module constructed in the previous theorem (unique up to isomorphism) is called the* **injective hull** *or the* **injective envelope** *of M. It is denoted $E_R(M)$.*

Theorem 23.8 *Let $M \subseteq E$ be R-modules. The following are equivalent:*

(1) E is a maximal essential extension of M.

(2) E is injective and $M \subseteq E$ is essential.

(3) $E \cong E_R(M)$.

(4) E is injective, and if $M \subseteq E' \subseteq E$ with E' injective, then $E' = E$.

Proof. (2) and (3) are equivalent by definition.

Assume (1). Let F be an essential extension of E. Then by transitivity, F is an essential extension of M, and by the maximality assumption, $E = F$. Thus by Proposition 23.4, E is injective. This proves (2).

Assume (2). Let E' be an injective module such that $M \subseteq E' \subseteq E$. By Theorem 16.4, $E \cong E' \oplus E''$ for some submodule E'' of E. Then $E'' \cap M = 0$, so by assumption (2), $E'' = 0$. This proves (4).

Assume (4). By Lemma 23.5 there exists a maximal essential extension E' of M that is contained in E and such that E' is injective. Hence by assumption (4), $E' = E$, so E is essential over M. Any essential extension of M that contains E would have to have E as a direct summand because E is injective, but then by the essential property the complementary direct summand would have to be 0. Thus (1) follows. $\square$

The following is now clear:

Corollary 23.9 *If E is an injective R-module, then $E_R(E) = E$.* $\square$

Theorem 23.10 *(This is more on Theorem 16.8.) Let k be a field, let $x_1, \ldots, x_n$ be variables over k, and let $R = k[x_1, \ldots, x_n]$. Let E be an R-module with the k-vector space basis $\{X_1^{-i_1} \cdots X_n^{-i_n} : i_1, \ldots, i_n \geq 0\}$, with R-multiplication on E induced by*

$$x_k X_1^{-i_1} \cdots X_n^{-i_n} = \begin{cases} X_1^{-i_1} \cdots X_{k-1}^{-i_{k-1}} X_k^{-i_k+1} X_{k+1}^{-i_{k+1}} \cdots X_n^{-i_n}, & \text{if } i_k \geq 1; \\ 0, & \text{otherwise.} \end{cases}$$

Then E is the injective hull of $R/(x_1, \ldots, x_n) = k$ and every element of E is annihilated by a power of $(x_1, \ldots, x_n)$.

Proof. By Theorem 16.8 we know that E is injective.

Set $\mathfrak{m} = (x_1, \ldots, x_n)$. Let $f \in E$. For each $i = 1, \ldots, n$ let a_i be a negative integer that is a lower bound on the exponents on X_i in any term of f with a non-zero coefficient. Then $\mathfrak{m}^{1-\Sigma a_i} f = 0$. This proves that every element of E is annihilated by a power of E.

Let f be a non-zero element of E. Let $(a_1, \ldots, a_n)$ be an n-tuple of non-positive integers such that $X_1^{a_1} \cdots X_d^{a_d}$ appears in f with a non-zero coefficient, and that if another monomial $X_1^{b_1} \cdots X_d^{b_d}$ appears in f with a non-zero coefficient then there exists i such that $a_i < b_i$. (The monomial $\underline{X}^{\underline{a}}$ can be taken to be a leading monomial under the ("negative") degree-lexicographic order, i.e., convert all negative exponents to positive and use the degree-lexicographic order there.) Then $x_1^{-a_1} \cdots x_d^{-a_d} f$ is the coefficient of $X_1^{a_1} \cdots X_d^{a_d}$ in f, which is non-zero. This proves that E is an essential extension of k. $\square$

Proposition 23.11 *If $M \subseteq N$, then $E_R(M)$ embeds in $E_R(N)$.*

Proof. In the diagram

$$\begin{tikzcd}
 & E_R(N) & \\
0 \arrow[r] & M \arrow[u] \arrow[r] \arrow[ur, phantom, "\circlearrowleft"] & E_R(M) \arrow[ul, dashed, "h"']
\end{tikzcd}$$

the homomorphism h must be injective, for otherwise since $M \to E_R(M)$ is essential, a non-zero element of M maps to 0 in $N \subseteq E_R(N)$, which is a contradiction. This gives the desired embedding. $\square$

Proposition 23.12 *Let P and Q be distinct prime ideals in a ring R. Then $E_R(R/P) \not\cong E_R(R/Q)$.*

Proof. Without loss of generality $P \not\subseteq Q$, and let $a \in P \setminus Q$. Suppose for contradiction that the two injective hulls are isomorphic. Call the module E. Then E is an essential extension of R/P and of R/Q. Thus for every non-zero $x \in E$ there exists $r \in R$ such that rx is non-zero in $R/P \subseteq E$. Hence there exists $s \in R$ such that srx is non-zero in R/Q, so that $asrx$ is non-zero in $R/Q \subseteq E$. Hence there exists $t \in R$ such that $tasrx$ is non-zero in $R/P \subseteq E$. Since $rx \in P$ and $tas \in P$, this gives a contradiction. $\square$

Proposition 23.13 *Let R be a ring, P a prime ideal in R and let M be an R-module. Then*

$$\mathrm{Hom}_{R_P}((R/P)_P, M_P) \cong \mathrm{Hom}_{R_P}((R/P)_P, (E_R(M))_P).$$

In particular, if $(R, \mathfrak{m})$ is a local ring, then

$$\mathrm{Hom}_R(R/\mathfrak{m}, M) \cong \mathrm{Hom}_R(R/\mathfrak{m}, E_R(M)).$$

Proof. Define $\varphi : \mathrm{Hom}_{R_P}((R/P)_P, M_P) \to \mathrm{Hom}_{R_P}((R/P)_P, (E_R(M))_P)$ by $\varphi(f) = i_M \circ f$, where $i_M : M_P \to (E_R(M))_P$ is the inclusion. Clearly φ is an injective R_P-module homomorphism. Let $g \in \mathrm{Hom}_{R_P}((R/P)_P, (E_R(M))_P)$. This g is uniquely determined by $g(1) \in (E_R(M))_P$. Suppose that $g(1) \neq 0$. Let $s \in R \setminus P$ such that $sg(1) \in E_R(M)$ is non-zero. Since $M \to E_R(M)$ is essential, there exists $r \in R$ such that $rsg(1)$ is non-zero in M. If $r \in P$, then $0 = g(0) = g(rs) = rsg(1)$, which is a contradiction. So necessarily r is not in P. But then the image of sg is in M, so that the image of g is in M_P. Thus φ is an isomorphism. □

Definition 23.14 *Note that in this section we proved that every R-module M has an injective resolution $0 \to I^0 \to I^1 \to I^2 \to \cdots$, where I^0 is an essential extension of M, I^1 is an essential extension of I^0/M, and for all $i \geq 2$, I^i is an essential extension of the cokernel of $I^{i-2} \to I^{i-1}$. Such an injective resolution is called a* **minimal injective resolution***.*

Exercise 23.15 Let $M \to L$ be an essential extension, let $L \to K$ be a homomorphism such that the composition $M \to L \to K$ is injective. Prove that $L \to K$ is injective.

Exercise 23.16 Prove that any two minimal injective resolutions of a module are isomorphic.

Exercise 23.17 Let R be a ring and let $P \in \operatorname{Spec} R$.

(1) Prove that the R-module $E_R(R_P/PR_P)$ is an essential extension of R/P.

(2) Prove that $E_R(R/P)$ is an R_P-modules. (Let $s \in R \setminus P$. First prove that multiplication by s on $E_R(R/P)$ is injective by using that $E_R(R/P)$ is essential over R/P. Then make a diagram with $g : E_R(R/P) \to E_R(R/P)$ being inclusion and $f : E_R(R/P) \to E_R(R/P)$ being multiplication by s. Prove that there exists $h : E_R(R/P) \to E_R(R/P)$ such that $h \circ f = g$.)

(3) Prove that $E_R(R/P) \cong E_{R_P}(R_P/PR_P)$ as R_P-modules.

(4) Prove that for any prime ideal Q containing P, $E_R(R/P) \cong E_{R_Q}(R_Q/PR_Q)$ as R_P-modules.

Exercise 23.18 Let R be a ring, I an ideal in R, and M a module over R/I. Prove that

$$\mathrm{Hom}_R(R/I, E_R(M)) \cong E_{R/I}(M).$$

24 Structure of injective modules

Theorem 24.1 *Let R be a Noetherian ring. Then every injective R-module is a direct sum of injective modules of the form $E_R(R/P)$ as P varies over prime ideals.*

Proof. Let E be any non-zero injective R-module. Let N be any non-zero finitely generated R-submodule of E. Let $P \in \operatorname{Ass} N$. Then R/P injects in N and hence in E. Hence by Lemma 23.5, there exists an injective submodule E' of E that is essential over R/P. By Theorem 23.8, $E' \cong E_R(R/P)$, and by Theorem 16.4, $E_R(R/P)$ is a direct summand of E.

Consider the set Λ of submodules of E that are direct sums of $E_R(R/P)$ as P varies over prime ideals of R. Then $\Lambda \neq 0$ by the previous paragraph. We impose a partial order on Λ: $\oplus_{\alpha \in S} E_R(R/P_\alpha) \le \oplus_{\alpha \in T} E_R(R/P_\alpha)$ if $S \subseteq T$. Every chain in Λ has an upper bound, so by Zorn's lemma Λ contains a maximal element I. Since R is Noetherian, I is injective, and since $I \subseteq E$, $E \cong I \oplus I'$ for some necessarily injective module I'. By repeating the previous argument for I' in place of E, by maximality of I we get that $I' = 0$. $\square$

Theorem 24.2 *If P is a prime ideal in a commutative ring R, then $E_R(R/P)$ is an indecomposable R-module. If R is Noetherian, then any non-zero indecomposable injective R-modules is of the form $E_R(R/P)$ for some prime ideal P, and every injective R-modules is a direct sum of indecomposable R-modules.*

Proof. First we show that $E_R(R/P)$ is indecomposable. Assume that there are proper R-submodules E_1 and E_2 such that $E_1 \cap E_2 = 0$ and $E_1 + E_2 = E_R(R/P)$. Since $E_R(R/P)$ is essential over R/P, for $i = 1, 2$ there exists a non-zero x_i in $E_i \cap (R/P)$. But then $x_1 x_2$ is non-zero in $E_1 \cap E_2 \cap (R/P)$, which gives a contradiction.

The previous theorem shows the rest. $\square$

Proposition 24.3 *Let R be a Noetherian ring and P a prime ideal in R. Then every element of $E_R(R/P)$ is annihilated by a power of P.*

Proof. Let x be a non-zero element of $E_R(R/P)$. If $Q \in \operatorname{Ass}(Rx)$, then $R/Q \subseteq Rx \subseteq E_R(R/P)$, and by Proposition 23.11, $E_R(R/Q) \subseteq E_R(E_R(R/P)) = E_R(R/P)$, and by indecomposability established in Theorem 24.2, $E_R(R/Q) = E_R(R/P)$. Then by Proposition 23.12, $Q = P$. It follows that P is the only associated prime of the finitely generated module Rx, so that some power of P annihilates x. $\square$

Exercise 24.4 Let $P \subsetneq Q$ be distinct prime ideals in a ring R. Prove that

$$\operatorname{Hom}_R(E_R(R/P), E_R(R/Q)) \neq 0 \qquad \text{and} \qquad \operatorname{Hom}_R(E_R(R/Q), E_R(R/P)) = 0.$$

Exercise 24.5 Let R be a ring and let $P, Q \in \operatorname{Spec} R$. Prove that $(E_R(R/P))_Q \cong E_{R_Q}(R_Q/PR_Q)$ as R_Q-modules.

Exercise 24.6 Let P and Q be prime ideals in a Noetherian ring R with $Q \not\subseteq P$. Prove that $(E_R(R/Q))_P = 0$. (Hint: Let x be non-zero in $E_R(R/Q)$. There exists $e \in \mathbb{N}$ such that $Q^e x$ is in R/Q. Let $s \in Q \setminus P$. Prove that $s^{e+1}x = 0$. This is certainly true if $e = 0$. For $e > 0$, $Q^{e-1}(sx)$ is in R/Q, so by induction on e we conclude that $s^e(sx) = 0$.)

Exercise 24.7 Let R be a Noetherian ring and let M be a finitely generated R-module. Let $I^\bullet$ be a minimal injective resolution of M (as in Definition 23.14). For each i write $I^i = \oplus_{P \in S_i} E_R(R/P)$ for some multi-set S_i of prime ideals in R. Prove that for every $P \in S_{i+1}$ there exists $Q \in S_i$ such that P contains Q.

Exercise 24.8 Let R be a Noetherian ring and let M be a finitely generated R-module. Write $E_R(M) \cong \oplus_{p \in \operatorname{Spec} R} E_R(R/p)^{\mu(p,M)}$. Prove that $\mu(p, M) = \dim_{\kappa(p)} \operatorname{Hom}_{R_p}(\kappa(p), M_p)$, where $\kappa(p) = R_p/pR_p$. Conclude that $\mu(p, M)$ is finite for all p, and is zero for all except finitely many p. (These numbers are called **Bass numbers** of M. More on them is in Section 28.)

Exercise 24.9 Prove that $\mathbb{Q}/\mathbb{Z} \cong \oplus E_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z})$ as p varies over the positive prime integers.

***Exercise 24.10** Let k be a field, x, y, z variables over k, and let P be any height two prime ideal in $k[[x, y, z]]$. Let n be the minimal number of generators of P. Show that

$$E_R(R/P^2) \cong E_R(R/P)^3 \oplus E_R(k)^{\binom{n-1}{2}}.$$

Exercise 24.11 Let M be a finitely generated module over a Noetherian ring R. Let E be an injective module containing M. Prove that $E \cong E_R(M)$ if and only if for all prime ideals p, the induced map $\operatorname{Hom}_{R_p}(\kappa(p), M_p) \to \operatorname{Hom}_{R_p}(\kappa(p), E_p)$ is an isomorphism.

25 Duality and injective hulls

Definition 25.1 *Let $(R, \mathfrak{m})$ be a Noetherian local ring and let M be an R-module. The* **socle** *of M is $\operatorname{soc}(M) = 0_M :_M \mathfrak{m} = \operatorname{ann}_M(\mathfrak{m})$.*

Proposition 25.2 *Let $(R, \mathfrak{m})$ be a local ring and let M be an R-module.*

(1) $\operatorname{soc}(M)$ is a vector space over $R/\mathfrak{m}$.

(2) If M is Artinian, then $\operatorname{soc}(M)$ is a finite-dimensional vector space.

(3) If M is Artinian and R is Noetherian, then $\operatorname{soc} M \subseteq M$ is essential.

(4) If M is Noetherian, then $\operatorname{soc}(M)$ is a finite-dimensional vector space.

(5) The socle of $E_R(R/\mathfrak{m})$ is $R/\mathfrak{m}$.

Proof. Since $\operatorname{soc}(M)$ is annihilated by $\mathfrak{m}$, it is a module over $R/\mathfrak{m}$, hence it is a vector space. This proves (1).

A submodule of an Artinian module is Artinian, so that $\operatorname{soc}(M)$ is an Artinian $R/\mathfrak{m}$-vector space, whence finite-dimensional. This proves (2).

Let $x \in M$ be non-zero. Then $Rx \supseteq \mathfrak{m}x \supseteq \mathfrak{m}^2 x \supseteq \cdots$, so that by Artinian property there exists $n \in \mathbb{N}$ such that $\mathfrak{m}^n x = \mathfrak{m}^{n+1} x$. Since R is Noetherian, $\mathfrak{m}$ is finitely generated and so we can apply Nakayama's lemma to get that $\mathfrak{m}^n x = 0$. Let e be the least non-negative integers such that $\mathfrak{m}^e x = 0$. Since x is non-zero, then e must be positive. By the choice of e then $\mathfrak{m}^{e-1} x$ is non-zero, and every element of $\mathfrak{m}^{e-1}$ is in $\operatorname{soc}(M)$. This proves (3).

A submodule of an Noetherian module is Noetherian, so $\operatorname{soc}(M)$ is a finitely generated R-module that is annihilated by $\mathfrak{m}$. Thus $\operatorname{soc}(M)$ is a finitely generated $R/\mathfrak{m}$-module, hence a finite-dimensional vector space. This proves (4).

Certainly $R/\mathfrak{m} \subseteq \operatorname{soc} E_R(R/\mathfrak{m})$. Let $x \in \operatorname{soc} E_R(R/\mathfrak{m})$ be non-zero. By the injective hull property there exists $s \in R$ such that sx is non-zero in $R/\mathfrak{m}$. Since $\mathfrak{m}x = 0$, necessarily $s \notin \mathfrak{m}$, so that s is a unit in R. But then $x \in R/\mathfrak{m}$, which proves (5). □

Proposition 25.3 *Let $(R, \mathfrak{m})$ be a local ring. Write $E = E_R(R/\mathfrak{m})$ and $\_^{\nu} = \operatorname{Hom}_R(\_, E)$. For an R-module M of finite length, $\ell(\mathrm{M}^{\nu}) = \ell(M)$.*

Proof. We will prove this by induction on $\ell(M)$. If $\ell(M) = 1$, then $M \cong R/\mathfrak{m}$ and $\mathrm{M}^{\nu} \cong (\mathrm{R}/\mathfrak{m})^{\nu} = \operatorname{Hom}_R(R/\mathfrak{m}, E) = \operatorname{soc}(E)$ which is a one-dimensional vector space by Proposition 25.2.

Now let $\ell(M) > 1$. There exists an exact sequence $0 \to R/\mathfrak{m} \to M \to N \to 0$, and $\ell(N) = \ell(M) - 1$. Since E is injective, $0 \to \mathrm{N}^{\nu} \to \mathrm{M}^{\nu} \to (\mathrm{R}/\mathfrak{m})^{\nu} \to 0$ is exact, so by induction $\ell(\mathrm{M}^{\nu}) = \ell(\mathrm{N}^{\nu}) + 1 = \ell(N) + 1 = \ell(M)$. □

Proposition 25.4 *Let $(R, \mathfrak{m})$ be a zero-dimensional Noetherian local ring and $E = E_R(R/\mathfrak{m})$. Then $\operatorname{Hom}_R(E, E) \cong R$.*

Proof. Since R is zero-dimensional, R has finite length, so by the previous result, $\ell(\mathrm{R}^{\nu}) = \ell(R)$. But $\mathrm{R}^{\nu} \cong E$, so $\ell(E) = \ell(R)$. Then Proposition 25.3 applies to E and $\ell(\mathrm{E}^{\nu}) = \ell(R)$, i.e., $\operatorname{Hom}_R(E, E)$ and R have the same length.

Let $r \in R$. Then multiplication by r is an element of $\operatorname{Hom}_R(E, E)$. Suppose that this multiplication is 0, i.e., that $rE = 0$. Then $\operatorname{Hom}_R(R/rR, E) \cong E$, and by Exercise 23.18, $E_{R/rR}(R/\mathfrak{m}) \cong E$. By Proposition 25.3 and what we have done in this proof, $\ell(E) = \ell(R)$ and $\ell(E) = \ell(R/rR)$, so that $\ell(rR) = 0$, so that $r = 0$. It follows that the natural map $R \to \operatorname{Hom}_R(E, E)$ is an inclusion, and by the length argument it must be surjective as well. □

Proposition 25.5 *Let $(R, \mathfrak{m})$ be a Noetherian local ring. Let $E = E_R(R/\mathfrak{m})$. Then*

$$\operatorname{Hom}_R(E, E) \cong \widehat{R} = \varprojlim R/\mathfrak{m}^n.$$

Proof. Let $E_n = \{x \in E : \mathfrak{m}^n x = 0\}$.

Observe:

(1) $E_1 \subseteq E_2 \subseteq E_3 \subseteq \cdots \subseteq E$, and by Proposition 24.3, $\cup_n E_n = E$.

(2) If $f \in \operatorname{Hom}_R(E,E)$, then the image of E_n under f is in E_n. Thus set f_n to be the restriction of f to $E_n \to E_n$.

(3) $\{\operatorname{Hom}_R(E_n,E_n)\}$ form an inverse system as any $g \in \operatorname{Hom}_R(E_{n+1},E_{n+1})$ maps to $\operatorname{Hom}_R(E_n,E_n)$ by restriction.

(4) Claim: $\operatorname{Hom}_R(E,E) \cong \lim_{\leftarrow} \operatorname{Hom}_R(E_n,E_n)$. Certainly any $f \in \operatorname{Hom}_R(E,E)$ maps to $\{f_n\}$ as defined above. If $\{f_n\}$ is zero, then $f=0$ since $E=\cup E_n$ and f is determined by all f_n. If $\{f_n\} \in \lim_{\leftarrow} \operatorname{Hom}_R(E_n,E_n)$, we can define $f: E \to E$ in the obvious way. This proves the claim.

Observe that $E_n = \{x \in E : \mathfrak{m}^n x = 0\} = \operatorname{Hom}_R(R/\mathfrak{m}^n, E)$. By Exercise 23.18, $E_n \cong E_{R/\mathfrak{m}^n}(R/\mathfrak{m})$. By Proposition 25.4, $\operatorname{Hom}_R(E_n,E_n) = \operatorname{Hom}_{R/\mathfrak{m}^n}(E_n,E_n) \cong R/\mathfrak{m}^n$. Finally,

$$\operatorname{Hom}_R(E,E) \cong \lim_{\leftarrow} \operatorname{Hom}_R(E_n,E_n) \cong \lim_{\leftarrow} R/\mathfrak{m}^n \cong \widehat{R}.$$

(Well, we need to check that the following square commutes:

$$\begin{array}{ccc} \operatorname{Hom}_R(E_{n+1},E_{n+1}) & \to & \operatorname{Hom}_R(E_n,E_n) \\ \downarrow & & \downarrow \\ R/\mathfrak{m}^{n+1} & \to & R/\mathfrak{m}^n \end{array}$$

But all we need to check is that the identity of $\operatorname{Hom}_R(E_{n+1},E_{n+1})$ comes to the same end either way, but this is easy.) $\square$

Proposition 25.6 *Let $(R,\mathfrak{m})$ be a Noetherian local ring. Then $E_R(R/\mathfrak{m})$ is a module over $\widehat{R}$ and $E_R(R/\mathfrak{m}) \otimes_R \widehat{R} \cong E_R(R/\mathfrak{m})$.*

Proof. We define $\varphi : E_R(R/\mathfrak{m}) \times_R \widehat{R} \to E_R(R/\mathfrak{m})$ as $\varphi(x, \{r_n\}_n) = r_l x$ where l is such that for all $n \geq l$, $r_n - r_l$ is in the annihilator of x. Since x is annihilated by a power of $\mathfrak{m}$ and since $\{r_n\}$ is a Cauchy sequence in R in the $\mathfrak{m}$-adic topology, this makes φ well-defined. It is straightforward to check that it is an R-bilinear map.

By the definition of tensor products there exists an R-module homomorphism $h : E_R(R/\mathfrak{m}) \otimes_R \widehat{R} \cong E_R(R/\mathfrak{m})$ such that $\varphi = h \cong \psi$, where ψ is the standard R-bilinear map $\psi : E_R(R/\mathfrak{m}) \times_R \widehat{R} \to E_R(R/\mathfrak{m}) \otimes_R \widehat{R}$.

It is clear that φ is surjective, and so h is surjective.

We first prove that every element of $E_R(R/\mathfrak{m}) \otimes_R \widehat{R}$ can be written in the form $x \otimes \{1\}_n$. Namely, let $y = \sum_{i=1}^k x_i \otimes \{r_{in}\}_n$ be an arbitrary element in the tensor product. By possibly taking different representatives of Cauchy sequences, we may without loss of generality assume that for all $i = 1, \ldots, k$, for all l, and for all $n \geq l$, $r_{in} - r_{il} \in \mathfrak{m}^l$. We now fix l to be a positive integer such that $\mathfrak{m}^l$ annihilates $x_1, \ldots, x_k$. Let $\mathfrak{m}^l = (a_1, \ldots, a_s)$. Then $\{r_{in}\}_n = \{r_{il}\}_n + \sum_{j=1}^s \{r'_{ijn} a_j\}$ for some $r'_{ijn} \in R$ such that $\sum_j r'_{ijn} a_j = r_{in} - r_{il}$. Since $\cap_n \mathfrak{m}^n = 0$, we may choose the r'_{ijn} so that $\{r'_{ijn}\}_n \in \widehat{R}$. Then

$$y = \sum_{i=1}^k x_i \otimes \{r_{in}\}_n = \sum_{i=1}^k \Big(x_i \otimes \big(\{r_{il}\}_n + \sum_{j=1}^s \{r'_{ijn} a_j\} \big) \Big)$$

$$= \sum_{i=1}^{k}\left(x_i \otimes \{r_{il}\}_n + x_i \otimes \sum_{j=1}^{s}\{r'_{ijn}a_j\}\right) = \sum_{i=1}^{k}\left(r_{il}x_i \otimes \{1\}_n + a_j x_i \otimes \sum_{j=1}^{s}\{r'_{ijn}\}\right)$$
$$= \sum_{i=1}^{k} r_{il}x_i \otimes \{1\}_n = (\sum_{i=1}^{k} r_{il}x_i) \otimes \{1\}_n.$$

Thus $y \in \ker(h)$ if and only if $\sum_{i=1}^{k} r_{il}x_i = 0$ in $E_R(R/\mathfrak{m})$, which means that $h = 0$. Thus h is a bijection. □

Proposition 25.7 *Let $(R, \mathfrak{m})$ be a Noetherian local ring and let $N \subseteq M$ be R-modules. Then $M = N$ if and only if $\mathrm{M}^\nu = \mathrm{N}^\nu$.*

Proof. By injectivity, the functor $\_^\nu$ is exact, so $\mathrm{M}^\nu = \mathrm{N}^\nu$ if and only if $(\mathrm{M/N})^\nu = 0$. Thus it suffices to prove that $M = 0$ if and only if $\mathrm{M}^\nu = 0$.

Certainly $\mathrm{M}^\nu = 0$ if $M = 0$. Suppose that $M \neq 0$. Let x be non-zero in M. Then applying $\_^\nu$ to the short exact sequence $0 \to Rx \to M \to M/Rx \to 0$ gives a surjection $\mathrm{M}^\nu \to (\mathrm{Rx})^\nu$, whence $\mathrm{M}^\nu = 0$ implies that $(\mathrm{Rx})^\nu = 0$. So by possibly replacing M by Rx, it suffices to prove the proposition in case M is generated by one element. But then $M/\mathfrak{m}M \cong R/\mathfrak{m}$, and it suffices to prove the proposition for $M = R/\mathfrak{m}$. But $\mathrm{M}^\nu \cong (\mathrm{R/m})^\nu$ is non-zero by Proposition 25.3. □

Corollary 25.8 *Let $(R, \mathfrak{m})$ be a Noetherian local ring. Then $E_R(R/\mathfrak{m})$ is Artinian.*

Proof. Let $M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$ be a descending chain of submodules of $E = E_R(R/\mathfrak{m})$. By Proposition 25.5, $\mathrm{E}^\nu = \widehat{R}$, and by exactness of the dual functor, $\widehat{R} \cong \mathrm{E}^\nu \twoheadrightarrow \mathrm{M}_0^\nu \to \to \mathrm{M}_1^\nu \twoheadrightarrow \cdots$. Thus $\mathrm{M}_\mathrm{n}^\nu = \widehat{R}/I_n$ for some ideal I_n, and $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$. Since $\widehat{R}$ is Noetherian, this chain must stabilize. Thus for some $l \geq 0$, $\widehat{I_l} = \widehat{I_n}$ for all $n \geq l$, and so $\mathrm{M}_\mathrm{l}^\nu = \mathrm{M}_\mathrm{n}^\nu$ for all $n \geq l$. But then by Proposition 25.7 we get that $M_l = M_n$ for all $n \geq l$. □

Theorem 25.9 (Matlis duality) *Let $(R, \mathfrak{m})$ be a Noetherian local ring and $E = E_R(R/\mathfrak{m})$. Then there exists an arrow-reversing bijection between finitely generated $\widehat{R}$-modules and Artinian R-modules as follows:*

(1) *If M is a finitely generated $\widehat{R}$-module, then $\mathrm{Hom}_{\widehat{R}}(M, E) = \mathrm{M}^\nu$ is an Artinian R-module.*
(2) *If N is an Artinian R-module, then $\mathrm{Hom}_R(N, E) = \mathrm{N}^\nu$ is a finitely generated $\widehat{R}$-module.*

Proof. Let M be a finitely generated $\widehat{R}$-module. Then there exists a surjection $\widehat{R}^n \twoheadrightarrow M$, so that $0 \to \mathrm{M}^\nu \to \mathrm{E}^{\nu n}$ is exact, whence M^ν is Artinian over R.

If N is Artinian over R, then its socle is finitely generated, say by n elements, so that the socle embeds in E^n, whence since $\mathrm{soc}\,(N) \subseteq N$ is essential by Proposition 25.2, N embeds in E^n. Then $\widehat{R}^n \cong (\mathrm{E}^\nu)^n$ maps onto N^ν, so that N^ν is finitely generated over $\widehat{R}$.

Obviously the two functions are arrow-reversing. It remains to prove that they are bijections, i.e., that the composition of the two in any order is identity. Note that there is always a map $K \to (\mathrm{K}^\nu)^\nu$ given by $k \mapsto (f \mapsto f(k))$ (for $f \in \mathrm{K}^\nu$). Actually, we have to be more careful, if K is an R-module, we have $K \to \mathrm{Hom}_{\widehat{R}}(\mathrm{Hom}_R(K, E), E)$ given by $k \mapsto (f \mapsto f(k))$; and if K is an $\widehat{R}$-module, we have $K \to \mathrm{Hom}_R(\mathrm{Hom}_{\widehat{R}}(K, E), E)$ given by $k \mapsto (f \mapsto f(k))$.

Let M be a finitely generated module over $\widehat{R}$. Then M is finitely presented, so there is an exact complex of the form $\widehat{R}^a \to \widehat{R}^b \to M \to 0$. By the previous paragraph we have a natural commutative diagram

$$\begin{array}{ccccccc} \widehat{R}^a & \to & \widehat{R}^b & \to & M & \to 0 \\ \downarrow & & \downarrow & & \downarrow & \\ (\widehat{\mathrm{R}}^{\nu\nu})^a & \to & (\widehat{\mathrm{R}}^{\nu\nu})^b & \to & \mathrm{M}^{\nu\nu} & \to 0 \end{array}$$

in which the rows are exact. Furthermore, all the maps are natural, the left two vertical maps are equalities, so that by the Snake Lemma, $M \to \mathrm{M}^{\nu\nu}$ is also the natural isomorphism and so equality.

If N is an Artinian R-module, we get an exact complex $0 \to N \to E^a \to E^b$ for some $a, b \in \mathbb{N}_0$, and similar reasoning as in the previous paragraph shows that $N = \mathrm{N}^{\nu\nu}$. $\square$

Exercise 25.10 Let $(R, \mathfrak{m})$ be a Noetherian local ring. Show that $\mathrm{ann}(E_R(R/\mathfrak{m})) = 0$. (Hint: consider $R/\mathrm{ann}\, E \to \mathrm{Hom}_R(E_R(R/\mathfrak{m}), E_R(R/\mathfrak{m})) \to \widehat{R}$.)

Exercise 25.11 Let R be a Noetherian ring, I an ideal in R, and P a prime ideal containing I. Show that $E_R(R/P)$ is not isomorphic to $E_{R/I}(R/P)$ if $I \neq 0$.

Exercise 25.12 Let $(R, \mathfrak{m})$ be a Noetherian local ring, let $E = E_R(R/\mathfrak{m})$, and let M be an R-module of finite length. Show that $\mu(M) = \dim_{R/\mathfrak{m}} \mathrm{soc}\,(\mathrm{Hom}_R(M, E))$.

Exercise 25.13 Let $(R, \mathfrak{m})$ be a Noetherian local ring and M an R-module. Prove that M is Artinian if and only if the following two conditions hold:

(1) $\mathrm{soc}\, M$ is a finite-dimensional vector space over $R/\mathfrak{m}$,

(2) every element of M is annihilated by a power of $\mathfrak{m}$.

Exercise 25.14 Let $(R, \mathfrak{m})$ be a Noetherian local ring. Let I be an $\mathfrak{m}$-primary ideal, and let $E = E_R(R/\mathfrak{m})$. Prove that $\mathrm{ann}_E(I)$ is a finitely generated R-module.

26 More on injective resolutions

We have seen that any left R-module has an injective resolution.

Definition 26.1 *Injective R-module M has* **finite injective dimension** *if there exists an injective resolution*

$$0 \to M \to I^0 \to I^1 \to \cdots \to I^{n-1} \to I^n \to 0$$

of M. The least integer n as above is called the **injective dimension** *of M.*

Theorem 26.2 *Let $(R, \mathfrak{m})$ be a Noetherian local ring, and let $E = E_R(R/\mathfrak{m})$.*

(1) Any Artinian R-module M has an injective resolution (even minimal injective resolution) in which each injective module is a finite direct sum of copies of E.

(2) If an Artinian R-module M has finite injective dimension d, then M has an injective resolution (even minimal injective resolution) of the form

$$0 \to M \to E^{b_0} \to E^{b_1} \to E^{b_2} \to \cdots \to E^{b_{d-1}} \to E^{b_d} \to 0$$

for some $b_i \in \mathbb{N}_0$.

Proof. By Proposition 25.2, $\operatorname{soc} M \subseteq M$ is essential and $\operatorname{soc} M$ is a finite-dimensional module over R/m. Say that n is the dimension of $\operatorname{soc} M$. Then $\operatorname{soc} M \cong (R/\mathfrak{m})^n \subseteq E^n$ is an essential extension. Since E^n is injective and since $\operatorname{soc} M \subseteq M$, there exists a homomorphism $f : M \to E^n$ such that the restriction of f to $\operatorname{soc}(M)$ is the inclusion map. Since $\operatorname{soc}(M) \to M$ is essential, f must be injective. Thus M embeds in E^n, and furthermore E^n is essential over M. Set $b_0 = n$. Now, E^n/M is an Artinian module, and we repeat the argument to get b_1, etc. This proves the first part of the proof.

Now suppose in addition that M has finite injective dimension d. Let $0 \to M \to I^0 \to \cdots \to I^d \to 0$ be an injective resolution of M, and let $0 \to M \to E^{b_0} \to E^{b_1} \to \cdots$ be an injective resolution as constructed above. Let C be the cokernel of $E^{b_{d-2}} \to E^{b_{d-1}}$. Then $0 \to M \to E^{b_0} \to E^{b_1} \to \cdots \to E^{b_{d-2}} \to E^{b_{d-1}} \to C \to 0$ is exact. By Schanuel's lemma (Theorem 18.8), the direct sum of C with some injective R-modules is isomorphic to an injective module, so that C must be injective, whence in $0 \to M \to E^{b_0} \to E^{b_1} \to \cdots$ we may take $b_{d+1} = 0$. ☐

Proposition 26.3 *Let $(R, \mathfrak{m})$ be a Noetherian ring, let $E = E_R(R/\mathfrak{m})$, and let M be an Artinian R-module. Let $0 \to M \to I^\bullet$ be a minimal injective resolution of M. Then $(\mathrm{I}^\bullet)^\nu \to \mathrm{M}^\nu \to 0$ is a minimal free resolution of M^ν over $\widehat{R}$, where $\_^\nu = \mathrm{Hom}_R(\_, E)$.*

In particular, by Matlis duality, if $\mathrm{injdim}_R(M) < \infty$, then $\mathrm{injdim}_R(M) = \mathrm{pd}_{\widehat{R}}(\mathrm{M}^\nu)$.

Proof. By Theorem 26.2, each I^i is a direct sum of copies of $E_R(R/\mathfrak{m})$. Since E is injective, $(\mathrm{I}^\bullet)^\nu \to \mathrm{M}^\nu \to 0$ is exact. By Proposition 25.5, $(\mathrm{I}^\mathrm{i})^\nu$ is a direct sum of copies of $\mathrm{E_R(R/\mathfrak{m})}^\nu = \widehat{R}$, hence a free $\widehat{R}$-module. Thus $(\mathrm{I}^\bullet)^\nu \to \mathrm{M}^\nu \to 0$ is a projective resolution of M^ν. If $(\mathrm{I}^\bullet)^\nu$ is not a minimal resolution, then up to a change of bases there exists j such that $(\mathrm{I}^\mathrm{j})^\nu \to (\mathrm{I}^{\mathrm{j}-1})^\nu$ can be taken as a direct sum of $\widehat{R} \overset{\mathrm{id}}{\to} \widehat{R}$ and of $F \to G$ for some free $\widehat{R}$-modules F and G. Then $(I^{j-1} \to I^j) = ((\mathrm{I}^\mathrm{j})^\nu \to (\mathrm{I}^{\mathrm{j}-1})^\nu)^\nu \cong (E \overset{\mathrm{id}}{\to} E) \oplus (\mathrm{G}^\nu \to \mathrm{F}^\nu)$. By exactness of $I^\bullet$, the copy of E in I^j that maps identically to $E \subseteq I^{j+1}$ has no non-zero submodule that is in the image of $I^{j-1} \to I^j$, which contradicts the minimality of the injective resolution. □

Proposition 26.4 *Let M be an R-module, and let $x \in R$ be a non-zerodivisor on R and on M. If $0 \to M \to I^\bullet$ is an injective resolution of M, then with $J^i = \mathrm{Hom}_R(R/xR, I^{i+1})$ and the induced maps on the J_i, $0 \to M/xM \to J^\bullet$ is an injective resolution of the R/xR module M/xM.*

In particular, if M has finite injective dimension, then $\mathrm{injdim}_{R/xR}(M/xM) \le \mathrm{injdim}_R M - 1$.

Proof. Let $0 \to M \to I^0 \to I^1 \to \cdots$ be an exact sequence of R-modules with each I^i injective. Apply $\mathrm{Hom}_R(R/xR, \_)$ to the injective part to get the complex

$$0 \to \mathrm{Hom}_R(R/xR, I^0) \to \mathrm{Hom}_R(R/xR, I^1) \to \cdots.$$

By Proposition 16.5, each $\mathrm{Hom}_R(R/xR, I^i)$ is an injective module over R/xR. The ith cohomology of the displayed co-complex is $\mathrm{Ext}^i_R(R/xR, M)$. As a projective resolution of the R-module R/xR is $0 \to R \overset{x}{\to} R \to 0$, it follows that $\mathrm{Ext}^i_R(R/xR, M) = 0$ for $i \ge 2$, that $\mathrm{Ext}^1_R(R/xR, M) = \mathrm{Hom}_R(R, M)/x\,\mathrm{Hom}_R(R, M) \cong M/xM$, and that $\mathrm{Ext}^0_R(R/xR, M) = \mathrm{Hom}_R(R/xR, M) = 0$. In particular, in the displayed co-complex above, $\mathrm{Hom}_R(R/xR, I^0)$ injects into $\mathrm{Hom}_R(R/xR, I^1)$, so that $\mathrm{Hom}_R(R/xR, I^1) \cong \mathrm{Hom}_R(R/xR, I^0) \oplus E$ for some necessarily injective (R/xR)-module E, so that the displayed co-complex yields the following co-complex with the same cohomology:

$$0 \to E \overset{d_2|_E}{\to} \mathrm{Hom}_R(R/xR, I^2) \to \cdots.$$

In particular, the cohomology at E is $\mathrm{Ext}^1_R(R/xR, M) = M/xM = \ker(d_2|_E)$, and the cohomology elsewhere is 0. Thus $0 \to M/xM \to J^\bullet$ is an exact co-complex of (R/xR)-modules, which finishes the proof. □

Corollary 26.5 (Rees) *Let M and N be R-modules, let $x \in R$ be a non-zerodivisor on R and on M such that $xN = 0$. Then for all $i \geq 0$,*

$$\operatorname{Ext}_R^{i+1}(N, M) \cong \operatorname{Ext}_{R/xR}^i(N, M/xM).$$

Proof. Let $I^\bullet$ and $J^\bullet$ be as in Proposition 26.4. Then for $i \geq 0$,

$$\begin{aligned}
\operatorname{Ext}_R^{i+1}(N, M) &= \frac{\ker(\operatorname{Hom}_R(N, I^{i+1}) \to \operatorname{Hom}_R(N, I^{i+2}))}{\operatorname{im}(\operatorname{Hom}_R(N, I^i) \to \operatorname{Hom}_R(N, I^{i+1}))} \\
&\cong \frac{\ker(\operatorname{Hom}_R(N \otimes_R (R/xR), I^{i+1}) \to \operatorname{Hom}_R(N \otimes_R (R/xR), I^{i+2}))}{\operatorname{im}(\operatorname{Hom}_R(N \otimes_R (R/xR), I^i) \to \operatorname{Hom}_R(N \otimes_R (R/xR), I^{i+1}))} \\
&\cong \frac{\ker(\operatorname{Hom}_{R/xR}(N, \operatorname{Hom}_R(R/xR, I^{i+1})) \to \operatorname{Hom}_{R/xR}(N, \operatorname{Hom}_R(R/xR, I^{i+2})))}{\operatorname{im}(\operatorname{Hom}_{R/xR}(N, \operatorname{Hom}_R(R/xR, I^i)) \to \operatorname{Hom}_{R/xR}(N, \operatorname{Hom}_R(R/xR, I^{i+1})))} \\
&= \frac{\ker(\operatorname{Hom}_{R/xR}(N, J^i) \to \operatorname{Hom}_{R/xR}(N, J^{i+1}))}{\operatorname{im}(\operatorname{Hom}_{R/xR}(N, J^{i-1}) \to \operatorname{Hom}_{R/xR}(N, J^i))} \\
&\cong \operatorname{Ext}_{R/xR}^i(N, M/xM),
\end{aligned}$$

where the third isomorphism is due to tensor-hom adjointness. $\square$

Proposition 26.6 *Let R be a Noetherian ring, let M be a finitely generated R-module and let I be an ideal in R such that $IM \neq M$. Then*

$$\operatorname{depth}_I(M) = \min\{l : \operatorname{Ext}_R^l(R/I, M) \neq 0\}.$$

In particular, the length of a maximal M-regular sequence in I does not depend on the sequence.

Proof. Let $d = \operatorname{depth}_I(M)$. If $d = 0$, then I is contained in an associated prime P of M. Since $P \in \operatorname{Ass} M$, R/P embeds in M. Hence $\operatorname{Hom}_R(R/I, R/P) \subseteq \operatorname{Hom}_R(R/I, M)$, and since the former is non-zero, $\operatorname{Hom}_R(R/I, M)$ is non-zero as well. Thus the equality holds if $d = 0$.

Now let $d > 0$. Let $x \in I$ be a non-zerodivisor on M. Then $0 \to M \xrightarrow{x} M \to M/xM \to 0$ is a short exact sequence, which yields the long exact sequence

$$\cdots \to \operatorname{Ext}_R^n(R/I, M) \xrightarrow{x} \operatorname{Ext}_R^n(R/I, M) \to \operatorname{Ext}_R^n(R/I, M/xM) \to \operatorname{Ext}_R^{n+1}(R/I, M) \xrightarrow{x}$$

Since $x \in I = \operatorname{ann}(R/I)$, the multiplications by x in the long exact sequence are all zero homomorphisms, so that for all $n \geq 0$,

$$0 \to \operatorname{Ext}_R^n(R/I, M) \to \operatorname{Ext}_R^n(R/I, M/xM) \to \operatorname{Ext}_R^{n+1}(R/I, M) \to 0$$

is exact. Since $\operatorname{depth}_I(M/xM) = d - 1$, by induction we get that $\operatorname{Ext}_R^n(R/I, M) = 0$ and $\operatorname{Ext}_R^{n+1}(R/I, M) = 0$ for all $n = 0, \ldots, d-2$, i.e., that $\operatorname{Ext}_R^n(R/I, M) = 0$ for all $n = 0, \ldots, d-1$, and $\operatorname{Ext}_R^{d-1}(R/I, M/xM) \cong \operatorname{Ext}_R^d(R/I, M)$ is non-zero. $\square$

Corollary 26.7 *If M is a finitely generated module over a Noetherian local ring $(R, \mathfrak{m})$, then for any ideal I in R,* $\operatorname{injdim}_R(M) \geq \operatorname{depth}_I(M)$. □

Proposition 26.8 *If M is a non-zero finitely generated module over a Noetherian local ring $(R, \mathfrak{m})$, then* $\operatorname{depth} R \leq \operatorname{injdim}_R(M)$.

Proof. Let $x_1, \ldots, x_d \in \mathfrak{m}$ be a maximal regular sequence on R. We abbreviate $x_1, \ldots, x_d$ as $\underline{x}$. Then $K_\bullet(\underline{x}; R)$ is the complex

$$0 \to K_d(\underline{x}; R) \to \cdots \to K_1(\underline{x}; R) \to K_0(\underline{x}; R) \to 0,$$

and it is a free resolution of $R/(\underline{x})$. Then $\operatorname{Hom}_R(K_\bullet(\underline{x}; R), M))$ is the complex

$$0 \to \operatorname{Hom}_R(K_0(\underline{x}; R), M) \to \operatorname{Hom}_R(K_1(\underline{x}; R), M) \to \cdots \to \operatorname{Hom}_R(K_d(\underline{x}; R), M) \to 0,$$

which is naturally isomorphic to

$$0 \to \operatorname{Hom}_R(K_0(\underline{x}; M)) \to \operatorname{Hom}_R(K_1(\underline{x}; M)) \to \cdots \to \operatorname{Hom}_R(K_d(\underline{x}; M)) \to 0.$$

Thus

$$\operatorname{Ext}^d_R(R/(\underline{x}), M) = \frac{\operatorname{Hom}_R(K_d(\underline{x}; M))}{\operatorname{im} \operatorname{Hom}_R(K_{d-1}(\underline{x}; M))} = \frac{M}{(\underline{x})M} \neq 0.$$ □

Lemma 26.9 *Let $(R, \mathfrak{m})$ be a Noetherian local ring, let N be a finitely generated R-module, and let $n \in \mathbb{N}_0$. Then* $\operatorname{injdim}_R(N) \leq n$ *if and only if* $\operatorname{Ext}^j_R(M, N) = 0$ *for all $j > n$ and all finitely generated R-modules M.*

Proof. One direction is clear. Let $0 \to N \to I^0 \to I^1 \to \cdots \to I^{n-1} \to C \to 0$ be exact, with all I^i injective. By Exercise 19.4, $\operatorname{Ext}^j_R(M, C) \cong \operatorname{Ext}^{j+n}_R(M, N)$ for all $j \geq 1$. From the assumption we then get that $\operatorname{Ext}^j_R(M, C) = 0$ for all $j \geq 1$ and all finitely generated R-modules M. In particular, for any short exact sequence $0 \to M' \to M \to M'' \to 0$ we get the exact sequence:

$$0 \to \operatorname{Hom}_R(M'', C) \to \operatorname{Hom}_R(M, C) \to \operatorname{Hom}_R(M', C) \to 0 = \operatorname{Ext}^1_R(M'', C),$$

so that $\operatorname{Hom}_R(\_, C)$ is exact on finitely generated R-modules, sot that by Baer's criterion Theorem 16.2, C is injective. It follows that $\operatorname{injdim} N \leq n$. □

Theorem 26.10 *Let $(R, \mathfrak{m})$ be a Noetherian local ring, let N be a finitely generated R-module. Then* $\operatorname{injdim}_R(N) = \sup\{l : \operatorname{Ext}^l_R(R/\mathfrak{m}, N) \neq 0\}$.

Proof. Clearly $\operatorname{injdim}_R(N) \geq \sup\{l : \operatorname{Ext}^l_R(R/\mathfrak{m}, N) \neq 0\}$, so if the latter is infinity, N must not have finite injective dimension. So we may assume that $n = \sup\{l : \operatorname{Ext}^l_R(R/\mathfrak{m}, N) \neq 0\} \in \mathbb{N}_0$.

Claim: $\operatorname{Ext}^j_R(M, N) = 0$ for all $j > n$ and all finitely generated R-modules. Proof of the claim: If $M = R/\mathfrak{m}$, this is given. If M has finite length, then we can prove this by induction on the length and the long exact sequence on Ext induced by a short exact sequence $0 \to R/\mathfrak{m} \to M \to C \to 0$. If M does not have finite length, i.e., if $\dim M > 0$, we take a prime filtration $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ of M, where for all i, $M_i/M_{i-1} \cong R/P_i$ for some prime ideal P_i in R. By trapping Ext of the middle module and by induction on the length of a prime filtration it suffices to prove that $\operatorname{Ext}^j_R(R/P, N) = 0$ for all $j > n$ and all prime ideals P in R. Let $s \in m \setminus P$. Then the short exact sequence $0 \to R/P \xrightarrow{s} R/P \to C \to 0$ induces for $j \geq 1$ the exact complex:

$$\operatorname{Ext}^{n+j}_R(L, N) \to \operatorname{Ext}^{n+j}_R(R/P, N) \xrightarrow{s} \operatorname{Ext}^{n+j}_R(R/P, N) \to \operatorname{Ext}^{n+j+1}_R(L, N).$$

By induction on the dimension of the module in the first entry, $\operatorname{Ext}^{n+j}_R(L, N)$ and $\operatorname{Ext}^{n+j+1}_R(L, N)$ are zero. Hence $\operatorname{Ext}^{n+j}_R(R/P, N) = s \operatorname{Ext}^{n+j}_R(R/P, N)$, and $\operatorname{Ext}^{n+j}_R(R/P, N)$ is a finitely generated R-module, so by Nakayama's lemma, $\operatorname{Ext}^{n+j}_R(R/P, N) = 0$. This proves the claim.

But then by Lemma 26.9, N has injective dimension at most n. □

Theorem 26.11 *Let $(R, \mathfrak{m})$ be a Noetherian local ring and let N be a finitely generated R-module of finite injective dimension. Then* $\operatorname{injdim}_R N = \operatorname{depth} R$. *If* $\operatorname{injdim}_R N = 0$, *then R is Artinian.*

Proof. Suppose that $\operatorname{injdim}_R N = 0$. Then N is injective. Suppose that N has a direct summand $E_R(R/P)$ for some prime ideal $P \neq m$. Let $s \in \mathfrak{m} \setminus P$ and let $x \in N$ be the image of $1 \in R/P$. Then by Exercise 23.17, $x/s, x/s^2, x/s^3, \ldots$ are elements of N, whence they generate a finitely generated R-module N. So there exists n such that N is generated by x/s^n. Hence $x/s^{n+1} = rx/s^n$ for some $r \in R$, whence $(1 - rs)x = 0 \in E_R(R/P)$. Since the elements of $R \setminus P$ are units on $E_R(R/P)$ it follows that $1 - rs \in P \subseteq \mathfrak{m}$, which is a contradiction. Thus $N = E_R(R/\mathfrak{m})^n$ for some $n \in \mathbb{N}^+$, and so N is Artinian and finitely generated. It follows that N has finite length, so that $\mathrm{N}^\nu = \widehat{R}^n$ has finite length as well, so that $\widehat{R}$ and hence R is Artinian and hence has depth 0.

Now suppose that $l = \operatorname{injdim}_R N > 0$. Suppose that $\operatorname{depth} R < l$. Let $x_1, \ldots, x_n \in \mathfrak{m}$ be a maximal regular sequence on R. Then we have a short exact sequence $0 \to R/\mathfrak{m} \to R/(x_1, \ldots, x_n) \to R/I \to 0$ for some ideal I, whence by Theorem 26.10 we get a long exact sequence

$$\cdots \to \operatorname{Ext}^l_R(R/I, N) \to \operatorname{Ext}^l_R(R, N) \to \operatorname{Ext}^l_R(R/\mathfrak{m}, N) \to 0,$$

where $\operatorname{Ext}^l_R(R/\mathfrak{m}, N) \neq 0$, but $\operatorname{Ext}^l_R(R, N) = 0$, which gives a contradiction. Thus $\operatorname{depth} R \geq \operatorname{injdim}_R N$. Proposition 26.8 proves the other inequality. $\square$

***Exercise 26.12** (Ischebeck) Let $(R, \mathfrak{m})$ be a Noetherian local ring, and let M and N be finitely generated R-module. Suppose that either M has finite projective dimension or that N has finite injective dimension. Prove that $\operatorname{depth} R - \operatorname{depth} M = \sup\{l : Ext^l_R(M, N) \neq 0\}$.

Exercise 26.13 Let $(R, \mathfrak{m})$ be a Noetherian local ring. Suppose that $R/\mathfrak{m}$ has finite injective dimension. Prove that R is a regular local ring. (Hint: By Matlis duality $\widehat{R}$ is a regular local ring.)

Exercise 26.14 Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of finitely generated modules over a Noetherian ring. Let I be an ideal in R such that $IM' \neq M'$, $IM \neq M$ and $IM'' \neq M''$.

i) Prove that $\operatorname{depth}_I(M) \geq \min\{\operatorname{depth}_I(M'), \operatorname{depth}_I(M'')\}$.

ii) Prove that $\operatorname{depth}_I(M') \geq \min\{\operatorname{depth}_I(M), \operatorname{depth}_I(M'') + 1\}$.

iii) Prove that $\operatorname{depth}_I(M'') \geq \min\{\operatorname{depth}_I(M), \operatorname{depth}_I(M') - 1\}$.

Exercise 26.15 Let $(R, \mathfrak{m})$ be a Cohen–Macaulay local ring. Let $x_1, \ldots, x_d$ be a system of parameters. Prove that $\dim \operatorname{soc}(\frac{R}{(x_1,\ldots,x_d)}) = \dim_{R/\mathfrak{m}} \operatorname{Ext}^d_R(R/\mathfrak{m}, R)$, and hence is independent of the system of parameters. This number is called the **Cohen–Macaulay type** of R.

Exercise 26.16 Give an example of a Noetherian local ring with systems of parameters $x_1, \ldots, x_d$ and $y_1, \ldots, y_d$ for which $\dim \operatorname{soc}(\frac{R}{(x_1,\ldots,x_d)}) \neq \dim \operatorname{soc}(\frac{R}{(y_1,\ldots,y_d)})$.

27 Gorenstein rings

Definition 27.1 *A Noetherian local ring $(R, \mathfrak{m})$ is* **Gorenstein** *if* $\mathrm{id}_R(R) < \infty$*. A Noetherian ring R is* **Gorenstein** *if for any maximal ideal $\mathfrak{m}$ of R, $R_\mathfrak{m}$ is Gorenstein.*

Proposition 27.2 *If R is a Gorenstein ring, then for any non-zerodivisor $x \in R$, R/xR is Gorenstein.*

Proof. This follows from Proposition 26.4. □

Theorem 27.3 *Every regular ring is Gorenstein.*

Proof. It suffices to prove that any regular local ring $(R, \mathfrak{m})$ is Gorenstein. By Theorem 14.3, for all finitely generated R-modules M, $\mathrm{pd}_R(M) \le \dim R$, whence $\mathrm{Ext}^j_R(M, R) = 0$ for all $j > \dim R$. But then by Lemma 26.9, $\mathrm{injdim}_R(R) \le \dim R$. □

The same proof shows that every finitely generated module N over a regular local ring R has injective dimension at most $\dim R$.

A ring is called **a complete intersection** if it is a quotient of a regular ring by a regular sequence. By what we have proved above, every complete intersection ring is Gorenstein. By Theorem 26.11 we even know that for a complete intersection ring R, $\mathrm{injdim}_R R = \mathrm{depth}\, R = \dim R$.

Theorem 27.4 *Let $(R, \mathfrak{m})$ be a 0-dimensional Noetherian local ring. The following are equivalent:*

(1) $R \cong E_R(R/\mathfrak{m})$.

(2) R is Gorenstein.

(3) $\dim_{R/\mathfrak{m}}(\mathrm{soc}\, R) = 1$.

(4) (0) *is an irreducible ideal in R (cannot be written as an intersection of two strictly larger ideals).*

Proof. Let $E = E_R(R/\mathfrak{m})$.

Certainly (1) implies (2) and (3) (the latter by Proposition 25.2).

Assume (3). Let $\mathrm{soc}\,(R) = (x)$. Let I be a non-zero ideal in R. Since R is Artinian, $\mathfrak{m}^l = 0$ for some l, and in particular, we may choose a least integer l such that $\mathfrak{m}^l I = 0$. Then $0 \ne \mathfrak{m}^{l-1} I \subseteq \mathrm{soc}\, R$. Necessarily $x \in \mathfrak{m}^{l-1} I \subseteq I$, and similarly $x \in J$. Thus the intersection of two non-zero ideals cannot be zero. Thus (4) holds.

If (4) holds and $\dim_{R/\mathfrak{m}}(\mathrm{soc}\, R) > 1$, choose $x, y \in \mathrm{soc}\, R$ that span a two-dimensional subspace of the socle. Then $(x) \cap (y) = (0)$, contradicting (4). This proves that (4) implies (3).

Assume (3). By Proposition 25.2, $\mathrm{soc}\, R \subseteq R$ is an essential extension. If $\mathrm{soc}\, R$ is one-dimensional, this says that R is essential over a homomorphic image of $R/\mathfrak{m}$, so that the essential extension R of $R/\mathfrak{m}$ injects in the maximal essential extension E of $R/\mathfrak{m}$. But

R has finite length, so by Proposition 25.3, $\ell(R) = \ell(\mathrm{R}^\nu) = \ell(E)$, whence $R \cong E$. This proves (1).

Now assume (2). By Theorem 26.2, there exists an exact sequence of the form

$$0 \to R \to E^{b_0} \to E^{b_1} \to \cdots \to E^{b_n} \to 0,$$

for some $b_i \in \mathbb{N}_0$. Apply the dual $\_^\nu = \mathrm{Hom}_R(\_, E)$ to get the exact sequence

$$0 \to (\mathrm{E}^{\mathrm{b_n}})^\nu \to \cdots \to (\mathrm{E}^{\mathrm{b_1}})^\nu \to (\mathrm{E}^{\mathrm{b_0}})^\nu \to \mathrm{R}^\nu \to 0,$$

and so by Proposition 25.4,

$$0 \to R^{b_n} \to \cdots \to R^{b_1} \to R^{b_0} \to E \to 0$$

is exact, so that E is finitely generated and has finite projective dimension over R. Thus by the Auslander–Buchsbaum formula (Theorem 13.6), $\mathrm{pd}_R\, E + \mathrm{depth}\, E = \mathrm{depth}\, R = 0$, whence $\mathrm{pd}_R\, E = 0$, so E is projective and hence free over R (by Fact 5.5 (6)). Thus $E \cong R^l$ for some l, but by Proposition 25.3, $\ell(E) = \ell(\mathrm{R}^\nu) = \mathrm{R}^\nu$, necessarily $l = 1$. This proves (1), and finishes the proof of the theorem. □

Theorem 27.5 *Let $(R, \mathfrak{m})$ be a Noetherian local ring. Then the following are equivalent:*

(1) R is Gorenstein.

(2) Any system of parameters $x_1, \ldots, x_d$ in R is a regular sequence and $R/(x_1, \ldots, x_d)$ is Gorenstein.

(3) Any system of parameters $x_1, \ldots, x_d$ in R is a regular sequence and the $(R/\mathfrak{m})$-vector space $((x_1, \ldots, x_d) : \mathfrak{m})/(x_1, \ldots, x_d)$ is one-dimensional.

Proof. The equivalence of (2) and (3) follows from the previous theorem.

Assume that R is Gorenstein. If R is injective, then by Theorem 26.11, R is Artinian, so (2) and (3) hold by the previous theorem. So assume that $\mathrm{injdim}_R\, R > 0$. Then by Theorem 26.11, $\mathrm{depth}\, R > 0$. Let $x \in \mathfrak{m}$ be a non-zerodivisor. Then by Proposition 26.4, R/xR is a Gorenstein ring, so by induction on $\mathrm{depth}\, R$, every system of parameters $x, x_2, \ldots, x_d$ in R is a regular sequence and $R/(x, x_2, \ldots, x_d)$ is Gorenstein. But then by Theorem 15.2, every system of parameters in R is a regular sequence, and by Proposition 26.4, (2) and (3) hold.

Now assume that (2) and (3) hold. Let $x_1, \ldots, x_d$ be a system of parameters in R. Then for all $j > d$, $\mathrm{Ext}^j_R(R/\mathfrak{m}, R) \cong \mathrm{Ext}^{j-d}_{R/(x_1,\ldots,x_d)}(R/\mathfrak{m}, R/(x_1, \ldots, x_d))$ by Corollary 26.5. Since by assumption $R/(x_1, \ldots, x_d)$ is Gorenstein and so an injective module over itself, $\mathrm{Ext}^{j-d}_{R/(x_1,\ldots,x_d)}(R/\mathfrak{m}, R/(x_1, \ldots, x_d)) = 0$. Since this holds for all $j > d$, by Theorem 26.10 says that $\mathrm{id}_R(R) \leq d$, so that R is Gorenstein. □

Proposition 27.6 *Let $(S, \mathfrak{n})$ be a regular local ring, and let $R = S/I$ be a zero-dimensional quotient of S, with minimal free S-resolution*

$$0 \to F_d \to F_{d-1} \to \cdots \to F_0 \to R \to 0.$$

Then R is Gorenstein if and only if $F_d \cong S$.

Proof. By the Auslander–Buchsbaum formula (Theorem 13.6), $d = \operatorname{pd}_S(R) = \operatorname{depth} S - \operatorname{depth} R = \operatorname{depth} S = \dim S$. By Exercise 8.9, $\operatorname{rank} F_d = \dim_{S/\mathfrak{n}} \operatorname{Tor}_d^S(R, S/\mathfrak{n})$. But $\operatorname{Tor}_d^S(R/S/\mathfrak{n}) \cong H_d(S/I \otimes_S K_\bullet(y_1, \ldots, y_d; S))$, where $\mathfrak{n} = (y_1, \ldots, y_d)$. This last homology is

$$\operatorname{ann}_{S/I}(y_1, \ldots, y_n) \cong \frac{I : (y_1, \ldots, y_d)}{I},$$

which equals the socle of S/I. Thus, $\operatorname{rank} F_d = 1$ if and only if S/I is Gorenstein. □

The following also immediately follows from Theorem 27.5:

Theorem 27.7 *Every Gorenstein ring is Cohen–Macaulay.* □

Example 27.8 If $(S, \mathfrak{n})$ is a regular local ring and $x_1, \ldots, x_d$ is a system of parameters, then $R = S/(x_1, \ldots, x_d)$ is a Gorenstein ring.

Exercise 27.9 Let $(S, \mathfrak{n})$ be a regular local ring of dimension d, and let $\mathfrak{n} = (y_1, \ldots, y_d)$. Let $x_1, \ldots, x_d$ be a system of parameters. Write $x_i = \sum_j a_{ij} y_j$. Prove that $\operatorname{soc}(S/(x_1, \ldots, x_d))$ is generated by the image of the determinant of the matrix a_{ij}.

Exercise 27.10 Let $(R, \mathfrak{m})$ be a Gorenstein local ring. Prove that $\operatorname{injdim}_R(R) = \dim R = \operatorname{depth} R$.

28 Bass numbers

This section lacks details.

Theorem 28.1 *Let R be a Noetherian ring. Let $I^\bullet$ be a minimal injective resolution of an R-module M. Then for all $P \in \operatorname{Spec}(R)$ and all $i \geq 0$, $\operatorname{Hom}_{R_P}(R_P/PR_P, (I^i)_P) \to \operatorname{Hom}_{R_P}(R_P/PR_P, (I^{i+1})_P)$ is the zero map.*

Proof. Let Q^i be the kernel of $I^i \to I^{i+1}$. Then $0 \to Q^i \to I^i \to I^{i+1} \to I^{i+2} \to \cdots$ is exact and $I^i = E_R(Q^i)$. Since localization and Hom are left-exact (see Exercise 2.6), it follows that

$$0 \to \operatorname{Hom}_{R_P}(R_P/PR_P, Q^i_P) \xrightarrow{f} \operatorname{Hom}_{R_P}(R_P/PR_P, I^i_P) \xrightarrow{g} \operatorname{Hom}_{R_P}(R_P/PR_P, I^{i+1}_P)$$

is exact. Since $I^\bullet$ is minimal, I^i is an essential extension of Q^i, so that by Proposition 23.13, $\operatorname{Hom}_{R_P}(R_P/PR_P, Q^i_P) \xrightarrow{f} \operatorname{Hom}_{R_P}(R_P/PR_P, I^i_P)$ is an isomorphism. Thus g is zero. $\square$

Definition 28.2 *Let M be a finitely generated module over a Noetherian ring R. Let $I^\bullet$ be any minimal injective resolution of M (recall Definition 23.14). For any prime ideal P of R, the ith* **Bass number** *of M with respect to P is the number of copies of $E_R(R/P)$ in I^i, and is denoted $\mu_i(P, M)$.*

By Exercise 23.16 and possibly more work, Bass numbers are well-defined.

Proposition 28.3 $\mu_i(P, M) = \dim_{R_P/PR_P} \operatorname{Ext}^i_{R_P}(R_P/PR_P, I^i_P)$.

Proof. Let $I^\bullet$ be a minimal injective resolution of M. By Exercise 16.9, $(I^\bullet)_P$ is an injective resolution of M_P. By Remarks 23.2 (and the definition of injective resolutions), $(I^\bullet)_P$ is a minimal injective resolution of M_P.

By Theorem 24.2, I^j is a direct sum of indecomposable injective modules of the form $E_R(R/Q)$ with Q prime ideals. By Exercises 24.6 and 23.17, $(I_j)_P$ is a direct sum of indecomposable injective modules of the form $E_R(R/Q)$ with Q prime ideals contained in P. The number of copies of $E_R(R/P)$ in I^j is the same as the number of copies of $E_R(R/P)$ in $(I^j)_P$, and equals $\dim_{R_P/PR_P} \operatorname{Hom}_{R_P}(R_P/PR_P, (I^i)_P)$.

Thus, by changing notation, we may assume that R is a Noetherian local ring with maximal ideal $\mathfrak{m}$, and we need to prove that $\mu_i(\mathfrak{m}, M) = \dim_{R/\mathfrak{m}} \operatorname{Hom}_R(R/\mathfrak{m}, I^i)$. Since $I^\bullet$ is minimal, by Theorem 28.1 all the maps in the complex $\operatorname{Hom}_R(R/\mathfrak{m}, I^\bullet)$ are 0. Thus $\mu_i(\mathfrak{m}, M) = \dim_{R/\mathfrak{m}} \operatorname{Ext}^i_R(R/\mathfrak{m}, M)$. $\square$

The proof above shows the following:

Corollary 28.4 *If R is Noetherian local with maximal ideal $\mathfrak{m}$, then $\operatorname{Ext}^i_R(R/\mathfrak{m}, M) = H^i(\operatorname{Hom}_R(R/\mathfrak{m}, I^\bullet)) \cong \operatorname{Hom}_R(R/\mathfrak{m}, I^i) = \mu_i(\mathfrak{m}, M)$.* $\square$

Corollary 28.5 *If $(R, \mathfrak{m})$ is a Noetherian ring and M a finitely generated R-module, then $\mu_i(P, M) < \infty$ for all i and all $P \in \operatorname{Spec} R$.*

Exercise 28.6 Prove that the following are equivalent for a Noetherian local ring $(R, \mathfrak{m})$:

(1) R is Gorenstein.

(2) R is Cohen–Macaulay and of type 1.

(3) R is Cohen–Macaulay and $\mu_{\dim R}(\mathfrak{m}, R) = 1$.

Exercise 28.7 Let $(R, \mathfrak{m})$ be a Cohen–Macaulay local ring. Prove that $\mu_i(\mathfrak{m}, R) = 0$ for all $i \neq \dim R$.

Exercise 28.8 Let $(R, \mathfrak{m})$ be Gorenstein local ring of dimension d.

(1) Prove that for all $P \in \operatorname{Spec} R$, $\mu_i(P, R) = 0$ for all $i \neq \operatorname{ht} P$.

(2) Prove that a minimal injective resolution of R looks like:

$$0 \to R \to \oplus_{\operatorname{ht} P=0} E_R(R/P) \to \oplus_{\operatorname{ht} P=1} E_R(R/P) \to \cdots \to \oplus_{\operatorname{ht} P=d} E_R(R/P) \to 0.$$

(The maps are not easy to understand.)

Definition 28.9 *The* **injective type** *of a Noetherian local ring $(R, \mathfrak{m})$ of dimension d is $\mu_d(\mathfrak{m}, R)$.*

Remark 28.10 Paul Roberts proved that if the injective type is 1, then R is Cohen–Macaulay. Costa, Huneke and Miller proved that if the injective type is 2 and the ring is a complete domain, then it is Cohen–Macaulay. Tom Marley showed that if R is complete and unmixed with injective type 2, then it is also Cohen–Macaulay.

29 Criteria for exactness

For any $m \times n$ matrix A with entries in a ring R and for any non-negative integer r, $I_r(A)$ denotes the ideal in R generated by the determinants of all the $r \times r$ submatrices of A. Since $I_r(A) \subseteq I_{r-1}(A)$, and for other reasons, by convention $I_0(A) = R$ for all A, even for the zero matrix.

Definition 29.1 *Let $\varphi : R^n \to R^m$ be a module homomorphism, and let M be an R-module. By the* **rank** *of φ with respect to M we mean the largest integer r such that $I_r(\varphi) \not\subseteq \operatorname{ann} M$. We denote this number $\operatorname{rank}(\varphi, M)$. If $M \neq 0$, certainly $\operatorname{rank}(\varphi, M) \geq 0$. By $I(\varphi, M)$ we denote $I_r(\varphi)$, where $r = \operatorname{rank}(\varphi, M)$. If $M = R$, we write $I(\varphi) = I(\varphi, R)$.*

Definition 29.2 *If I is an ideal in R and M is an R-module, we set* $\operatorname{depth}_I(M) = \inf\{l \in \mathbb{N}_0 : \operatorname{Ext}^l_R(R/I, M) \neq 0\}$. *By convention,* $\operatorname{depth}_I(M) = \infty$ *if* $IM = M$.

Note that if R is Noetherian and M is finitely generated, this (even the convention part) is the usual local definition of depth by Proposition 26.6.

In the sequel, you may want to think of M always finitely generated. Then it is clear from the definition of regular sequences that $\operatorname{depth}_I(M) = \operatorname{depth}_{I(R/\operatorname{ann} M)}(M)$. It is an exercise (Exercise 29.8) that the same equality also holds for general M.

Theorem 29.3 (Neal McCoy)*Let R be a commutative ring and let M be an R-module. Let $A = (a_{ij})$ be an $m \times n$ matrix with entries in R. Then the system of equations*

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + \cdots + a_{2n}x_n = 0 \\ \qquad\qquad \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = 0 \end{cases}$$

has no non-zero solution $(x_1, \ldots, x_n) \in M^n$ if and only if $\sup\{l \mid (0 :_M I_l(A)) = 0\} = n$.

Proof. By possibly adding a few zero rows we may assume that $m \geq n$. Let $d = \sup\{l|(0 :_M I_l(A)) = 0\}$. Note that $d < \infty$.

Suppose that $d < n$. So $(0 :_M I_d(A)) = 0 \subsetneq (0 :_M I_{d+1}(A))$. Then there exists non-zero $m \in M$ such that $mI_{d+1}(A) = 0$, and there exists a $d \times d$ submatrix of A such that its minor multiplied by m is not zero. Without loss of generality this submatrix B consists of the first d rows and the first d columns of A. Let C be the submatrix of A consisting of the first $d+1$ rows and the first $d+1$ columns. Set $x_j = y_j m$ for $j \leq d+1$, where y_j is the determinant of the submatrix of C obtained by removing the jth row and the last column, and let $x_j = 0$ for $j > d+1$. Then $(x_1, \ldots, x_n)$ is a non-zero solution.

Now let $(x_1, \ldots, x_n) \in M^n$ be a non-zero solution. Let B be any $n \times n$ submatrix of A. Then B times the column vector $(x_1, \ldots, x_n) = 0$, so that $(\det B)I = (\operatorname{adj} B)B$ annihilates $x_1, \ldots, x_n$. Since B was arbitrary, we get that $I_n(A)$ annihilates $(x_1, \ldots, x_n)$, so that $n < d$. ∎

Theorem 29.4 (Acyclicity lemma, due to Peskine and Szpiro, [7]) *Let R be a Noetherian ring, let I be an ideal in R. and let $M_\bullet$ be the complex* $0 \to M_n \xrightarrow{d_n} M_{n-1} \xrightarrow{d_{n-1}} \cdots \to M_2 \xrightarrow{d_2} M_1 \xrightarrow{d_1} M_0$ *of R-modules such that for all $i \geq 1$,*

(1) $\operatorname{depth}_I(M_i) \geq 1$*, and*

(2) $H_i(M_\bullet) = 0$ *or* $\operatorname{depth}_I(H_i(M_\bullet)) = 0$.

Then $M_\bullet$ is exact.

Proof. We will prove more: $M_\bullet$ is exact, and for each i, $\operatorname{im} d_i$ has I-depth at least i.

First we prove that d_n is injective. Otherwise, the non-zero module $H_n(M_\bullet) = \ker d_n$ has I-depth zero and is contained in M_n which has positive I-depth, and this is a contradiction. Thus $\operatorname{im} d_n \cong M_n$ has I-depth at least n. So we may assume that $n > 1$.

If $i < n$, we have the complex $0 \to \operatorname{im} d_{i+1} \to M_i \to \cdots \to M_1$, which yields short exact sequences

$$0 \to \operatorname{im} d_{i+1} \to M_i \to \frac{M_i}{\operatorname{im} d_{i+1}} \to 0, \qquad 0 \to H_i(M_\bullet) \to \frac{M_i}{\operatorname{im} d_{i+1}} \xrightarrow{d_i} \operatorname{im} d_i \to 0.$$

For induction we assume that the I-depth of $\operatorname{im} d_{i+1} \geq i+1$. For all $j \leq i$, the long exact sequence on homology induced by the first sequence gives us $\operatorname{Ext}_R^{j-1}(R/I, M_i) = 0 \to \operatorname{Ext}_R^{j-1}(R/I, M_i/\operatorname{im} d_{i+1}) \to \operatorname{Ext}_R^{j}(R/I, \operatorname{im} d_{i+1}) = 0$, so that $\operatorname{depth}_I(M_i/\operatorname{im} d_{i+1}) \geq i$. If $H_i(M_\bullet) = 0$, this proves that $\operatorname{im} d_i$ has I-depth at least i. Otherwise, the second sequence gives $0 \to \operatorname{Ext}_R^0(R/I, H_i(M_\bullet)) \to \operatorname{Ext}_R^0(R/I, M_i/\operatorname{im} d_{i+1})$, and $0 \neq \operatorname{Ext}_R^0(R/I, H_i(M_\bullet))$, $\operatorname{Ext}_R^0(R/I, M_i/\operatorname{im} d_{i+1}) \neq 0$, so that $\operatorname{depth}_I(M_i/\operatorname{im} d_{i+1}) = 0$, which gives a contradiction. □

Lemma 29.5 *Let R be a Noetherian ring, let M be a non-zero R-module, Let F, G, H be finitely generated free R-modules, and let $F \xrightarrow{\alpha} G \xrightarrow{\beta} H$ be a complex such that $I(\alpha, M) = I(\beta, M) = R$. Then $F \otimes_R M \to G \otimes_R M \to H \otimes_R M$ is exact if and only if* $\operatorname{rank}(\alpha, M) + \operatorname{rank}(\beta, M) = \operatorname{rank} G$.

Proof. For any R-module N, $N \otimes_R M \cong N \otimes_R M \otimes_{R/\operatorname{ann} M} (R/\operatorname{ann} M) \cong N \otimes_{R/\operatorname{ann} M} M$, so that for both implications we may assume that $\operatorname{ann} M = 0$. Thus $\operatorname{rank}(\alpha, M) = \operatorname{rank}(\alpha)$ and $\operatorname{rank}(\beta, M) = \operatorname{rank}(\beta)$. Note that with the assumption that $I(\alpha) = I(\beta) = R$, both conditions are local, so that we may assume that R is local.

The assumption $I(\alpha) = R$ means that some $\operatorname{rank}(\alpha)$-minor is invertible. Up to a change of basis α can be written as a matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & A \end{bmatrix}$$

for some submatrix A of rank $\operatorname{rank}(\alpha) - 1$ and with $I(A) = R$. Thus by induction α can be written as a matrix whose $\operatorname{rank}(\alpha)$ diagonal entries are 1, and all other entries are 0. Thus $\ker \alpha$ and $\operatorname{coker} \alpha$ are free R-modules, and $G \cong \operatorname{coker} \alpha \oplus \operatorname{im} \alpha$. Similarly, $\ker \beta$ is free, and $F \xrightarrow{\alpha} \ker \beta$ yields $\ker \beta \cong E \oplus \operatorname{im} \alpha$ for some free R-module E. Note that the rank of the free module $G/\ker \beta$ is $\operatorname{rank} \beta$, and that $\operatorname{rank}(\alpha) = \operatorname{rank}(\operatorname{im} \alpha)$.

Then $F \otimes_R M \to G \otimes_R M \to H \otimes_R M$ is exact if and only if $E \otimes_R M = 0$, which for Noetherian local rings holds if and only if one or the other module is 0. Since $M \neq 0$, $E = 0$. Thus $F \otimes_R M \to G \otimes_R M \to H \otimes_R M$ is exact if and only if $ker\beta = \operatorname{im} \alpha$, i.e., if and only if $\operatorname{rank} G = \operatorname{rank}(\alpha) + \operatorname{rank}(\beta)$. □

Theorem 29.6 (Buchsbaum–Eisenbud exactness criterion, [2]) *Let R be a Noetherian ring, let M be a non-zero R-module, and let $F_\bullet$ be the complex*

$$F_\bullet : \quad 0 \to F_n \xrightarrow{\delta_n} F_{n-1} \xrightarrow{\delta_{n-1}} \cdots \to F_2 \xrightarrow{\delta_2} F_1 \xrightarrow{\delta_1} F_0,$$

where all F_i are finitely generated free R-modules. Then $F_\bullet \otimes_R M$ is exact if and only if the following two conditions are satisfied for all $i \geq 1$:

(1) $\operatorname{rank}(\delta_i, M) + \operatorname{rank}(\delta_{i+1}, M) = \operatorname{rank} F_i$,

(2) $\operatorname{depth}_{I(\delta_i,M)}(M) \geq i$.

Proof. Note that all δ_i can be thought of as (finite) matrices. Recall that if $\delta_i \otimes \mathrm{id}_M = 0$, then $\operatorname{rank}(\delta_i, M) = 0$, $I(\delta_i, M) = R$, and $\operatorname{depth}_{I(\delta_i,M)}(M) = \infty$.

Suppose that conditions (1) and (2) hold. To prove the exactness of $F_\bullet \otimes_R M$, it suffices to do so after localization at all (maximal) prime ideals – the hypotheses are still satisfied, as the ranks cannot decrease as the ideals $I(\delta_i, M)$ contain non-zerodivisors. So let m be the unique maximal ideal in R. Set $d = \operatorname{depth}_m(M)$. If $i > d$, then $\operatorname{depth}_{I(\delta_i,M)}(M) \geq i$ implies that $I(\delta_i, M) = R$. Let $F'_d = \operatorname{coker}(\delta_{d+1})$. Thus by Lemma 29.5 and assumptions,

$$0 \to F_n \otimes M \to F_{n-1} \otimes M \to \cdots \to F_{d+1} \otimes M \to F_d \otimes M \to F'_d \otimes M \to 0,$$

is exact, and

$$0 \to F'_d \otimes M \to F_{d-1} \otimes M \to F_{d-2} \otimes M \to \cdots \to F_2 \otimes M \to F_1 \otimes M \to F_0 \otimes M,$$

is a complex. If the last complex is not exact, by further localization we may assume that the complex is not exact but is exact after localization at any non-maximal prime ideal. If the complex above is not exact at the ith spot, by the localization assumption every element of the ith homology is annihilated by some power of m, so R/m embeds in this homology, so that its m-depth is 0. But then with $I = m$ we may apply the Acyclicity Lemma (Theorem 29.4) to get that $F_\bullet \otimes M$ is exact.

Now suppose that $F_\bullet \otimes_R M$ is exact. By Theorem 29.3, $0 :_M (I_{\operatorname{rank} F_n}(\delta_n)) = 0$, so that $\operatorname{rank}(\delta_n, M) = \operatorname{rank} F_n$ and $I(\delta_n)$ does not consist of zerodivisors on M. It follows that $\operatorname{depth}_{I(\delta_n,M)}(M) \geq 1$. Suppose we have proved that $\operatorname{depth}_{I(\delta_i,M)}(M) \geq 1$ for $i = n, n-1, \ldots, l+1$. Let U be the set of all non-zerodivisors on M. Then $U^{-1}(F_\bullet \otimes M)$ is still exact, and $\operatorname{depth}_{I(\delta_l,M)}(M) \geq 1$ if and only if $\operatorname{depth}_{U^{-1}I(\delta_l,U^{-1}M)}(U^{-1}M) \geq 1$. So temporarily we assume that $U^{-1}R = R$. Then $I(\delta_n, M) = \cdots = I(\delta_{l+1}, M) = R$, and as in the previous part, $F_\bullet \otimes M$ splits into two exact parts, such that the first map in the second is δ_l, and so by the case n, $I(\delta_l, M) \geq 1$. Thus we have proved so far that for all i, $\operatorname{depth}_{I(\delta_i,M)}(M) \geq 1$.

Thus by Lemma 29.5, condition (1) holds after inverting all non-zerodivisors on M, so (1) holds over R.

It remains to prove that (2) holds if $F_\bullet \otimes M$ is exact. Suppose that (2) does not hold, and let k be the largest integer such that $l = \operatorname{depth}_{I(\delta_k,M)}(M) < k$. Let $x_1, \ldots, x_l \in$

$I(\delta_k, M)$ be a maximal M-regular sequence. Then there exists $m \in \operatorname{Spec} R$ such that m contains I and is associated to $M/(x_1, \dots, x_l)M$. After localization at m, $F_\bullet \otimes M$ is still exact, and we still have k the largest integer for which $\operatorname{depth}_{I(\delta_k,M)}(M) < k$. So without loss of generality we may assume that R is a Noetherian local ring and that the maximal ideal m is associated to $M/(x_1, \dots, x_l)M$. We have $\operatorname{depth}_m(M) = l < k$. Also, since $\operatorname{depth}_{I(\delta_i,M)}(M) \geq i$ for all $i > k$, necessarily $I(\delta_i, M) = R$ for all $i > k$. By splitting off as in the first part, without loss of generality we may assume that $k = n$. Then $\operatorname{depth}_{I(\delta_n,M)}(M) = \operatorname{depth}_m(M) = l < n$. By what we have proved, $n \geq 2$. Consider the short exact sequence $0 \to \ker(\delta_{n-1} \otimes \mathrm{id}_M) \to F_{n-1} \otimes M \to \operatorname{im}(\delta_{n-1} \otimes \mathrm{id}_M) \to 0$.

First assume that $\operatorname{im} \delta_{n-1} \otimes M = 0$. This still holds if we pass to $R/\operatorname{ann} M$, the complex $F_\bullet \otimes M \otimes (R/\operatorname{ann} M)$ is still exact, and the ranks of the maps remain unchanged. So temporarily we assume that $\operatorname{ann} M = 0$. Then for all i, $\operatorname{rank}(\delta_i, M) = \operatorname{rank}(\delta_i)$. By what we have already proved under the assumption that $F_\bullet \otimes M$ is exact, $\operatorname{rank}(\delta_n) = \operatorname{rank}(\delta_n, M) = \operatorname{rank} F_n = \operatorname{rank} F_{n-1}$. Thus $I(\delta_n, M)$ is the determinant of δ_n. Then $0 \to F_n \overset{\delta_n}{\to} F_{n-1} \to 0$ is a complex that is exact when tensored with M, and it is even exact when tensored with $M/(\det \delta_n)M$. But then if $(\det \delta_n)M \neq M$, we do not get the correct rank conditions, so we have a contradiction. So necessarily $(\det \delta_n)M = M$, whence $\operatorname{depth}_{(I(\delta_n,M)}(M) = \infty$, contradicting the assumptions.

Thus $\operatorname{im} \delta_{n-1} \otimes M \neq 0$. The long exact sequence on cohomology on $0 \to \ker(\delta_{n-1} \otimes \mathrm{id}_M) \to F_{n-1} \otimes M \to \operatorname{im}(\delta_{n-1} \otimes \mathrm{id}_M) \to 0$ gives

$$0 = \operatorname{Ext}^{i-1}(R/m, F_{n-1} \otimes M) \to \operatorname{Ext}^{i-1}(R/m, \operatorname{im} \delta_{n-1} \otimes M) \to 0 = \operatorname{Ext}^i(R/m, \ker(\delta_{n-1} \otimes \mathrm{id}_M))$$

for all $i \leq l - 1$, so that $\operatorname{depth}_m(\operatorname{im} \delta_{n-1} \otimes M) \geq l - 1$. Also,

$$0 \to \operatorname{Ext}^{l-1}(R/m, \operatorname{im} \delta_{n-1} \otimes M) \to \operatorname{Ext}^l(R/m, \ker(\delta_{n-1} \otimes \mathrm{id}_M)) \to \operatorname{Ext}^l(R/m, F_{n-1} \otimes M)$$

is exact. Note that $\operatorname{Ext}^l(R/m, \ker(\delta_{n-1} \otimes \mathrm{id}_M)) = \operatorname{Ext}^l(R/m, \operatorname{im}(\delta_n \otimes \mathrm{id}_M)) \cong \operatorname{Ext}^l(R/m, F_n \otimes \mathrm{id}_M))$, so that the last two modules in the display are non-zero. Furthermore,‘ the last map in the display is up to isomorphism $\operatorname{Ext}^l(R/m, M) \otimes F_n \to \operatorname{Ext}^l(R/m, M) \otimes F_{n-1}$ induced by δ_n. Suppose that some $\operatorname{rank}(\delta_n, M)$ minor of δ_n is not in m. Then it is a unit, so that $\operatorname{im} \delta_n \otimes M$ is a direct summand of $F_{n-1} \otimes M$, whence by work similar to what we did in the previous paragraph, $I(\delta_n, M) = R$, which is a contradiction. So we may assume that all $\operatorname{rank}(\delta_n, M)$ minors are in m. Since m annihilates $\operatorname{Ext}^l(R/m, M)$, we have that the last map in the display above is not injective. Thus $\operatorname{depth}_m(\operatorname{im} \delta_{n-1} \otimes M) = l - 1$.

By exactness assumption, $\ker(\delta_{n-i} \otimes \mathrm{id}_M) = \operatorname{im}(\delta_{n-i+1} \otimes \mathrm{id}_M)$. The short exact sequences $0 \to \operatorname{im}(\delta_{n-i+1} \otimes \mathrm{id}_M) \to F_{n-i} \otimes M \to \operatorname{im}(\delta_{n-i} \otimes \mathrm{id}_M) \to 0$ for $i = 2, \dots, l$ and the long exact sequences on cohomology then give that for all $\operatorname{depth}_m(\operatorname{im} \delta_{n-i} \otimes M) = l - i$. In particular, $\operatorname{depth}_m(\operatorname{im} \delta_{n-l} \otimes M) = 0$. This says that the module $F_{n-l-1} \otimes M$ has a submodule of depth 0, so that $F_{n-l-1} \otimes M$ and hence M have depth 0, which contradicts what we have proved. $\square$

Exercise 29.7 (McCoy) Let R be a commutative ring. Prove that an $n \times n$ matrix A with entries in R is a zero divisor in the ring of $n \times n$ matrices over R if and only if $\det A$ is a zerodivisor in R.

Exercise 29.8 Let R be a Noetherian ring, and let I be an ideal in R. Prove or disprove the following (using Definition 29.2):

(1) If $I \subseteq J$, then $\operatorname{depth}_I(M) \leq \operatorname{depth}_J(M)$.
(2) $\operatorname{depth}_I(M) = \operatorname{depth}_{I+\operatorname{ann}(M)}(M)$.
(3) $\operatorname{depth}_I(M) = \operatorname{depth}_{I(R/\operatorname{ann} M)}(M)$.
(Hint: Without loss of generality $J = I + (x)$. Use the short exact sequence $0 \to N \to R/I \to R/(I + (x)) \to 0$. Since $N \cong R/K$ for some ideal K containing I, we get the result by Noetherian induction and the long exact sequence on cohomology.

Exercise 29.9 Use Theorem 29.6 to analyze the complex

$$F_\bullet : \qquad 0 \to \mathbb{Q} \xrightarrow{1} \mathbb{Q} \xrightarrow{0} \mathbb{Q} \xrightarrow{1} \mathbb{Q} \xrightarrow{0} \mathbb{Q} \xrightarrow{1} \mathbb{Q},$$

with $M = \mathbb{Q}$. Repeat for $R = \mathbb{Q}[x,y]/(xy)$, $M = (R/(y))_{(y)} \cong \mathbb{Q}(x)$, and the complex

$$F_\bullet : \qquad 0 \to R \xrightarrow{x} R \xrightarrow{y} R \xrightarrow{x} R \xrightarrow{y} R \xrightarrow{x} R.$$

Appendix A. Tensor products

Definition 1 *Let M, N and V be modules over a ring R. A function $\varphi : M \times N \to V$ is* **R-bilinear** *(or bilinear over R) if for all $m \in M$ and all $n \in N$, the functions $\varphi(m, \_) : N \to V$ and $\varphi(\_, n) : M \to V$ are both R-module homomorphisms.*

Definition 2 *Let M and N be modules over a ring R. A* **tensor product** *T of M and N over R is an R-module with the following properties:*

(1) There exists an R-bilinear map $\varphi : M \times N \to T$.

(2) For any R-module V and any R-bilinear map $\psi : M \times N \to V$ there exists a unique R-module homomorphism $g : T \to V$ such that $\psi = g \circ \varphi$.

The definition of the tensor product can be drawn with the following commutative diagram (exclamation mark g stands for uniqueness):

$$\begin{tikzcd} M \times N \arrow[r, "\varphi"] \arrow[dr, "\psi"'] \arrow[dr, phantom, "\circlearrowleft", shift left=3ex] & T \arrow[d, dashed, "\exists! g"] \\ & V \end{tikzcd}$$

Lemma 3 *Any two tensor products of M and N over R are isomorphic R-modules.*

Proof. Suppose that T and T' are both tensor products of M and N over R with corresponding bilinear maps φ and φ' from $M \times N$. By the defining property there exist unique $g : T \to T'$ and $g' : T' \to T$ such that $g \circ \varphi = \varphi'$ and $g' \circ \varphi' = \varphi$. Then $(g' \circ g) \circ \varphi = g' \circ (g \circ \varphi) = g' \circ \varphi' = \varphi$. Thus both $g' \circ g$ and identity make the following diagram commute.

$$\begin{tikzcd} M \times N \arrow[r, "\varphi"] \arrow[dr, "\varphi"'] \arrow[dr, phantom, "\circlearrowleft", shift left=3ex] & T \arrow[d, dashed, "{g' \circ g, \mathrm{id}_T}"] \\ & T \end{tikzcd}$$

Thus by the uniqueness part in the definition of tensor products, $g' \circ g = \mathrm{id}_T$. Similarly, $g \circ g' = \mathrm{id}_{T'}$. Thus g and g' are isomorphisms. $\square$

Definition 4 *We only need tensor products up to isomorphisms. We denote the tensor product of M and N over R — if it exists — as $M \otimes_R N$. Let $\varphi : M \times N \to M \otimes_R N$ be the corresponding bilinear map. For any $m \in M$ and $n \in N$ we denote $\varphi(m, n)$ as $m \otimes_R n$ or as $m \otimes n$.*

Remark 5 For all $m, m' \in M$, $n, n' \in N$ and $r \in R$, bilinearity of $\varphi : M \times N \to M \otimes_R N$ gives:

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

Proposition 6 *Suppose that $M \otimes_R N$ exists with the bilinear map $\varphi : M \times N \to M \otimes_R N$. Then every element of $M \otimes_R N$ is of the form $\sum_{i=1}^{s} r_i(m_i \otimes n_i)$ with $r_i \in R$, $m_i \in M$ and $n_i \in N$.*

Proof. Let T be the subset of $M \otimes_R N$ consisting of finite sums as in the description. Then T is an R-submodule of $M \otimes_R N$. For any R-module V with a bilinear map $\psi : M \times N \to V$ there exists a unique R-module homomorphism $g : M \otimes_R N \to V$ such that $g \circ \varphi = \psi$. By definition the image of φ is in T, so let $\varphi' : M \times N \to T$ be this bilinear map. Let g' be the restriction of g to T. Then $g' : T \to V$ and $g' \circ \varphi' = \psi$. Then for any $m \otimes n$ in T, $g'(m \otimes n) = g' \circ \varphi'(m, n) = \psi(m, n)$ is uniquely determined, so similarly g' is uniquely determined on all of T. Thus the pair (T, φ') satisfies the conditions of tensor products, so that $T = M \otimes_R N$. $\square$

Do tensor products exist? The standard proof goes as follows: Let F be a free R-module whose basis elements are of the form $E_{m,n}$ as m varies over all elements of M and n over all elements of N. (So the basis is often an infinite set.) We let U be the R-submodule of F generated by elements of the following form:

$$\begin{aligned}
&E_{m+m',n} - E_{m,n} - E_{m',n}, \\
&E_{m,n+n'} - E_{m,n} - E_{m,n'}, \\
&E_{rm,n} - rE_{m,n}, \\
&E_{m,rn} - rE_{m,n}.
\end{aligned}$$

One can prove that F/U satisfies the universal property of tensor product of M and N over R and thus it equals $M \otimes_R N$.

The next few propositions give a different proof of the existence of tensor products.

Proposition 7 *Let M be an arbitrary R-module and F a free R-module with basis B. Then $M \otimes_R F \cong \oplus_{i \in B} M$.*

Proof. Set $G = \oplus_{i \in B} M$. We define $\varphi : M \times F \to G$ as $\varphi(m, (r_i)_{i \in B}) = (r_i m)_{i \in B}$. It is straightforward to verify that φ is bilinear. Let V be any R-module with a bilinear map $\psi : M \times F \to V$. For any $i \in B$ let $E_i \in F$ be the element whose ith entry is 1 and all other entries are 0. We define $g : G \to V$ as $g(mE_i) = \psi(m, E_i)$. Then g restricted to

ME_i is an R-module homomorphism, and by the direct sum properties g is an R-module homomorphism. Furthermore, $g \circ \varphi = \psi$, and g is the unique map that satisfies this property. $\square$

As a consequence, for any R-module M, $M \otimes_R R \cong M$, and for any positive integers m and n, $R^m \otimes_R R^n \cong R^{mn}$.

Proposition 8 *Suppose that $M \otimes_R N$ exists and suppose that N' is a homomorphic image of N. Then $M \otimes_R N'$ exists as well. More specifically, if K is the kernel of the map $\pi : N \to N'$, then*

$$M \otimes_R N' = \frac{M \otimes_R N}{T},$$

where T is the submodule of $M \otimes_R N$ generated by elements of the form $m \otimes k$ for $m \in M$ and $k \in K$.

Similarly, if M' is a homomorphic image of M, then $M' \otimes_R N$ exists.

Proof. Let $\varphi : M \times N \to M \otimes_R N$ be the bilinear form from the definition of the tensor product. We define $\widetilde{\varphi} : M \times N' \to (M \otimes_R N)/T$ as follows. Let $m \in M$ and $n' \in N'$. By definition there exists $n \in N$ such that $n \mapsto n'$. We define $\widetilde{\varphi}(m, n')$ as the image of $\varphi(m, n) = m \otimes n$. This is well-defined: if $n_2 \in N$ also maps to n', then $n_2 - n \in K$, and $\varphi(m, n) - \varphi(m, n_2) = \varphi(m, n - n_2) \in T$, so that $\widetilde{\varphi}$ is is well-defined. It is also bilinear becase φ is.

Suppose that V is another R-module with a bilinear map $\psi' : M \times N' \to V$. Then $\psi = \psi' \circ (\mathrm{id}_M \times \pi) : M \times N \to M \times N'$ with ψ gives a bilinear map $\psi : M \times N \to V$. By definition of tensor products there exists a unique R-module homomorphism $g : M \otimes_R N \to V$ such that $g \circ \varphi = \psi$. Then for any $m \in M$ and $k \in K$, $g(m \otimes k) = g \circ \varphi(m, k) = \psi(m, k) = \psi' \circ (\mathrm{id}_M \times \pi)(m, k) = \psi'(m, 0) = \psi'(m, 0 \cdot 0) = 0\psi'(m, 0) = 0$. Thus g is zero on T, so g induces an R-module homomorphism $g' : (M \otimes_R N)/T \to V$ such that $g' \circ \varphi' = \psi'$. Since all elements of $M \otimes_R N$ are finite sums of elements of the form $\varphi(m, n) = m \otimes n$, then elements of $(M \otimes_R N)/T$ are finite sums of elements of the form $\widetilde{\varphi}(m, n')$, and so g' is uniquely determined by ψ'. Thus by the definition of tensor products, $M \otimes_R N'$ is as specified. $\square$

Corollary 9 *For any R-modules M and N, $M \otimes_R N$ exists.*

Proof. Let F be a free R-module mapping onto N. By Proposition 7, $M \otimes_R F$ exists, and by Proposition 8, $M \otimes_R N$ exists. $\square$

Proposition 10 *Let M, N, N' be R-modules and let $f : N \to N'$ be an R-module homomorphism. Then there exists a unique R-module homomorphism $M \otimes_R N \to M \otimes_R N'$ taking $m \otimes n$ to $m \otimes f(n)$. This homomorphism is written as $\mathrm{id}_M \otimes f$.*

Proof. We define $\psi : M \times N \to M \otimes_R N'$ as $\psi(m, n) = m \otimes f(n)$. This is a bilinear map, and the rest follows from the definition of the tensor product of $M \otimes_R N$. $\square$

Corollary 11 *Let* $0 \to K \xrightarrow{i} N \xrightarrow{\pi} N' \to 0$ *be a short exact sequence of* R*-modules. Then for any* R*-module* M*,*

$$M \otimes_R K \xrightarrow{\mathrm{id}_M \otimes i} M \otimes_R N \xrightarrow{\mathrm{id}_M \otimes \pi} M \otimes_R N' \to 0$$

is exact.

Proof. Exactness is due to Proposition 8. □

With notation as in the Corollary, $\mathrm{id}_M \otimes i$ need not be injective. For example, let R be a Noetherian ring and I a proper ideal in R. Then $0 \to I \to R \to R/I \to 0$ is a short exact sequence. When we tensor with R/I, by the corollary the following is exact:

$$I \otimes_R (R/I) \to R \otimes_R R/I \to R/I \otimes_R R/I \to 0.$$

The first map is zero as the inclusion $I \subseteq R$ makes $i \otimes \overline{r}$ go to $i \otimes \overline{r} = i(1 \otimes \overline{r}) = 1 \otimes \overline{ir}) = 1 \otimes 0 = 0$.

Exercises for Appendix A

1 Prove that for any $m \in M$, $m \otimes 0 = 0$.

2 Let M and N be R-modules. Prove that $M \otimes_R N \to N \otimes_R M$ with $m \otimes n \mapsto n \otimes m$ is an isomorphism.

3 Let M, N, T be a R-modules. Prove that $M \otimes_R (N \otimes_R T)$ is naturally isomorphic to $(M \otimes_R N) \otimes_R T$.

4 Let M be an R-module and I an ideal in R. Prove that $M \otimes_R R/I \cong M/IM$.

5 Let M be an R-module and S an R-algebra. Prove that $M \otimes_R S$ is an S-module.

6 Let M be an R-module and $x_1, \ldots, x_n$ variables over R. Prove that $M \otimes_R R[x_1, \ldots, x_n] \cong M[x_1, \ldots, x_n]$, the R-module (and the $R[x_1, \ldots, x_n]$-module) consisting of finite sums of the form $\sum m_\nu \underline{x}^{\underline{\nu}}$.

7 Let $x_1, \ldots, x_n, y_1, \ldots, y_m$ be variables over R. Let I be an ideal in $R[x_1, \ldots, x_n]$ and J an ideal in $R[y_1, \ldots, y_m]$. Prove that

$$R[x_1, \ldots, x_n]/I \otimes_R R[y_1, \ldots, y_m]/J \cong R[x_1, \ldots, x_n, y_1, \ldots, y_m]/(I + J).$$

8 Prove that for any variable x over R, $R[x] \otimes_R R[x]$ is isomorphic to a polynomial ring in two variables over R.

9 Let M, N be R-modules and S a multiplicatively closed subset of R. Prove the natural isomorphisms in the following:

$$M \otimes_R S^{-1}N \cong (S^{-1}M) \otimes_R N \cong S^{-1}(M \otimes_R N).$$

Consequently, $S^{-1}M \cong S^{-1}(M \otimes_R R) \cong M \otimes_R S^{-1}R$.

References

1. M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, 1969.
2. D. Buchsbaum and D. Eisenbud, What makes a complex exact?, *J. Algebra* **25** (1973), 259–268.
3. F. Chazal and B. Michel, An introduction to Topological Data Analysis: fundamental and practical aspects for data scientists, preprint, ArXiv 1710.04019v1.
4. C. Huneke and I. Swanson, *Integral Closure of Ideals, Rings, and Modules*, London Mathematical Society Lecture Note Series, 336. Cambridge University Press, Cambridge, 2006. The book and a list of known errors are also accessible for downloading from `http://www.reed.edu/~iswanson/book`.
5. I. Kaplansky, Projective modules, *Ann. of Math* **68** (1958), 372–377.
6. J. Mermin, Three simplicial resolutions, in *Progress in commutative algebra 1*, de Gruyter, Berlin, pp. 127–141, (2012).
7. C. Peskine and L. Szpiro, Dimension projective finie et cohomologie locale, *Inst. Hautes Études Sci. Publ. Math.* **42** (1973), 49–119.
8. D. Quillen, Projective modules over polynomial rings, *Invent. Math.* **36** (1976), 166–172.
9. J. P. Serre, Modules projectifs et espaces fibrés à fibre vectorielle. (French) Séminaire P. Dubreil, M.-L. Dubreil-Jacotin et C. Pisot, 1957/58, Fasc. 2, Exposé 23 18 pp. Secrétariat mathématique, Paris, 1958.
10. Suslin, A. A., Projective modules over polynomial rings are free. (Russian). *Dokl. Akad. Nauk SSSR* **229** (1976), 1063–1066.

Index