Homological Algebra

Irena Swanson, Rome, Spring 2010

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

These lecture notes were delivered at University Roma Tre between March and May 2010. I was invited by Professor Stefania Gabelli and funded by INDAM. I am grateful to Stefania, to INDAM, and to the students.

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.

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.

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 $|i|$.

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

A complex is called a **short exact sequence** if it is an exact complex of the form

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

A **long exact sequence** is simply an exact complex that may be longer but is not necessarily longer; typically long exact sequences arise in some natural way from short exact sequences (see Theorem 4.4).

Remark 1.1 Note that 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 **cocomplex**. The nth **cohomology module** of such a cocomplex $C^\bullet$ is

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

4. Free and projective resolutions. 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 2) 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. Namely, to construct a free resolution, 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.

Note: 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. Injective resolutions. Let M be an R-module. An **injective resolution** of M is a cocomplex

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

where the I^n are injective modules over R (definition of injective modules is in Section 21) and where

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

is exact. Also injective resolutions are not uniquely determined, and we sometimes call the latter exact cocomplex an injective resolution.

6. Other ways to make complexes. Let $C_\bullet = \cdots \to C_n \xrightarrow{d_n} C_{n-1} \xrightarrow{d_{n-1}} C_{n-2} \to \cdots$ be a complex of R-modules.

(1) **Homology complex:** We can immediately form the trivial complex $H(C_\bullet)$, where the nth module is $H_n(C_\bullet)$, and all the complex maps are zero (which we may want to think of as the maps induced by the original complex maps).

If M is an R-module, we can form the following natural complexes:

(2) **Tensor product:**

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

It is straightforward to verify that this is still a complex.

(3) **Hom from M**, denoted $\mathrm{Hom}_R(M, C_\bullet)$, is:

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

where $\mathrm{Hom}(M, d_n) = d_n \circ \_$. It is straightforward to verify that this is still a complex.

(4) **Hom into M**, denoted $\mathrm{Hom}_R(C_\bullet, M)$, is:

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

where $\mathrm{Hom}(d_n, M) = \_ \circ d_n$. It is straightforward to verify that this is now a cocomplex.

(5) **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 also form a tensor product of complexes, which can be considered as some kind of 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, or better yet, where the vertical maps are signed by the degrees in $C_\bullet$, meaning that $C_n \otimes K_m \to C_n \otimes K_{m-1}$ is $(-1)^n e_m$. Note that this "bicomplex" is a complex along all vertical and along all horizontal strands.

However, this "bicomplex" has more structure, which one could think of as a "complex along the 45° angle". Namely, we get a natural **total complex** of the tensor product of $C_\bullet$ and $K_\bullet$ in the following way: 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 is in $C_{i-1} \otimes K_{n-i}$ and the second in $C_i \otimes K_{n-i-1}$. This new construction is still a complex:

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

(6) There are also other natural methods to produce further complexes, and here is one arising from a complex $C_\bullet$ of left R-modules and an ideal J in R: **global sections with support in J**:

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

where for any R-module M, $\Gamma_J(M) = \{m \in M : J^n m = 0 \text{ for some } n\}$ is an R-submodule of M, and the induced maps in $\Gamma_J(C_\bullet)$ are the restrictions of the original maps. It is straightforward to verify that $\Gamma_J(C_\bullet)$ is still a complex. If $C_\bullet$ is an injective resolution of an R-module M, then the cohomologies of $\Gamma_J(C_\bullet)$ are the **local cohomology** modules of M with support in J.

7. Some special complexes.

(1) Let R be a ring, M a left R-module, and x an element of the center of 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 numbers under M are there only to note which copy of M is considered to be in which numerical place in the complex.

(2) If $x_1,\dots,x_n$ are in the center of M, then the **Koszul complex** $K_\bullet(x_1,\dots,x_n;M)$ of $x_1,\dots,x_n$ and M is the total complex of $K_\bullet(x_1,\dots,x_{n-1};M)\otimes K_\bullet(x_n;R)$, defined inductively. It is easy to see that $K_\bullet(x_1,\dots,x_n;M)$ has other isomorphic definitions, such as $K_\bullet(x_1,\dots,x_n;M)\cong K_\bullet(x_1,\dots,x_n;R)\otimes_R M\cong K_\bullet(x_1;M)\otimes K_\bullet(x_2,\dots,x_n;R)$, et cetera.

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

$$\left(\begin{array}{ccccccc} 0 & \to & M & \xrightarrow{x_1} & M & \to & 0 \\ & & 1 & & 0 & & \end{array}\right)\otimes\left(\begin{array}{ccccccc} 0 & \to & R & \xrightarrow{x_2} & R & \to & 0 \\ & & 1 & & 0 & & \end{array}\right)$$

we get the total complex

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

(Really we do not need to write the numerical subscripts, but it helps the first time in the construction.) It is easy to show that this is a complex. It is exact at the second place if and only if the ideal (x_1,x_2) contains a non-zerodivisor; it is exact in the middle (in the first place) if and only if every equation of the form $ax_1=bx_2$ with $a,b\in R$ has the property that there exists $c\in R$ with $a=cx_2$ and $b=cx_1$. (So x_1,x_2 is a regular sequence, see Definition 5.4, Section 10).

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

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

(3) There is another construction of complexes that, after some preliminary verifications, mimics the construction of Koszul complexes. We first need some definitions. Here we assume that R is a commutative ring.

If M is an R-module, we define the **n-fold tensor product of** M to be denoted $M^{\otimes n}$: $M^{\otimes 1} = M$, $M^{\otimes 2} = M \otimes M$, 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 $B = \{e_{i_1} \wedge \cdots \wedge e_{i_n} : 1 \leq i_1 < i_2 < \cdots < e_{i_n} \leq m\}$. If $m = 1$ or $m = n$, clearly B 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 $x_1, \ldots, x_m \in R$ we can now define a complex

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

where the map $\wedge^n R^m \to \wedge^{n-1} R^m$ 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 1.2 Verify the following:

(1) $G_\bullet(x; R) = K(x; R)$.
(2) $G_\bullet(x_1, \ldots, x_{n-1}; R) \otimes_R G_\bullet(x_n; R) \cong G_\bullet(x_1, \ldots, x_n; R)$.
(3) Verify that $G_\bullet(x_1, \ldots, x_n; R)$ is a complex and that it equals $K_\bullet(x_1, \ldots, x_m; R)$.

Exercise 1.3 Let R be a commutative ring, let M be an R-module, and let $x_1, \ldots, x_n \in R$. Prove that $H_n(K_\bullet(x_1, \ldots, x_n; M)) = \operatorname{ann}_M(x_1, \ldots, x_n)$.

(1) There are other special complexes, such as the Eagon-Northcott complex. Whereas the Koszul complex is measuring to some extent whether an ideal is generated by a regular sequence (see Definition 5.4, Section 10), the Eagon-Northcott complex behaves well also for powers of ideals generated by a regular sequence. (More on this in ??.)

8. Special homologies.

(1) **Tor:** If M and N are R-modules, and if $F_\bullet$ is a projective resolution of M, then $\operatorname{Tor}_n^R(M, N) = H_n(F_\bullet \otimes N)$. It takes some work to prove that $\operatorname{Tor}_n^R(M, N) \cong \operatorname{Tor}_n^R(N, M)$, or in other words, that if $G_\bullet$ is a projective resolution of N, then $\operatorname{Tor}_n^R(M, N) \cong H_n(M \otimes G_\bullet)$. (See Section 7.)
(2) **Ext:** If M and N are R-modules, and if $F_\bullet$ is a projective resolution of M, then $\operatorname{Ext}_R^n(M, N) = H^n(\operatorname{Hom}_R(F_\bullet, N))$. It takes some work to prove that

$\mathrm{Ext}^n_R(M,N) \cong H^n(\mathrm{Hom}_R(M,I_\bullet))$, where $I_\bullet$ is an injective resolution of N. (See Section 17.)

(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 $H^n_J(M) = H^n(\Gamma_J(I))$, where $I_\bullet$ is an injective resolution of M. (See ??? Time?)

9. 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 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.

10. How does one determine exactness of a (part of a) complex? We list here a few answers, starting with fairly vague ones:

(1) From theoretical aspects as above;
(2) after a concrete computation;
(3) Buchsbaum-Eisenbud criterion (see ??);
(4) knowledge of special complexes, such as Koszul complexes, the Hilbert-Burch complex (see Exercise 1.10)...;
(5) and a more concrete tool/answer: the Snake Lemma. We state below two versions. Proofs require some diagram chasing, and we leave it to the reader.

Lemma 1.4 (Snake Lemma, version I) *Assume that the rows in the following commutative diagram are exact and that β and δ are isomorphisms:*

$$\begin{array}{ccccccccc}
A & \stackrel{a}{\to} & B & \stackrel{b}{\to} & C & \stackrel{c}{\to} & D & \stackrel{d}{\to} & E \\
\downarrow\alpha & & \downarrow\beta & & \downarrow\gamma & & \downarrow\delta & & \downarrow\epsilon \\
A' & \stackrel{a'}{\to} & B' & \stackrel{b'}{\to} & C' & \stackrel{c'}{\to} & D' & \stackrel{d'}{\to} & E'.
\end{array}$$

Then if ϵ is injective, γ is surjective; and if ϵ is surjective, γ is injective.

Lemma 1.5 (Snake Lemma, version II) *Assume that the rows in the following commutative diagram are exact:*

$$\begin{array}{ccccccccc}
 & & B & \stackrel{b}{\to} & C & \stackrel{c}{\to} & D & \to & 0 \\
 & & \downarrow\beta & & \downarrow\gamma & & \downarrow\delta & & \\
0 & \to & B' & \stackrel{b'}{\to} & C' & \stackrel{c'}{\to} & D'. & &
\end{array}$$

Then

$$\ker\beta \to \ker\gamma \to \ker\delta \to \mathrm{coker}\,\beta \to \mathrm{coker}\,\gamma \to \mathrm{coker}\,\delta$$

is exact, where the first two maps are the restrictions of b and c, respectively, the last two maps are the natural maps induced by b' and c', respectively, and the middle map is the *so-called* **connecting homomorphism**. *We describe this homomorphism here explicitly: let $x \in \ker\delta$. Since c is surjective, there exists $y \in C$ such that $x = c(y)$. Since the diagram commutes, $c'\gamma y = \delta c y = \delta x = 0$, so that $\gamma y \in \ker c' = \operatorname{im} b'$. Thus $\gamma y = b'(z)$ for some $z \in B'$. Then the connecting homomorphism takes x to the image of z in* $\operatorname{coker}\beta$. *A reader should verify that this is a well-defined map. But this version of the Snake Lemma says even more: If b is injective, so is* $\ker\beta \to \ker\gamma$; *and if c' is surjective, so is* $\operatorname{coker}\gamma \to \operatorname{coker}\delta$.

<u>11. Minimal free resolutions</u> In certain contexts one can talk about a free resolution with certain minimal conditions. Namely, while constructing the free resolution (see 4. above), we may want to choose at each step a free module with a minimal number of generators. If at each step we choose a minimal such generating set, we get a resolution of the form

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

The number b_i is called the **ith Betti number** of M. (See Exercise 3.7 to see that these are well-defined.)

If R is a polynomial ring $k[x_1, \ldots, x_n]$ in variables $x_1, \ldots, x_n$ over a field k, and if M is a finitely generated R-module generated by homogeneous elements, we may even choose all the generators of all the kernels in the construction of a free resolution to be homogeneous as well. In this case, we may make a finer partition of each b_i, as follows. We already know that M is minimally generated by b_0 homogeneous elements, but these b_0 elements can be 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. Thus 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 a certain degree map to a homogeneous element of M of the same degree. 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, a resolution of the homogeneous $k[x, y, z]$-module $M = R/(x^2, xy, yz^2, y^4)$ can be written as

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

Note that the columns of matrices are supposed to be 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:

$$\begin{array}{lcccc} & 0 & 1 & 2 & 3 \\ 0: & 1 & & & \\ 1: & & 2 & 1 & \\ 2: & & 1 & 1 & \\ 3: & & 1 & 1 & \\ 4: & & & 1 & 1 \end{array}$$

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. 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 very recent work of Eisenbud and Schreyer (and Weyman, Floystad, Boij, Sederberg), 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.

12. Splitting of complexes. 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.

13. 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, and for each homomorphism $f : M \to N$ in the domain category, $\mathcal{F}(f) : \mathcal{F}(M) \to \mathcal{F}(N)$ is a homomorphism, with two additional restrictions. The first restriction is that for all objects M, $\mathcal{F}(\mathrm{id}_M) = \mathrm{id}_{\mathcal{F}(M)}$. The second restriction has two possibilities. A functor is **covariant** if for all homomorphisms f, g in the domain category for which the composition $f \circ g$ is defined, we have $\mathcal{F}(f \circ g) = \mathcal{F}(f) \circ \mathcal{F}(g)$. A functor is **contravariant** if for all f, g as above, we have $\mathcal{F}(f \circ g) = \mathcal{F}(g) \circ \mathcal{F}(f)$.

A functor is **left-exact** if whenever it is applied to a short exact sequence, it produces a complex that is exact everywhere except possibly at the rightmost non-zero module. Similarly, a functor is **right-exact** if whenever when applied to a short exact sequence, it gives a complex that is exact everywhere except possibly at the leftmost non-zero module. A functor is **exact** if it is both left-exact and right-exact.

It is easy to verify 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 $0 \to A \to B \to C$. 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 $A \to B \to C \to 0$. 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 $A \to B \to C \to 0$. 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 $0 \to A \to B \to C$.

We have seen some functors: $\mathrm{Hom}_R(M, \_)$, $\mathrm{Hom}_R(\_, M)$, $M \otimes_R \_$, $\Gamma_J(\_)$, $\wedge^n(\_)$. Verify that these are functors, determine which ones are covariant, and determine their exactness properties (see Exercise 1.7).

Definition 1.6 *An R-module M is* **flat** *if $M \otimes_R \_$ is exact.*

Thus by Exercise 1.7 below, M is flat if and only if $f \otimes \mathrm{id}_M$ is injective whenever f is injective.

Exercise 1.7 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 $M \otimes_R \_$ is right-exact.
(3) Determine the exactness properties of $\Gamma_J(\_)$.

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. Under what conditions are any of these equivalent?

(1) There exists $f : M_3 \to M_2$ such that $hf = 1_{M_3}$.
(2) There exists $e : M_2 \to M_1$ such that $eg = 1_{M_1}$.
(3) $M_2 \cong M_3 \oplus M_1$.

Exercise 1.9 Let R be a domain and I a non-zero ideal such that for some $n, m \in \mathbb{N}$, $R^n \cong R^m \oplus I$. The goal is to prove that I is free. By localization we know that $m+1 = n$.

(1) 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 $Ad = 0$.
(2) 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.
(3) Prove that $I \cong (d_1, \ldots, d_n)$.
(4) 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 $t \in R$.

Exercise 1.11 Let R be a commutative ring, $x_1, \ldots, x_n \in R$, and let M be an R-module. Prove that $H_0(K_\bullet(x_1, \ldots, x_n; M)) = M/(x_1, \ldots, x_n)M$ and that $H_n(K_\bullet(x_1, \ldots, x_n; M)) = \mathrm{ann}_M(x_1, \ldots, x_n)$.

2 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.

Definition 2.1 *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 2.2

(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.

Proposition 2.3 *Let F, M and N be (left) R-modules. If F is free, $f : M \to N$ is surjective, and $g : F \to N$, then there exists $h : F \to M$ such that $f \circ h = g$. This is typically drawn as follows:*

$$\begin{tikzcd}
 & F \arrow[dl, dashed] \arrow[d] \arrow[dl, phantom, shift left=3ex, "\circlearrowleft"] & \\
M \arrow[r] & N \arrow[r] & 0
\end{tikzcd}$$

Proof. Let X be a basis of F. For all $x \in X$, let $m_x \in M$ such that $f(m_x) = g(x)$. Then by the first fact above there exists a homomorphism $h : F \to M$ extending the function $x \mapsto m_x$, and the rest is easy. $\square$

Definition 2.4 *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*

$$\begin{tikzcd}
 & P \arrow[dl, dashed] \arrow[d] \arrow[dl, phantom, shift left=3ex, "\circlearrowleft"] & \\
M \arrow[r] & N \arrow[r] & 0
\end{tikzcd}$$

Theorem 2.5 *The following are equivalent for a left R-module P:*

(1) P is projective.

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

(3) If $M \overset{f}{\twoheadrightarrow} P$, then there exists $h : P \to M$ such that $f \circ h = \mathrm{id}_P$.

(4) If $M \overset{f}{\twoheadrightarrow} P$, then $M \cong P \oplus \ker f$.

(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 F with $F \overset{f}{\twoheadrightarrow} P$, there is $h : P \to F$ such that $f \circ h = \mathrm{id}_P$.

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

Proof. By Exercise 1.7, $\mathrm{Hom}_R(P, \_)$ 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 $M \overset{f}{\twoheadrightarrow} N$ is onto. But this is equivalent to P being projective. Thus (1) $\Leftrightarrow$ (2).

(1) $\Rightarrow$ (3): follows by the definition of projective modules and

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

where the vertical map is the identity map.

(3) $\Rightarrow$ (4): We start with a short exact sequence $0 \to \ker f \to M \overset{f}{\twoheadrightarrow} P$. Now you may either follow Exercise 1.8, or follow the independent proof of the relevant part below. Define $\varphi : P \oplus \ker f \to M$ by $\varphi(a, b) = a + h(b)$. This is a module homomorphism, $\ker \varphi$ consists of all those (a, b) for which $a + h(b) = 0$. For such (a, b), $b = f \circ h(b) = f(-a) = 0$ since $a \in \ker f$, so that $b = 0$ and hence $a = -h(b) = 0$, 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 $m = (m - h \circ f(m)) + h(f(m)) \in \mathrm{im}\, \varphi$. This proves that φ is an isomorphism.

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

(5) $\Rightarrow$ (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 2.3, the following diagram commutes:

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

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 (1) through (5) are all equivalent. Clearly (3) implies (6) for any free module F that maps onto P, and (6) implies (5) by the same proof as the proof of (3) implying (4).

Certainly (7) implies (6). Now assume (6). If $g : P \to P$, and $f \circ h = \mathrm{id}_P$, then $f \circ (h \circ g) = g$, which proves (7). $\square$

Facts 2.6

(1) Every free module is projective.

(2) 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. If R is a Dedekind domain that is not a principal ideal domain, then any non-principal ideal is a non-free projective module.

(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, $1 = \sum_i n_i e_i$ 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, $n_i = m a_i$ 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 (**'Kaplanskyproj'**).

(6) If (R, m) 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 $0 \to K \to R^n \to P \to 0$. Since P is projective, $R^n \cong K \oplus P$, and so $(\frac{R}{m})^n \cong \frac{K}{mK} \oplus \frac{P}{mP}$ are vector spaces over R/m. By dimension count, $\frac{K}{mK}$ has dimension 0, and since K is finitely generated, by Nakayama's lemma $K = 0$.

(7) Kaplansky **'Kaplanskylocal'** proved that every projective module over a commutative Noetherian local ring is free.

(8) Quillen and Suslin **'Quillen'**, **'Suslin'** proved that every projective module over a polynomial ring over a field is free.

Definition 2.7 *Let R be a commutative ring. A vector $[a_1, \ldots, a_n] \in R^n$ is* **unimodular** *if $(a_1, \ldots, a_n)R = R$.*

Every unimodular vector v gives rise to a projective module: Let P be the cokernel P of the map $v^T : R \to R^n$. By Exercise 1.8, P is a direct summand of R^n, hence projective. In fact, in this case, the $P \oplus R \cong R^n$.

Definition 2.8 *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, but the converse is not true. (Example?) Serre proved **'Serrestablyfree'** that every stably free module over a polynomial ring over a field is free. We proved above that every unimodular vector gives rise to a stably free module.

Proposition 2.9 *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 $\wedge^n$.

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

□

Definition 2.10 *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 2.11 *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. Let $0 \to K \to R^n \to P \to 0$ be a short exact sequence with K finitely generated. By Theorem 2.5, 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. But for a finitely presented module P, and for any multiplicatively closed set W in R, $W^{-1}(\operatorname{Hom}_R(P, \_)) \cong \operatorname{Hom}_{W^{-1}R}(W^{-1}P, W^{-1}(\_))$. (Verify in Exercise 2.13.)$\square$

Exercise 2.12 (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 R-module.

Exercise 2.13 Let P be a finitely presented module over a commutative ring R. Let W be a multiplicatively closed set in R. Prove that $W^{-1}(\operatorname{Hom}_R(P, \_)) \cong \operatorname{Hom}_{W^{-1}R}(W^{-1}P, W^{-1}(\_))$.

Exercise 2.14 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 not free.

Exercise 2.15 Let D be a Dedekind domain. Prove that every ideal in D is a projective D-module.

Exercise 2.16 Let R be a commutative Noetherian domain in which every ideal is a projective R-module. Prove that R is a Dedekind domain.

Exercise 2.17 Find a Dedekind domain that is not a principal ideal domain. Give another example of a projective module that is not free.

Exercise 2.18 If P is a finitely generated projective module over a ring R, show that $\operatorname{Hom}_R(P, R)$ is also a projective R-module. If Q is a projective R-module, prove that $P \otimes_R Q$ is also a projective R-module.

3 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 3 makes sense. It is easy to make up also the definition of flat resolutions: in that case the relevant modules have to be flat.

Remarks 3.1

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

Definition 3.2 *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 is called the* **projective dimension of** *M, and is denoted $\mathrm{pd}_R(M)$.*

Examples 3.3

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

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

(3) If $R = \frac{k[x,y]}{(xy)}$, where k is a field and x and y are variables over k, then $R/(x)$ 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? Let's postpone this discussion a bit.

Theorem 3.4 (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:

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

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 $\pi : P_1 \to P_2$ that makes the following diagram commute:

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

Now let $x \in K_1$. Then $\alpha_2 \circ \pi \circ i_1(x) = \beta \circ \alpha_1 \circ i_1(x) = 0$, so that $\pi \circ i_1(x) \in \ker \alpha_2 = \operatorname{im} i_2$, whence $\pi \circ i_1(x) = i_2(y)$ 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

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

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 $\psi(a, b) = i_2(a) - \pi(b)$. This is an R-module homomorphism, $\psi \circ \varphi(x) = \psi(\kappa(x), i_1(x)) = i_2 \circ \kappa(x) - \pi \circ i_1(x)$, which is 0 since the displayed diagram commutes. Let $(a, b) \in \ker \psi$. Then $i_2(a) = \pi(b)$, so that $0 = \alpha_2 \circ i_2(a) = \alpha_2 \circ \pi(b) = \beta \circ \alpha_1(b)$. Since β is an isomorphism, $\alpha_1(b) = 0$, so that $b = i_1(x)$ for some $x \in K_1$. But then $i_2(a) = \pi(b) = \pi \circ i_1(x) = i_2 \circ \kappa(x)$, whence by the 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 $\alpha_2(z) = \alpha_2 \circ \pi(y)$, whence $z - \pi(y) \in \ker \alpha_2 = \operatorname{im} i_2$, whence $z = (z - \pi(y)) - \pi(-y) \in \operatorname{im} \psi$, 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 2.5 proves the theorem. □

Theorem 3.5 (Generalized Schanuel's lemma) *Let R be a ring. Suppose that $0 \to K \to P_k \to P_{k-1} \to \cdots \to P_1 \to P_0 \to M \to 0$ and $0 \to L \to Q_k \to Q_{k-1} \to \cdots \to Q_1 \to Q_0 \to M \to 0$ are exact sequences of R-modules, and that all the P_i and Q_i are projective. Let $P_{odd} = \oplus_{i\ odd} P_i$, $P_{even} = \oplus_{i\ even} P_i$, $Q_{odd} = \oplus_{i\ odd} Q_i$, $Q_{even} = \oplus_{i\ even} Q_i$. Then*

(1) If k is even, $K \oplus Q_{even} \oplus P_{odd} \cong L \oplus Q_{odd} \oplus P_{even}$.

(2) If k is odd, $K \oplus Q_{odd} \oplus P_{even} \cong L \oplus Q_{even} \oplus P_{odd}$.

Proof. We only sketch the proof by induction, the base case having been proved in Theorem 3.4. The two sequences can be split into the following four exact sequences:

$$\begin{array}{ll} 0 \to K \to P_k \to K' \to 0, & 0 \to K' \to P_{k-1} \to \cdots \to P_1 \to P_0 \to M \to 0, \\ 0 \to L \to Q_k \to L' \to 0, & 0 \to L' \to Q_{k-1} \to \cdots \to Q_1 \to Q_0 \to M \to 0. \end{array}$$

By induction, K' direct sum with some projective module A is isomorphic to L' direct sum with some projective module B. Then the two short exact sequences above yield the short exact sequences below:

$$0 \to K \to P_k \oplus A \to K' \oplus A \to 0,$$
$$0 \to L \to Q_k \oplus B \to L' \oplus B \to 0.$$

Then by the first version of Schanuel's lemma Theorem 3.4, at least by the proof in which we allow the extreme right modules to not necessarily be identical but only isomorphic, $K \oplus Q_k \oplus B \cong L \oplus P_k \oplus A$. Now it remains to prove that the forms for odd and even k are as given. $\square$

Theorem 3.6 (Minimal resolutions over Noetherian local rings) *Let (R, m) be a Noetherian local ring, and let M be a finitely generated R-module with finite projective dimension n. Define $b_0 = \mu(M)$, so that we have a part of a free resolution of M over R: $R^{b_0} \to M \to 0$. Then recursively, after $b_0, \dots, b_i$ have been defined and $R^{b_i} \to R^{b_{i-1}} \to \cdots \to R^{b_1} \to R^{b_0} \to M \to 0$ is exact, let b_{i+1} be the number of generators of the kernel of $R^{b_i} \to R^{b_{i-1}}$, so that we can extend the beginning of the resolution by one step. 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 assumption there exists a projective resolution $0 \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to M \to 0$. Let K be the kernel of $R^{b_n} \to R^{b_{n-1}}$ in our construction. Then by the generalized Schanuel's lemma Theorem 3.5, the direct sum of K and some projective R-module is isomorphic to another projective R-module, whence it follows quickly from the definitions of projective modules that K is also projective. Since K is a submodule of a finitely generated R-module and R is Noetherian, K is also finitely generated, so that by Facts 2.6 (6), K is free. This means that our minimal resolution construction is at most as long as the minimal projective resolution, and so by minimality $b_n \neq 0$ and $b_{n+1} = 0$. $\square$

Exercise 3.7 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 8.6) initely generated R-module has finite projective dimension. Let n be the projective dimension of M. 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 $b_{n+1} = 0$ and $b_n \neq 0$.

Exercise 3.8 Prove that $\mathrm{pd}_R(M_1 \oplus M_2) = \sup\{\mathrm{pd}_R(M_1), \mathrm{pd}_R(M_2)\}$.

Exercise 3.9 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 $F_\bullet \cong G_\bullet$.

4 General manipulations of complexes

We need to develop more general tools that will be applicable to projective and free resolutions, and also to injective resolutions and other complexes.

try to avoid multiple words

Let $C_\bullet = \quad \cdots C_{n+1} \overset{d_{n+1}}{\to} C_n \overset{d_n}{\to} C_{n-1} \to \cdots$ be a complex. We introduce the common terminology that the elements of $\ker d_n$ are called the **nth cycles**, and that the elements of $\operatorname{im} d_{n+1}$ are also referred to as the **nth boundaries**. For this reason we also sometimes write $B_n = \operatorname{im} d_{n+1}$, $Z_n = \ker d_n$. These are simply names that do not change anything, and I try not to use too many words when one will do, but the following point of view can be useful, and often notationally shorter: the complex $C_\bullet$ can be thought of as a **differential module** $(\oplus_n C_n, d_\bullet)$, where $d_\bullet : \oplus_n C_n \to \oplus_n C_n$, with $d_\bullet|_{C_n} = d_n$, is called the **differential** and has degree -1 as the image of C_n under $d_\bullet$ is in C_{n-1}. The word differential also connotes that ${d_\bullet}^2 = 0$, which is on the complex side the same thing as saying that $C_\bullet$ is a complex. Another example of a differential module is $(\oplus_n H_n(C_\bullet), 0)$.

Definition 4.1 *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, $d'_n \circ f_n = f_{n-1} \circ d_n$. In the differential graded modules terminology, this says that $f_\bullet$ has degree 0, and we can also write this as $d' \circ f_\bullet = f_\bullet \circ d$. We can also draw this as a commutative diagram:*

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

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

Definition 4.2 *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.*

An example of a short exact sequence of complexes is constructed in Proposition 5.1 in the next section, and in Proposition 6.5 later on, etc.

Lemma 4.3 *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 $C_n \oplus C'_n \oplus C''_n$. Since both C'_n and C''_n are projective, so is C_n. $\square$

Theorem 4.4 (Short exact sequence of complexes yields a long exact sequence on homology) *Let $0 \to C_\bullet{}' \xrightarrow{f_\bullet} C \xrightarrow{g_\bullet} C'' \to 0$ 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 and g, and the Δ maps are the connecting homomorphisms as in Lemma 1.5.

Proof. By assumption we have the following commutative diagram with exact rows:

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

By the Snake Lemma Lemma 1.5, we get the following exact sequences for all n:

$$0 \to \ker d'_n \xrightarrow{f_n} \ker d_n \xrightarrow{g_n} \ker d''_n,$$
$$\operatorname{coker} d'_n \xrightarrow{f_n} \operatorname{coker} d_n \xrightarrow{g_n} \operatorname{coker} d''_n \to 0,$$

where the actual maps are only those naturally induced by the marked maps. We even have the following commutative diagram with exact rows:

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

Now another application of Lemma 1.5 yields exactly the desired sequence. $\square$

The following is now immediate:

Corollary 4.5 *Let $0 \to C_\bullet{}' \to C_\bullet \to C_\bullet{}'' \to 0$ be a short exact sequence of complexes. If $C_\bullet{}'$ and $C_\bullet{}''$ have zero homology, so does $C_\bullet$.* $\square$

Definition 4.6 *A map $f_\bullet : C_\bullet \to C_\bullet{}'$ (of degree 0) of complexes is* **null-homotopic** *if there exist maps $s_n : C_n \to C'_{n+1}$ such that for all n, $f_n = d'_{n+1} \circ s_n + s_{n-1} \circ d_n$. Maps $f_\bullet, g_\bullet : C_\bullet \to C_\bullet{}'$ are* **homotopic** *if $f_\bullet - g_\bullet$ is null-homotopic.*

Proposition 4.7 *If $f_\bullet$ and $g_\bullet$ are homotopic, then $f_* = g_*$ (recall Definition 4.2).*

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 $H_n(C_\bullet{}')$.□

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

Proposition 4.8 *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 $\mathrm{Hom}_R(g_\bullet, M)$;

Theorem 4.9 (Comparison Theorem) *Let $P_\bullet : \quad \cdots \to P_2 \to P_1 \to P_0 \to M \to 0$ be a complex with all P_i projective. Let $C_\bullet : \quad \cdots \to C_2 \to C_1 \to C_0 \to N \to 0$ 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:

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

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 $\mathrm{im}(f_n \circ d_{n+1}) \in \ker \delta_n = \mathrm{im}\, \delta_{n+1}$. But then we get the following commutative diagram, with the horizontal row exact (but the vertical row only meant as a composition of maps):

$$\begin{tikzcd}
 & P_{n+1} \arrow[d, "d_{n+1}"] \arrow[ddl, dashed, "f_{n+1}"'] & \\
 & P_n \arrow[d, "f_n"] & \\
C_n \arrow[r, "\delta_{n+1}"] & \mathrm{im}\, \delta_{n+1} \arrow[r] & 0
\end{tikzcd}$$

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 much 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:

$$\begin{tikzcd}
 & P_0 \arrow[dl, dashed, "s_0"'] \arrow[d, "f_0 - g_0"] \arrow[dl, phantom, shift left=4, "\circlearrowleft"] & \\
C_1 \arrow[r, "\delta_1"] & \operatorname{im}\delta_1 \arrow[r] & 0
\end{tikzcd}$$

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

$$\begin{tikzcd}
 & P_{n+1} \arrow[dl, dashed, "s_{n+1}"'] \arrow[d, "f_{n+1} - g_{n+1} - s_n \circ d_{n+1}"] \arrow[dl, phantom, shift left=4, "\circlearrowleft"] & \\
C_{n+2} \arrow[r, "\delta_{n+1}"] & \operatorname{im}\delta_{n+2} \arrow[r] & 0
\end{tikzcd}$$

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. $\square$

5 More on Koszul complexes

We now take a break from the general manipulations of complexes and apply them to Koszul complexes. See page 6 for the definition. In particular, the results of this section will allow us to construct a Koszul complex on n elements more functorially than with the inductive definition given before.

Proposition 5.1 *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 we get a short exact sequence of complexes*

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

with maps on the nth level as follows: $C_n \to (C_n \otimes R) \oplus (C_{n-1} \otimes R) \cong C_n \oplus C_{n-1}$ takes a to $(a, 0)$ and $C_n \oplus C_{n-1} \to (C_\bullet[-1])_n = C_{n-1}$ takes (a, b) to b.

Proof. Certainly 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. The point is to construct the differentials on the three complexes that make all the relevant squares commutative. There is no choice in constructing the differentials on $C_\bullet$ and $C_\bullet[-1]$, those are already given, so the point is to find a good differential on $C_\bullet \otimes K_\bullet$. Observe that $\delta_n : C_n \oplus C_{n-1} \to C_{n-1} \oplus C_{n-2}$ taking (a, b) to $(d_n(a) + (-1)^{n-1} x b, d_{n-1}(b))$ for all n does make $0 \to C_\bullet \to C_\bullet \otimes K_\bullet \to C_\bullet[-1] \to 0$ into a short exact sequence of complexes. $\square$

Corollary 5.2 *With hypotheses as above, we get a long exact sequence*

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

Proof. First of all, $H_{n-1}(C_\bullet) = H_n(C_\bullet[-1])$, so that the long exact sequence above is a consequence of the previous proposition and of Theorem 4.4. Furthermore, we need to go through the proof of the previous proposition, of Theorem 4.4, and of the Snake Lemma Lemma 1.5, to verify that the connecting homomorphisms are indeed just multiplications by x. □

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

$$0 \to \frac{H_n(C_\bullet)}{xH_n(C_\bullet)} \to H_n(C_\bullet \otimes K_\bullet) \to \operatorname{ann}_{H_{n-1}(C_\bullet)}(x) \to 0 \tag{5.3}$$

for all n, where $\operatorname{ann}_M(N)$ denotes the set of all elements of M that annihilate N.

Definition 5.4 *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.*

Corollary 5.5 *Let $x_1, \ldots, x_n$ be a regular sequence on a commutative ring R. Then*

$$H_i(K_\bullet(x_1, \ldots, x_n; R)) = \begin{cases} 0 & \text{if } i > 0; \\ \frac{R}{(x_1, \ldots, x_n)} & \text{if } i = 0. \end{cases}$$

Thus $K_\bullet(x_1, \ldots, x_n; R)$ is a free resolution of $\frac{R}{(x_1, \ldots, x_n)}$.

Proof. This is trivially verified if $n = 1$. Now let $n > 1$. Let $C_\bullet = K_\bullet(x_1, \ldots, x_{n-1}; R)$, $K_\bullet = K_\bullet(x_n; R)$. By the short exact sequences above, by induction on n, $H_i(K_\bullet(x_1, \ldots, x_n; R)) = H_i(C_\bullet \otimes K_\bullet) = 0$ if $i > 1$ (as $H_i(C_\bullet)$ and $H_{i-1}(C_\bullet)$ are both 0). If $i = 1$, we get

$$0 \to 0 = \frac{H_1(C_\bullet)}{x_n H_1(C_\bullet)} \to H_1(C_\bullet \otimes K_\bullet) \to \operatorname{ann}_{H_0(C_\bullet)}(x_n) \to 0,$$

so that $H_1(C_\bullet \otimes K_\bullet) \cong \operatorname{ann}_{H_0(C_\bullet)}(x_n)$, and by induction this is $\operatorname{ann}_{R/(x_1, \ldots, x_{n-1})}(x_n)$. Since x_n is a non-zerodivisor on $R/(x_1, \ldots, x_{n-1})$, we get that $H_1(K_\bullet(x_1, \ldots, x_n; R)) = H_1(C_\bullet \otimes K_\bullet) = 0$. Finally, for $i = 0$, the short exact sequence gives $\frac{H_0(C_\bullet)}{x_n H_0(C_\bullet)} \cong H_0(C_\bullet \otimes K_\bullet)$, and again by induction on n this says that $H_0(K_\bullet(x_1, \ldots, x_n; R)) = H_0(C_\bullet \otimes K_\bullet) \cong \frac{H_0(C_\bullet)}{xH_0(C_\bullet)} \cong R/(x_1, \ldots, x_n)$. □

Exercise 5.6 (Depth sensitivity of Koszul complexes) Let R be a commutative ring and M an R-module. Let $x_1, \ldots, x_n \in R$. Assume that $x_1, \ldots, x_l$ is a regular sequence on M for some $l \leq n$. Prove that $H_i(K_\bullet(x_1, \ldots, x_n; M)) = 0$ for $i = n, n-1, \ldots, n-l+1$.

Exercise 5.7 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 $H_n(K_\bullet(x_1, \ldots, x_n; M))$.

Exercise 5.8 Let $I = (x_1, \ldots, x_n) = (y_1, \ldots, y_m)$ be an ideal contained in the Jacobson radical of a commutative ring 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 $i = m, m-1, \ldots, m-l+1$.

6 General manipulations applied to projective resolutions

Proposition 6.1 *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*

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

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

Proof. This is just an application of the Comparison Theorem Theorem 4.9. □

Corollary 6.2 *Let $P_\bullet$ and $Q_\bullet$ be projective resolutions of M. Then there exists a map of complexes $f_\bullet : P_\bullet \to Q_\bullet$ such that*

$$\begin{array}{ccccc} P_\bullet & \to & M & \to 0 \\ \downarrow f_\bullet & & \downarrow \mathrm{id}_M & \\ Q_\bullet & \to & N & \to 0 \end{array}$$

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

Corollary 6.3 *Let $P_\bullet$ and $Q_\bullet$ be projective resolutions of M. Then for any additive functor $\mathcal{F}$, the homologies of $\mathcal{F}(P_\bullet)$ and of $\mathcal{F}(Q_\bullet)$ are isomorphic.*

Proof. By Corollary 6.2 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 4.9, $f_\bullet \circ g_\bullet$ and id are homotopic, whence so are $\mathcal{F}(f_\bullet \circ g_\bullet)$ and $\mathcal{F}(\mathrm{id})$. Thus by Proposition 4.7, 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. □

Lemma 6.4 *Suppose that*

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

is a commutative diagram, in which the bottom row is a short exact sequence of modules and the top row is a short exact sequence of complexes. If $C_\bullet{}'$ is a projective resolution of M' and $C_\bullet{}''$ is a projective resolution of M'', then $C_\bullet$ is a projective resolution of M.

Proof. By Corollary 4.5 we know that $C_\bullet \to M \to 0$ has no homology, and by Lemma 4.3 we know that all the modules in $C_\bullet$ are projective. This proves the lemma. $\square$

Proposition 6.5 *Let $C_\bullet{}'$ be a projective resolution of M' and let $C_\bullet{}''$ be a projective resolution of M''. Suppose that $0 \to M' \to M \to M'' \to 0$ is a short exact sequence. Then there exists a projective resolution $C_\bullet$ such that*

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

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

Proof. Define $C_n = C'_n \oplus C''_n$, giving the modules of $C_\bullet$, with the horizontal maps in the short exact sequence $0 \to C'_n \stackrel{i_n}{\to} C_n \stackrel{\pi_n}{\to} C''_n \to 0$ the obvious maps. We have to work harder to construct the differential maps on $C_\bullet$.

Consider the following set-up with exact rows:

$$\begin{array}{ccccccccc} \cdots \to & C''_2 & \to & C''_1 & \to & C''_0 & \to & M'' & \to 0 \\ & & & & & & & || & \\ \cdots \to & C'_1 & \to & C'_0 & \to & M & \to & M'' & \to 0 \end{array}$$

By the Comparison Theorem (Theorem 4.9), 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 filled-in displayed diagram above commute.

Now 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 $n \geq 1$. The reader should verify the rest. $\square$

Exercise 6.6 Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules. Prove that $\mathrm{pd}_R(M) \leq \sup\{\mathrm{pd}_R(M'), \mathrm{pd}_R(M'')\}$. 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 6.7 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 6.8 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 $\mathrm{pd}_R(M) \leq n$ if and only if M_n is projective. Prove that if $\mathrm{pd}_R(M) \geq n$, then $\mathrm{pd}_R(M) = \mathrm{pd}(M_n) - n$.

Exercise 6.9 Let R be a Noetherian ring and M a finitely generated R-module Prove that $\mathrm{pd}_R(M) = \sup\{\mathrm{pd}_{R_p}(M_p) : p \in \operatorname{Spec} R\}$.

7 Tor

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

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

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 $\mathrm{Tor}_n^R(M, \_)$ is independent of the projective resolution $P_\bullet$ of M. This follows from Corollary 6.3.

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

3. Tor_0. $\mathrm{Tor}_0^R(M, N) \cong M \otimes_R N$. 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 $\mathrm{Tor}_0^R(M, N) = H_0(P_\bullet \otimes_R N) = (P_0 \otimes_R N)/\operatorname{im}(P_1 \otimes_R N) \cong M \otimes_R N$.

4. What if M is projective? If M is projective, then $\mathrm{Tor}_n^R(M, N) = 0$ 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 flat? If N is flat, then $\mathrm{Tor}_n^R(M, N) = 0$ 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

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

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 Proposition 6.5 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 4.4.

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 $P_\bullet$, and by the Comparison Theorem Theorem 4.9, the two maps are homotopic. Thus $\mu_x \otimes \operatorname{id}_N$ and 0 are homotopic on $P_\bullet \times N$, whence by Proposition 4.7, $(\mu_x \otimes \operatorname{id}_N)_* = 0$. But $(\mu_x \otimes \operatorname{id}_N)_*$ 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 P_i part of the projective resolution $P_\bullet$ of M). 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).

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 quite have symmetric results for M and N in $\operatorname{Tor}_n^R(M, N)$.

Theorem 7.1 *Let R be a commutative ring and let M and N be R-modules. Then for all n,* $\operatorname{Tor}_n^R(M, N) \cong \operatorname{Tor}_n^R(N, M)$.

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: $\overline{\operatorname{Tor}}_n^R(M, N) = H_n(M \otimes_R Q_\bullet)$. The goal is to actually prove that $\operatorname{Tor}_n^R(M, N) \cong \overline{\operatorname{Tor}}_n^R(M, N)$ (for which we do not need a commutative ring).

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

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:

$$\begin{array}{ccccccccc}
 & & & & & & \overline{\mathrm{Tor}}_1^R(M,Q_0)=0 & & \\
 & & & & & & \downarrow & & \\
 & & & & 0 & & \overline{\mathrm{Tor}}_1^R(M,N) & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & M_1\otimes N_1 & \to & P_0\otimes N_1 & \to & M\otimes N_1 & \to & 0 \\
 & & \downarrow\alpha & & \downarrow\beta & & \downarrow\gamma & & \\
0 & \to & M_1\otimes Q_0 & \to & P_0\otimes Q_0 & \to & M\otimes Q_0 & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & M_1\otimes N & \to & P_0\otimes N & \to & M\otimes N & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

By the 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 1.5), $\ker\beta \to \ker\gamma \to \operatorname{coker}\alpha \to \operatorname{coker}\beta \to \operatorname{coker}\gamma \to 0$ 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. Note that the maps between the tensor products above are the natural maps. But we also have 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, which proves that for all R-modules M and N, $\mathrm{Tor}_1^R(M,N) = \overline{\mathrm{Tor}}_1^R(M,N)$.

But the commutative diagram 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:

$$\begin{array}{ccccccc}
 & & & & \overline{\mathrm{Tor}}_1^R(M_1,Q_0)=0 & & \\
 & & & & \downarrow & & \\
 & & & & \overline{\mathrm{Tor}}_1^R(M_1,N) & & 0 \\
 & & & & \downarrow & & \downarrow \\
\mathrm{Tor}_1^R(P_0,N_1)=0 & \to & \mathrm{Tor}_1^R(M,N_1) & \to & M_1\otimes N_1 & \xrightarrow{f} & P_0\otimes N_1 \\
 & & & & \downarrow\alpha & & \downarrow\beta \\
 & & 0 & \to & M_1\otimes Q_0 & \xrightarrow{g} & P_0\otimes Q_0
\end{array}$$

From this diagram we see that $\overline{\mathrm{Tor}}_1^R(M_1,N)$ is the kernel of α, and since g is injective, it 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 $\overline{\mathrm{Tor}}_1^R(M_1,N) \cong \mathrm{Tor}_1^R(M,N_1)$.

Thus, so far we 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 symmetric versions, for all $n \geq 2$,

$$\begin{aligned}
\overline{\mathrm{Tor}}_n^R(M, N) &\cong \overline{\mathrm{Tor}}_1^R(M, N_{n-1}) \\
&\cong \mathrm{Tor}_1^R(M, N_{n-1}) \\
&\cong \overline{\mathrm{Tor}}_1^R(M_1, N_{n-2}) \\
&\cong \mathrm{Tor}_1^R(M_2, N_{n-3}) \text{ (if } n \geq 3) \\
&\cong \cdots \\
&\cong \mathrm{Tor}_1^R(M_{n-2}, N_1) \\
&\cong \overline{\mathrm{Tor}}_1^R(M_{n-1}, N) \\
&\cong \mathrm{Tor}_1^R(M_{n-1}, N) \\
&\cong \mathrm{Tor}_n^R(M, N),
\end{aligned}$$

which finishes the proof of the theorem. □

Now the following are easy corollaries:

Corollary 7.2 *If M is flat, then $\mathrm{Tor}_n^R(M, \_) = 0$ for all $n \geq 1$.* □

Corollary 7.3 *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 $n = 1$, this follows from the long exact sequence on homology (6.) and the previous corollary. For higher n, this follows by induction, 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 short exact sequences $0 \to M_n \to L_{n-1} \to M_{n-1} \to 0$ and $0 \to M_{n-1} \to L_{n-2} \cdots \to L_1 \to L_0 \to M \to 0$. □

Corollary 7.4 *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... □

Definition 7.5 *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 is* **torsion-free** *if no non-zero element is annihilated by any non-zerodivisor in R.*

The following may justify the name “Tor”.

Theorem 7.6 (Tor and torsion) *Let M and N be modules over a commutative domain R. Then for all $n \geq 1$, $\mathrm{Tor}_n^R(M, N)$ is torsion.*

Proof. First suppose that N is torsion. Then $P_n \otimes N$ is torsion for all n, whence $\mathrm{Tor}_n^R(M, N)$ 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 by Corollary 7.4 the short exact sequence $0 \to N \to N \otimes K \to (N \otimes K)/N \to 0$ gives a long exact sequence on homology:

$$\mathrm{Tor}_{n+1}^R(M, N \otimes K) \to \mathrm{Tor}_{n+1}^R(M, (N \otimes K)/N) \to \mathrm{Tor}_n^R(M, N) \to \mathrm{Tor}_n^R(M, N \otimes K).$$

For $n \geq 1$, $\mathrm{Tor}_{n+1}^R(M, N \otimes K) = \mathrm{Tor}_n^R(M, N \otimes K) = 0$ by Corollary 7.2, so that $\mathrm{Tor}_n^R(M, N) \cong \mathrm{Tor}_{n+1}^R(M, (N \otimes K)/N)$, and the latter is flat by the previous case.

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 $0 \to N' \to N \to N'' \to 0$ and by using the previous two cases we get the desired conclusion. □

Exercise 7.7 Let I and J be ideals in a commutative ring R. Prove that $\mathrm{Tor}_1(R/I, R/J) \cong \frac{I \cap J}{IJ}$.

Exercise 7.8 Let (R, 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 Theorem 3.6 we know that each F_n has finite rank. Prove that $\operatorname{rank} F_n = \dim_{R/m} \mathrm{Tor}_n^R(M, R/m)$.

8 Regular rings, part I

Theorem 8.1 *Let (R, m) be a Noetherian local ring. Then the following are equivalent:*

(1) $\mathrm{pd}_R(R/m) \leq n$.

(2) $\mathrm{pd}_R(M) \leq n$ *for all finitely generated R-modules M.*

(3) $\mathrm{Tor}_i^R(M, R/m) = 0$ *for all $i > n$ and all finitely generated R-modules M.*

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

Now let M be a finitely generated R-module. Let $P_\bullet$ be its minimal free resolution as in Theorem 3.6. By minimality, the image of $P_i \to P_{i-1}$ for $i \geq 1$ is in mP_{i-1}. Thus all the maps in $P_\bullet \otimes R/m$ are 0, so that $\mathrm{Tor}_i^R(M, R/m) = P_i/mP_i$. If we assume (3), these maps are 0 for $i > n$, and since P_i is finitely generated, it follows by Nakayama's lemma that $P_i = 0$ for $i > n$, whence $\mathrm{pd}_R(M) \leq n$. □

The same proof shows the graded version of the Hilbert Syzygy Theorem:

Theorem 8.2 *Let R be a polynomial ring in n variables over a field. Then every graded finitely generated R-module has finite projective dimension at most n.* $\square$

Definition 8.3 *A Noetherian local ring (R, m) is* **regular** *if $\mathrm{pd}_R(R/m) < \infty$.*

Definition 8.4 *A Noetherian local ring (R, m) is* **regular** *if the minimal number of generators of m is the same as the Krull dimension of R.*

It turns out that the two definitions of regularity coincide. We will prove this later in Section 13. 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 at a prime ideal is regular if we do not use the homological definition. But here is an easy proof of this fact using the homological definition:

Theorem 8.5 *Let (R, m) be a regular local ring, using Definition 8.3. Then for any prime ideal P in R, R_P is regular (under the same definition).*

Proof. By Theorem 8.1, R/P has a finite projective resolution. Since a localization of a projective module is projective and localization is flat, we get a finite projective resolution of $(R/P)P = R_P/PR_P$. Hence by Theorem 8.1, since PR_P is the unique maximal ideal of R_P, R_P is regular. $\square$

Theorem 8.6 *Let R be a polynomial ring in n variables over a field. Then every finitely generated R-module has finite projective dimension.*

Proof. Let M be a finitely generated R-module. Let $R^m \xrightarrow{\alpha} R^n \to M \to 0$ be exact. Here, α is an $n \times m$ 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. 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 Theorem 8.2, 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 $H_0(F_\bullet \otimes_S (S/(1-t)S)) = \mathrm{Tor}_0^S(\widehat{M}, S/(1-t)S) = H_0(0 \to \widehat{M} \xrightarrow{1-t} \widehat{M} \to 0) = \widehat{M}/(1-t)\widehat{M}$, which is the cokernel of $\widehat{\alpha} \otimes_S (S/(1-t)S) = \alpha$, so it is M. $\square$

Exercise 8.7 Let (R, m) be a Noetherian local ring and let M be a finitely generated R-module. Prove that $\mathrm{pd}_R(M) = \sup\{n : \mathrm{Tor}_n^R(M, R/m) \neq 0\}$.

9 Review of Krull dimension

Definition 9.1 *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. *This 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 is no intermediate prime ideal.

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**. It takes some work to prove that indeed these rings are catenary, and typically it is proved via a strengthened form of the Noether normalization lemma in the case of fields or via formal equidimensionality. We will not present a proof in class, but a reader may consult Appendix B in [3].

Definition 9.2 *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* $\operatorname{ht}(I)$, *and is either a nonnegative integer or* ∞. *The* **(Krull) dimension** *of a ring* R, *denoted* $\dim R$, *is the supremum of all the heights of prime ideals in* R.

The Krull dimension of a field is 0, the Krull dimension of a principal ideal domain 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 9.3 (Krull Principal Ideal Theorem, or Krull's Height Theorem) *Let* R *be a Noetherian ring, let* $x_1, \ldots, x_n \in R$, *and let* P *be a prime ideal in* R *minimal over* $(x_1, \ldots, x_n)$. *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, no prime ideal is strictly contained in it, so that $\operatorname{ht} P = 0$.

Next we prove the case $n = 1$. Suppose that there exist prime ideals $P_0 \subsetneq Q \subsetneq P$. 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 QR_Q has height 0, which contradicts the existence of P_0.

Now let $n \geq 2$. Let $P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_n \subsetneq P$ be a chain of prime ideals. If $x_1 \in P_0$, then P/P_0 is minimal over the ideal $(x_2, \ldots, x_n)(R/P_0)$, so that by induction on n, $\mathrm{ht}(P/P_0) \leq n-1$, 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 $i \in \{0, \ldots, n\}$. Suppose that $i > 1$. Then by denoting P as P_{n+1}, 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. By primary decomposition there exists a prime ideal Q in this domain that is minimal over the image of (x_1), and by the case $n = 1$, the height of that prime ideal 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. Note that Q 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 $(x_2, \ldots, x_n)(R/P_1)$, so that by induction on n, $\mathrm{ht}(P/P_1) \leq n-1$, which gives a contradiction to the existence of the long chain of prime ideals. □

Corollary 9.4 *Every prime ideal in a Noetherian ring has finite height.*

Proof. Since every ideal is finitely generated, by Theorem 9.3 its height is at most the (finite) number of generators. □

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

For a converse of the Krull Principal Ideal Theorem we will need a form of the Prime Avoidance Theorem, see Exercise 9.12.

---

* A review of primary modules is in Section 10.

Theorem 9.5 (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 $(x_1, \ldots, x_n)$.*

Proof. By localizing without loss of generality we may assume that R is a Noetherian local ring in which P is the only maximal ideal.

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 $n > 0$. By primary decomposition results we know that R has only finitely many minimal primes. By Prime Avoidance there exists $x_1 \in P$ that avoids all these finitely many minimal primes. If P has height 1, it is the only prime ideal in addition to the minimal prime ideals, so that P is minimal over (x_1), as desired. So suppose that P has height $n > 1$. By primary decomposition there exist finitely many prime ideals in R that are minimal over (x_1). Let $x_2 \in P$ avoid all these finitely many primes. If $n = 2$, P is the only prime ideal in R that contains (x_1, x_2), so that P is minimal over the two-generated ideal (x_1, x_2), as desired. If $n > 2$, continue by finding $x_3 \in P$ that avoids all the prime ideals in R that are minimal over (x_1, x_2), etc. We stop after we construct $x_1, \ldots, x_n \in P$ such that P is minimal over $(x_1, \ldots, x_n)$. □

Note that a modified form of the Krull Principal Ideal Theorem says that if a prime ideal in a Noetherian ring is minimal over an ideal generated by a regular sequence of length n, then the height of that prime ideal is exactly n.

Definition 9.6 *Let R be a commutative ring and let M be an R-module. The* **Krull dimension** *of M is $\dim(R/\operatorname{ann}(M))$.*

Proposition 9.7 *Let (R, m) be a Noetherian local ring and let M be a finitely generated R-module. Then M has finite Krull dimension, and $\dim M$ is the smallest number n of elements $x_1, \ldots, x_n$ in m such that $(x_1, \ldots, x_n) + \operatorname{ann} M$ is m-primary. Or equivalently, $\operatorname{ht} m$ is the smallest number n of elements $x_1, \ldots, x_n \in m$ such that $(x_1, \ldots, x_n)$ is m-primary.*

Proof. We only prove the second part, but that follows from the Krull Principal Ideal Theorem and its converse. □

Proposition 9.8 *Let (R, m) be a Noetherian local ring and let M be a finitely generated R-module of positive dimension. Let $x \in m$ not be in any prime ideal minimal over $\operatorname{ann}(M)$. Then $\dim(M/xM) = \dim M - 1$.*

Proof. Left to the reader. □

Proposition 9.9 *Let (R, 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) $\dim M \le \max\{\dim M', \dim M''\}$,

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

Proof. Let $x_1, \ldots, x_n \in m$. By the right-exactness of the tensor product, tensoring with $R/(x_1, \ldots, x_n)$ yields the following exact complex:

$$M'/(x_1, \ldots, x_n)M' \to M/(x_1, \ldots, x_n)M \to M''/(x_1, \ldots, x_n)M'' \to 0.$$

By the proof (!) of the converse of the Krull Principal Ideal Theorem, we may choose $x_1, \ldots, x_n$ such that $n = \max\{\dim M', \dim M''\}$ so that $(x_1, \ldots, x_n) + \operatorname{ann} M'$ and $(x_1, \ldots, x_n) + \operatorname{ann} M$ are m-primary. This means that the modules $M'/(x_1, \ldots, x_n)M'$ and $M''/(x_1, \ldots, x_n)M''$ have dimension 0, i.e., that they have finite length. But then the middle module $M/(x_1, \ldots, x_n)M$ also has finite length, so that $(x_1, \ldots, x_n) + \operatorname{ann} M$ is m-primary, whence $\dim M \le n$. This proves (1).

Now suppose that $x_1, \ldots, x_n$ are chosen so that $n = \dim M$ and $(x_1, \ldots, x_n) + \operatorname{ann} M$ is m-primary. Then $M/(x_1, \ldots, x_n)M$ has finite length, and so necessarily $M''/(x_1, \ldots, x_n)M''$ has finite length, which proves that $\dim M'' \le \dim M$. But with our homological algebra, we can extend the displayed exact complex above further:

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

Since $(\underline{x}) + \operatorname{ann} M'' \subseteq \operatorname{ann} \operatorname{Tor}_1^R(M'', R/(\underline{x}))$ by Property 7. of Tor, we have that $\operatorname{Tor}_1^R(M'', R/(\underline{x}))$ has finite length, so that $M'/(\underline{x})M'$ has finite length, whence $\dim M' \le n$. This finishes the proof of (2). □

Definition 9.10 *We have seen that in a Noetherian local ring (R, m), m is minimal over an ideal generated by* $\dim R$ *elements. Note that such an ideal is m-primary. Any sequence of* $\dim R$ *elements that generate an m-primary ideal is called* **a system of parameters**.

Obviously, every system of parameters in a Noetherian local ring has the same length.

Exercise 9.11 Let $P'' \subsetneq P'$ 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 9.3.)

Exercise 9.12 (Prime Avoidance) Let I be an ideal contained in the union $\cup_{i=1}^n P_n$, where $P_1, \ldots, P_n$ are ideals, at most two of which are not prime. 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.

Exercise 9.13 Find an example of a Noetherian ring of infinite Krull dimension.

Exercise 9.14 Let (R, m) be a Noetherian local ring, and let M be a finitely generated R-module of dimension d. Let $x_1, \ldots, x_n \in m$. Then $M/(x_1, \ldots, x_n)M$ has dimension at least $n - k$.

Exercise 9.15 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 $d = 1$.

10 Regular sequences

Recall Definition 5.4: $x_1, \ldots, x_n \in R$ is a **regular sequence** on a module M if $(x_1, \ldots, x_n)M \neq M$ and if for all $i = 1, \ldots, n$, x_i is a non-zerodivisor on $M/(x_1, \ldots, x_{i-1})M$. We say that this regular sequence has **length n**.

It is not clear that $x_1, \ldots, x_n$ being a regular sequence forces these elements to form a regular sequence in any order. In fact, it is not true in general. 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 10.1 *Let R be a commutative ring, M an R-module and I an ideal in R. The* **I-depth** *of M or the* **grade** *of M with respect to I, 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.*

The following are some straightforward facts:

(1) If $x_1, x_2, \ldots \in I$ is a regular sequence on M, then for all n, $(x_1, \ldots, x_n)M \subsetneq (x_1, \ldots, x_{n+1})M$.
(2) If M is Noetherian, then $\operatorname{depth}_I(M) < \infty$.
(3) For any Noetherian ring R, for any proper ideal I, and any finitely generated R-module M, $\operatorname{depth}_I M \leq \dim M, \operatorname{ht} I$.

We would like a parallel to Theorem 9.5 for sequences giving correct height. It is not enough to simply avoid all the minimal primes, we need to avoid zerodivisors. To understand the structure of zerodivisors, we first need a quick detour into primary decompositions.

Here is a quick review of the theory in case R is Noetherian and M is a finitely generated module over R.

(4) 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 it is nilpotent as a function.

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

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

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

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

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 $N : m = P$.

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

(9) Every submodule N of M can be written as a finite intersection of primary submodules. If we remove redundancies, the set of prime ideals P such that a P-primary submodule appears in the decomposition is uniquely determined. Such prime ideals are called **associated primes** of N, and their set is usually denoted $\mathrm{Ass}(M/N)$.

(10) If $N = \cap_i N_i$ is a (minimal) primary decomposition of N in M, then $0 = \cap_i (N_i/N)$ is a (minimal) primary decomposition of 0 in M/N, and of course the set of associated primes of N in M is the set of associated primes of 0 in M/N.

(11) The prime ideals that are minimal over $\mathrm{ann}(M)$ are called **minimal prime ideals** of M, and the set of all such is denoted $\mathrm{Min}(M)$. This set is always contained in $\mathrm{Ass}(M)$.

(12) For any $P \in \mathrm{Min}\, M$, 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.

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

Proposition 10.2 (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* $\operatorname{ann} M$ *(i.e., to M), then all regular sequences in I on M have length* 0*, and we are done. Othewise, we first choose $x_1 \in I$ that is not in any prime ideal associated to* $\operatorname{ann} M$ *(i.e., to M). We can do this by Prime Avoidance. If I is contained in some prime ideal associated to $M/(x_1)M$, i.e., to $(x_1)+\operatorname{ann} M$, 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 (x_1). If I is contained in some prime ideal associated to $M/(x_1, x_2)M$, i.e., to $(x_1, x_2) + \operatorname{ann} M$, 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 (x_1, x_2). And we continue in this way.*

Clearly this procedure constructs some regular sequence, and it must terminate. What is not clear that all choices of $x_1, \ldots, x_n$ of maximal length have the same length. We give an elementary proof of this fact in Proposition 10.7.

We can detect the existence of some regular sequences via Koszul complexes:

Proposition 10.3 *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 exists $y_1, \ldots, y_n \in R$ 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 $l > 0$. We will use Exercise 1.3 that says that $H_n(K_\bullet(x_1, \ldots, x_n; M)) = \operatorname{ann}_M(x_1, \ldots, x_n)$ for all $x_1, \ldots, x_n$ and M. By assumption, $\operatorname{ann}_M(x_1, \ldots, x_n) = 0$, so that $(x_1, \ldots, x_n)$ is not contained in any prime ideal that is associated to M. Thus by the strengthened form of Prime Avoidance, there exists $y_1 \in (x_1, \ldots, x_n)$ that is a minimal generator of the ideal such that $\operatorname{ann}_M(y_1) = 0$. In other words, y_1 is a non-zerodivisor on M. By Exercise 5.7 we may assume that $y_1 = x_1$: all the hypotheses are still satisfied. If $l = 1$, we are done. Otherwise, Equation (5.3) implies that for all $H_i(K_\bullet(x_2, \ldots, x_n; M))/x_1 H_i(K_\bullet(x_2, \ldots, x_n; M)) = 0$. Thus by Nakayama's lemma, $H_i(K_\bullet(x_2, \ldots, x_n; M)) = 0$ for $i = n, n-1, \ldots, n-l+1$. Since $H_n(K_\bullet(x_2, \ldots, x_n; M)) = 0$ trivially as n is strictly larger than the number of elements in $\{x_2, \ldots, x_n\}$, this really simply says that $H_i(K_\bullet(x_2, \ldots, x_n; M)) = 0$ for $i = n-1, \ldots, n-l+1$. Then by induction on n the conclusion follows. $\square$

Proposition 10.4 *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 when we permute two consecutive elements, i.e., it suffices to prove that if a, b is a regular sequence on M, so is b, a. If $ax = by$ for some $x, y \in M$, then by assumption $y = az$ for some $z \in M$, so that $a(x - bz) = 0$, and since a is a non-zerodivisor on M, $x = bz$. Thus a is a non-zerodivisor on M/bM. If $bx = 0$ for some $x \in M$, then $bx \in aM$, so by assumption $x \in aM$. Write $x = ax_1$ for some $x_1 \in M$. Then $0 = bx = bax_1$, and since a is a non-zerodivisor on M, $bx_1 = 0$. By repeating this process, we get that $x_1 \in aM$, whence $x \in a^2M$, so that $x \in \cap a^k M = 0$. This proves that b, a 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. If 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 $x_1, \ldots, x_n$ with imposed arbitrary powers form a regular sequence on M. $\square$

Note that the proof above shows more:

Corollary 10.5 *Whenever a, b is a regular sequence on M and b is a non-zerodivisor on M, then b, a is a regular sequence on M.* $\square$

Proposition 10.6 *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. If $x_1, \ldots, x_k \in I$ is a maximal regular sequence, there exists $w \in M \setminus (x_1, \ldots, x_k)M$ such that $wI \subseteq (x_1, \ldots, x_k)M$.*

Proof. It suffices to prove that if M has I-depth zero, then there exists a non-zero element $w \in M$ such that $Iw = 0$. The assumption on I-depth zero implies that I is contained in an associated prime ideal P of M, so that there exists $w \in M$ such that $P = (0_M) : w$. Hence $Iw \subseteq Pw = 0$. $\square$

Proposition 10.7 *Let I be an ideal in a Noetherian ring R. Let M be a finitely generated R-module. Let $x_1, \ldots, x_n \in I$ be a maximal regular sequence on M. Then every maximal regular sequence on M of elements in I has length n.*

Proof. Let $y_1, \ldots, y_m \in I$ be another regular sequence on M. Without loss of generality $n \le m$. 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 10.6 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 $w \in x_1M$, which is not the case, so necessarily $w' \notin y_1M$. Also, $Ix_1w' = y_1Iw \subseteq y_1x_1M$, so that $Iw' \subseteq y_1M$, so that I consists of zerodivisors on M/y_1M. Thus $m = 1$ as well.

Now suppose that $n > 0$ 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 Corollary 10.5, $c, x_1, \ldots, x_{n-1}$ 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, $n \le n-1$, which gives a contradiction. Thus $m \le n$, and by the minimality of n, $m = n$. $\square$

We can make Proposition 10.6 more precise:

Proposition 10.8 *Let (R, m) be a Noetherian local ring and let M be a finitely generated R-module of depth k. Let $x_1, \ldots, x_k \in m$ form a regular sequence on M. Then*

(1) 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 $m = \operatorname{ann}(w)$,

(3) and there exists an injection $R/m \to M/(x_1, \ldots, x_k)M$ (taking 1 to w).

Proof. If the (finite) set of associated primes of $M/(x_1, \ldots, x_k)M$ does not include m, then by Prime Avoidance we can find $x_{k+1} \in m$ which is a non-zerodivisor on $M/(x_1, \ldots, x_k)M$, which contradicts the definition of depth of M being k. Thus m is associated to $M/(\underline{x})M$, i.e., to $(\underline{x}) + \operatorname{ann} M$. This means that $m = ((\underline{x}) + \operatorname{ann} M) : y$. Then $ymM \subseteq ((\underline{x}) + \operatorname{ann} M)M = (\underline{x})M$. If $yM \subseteq (\underline{x})M$, then $y \in (\underline{x}) + \operatorname{ann} M$, which contradicts that $m = ((\underline{x}) + \operatorname{ann} M) : y$.

Then $zm \in (\underline{x})M$, so that $m \subseteq ((\underline{x})M : z) \subsetneq R$, so that $m = ((\underline{x})M : z)$. Now set w to be the image of z in $M/(\underline{x})M$. The rest is easy. $\square$

Exercise 10.9 Prove that if $x \in I$ is a non-zerodivisor on M, then $\operatorname{depth}_I(M/xM) = \operatorname{depth}_I(M) - 1$.

Exercise 10.10 Prove that $\operatorname{depth}_I(M \oplus N) = \min\{\operatorname{depth}_I(M), \operatorname{depth}_I(N)\}$.

Exercise 10.11 Prove that $\operatorname{depth}_I(M) = \operatorname{depth}_{\sqrt{I}}(M)$.

Exercise 10.12 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 13.13.) (Hint: Koszul complex for the last part.)

11 Regular sequences and Tor

Proposition 11.1 *Let M and N be finitely generated modules over a Noetherian local ring (R, m), and suppose that M has finite projective dimension n and that $m \in \operatorname{Ass} N$. Then $\operatorname{Tor}_n^R(M, N) \neq 0$.*

Proof. Since $m \in \operatorname{Ass} N$, there exists a short exact sequence $0 \to R/m \to N \to L \to 0$. Then we get the induced long exact sequence on Tor, with the relevant part being

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

Since M has projective dimension n, $\operatorname{Tor}_{n+1}^R(M, L) = 0$, and by Exercise 8.7, $\operatorname{Tor}_n^R(M, R/m) \neq 0$. Hence by the exactness of the complex above, $\operatorname{Tor}_n^R(M, N) \neq 0$. □

Corollary 11.2 *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 11.1, $\operatorname{Tor}_n^R(M, N) \neq 0$, so that $n' \geq n$. By symmetry, $n \geq n'$. □

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 11.3 *Let (R, m) be a Noetherian local ring and let M be a 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 10.2, there exists a sequence $x_1, \ldots, x_d \in m$ that is regular on R and on M. By Exercise 5.6, $K_\bullet(x_1, \ldots, x_d; R)$ is a free resolution of $R/(x_1, \ldots, x_d)$, and $K_\bullet(x_1, \ldots, x_d; M)$ is a free resolution of $M/(x_1, \ldots, x_d)M$.

Let $n = \operatorname{pd}_R(M)$. By Proposition 10.8, m is associated to $R/(x_1, \ldots, x_d)$, and so by Proposition 11.1,

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

is non-zero. Thus $n = 0$. But then M is a projective R-module, and hence free, whence $\operatorname{depth} M = \operatorname{depth} R$. □

Proposition 11.4 *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) In general, if $K = \ker(R^{\mu(M)} \to M)$ then K/xK has projective dimension $n-1$ over R/xR.

Proof. Let $0 \to F_n \to F_{n-1} \to \cdots \stackrel{\alpha}{\to} F_1 \to F_0 \to M \to 0$ be exact, where all F_i are finitely generated projective and hence free over R, and where for all $i \geq 0$, the map $F_{i+1} \to F_i$ has image in mF_i. If we tensor this with $R/(x)$, we get the complex

$$0 \to \frac{F_n}{xF_n} \to \frac{F_{n-1}}{xF_{n-1}} \to \cdots \stackrel{\alpha}{\to} \frac{F_1}{xF_1} \to \frac{F_0}{xF_0} \to 0.$$

Its homology at the ith place for $i > 0$ is $\operatorname{Tor}_i^R(M, R/(x))$. Since $R/(x)$ has projective dimension 1, the displayed complex has zero homology at places $i \geq 2$. Also,

$$\operatorname{Tor}_0^R(M, R/(x)) = H_0(M \otimes (0 \to R \stackrel{x}{\to} R \to 0)) = H_0(0 \to M \stackrel{x}{\to} M \to 0) = M/xM,$$

and

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

If x is a non-zerodivisor on M, then $\operatorname{Tor}_1^R(M, R/(x)) = 0$, so that

$$0 \to \frac{F_n}{xF_n} \to \frac{F_{n-1}}{xF_{n-1}} \to \cdots \stackrel{\alpha}{\to} \frac{F_1}{xF_1} \to \frac{F_0}{xF_0} \to \frac{M}{xM} \to 0,$$

is exact (the last part by right exactness by tensoring with $R/(x)$). So we got a finite free resolution of M/xM over $R/(x)$ and since the original resolution of M was minimal, so is this one, which means that the projective dimension of M/xM over R/xR is n.

In general,

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

is exact, giving a minimal finite free resolution of $\frac{F_1}{xF_1+\operatorname{im}\alpha}$ over $R/(x)$. However, 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 11.5 (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. First suppose that $\operatorname{depth} M = 0$. Then by Proposition 10.8, m is associated to M. Let $d = \operatorname{depth} R$. There exists $x_1, \ldots, x_d \in m$ that form a regular sequence on R. Then again by Proposition 10.8, m is associated to $R/(x_1, \ldots, x_d)$. Since $R/(x_1, \ldots, x_d)$ also has a minimal finite free resolution via the Koszul complex of length d, so its projective dimension is d. By Corollary 11.2, $\operatorname{depth} R = d = \operatorname{pd} M = \operatorname{pd} M + \operatorname{depth} M$.

Now suppose that $\operatorname{depth} M > 0$. By Proposition 11.3 $\operatorname{depth} R > 0$. Thus by Proposition 10.2 there exists $x \in m$ that is a non-zerodivisor on M and on R. By Proposition 11.4, M/xM has finite projective dimension over R/xR, and this projective dimension equals $\operatorname{pd} M$. Also, M/xM has depth exactly one less than $\operatorname{depth} M$, and $\operatorname{depth} R/(x) = \operatorname{depth} R - 1$, whence by induction on $\operatorname{depth} R$ we get the desired equality. □

Exercise 11.6 Go through this section and remove the finitely generated assumption wherever possible.

12 Cohen–Macaulay rings and modules

Definition 12.1 *A Noetherian local ring (R, m) is* **Cohen–Macaulay** *if m contains a regular sequence of length equal to the dimension of R. 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 m in R, M_m is a Cohen–Macaulay R_m-module.*

The following are again easy facts:

(1) $\mathbb{Z}$, principal ideal domains, and fields are Cohen–Macaulay.

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

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

(4) Let (R, m) be a Noetherian local ring, let M be a Cohen–Macaulay R-module, and let $x_1, \ldots, x_n \in m$ form a regular sequence on M. Then $M/(x_1, \ldots, x_n)M$ is Cohen–Macaulay.

(5) In a Cohen–Macaulay local ring, some system of parameters forms a regular sequence. Also, every maximal regular sequence in m is a system of parameters.

Theorem 12.2 *The following are equivalent for a Noetherian local ring (R, m):*

(1) R is Cohen–Macaulay.

(2) Some system of parameters in R forms a regular sequence.

(3) Every system of parameters in R forms a regular sequence.

Proof. Clearly (1) is equivalent to (2), and (3) implies both (1) and (2). Now suppose that (1) and (2) hold. Let $d = \dim R$ and let $y_1, \ldots, y_d$ be a system of parameters. We need to prove that $y_1, \ldots, y_d$ is a regular sequence. If $d = 0$, there is nothing to prove. If $d = 1$, then R has only finitely many primes: all the minimal primes and m. Since by (2) 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, but 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 that is a regular sequence. By construction of non-zerodivisors and parameters, since it is a matter of avoiding finitely many primes that do not contain m, there exists $c \in m$ such that $x_1, \ldots, x_{d-1}, c$ is a regular sequence and such that $y_1, \ldots, y_{d-1}, c$ is a system of parameters. By Proposition 10.4, $c, x_1, \ldots, x_{d-1}$ is a regular sequence, and certainly $c, y_1, \ldots, y_{d-1}$ is a system of parameters. Since c is a non-zerodivisor, $\dim(R/(c)) = \dim R - 1$ and $\operatorname{depth}(R/(c)) = \operatorname{depth} R - 1$. Thus $R/(c)$ is a Cohen–Macaulay ring. By induction on d, then $y_1, \ldots, y_{d_1}$ is a regular sequence on $R/(c)$, so that $c, y_1, \ldots, y_{d-1}$ is a regular sequence in R. Again by Proposition 10.4, $y_1, \ldots, y_{d-1}, c$ is a regular sequence, and then by passing to $R/(y_1, \ldots, y_{d-1})$ and the case $d = 1$, $y_1, \ldots, y_d$ is a regular sequence. $\square$

Corollary 12.3 *Let (R, m) be a Cohen–Macaulay local ring and let P be a prime ideal in R. Then R_P is a Cohen–Macaulay local ring, and $\operatorname{ht} P + \dim(R/P) = \dim R$.*

Furthemore, if $x_1, \ldots, x_d$ is any regular sequence, than any prime ideal associated to $(x_1, \ldots, x_d)$ is minimal over the ideal.

Proof. Certainly by the definition of dimension, we always have $\operatorname{ht} P + \dim(R/P) \leq \dim R = d$.

By Theorem 9.5, actually by its proof, there exists a part of a system of parameters $x_1, \ldots, x_n \in P$ such that P is minimal over $(x_1, \ldots, x_n)$ and $n = \operatorname{ht} P$. These can be extended to a system of parameters $x_1, \ldots, x_d$. By Theorem 12.2, $x_1, \ldots, x_d$ 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 the theorem, R_P is Cohen–Macaulay. It remains to prove the dimension/height equality.

We will prove more generally that if $P \in \operatorname{Ass}(R/(x_1, \ldots, x_n))$, where $x_1, \ldots, x_d$ is a regular sequence, then $\dim(R/P) = d - n$. If we prove that, then since $\operatorname{ht} P \geq n$, by the inequality in the first part, $\operatorname{ht} P = n$.

If $n = d$, there is nothing to prove. So suppose that $n < d$. Let $J = ((x_1, \ldots, x_n) : P) \subseteq J' = ((x_1, \ldots, x_n, x_{n+1}) : P)$. By Proposition 10.6 J is properly contains $(x_1, \ldots, x_n)$. Suppose that $J' = (x_1, \ldots, x_{n+1})$. Then for all $w \in J (\subseteq J')$, $w = \sum_{i=1}^{n-1} x_i z_i$ for some

$z_i \in R$, whence $Pw \subseteq (x_1, \ldots, x_n)$ means that $Pz_{n+1} \subseteq (x_1, \ldots, x_n)$, so that $z_{n+1} \in J$ and $w \in (x_1, \ldots, x_n) + x_{n+1}J$. Thus by Nakayama's lemma, $J = (x_1, \ldots, x_n)$, which is a contradiction. Thus J' properly contains $(x_1, \ldots, x_{n+1})$. So P consists of zerodivisors on $R/(x_1, \ldots, x_{n+1})$. Let Q be a prime ideal associated to $R/(x_1, \ldots, x_{n+1})$ that contains P. But x_{n+1} is in Q and not in P, so that $P \neq Q$. Also, Q is associated to $(x_1, \ldots, x_{n+1})$, so that by induction on $d - n$, $\dim(R/Q) = d - n - 1$. But then $\dim(R/P) \geq \dim(R/Q) + 1 = d - n$, but always $\dim(R/P) + \operatorname{ht} P \leq \dim R = d$, from which we conclude that $\dim(R/P = d - n = \dim R - \operatorname{ht} P$. ☐

Exercise 12.4 Prove that $\mathbb{Q}[[x^2, x^3]]$ is Cohen–Macaulay but is not regular either by Definition 8.3 or by Definition 8.4.

Exercise 12.5 Prove that $\mathbb{Q}[x, y, u, v]/(x, y)(u, v)$ is not Cohen–Macaulay.

Exercise 12.6 Prove that a localization of a Cohen–Macaulay module is Cohen–Macaulay.

Exercise 12.7 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 12.8 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 13.4.)

13 Regular rings, part II

Here we tie some loose ends from Section 8.

Proposition 13.1 *Let R be a Noetherian ring. Suppose that $P = (x_1, \ldots, x_d)$ is a prime ideal of height d that lies in the Jacobson radical. Then $(x_1, \ldots, x_{d-1})$ is a prime ideal.*

Proof. Let q be a prime ideal minimal over J contained in P. By the generalized Krull principal ideal theorem, $q \neq P$. Suppose that $q \neq J$. Let $a \in q \setminus J$. 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. But then since R is local, $a \in J$, which is a contradiction. This proves that J is a prime ideal, strictly contained in P. ☐

Theorem 13.2 *Let (R, m) be a Noetherian local ring. Then the following are equivalent:*

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

Proof. We have established in Theorem 8.1 that (1) implies (2), that (2) implies (3), and that (3) implies that $\mathrm{pd}_R(R/m) \le \dim R$. Thus (3) implies (4), and Theorem 8.1 then establishes that (4) implies (5) and that (5) implies (6). Certainly (7) implies (8). If m is generated by a regular sequence, then the number of generators of m is at most $\dim R$, but by the Krull Principal Ideal Theorem (Theorem 9.3), m must be generated by exactly $\dim R$ elements. Then the previous corollary proves that (8) implies (1).

Now assume (6). Then R/m has finite projective dimension over R. By the Auslander-Buchsbaum formula, $\operatorname{depth} R = \mathrm{pd}_R(R/m) + \operatorname{depth}(R/m)$. If $\operatorname{depth} R = 0$, then $\mathrm{pd}_R(R/m) = 0$, so R/m is a projective hence free R-module, whence $R = R/m$ is a field, so that (4) holds. Now let $\operatorname{depth} R > 0$. Let $x \in m$ avoid all non-zerodivisors and m^2. This is possible by Prime Avoidance. Since $x \notin m^2$, it is part of a minimal generating set of m. Let $x, x_2, \dots, x_n$ be a minimal generating set of m. Let $J = (x_2, \dots, x_n)$. Note that $(x) \cap J = xm$. Thus

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

is even a direct sum of $R/(x)$-modules: $\frac{m}{xm} \cong \frac{(x)}{xm} \oplus \frac{J+xm}{xm}$. Thus by taking isomorphic copies we get that $\frac{m}{xm} \cong \frac{R}{m} \oplus \frac{J}{J \cap xm}$. As x is a non-zerodivisor on R and hence on $\mathfrak{m}$, by Proposition 11.4 (1), the $R/(x)$-module m/xm has finite projective dimension. Thus its direct summand, the $R/(x)$-module $\frac{R}{m}$, also has finite projective dimension. But then by induction on the number of generators of m, every minimal generating set of the $R/(x)$-ideal $\frac{m}{(x)}$ is a regular sequence. What this proves is that $x, x_2, \dots, x_n$ is a regular sequence in R. As a regular sequence can have at most $\dim R$ elements, but a minimal generating set of m has to have at least $\dim R$ elements, it follows that $n = \dim R$. So a system of parameters is a regular sequence. But every minimal generating set of m is a system of parameters, so by Theorem 12.2, every minimal generating set of m is a regular sequence. Thus (6) implies (7).

Thus we have proved that (1) through (8) are equivalent. Certainly (8) implies (9). Now assume (9). We may choose $y_1 \in m$ to avoid m^2 and all the minimal prime ideals, then we choose $y_2 \in m$ to avoid m^2 and all the prime ideals minimal over (y_1), after which we choose $y_3 \in m$ but not in m^2 and not in any prime ideals minimal over (y_1, y_2), etc., as long as Prime Avoidance allows us to construct these y_i. In other words, we construct y_{i+1} as long as $i < \dim R$ (as all primes minimal over $(y_1, \dots, y_i)$ in our construction have height equal to i) and as long as i is strictly less than the minimal number of a generating set, or in short, we construct $y_1, \dots, y_d$, where $d = \dim R$, $(y_1, \dots, y_d) = m$, and for all $i \le d$, $\mathrm{ht}(y_1, \dots, y_i) = i$. By Proposition 13.1, for all $i = 0, \dots, d$, $(y_1, \dots, y_i)$ is a prime ideal, which proves that $y_1, y_2, \dots, y_d$ is a regular sequence. Thus (9) implies (8), and we have completed the proof of the theorem. □

With this theorem we can now see that the Definitions 8.3 and 8.4 of regularity describe identical rings. More generally, we have a new definition:

Definition 13.3 *A Noetherian ring R is* **regular** *if for all maximal ideals m in R, R_m is regular (by either of the definitions 8.3 and/or 8.4). By the previous theorem, R is regular if and only if for all prime ideals P in R, R_P is regular.*

Examples 13.4

(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 $k[x_1, \dots, x_n]$ over a field is regular. Every power series ring $k[[x_1, \dots, x_n]]$ in indeterminates over a field is regular.
(4) Every regular ring is Cohen–Macaulay.
(5) Let R be a regular ring. Let X be a variable over R. Then $R[X]$ is regular. Proof: Let M be a maximal ideal in $R[X]$. It suffices to prove that $R[X]_M$ is regular. Let $m = M \cap R$. Then $R[X]_M$ is a localization of R_m, so without loss of generality we may assume that R is a regular local ring, and that M contracts to the maximal ideal m in R. Then, since $(R/m)[X]$ is a principal ideal domain, M is either $mR[X]$ or $mR[X] + (f)$ for some monic polynomial 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 if R is regular. In the second case, $R[X]_M$ has dimension strictly bigger than R, in fact, bigger by 1, and $MR[X]_M$ is generated by one more element than m, which again proves that $R[X]_M$ is regular.

Theorem 13.2 proves that if a prime ideal of a Noetherian ring is generated by d elements, where d is the height of that prime ideal, the localization at that prime ideal is a very special ring. We can say more about those generators even globally, albeit only in Noetherian local rings to start with:

We can extend Proposition 13.1 now:

Proposition 13.5 *Let R be a Noetherian ring. Suppose that $P = (x_1, \ldots, x_d)$ is a prime ideal of height d that lies in the Jacobson radical. Then $x_1, \ldots, x_d$ is a regular sequence in R, and for any $i \in \{0, \ldots, d\}$ $(x_1, \ldots, x_i)$ is a prime ideal of height i.*

Proof. By Proposition 13.1, $J = (x_1, \ldots, x_{d-1})$ is a prime ideal. To prove that J has height $d-1$, it suffices to prove that JR_P has height $d-1$. But by Theorem 13.2 R_P is a regular local ring, so $x_1, \ldots, x_d$ is a regular sequence in R_P, so JR_P and J have height $d-1$.

Thus similarly by induction each $(x_1, \ldots, x_i)$ is a prime ideal of height i. $\square$

Question 13.6 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, $\operatorname{pd}_R(M) \le \dim R$.

Theorem 13.7 *Let $R = k[X_1, \ldots, X_n]$ and let M be a finitely generated graded R-module. Then $\operatorname{pd}_R(M) \le \dim R$.*

Proof. Let $F_\bullet$ be a minimal free resolution of M, minimal in the sense that at every step in the construction a minimal number of homogeneous generators is taken. If $m = (X_1, \ldots, X_n)$, then $(F_\bullet)_m$ is a minimal free resolution of M_m, so $F_{n+1} = 0$. $\square$

Remark 13.8 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 [3] (and you will need to know the basics on integral closure that this section refers to from earlier in the 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 $[y \ x \ \ -2z]$, so that $J_{R/k} = (x, y, z)R$. Hence by the Jacobian criterion $R_{(x,y,z)}$ is not regular, but all other proper localizations of R are regular.

Note that 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 Zariski-closed set.

Proposition 13.9 (Hironaka) *Let $(R, m) \subseteq (S, n)$ 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 $(x_1, \ldots, x_d) = m$. Recall from [1] that $\dim R = \dim S$ and that $n \cap R = m$.

If S is free, then as an R-module, $\operatorname{depth}_m S = \operatorname{depth}_m R$, and even $x_1, \ldots, x_d$ 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 $\operatorname{depth} S \geq d$. However, $d \leq \operatorname{depth} S \leq \dim S = \dim R = d$, so 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 12.2, $x_1, \ldots, x_d$ is a regular sequence on S. Thus $\operatorname{depth}_m S \geq d$. But the Auslander–Buchsbaum formula says that $\operatorname{pd}_R(S) + \operatorname{depth}_R(S) = \operatorname{depth}_R(R) = d$, whence $\operatorname{pd}_R(S) = 0$, so S is a projective R-module. But since R is Noetherian local and S is finitely generated, S is a free R-module. $\square$

This theorem is very useful for determining when an affine domain S (or other rings) is Cohen–Macaulay. Namely, we can first find a Noether normalization R of the given domain, and then apply the Theorem.

Exercise 13.10 Give examples of Cohen–Macaulay rings that are not Cohen–Macaulay.

Exercise 13.11 Prove that every regular local ring is a domain. Give examples of regular rings that are not domains.

Exercise 13.12 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 13.13 (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. (Confer with Exercise 10.12.)

Exercise 13.14 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.)

14 Injective and divisible modules

Definition 14.1 *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:*

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

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:

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

The following are trivial to show:

Lemma 14.2

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

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

Compare the following to Theorem 2.5:

Theorem 14.3 *Let E be a left R-module. The following are equivalent:*

(1) E is an injective R-module.

(2) $\mathrm{Hom}_R(\_, E)$ 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) if and only if (2): By the left-exactness of $\mathrm{Hom}_R(\_, E)$ for all E, it suffices to prove that if $f : M \to N$ is injective, then $\mathrm{Hom}_R(N, E) \xrightarrow{\_\circ f} \mathrm{Hom}_R(M, E)$ is onto. But this follows from the definition of injective modules. The converse is along the same lines.

If E is injective, then

$$\begin{tikzcd}
& E & \\
0 \arrow[r] & E \arrow[u, "id"] \arrow[r, "f"] & M
\end{tikzcd}$$

yields the map h as desired for (3), whence (1) implies (3) by Exercise 1.8.

Now assume (3), and **assume for now** that every R-module is contained in an injective R-module (Theorem 14.14). Let I be an injective R-module that contains E. Then by assumption E is a direct summand of an injective module, hence injective by Lemma 14.2. $\square$

Proposition 14.4 (Base change – of sorts) *If E is an injective left R-module and S is an R-algebra, then $\mathrm{Hom}_R(S,E)$ is an injective left S-module.*

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

By parts (1) and (2) of the previous proposition it suffices to prove that $\mathrm{Hom}_S(\_, \mathrm{Hom}_R(S,E))$ is exact. But by tensor-hom adjointness, $\mathrm{Hom}_S(\_, \mathrm{Hom}_R(S,E)) \cong \mathrm{Hom}_R(\_ \otimes_S S, E) \cong \mathrm{Hom}_R(\_, E)$, which is exact, also by parts (1) and (2) of the previous proposition. $\square$

Example 14.5 If E is an injective R-module and I is an ideal in R, then $\mathrm{Hom}_R(R/I, E) \cong \{e \in E : Ie = 0\} = (0_E : I)$ is an injective module over R/I.

Theorem 14.6 **(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 definition. Now let's assume the ideal definition and assume that we have an injective module homomorphism $f : M \to N$ and a module homomorphism $g : M \to E$. We may think of M as a submodule of N, i.e., that f is the inclusion.

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, f). We partially order Λ by imposing $(H, h) \leq (L, l)$ 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, and that $f : H \to N$, defined by $f(x) = h_i(x)$ if $x \in H_i$, is a homomorphism. 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 $I = H : x$. This is an ideal of R. Define $\tilde{g} : I \to E$ by $\tilde{g}(i) = h(ix)$. This 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 $H = N$. $\square$

Now we can add to Lemma 14.2:

Lemma 14.7 *If the ring is Noetherian, then a direct sum of injective modules is injective.*

Proof. 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 $imf \in \oplus_{\alpha \in T} E_\alpha$ for some finite subset T. But then by Lemma 14.2 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 says that $\oplus_\alpha E_\alpha$ is injective. $\square$

Definition 14.8 *An R-module M is* **divisible** *if for all $a \in R$ that is a non-zerodivisor in R and for all $m \in M$ there exists $n \in M$ such that $m = an$.*

Examples 14.9

(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 14.10 *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

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

gives that $ah(1) = m$. $\square$

Recall the definition of torsion-free modules Definition 7.5.

Proposition 14.11 *Any torsion-free and divisible module over a domain is injective.*

Proof. 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 $h : R \to I$ be $h(r) = rx$. 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, $g(i) = ix$. $\square$

Proposition 14.12 *A divisible module over a principal ideal domain is injective.*

Proof. By Baer's criterion, 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. $\square$

Examples 14.13

(1) Every field is an injective module over itself.

(2) If R is a principal ideal domain, then its field of fractions is an injective R-module.

Theorem 14.14 *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 14.4, $E = \mathrm{Hom}_{\mathbb{Z}}(R, E_Z)$ 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 14.4 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. $\square$

Note that this finishes the proof of Theorem 14.3.

15 Injective resolutions

Theorem 14.14 that we just proved shows that every module has an injective resolution, where the definition is as follows:

Definition 15.1 *An* **injective resolution** *of an R-module M is a cocomplex 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 15.2 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.

Example 15.3 Let k be a field, let $x_1, \ldots, x_n$ ba variables over k, and let $R = k[x_1, \ldots, x_n]$. Let E be an R-module with the k-vector space basis $\{X_1^{-i_1} \cdots X_n^{-i_n} : i_1, \ldots, i_n \geq 1\}$, and R-multiplication on E is induced by

$$x_k X_1^{-i_1} \cdots X_n^{-i_n} = \begin{cases} X_1^{-i_1} \cdots X_{k-1}^{-i_{k-1}} X_k^{-i_k+1} \cdots X_{k+1}^{-i_{k+1}} \cdots X_n^{-i_n}, & \text{if } i_k \geq 2; \\ 0, & \text{otherwise.} \end{cases}$$

We will eventually prove that E is injective over a localization of R at $(x_1, \ldots, x_n)$. Note that E is not Noetherian. It is, however, Artinian (as we will prove).

Theorem 15.4 (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 cocomplex, and let $I^\bullet : \quad 0 \to N \to I^0 \to I^1 \to I^2 \to \cdots$ be a cocomplex with all I^i injective. Then for any $f \in \operatorname{Hom}_R(M, N)$ there exists a map of cocomplexes $f^\bullet : C^\bullet \to I^\bullet$ that extends f, i.e., such that $f^{-1} = f$. Moreover, any two such liftings $f^\bullet$ are homotopic.*

Proof. Let the cocomplex 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

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

Now suppose that we have f^{n-1}, f^n, and we want to construct f^{n+1}. 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 $\operatorname{im} d^{n-1} = \ker d^n$ 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:

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

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. $\square$

Corollary 15.5 *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*

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

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

The following has a proof similar to Corollary 6.3:

Corollary 15.6 *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.* □

And the following has a proof similar to Proposition 6.5:

Proposition 15.7 *Let $I^{\bullet\prime}$ be an injective resolution of M' and let $I^{\bullet\prime\prime}$ be an injective resolution of M''. Suppose that $0 \to M^{\bullet\prime} \to M^\bullet \to M^{\bullet\prime\prime} \to 0$ is a short exact sequence. Then there exists an injective resolution $I^\bullet$ such that*

$$\begin{array}{cccccccc} 0 \to & M' & \to & M & \to & M'' & \to 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 \to & I^{\bullet\prime} & \to & I^\bullet & \to & I^{\bullet\prime\prime} & \to 0 \end{array}$$

is a commutative diagram, in which the bottom row is a 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 $I^{\bullet\prime}$ be $\delta^{\bullet\prime}$, and the maps on $I^{\bullet\prime\prime}$ be $\delta^{\bullet\prime\prime}$. Consider the diagram in which the rows are exact:

$$\begin{array}{cccccccccccc} 0 \to & M' & \stackrel{i}{\to} & M & \stackrel{\delta''^{-1}\circ p}{\longrightarrow} & I''^0 & \stackrel{\delta''^0}{\to} & I''^1 & \stackrel{\delta''^1}{\to} & I''^2 & \to \cdots \\ & \downarrow= & & & & & & & & & \\ 0 \to & M' & \stackrel{\delta'^{-1}}{\to} & I'^0 & \stackrel{\delta'^0}{\to} & I'^1 & \stackrel{\delta'^1}{\to} & I'^2 & \stackrel{\delta'^2}{\to} & I'^3 & \to \cdots \end{array}$$

By the Comparison Theorem for injectives, there exist the maps as below that make all squares commute:

$$\begin{array}{cccccccccccc} 0 \to & M' & \stackrel{i}{\to} & M & \stackrel{\delta''^{-1}\circ p}{\longrightarrow} & I''^0 & \stackrel{\delta''^0}{\to} & I''^1 & \stackrel{\delta''^1}{\to} & I''^2 & \to \cdots \\ & \downarrow= & & \downarrow f^0 & & \downarrow f^1 & & \downarrow f^2 & & \downarrow f^3 & \\ 0 \to & M' & \stackrel{\delta'^{-1}}{\to} & I'^0 & \stackrel{\delta'^0}{\to} & I'^1 & \stackrel{\delta'^1}{\to} & I'^2 & \stackrel{\delta'^2}{\to} & I'^3 & \to \cdots \end{array}$$

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. □

16 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 M. We define

$$\overline{\operatorname{Ext}}^n_R(M, N) = H^n(\operatorname{Hom}_R(M, I^\bullet)).$$

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 $\overline{\operatorname{Ext}}^n_R(\_, N)$ is independent of the injective resolution $I^\bullet$ of N. This follows from Corollary 15.6.

2. Ext has no terms of negative degree. $\overline{\operatorname{Ext}}^n_R(\_, N) = 0$ if $n < 0$. This follows as $I^\bullet$ has only zero modules in negative positions.

3. $\overline{\operatorname{Ext}}^0$. $\overline{\operatorname{Ext}}^0_R(M, N) \cong \operatorname{Hom}_R(M, N)$. Proof: By assumption $0 \to N \to I^0 \to I^1$ is exact, and as $\operatorname{Hom}(M, \_)$ is left-exact, $0 \to \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_R(I^0, N) \to \operatorname{Hom}_R(I^1, N)$ is exact as well. Thus $\overline{\operatorname{Ext}}^0_R(M, N) = H^0(\operatorname{Hom}_R(M, I^\bullet)) = \ker(\operatorname{Hom}_R(I^0, N) \to \operatorname{Hom}_R(I^1, N)) = \operatorname{Hom}_R(M, N)$.

4. What if M is projective? If M is projective, then $\overline{\operatorname{Ext}}_R^n(M, N) = 0$ 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, $\operatorname{Hom}_R(M, P_{n-1}) \to \operatorname{Hom}_R(M, P_n) \to \operatorname{Hom}_R(M, P_{n+1})$ is exact as well, giving that the nth cohomology of $\operatorname{Hom}_R(M, I^\bullet)$ is 0 if $n > 0$.

5. What if N is injective? If N is injective, then $\overline{\operatorname{Ext}}_R^n(M, N) = 0$ 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

$$\cdots \to \operatorname{Ext}_R^{n-1}(M, N'') \to \operatorname{Ext}_R^n(M, N') \to \operatorname{Ext}_R^n(M, N) \to \operatorname{Ext}_R^n(M, N'') \to \operatorname{Ext}_R^{n+1}(M, N') \to \cdots.$$

The proof goes as follows. Let $I^{\bullet\prime}$ be an injective resolution of N', and let $I^{\bullet\prime\prime}$ be an injective resolution of N''. Then by Proposition 15.7 there exists an injective resolution $I^\bullet$ of N such that

$$\begin{array}{ccccccc}
0 \to & N' & \to & N & \to & N'' & \to 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
0 \to & I^{\bullet\prime} & \to & I^\bullet & \to & I^{\bullet\prime\prime} & \to 0
\end{array}$$

is a commutative diagram in which the rows are exact. In particular, we have a short exact sequence $0 \to I^{\bullet\prime} \to I^\bullet \to I^{\bullet\prime\prime} \to 0$, and since this is a split exact sequence, it follows that $0 \to \operatorname{Hom}_R(M, I^{\bullet\prime\prime}) \to \operatorname{Hom}_R(M, I^\bullet) \to \operatorname{Hom}_R(M, I^{\bullet\prime}) \to 0$ is still a short exact sequence of complexes. The rest follows from Theorem 4.4.

Exercise 16.1 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 $\operatorname{Ext}_R^n(M, N) \to \operatorname{Ext}_R^n(M, N)$ in the long exact sequence above are also multiplications by x.

Exercise 16.2 Prove that for any R-modules M and N, $\operatorname{ann} M + \operatorname{ann} N \subseteq \operatorname{ann} \overline{\operatorname{Ext}}_R^n(M, N)$.

Exercise 16.3 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 $i \geq 1$, $\overline{\operatorname{Ext}}_R^i(M, N_n) \cong \overline{\operatorname{Ext}}_R^{i+n}(M, N)$.

17 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

$$\operatorname{Ext}_R^n(M, N) = H^n(\operatorname{Hom}_R(P_\bullet, N)).$$

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 $\operatorname{Ext}_R^n(M, \_)$ is independent of the projective resolution $P_\bullet$ of M. This follows from Corollary 6.3.

2. Ext has no terms of negative degree. $\mathrm{Ext}_R^n(M, \_) = 0$ if $n < 0$. This follows as $P_\bullet$ has only zero modules in negative positions.

3. Ext^0. $\mathrm{Ext}_R^0(M, N) \cong \mathrm{Hom}_R(M, N)$. 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 $\mathrm{Ext}_R^0(M, N) = H^0(\mathrm{Hom}_R(P_\bullet, N)) = \ker(\mathrm{Hom}_R(P_0, N) \to \mathrm{Hom}_R(P_1, N)) = \mathrm{Hom}_R(M, N)$.

4. What if M is projective? If M is projective, then $\mathrm{Ext}_R^n(M, N) = 0$ 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 $\mathrm{Ext}_R^n(M, N) = 0$ 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, $\mathrm{Hom}_R(P_{n-1}, N) \to \mathrm{Hom}_R(P_n, N) \to \mathrm{Hom}_R(P_{n+1}, N)$ is exact as well, giving that the nth cohomology of $\mathrm{Hom}_R(P_\bullet, N)$ 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

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

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 Proposition 6.5 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 $0 \to \mathrm{Hom}_R(P_\bullet{}'', N) \to \mathrm{Hom}_R(P_\bullet, N) \to \mathrm{Hom}_R(P_\bullet{}', N) \to 0$ is still a short exact sequence of complexes. The rest follows from Theorem 4.4.

7. Ext and annihilators. For any M, N and n, $\operatorname{ann} M + \operatorname{ann} N \subseteq \operatorname{ann} \mathrm{Ext}_R^n(M, N)$. Proof: Since $\mathrm{Ext}_R^n(M, N)$ is a quotient of a submodule of $\mathrm{Hom}_R(P_n, N)$, 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 4.9, the two maps are homotopic. Thus $\mathrm{Hom}_R(\mu_x, N)$ and 0 are homotopic on $\mathrm{Hom}_R(P_\bullet, N)$, whence by Proposition 4.7, $\mathrm{Hom}_R(\mu_x, N)_* = 0$. In other words, multiplication by x on $\mathrm{Hom}_R(P_\bullet, N)$ 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 $i \geq 1$, $\mathrm{Ext}_R^i(M_n, N) \cong \mathrm{Ext}_R^{i+n}(M, N)$. 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 $\mathrm{Ext}_R^n(M, N)$ 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 $\mathrm{Hom}_R(P_n, N)$ is finitely generated, whence so is $\mathrm{Ext}^n_R(M, N)$.

Exercise 17.1 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 $\mathrm{Ext}^n_R(M, N) \to \mathrm{Ext}^n_R(M, N)$ in the long exact sequence are also multiplications by x.

18 The two definitions of Ext are isomorphic

Theorem 18.1 *Let R be a commutative ring and let M and N be R-modules. Then for all n, $\mathrm{Ext}^R_n(M, N) \cong \overline{\mathrm{Ext}}^R_n(M, N)$.*

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 1.5), $0 \to \ker\alpha \to \ker\beta \to \ker\gamma \to \operatorname{coker}\alpha \to \operatorname{coker}\beta$ 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:

$$
\begin{array}{ccccccc}
\mathrm{Hom}(P_0, I^0) & \xrightarrow{g} & \mathrm{Hom}(M_1, I^0) & \to & 0 & & \\
\downarrow\beta & & \downarrow\gamma & & & & \\
\mathrm{Hom}(P_0, N_1) & \xrightarrow{f} & \mathrm{Hom}(M_1, N_1) & \to & \mathrm{Ext}_R^1(M, N_1) & \to & \mathrm{Ext}_R^1(P_0, N_1) = 0 \\
\downarrow & & \downarrow & & & & \\
0 & & \overline{\mathrm{Ext}}_R^1(M_1, N) & & & & \\
 & & \downarrow & & & & \\
 & & \overline{\mathrm{Ext}}_R^1(M_1, I^0) = 0 & & & &
\end{array}
$$

From this diagram we see that $\overline{\mathrm{Ext}}_R^1(M_1, N)$ is the cokernel of γ, and since g is injective, it is the cokernel of $\gamma \circ g = f \circ \beta$. But $\mathrm{Ext}_R^1(M, N_1)$ is the cokernel of f and hence of $f \circ \beta$, which proves that $\overline{\mathrm{Ext}}_R^1(M_1, N) \cong \mathrm{Ext}_R^1(M, N_1)$.

Thus, so far we proved that for all M, N, $\overline{\mathrm{Ext}}_R^1(M, N) \cong \mathrm{Ext}_R^1(M, N)$, 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, $\overline{\mathrm{Ext}}_R^1(M_1, N) \cong \mathrm{Ext}_R^1(M, N_1)$.

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 $n \geq 2$,

$$
\begin{aligned}
\overline{\mathrm{Ext}}_R^n(M, N) &\cong \overline{\mathrm{Ext}}_R^1(M, N_{n-1}) \\
&\cong \mathrm{Ext}_R^1(M, N_{n-1}) \\
&\cong \overline{\mathrm{Ext}}_R^1(M_1, N_{n-2}) \\
&\cong \mathrm{Ext}_R^1(M_2, N_{n-3}) \text{ (if } n \geq 3) \\
&\cong \cdots \\
&\cong \mathrm{Ext}_R^1(M_{n-2}, N_1) \\
&\cong \overline{\mathrm{Ext}}_R^1(M_{n-1}, N) \\
&\cong \mathrm{Ext}_R^1(M_{n-1}, N) \\
&\cong \mathrm{Ext}_R^n(M, N),
\end{aligned}
$$

which finishes the proof of the theorem. $\square$

19 Ext and extensions

Definition 19.1 *An* **extension** e *of groups or 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:*

$$\begin{array}{rccccccccc} e: & 0 & \to & N & \to & K & \to & M & \to & 0 \\ & & & || & & \downarrow\cong & & || & & \\ e': & 0 & \to & N & \to & K' & \to & M & \to & 0 \end{array}$$

An extension is **split** *if it is equivalent to*

$$0 \to N \xrightarrow{(1,0)} N \oplus M \to M \to 0.$$

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

$$0 \to \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(K,N) \to \mathrm{Hom}_R(N,N) \stackrel{\delta}{\to} \mathrm{Ext}^1_R(M,N).$$

In particular, if $\mathrm{Ext}^1_R(M,N)=0$, then the identity map on N lifts to a homomorphism $K \to N$, so e is split.

In general, without assuming $\mathrm{Ext}^1_R(M,N)=0$, 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 19.2 *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

$$\begin{array}{rccccccccc} e: & 0 & \to & N & \stackrel{i}{\to} & K & \stackrel{p}{\to} & M & \to & 0 \\ & & & || & & \downarrow\varphi & & || & & \\ e': & 0 & \to & N & \stackrel{i'}{\to} & K' & \stackrel{p'}{\to} & M & \to & 0 \end{array}$$

where φ is an isomorphism. From this we get

$$\begin{array}{cccccccc} 0 \to & \mathrm{Hom}_R(M,N) & \to & \mathrm{Hom}_R(K,N) & \to & \mathrm{Hom}_R(N,N) & \stackrel{\delta}{\to} & \mathrm{Ext}^1_R(M,N) \\ & || & & \uparrow\varphi & & || & & || \\ 0 \to & \mathrm{Hom}_R(M,N) & \to & \mathrm{Hom}_R(K',N) & \to & \mathrm{Hom}_R(N,N) & \stackrel{\delta'}{\to} & \mathrm{Ext}^1_R(M,N) \end{array}$$

which 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. Now let $g \in \mathrm{Ext}^1_R(M,N)$. Let F be a free R-module mapping onto M, and let C be the kernel. Then we have the short exact sequence $0 \to C \stackrel{\alpha}{\to} F \stackrel{\beta}{\to} M \to 0$, which gives the exact sequence

$$\to \mathrm{Hom}_R(C,N) \stackrel{\gamma}{\to} \mathrm{Ext}^1(M,N) \to \mathrm{Ext}^1_R(F,N)=0,$$

so there exists $h \in \mathrm{Hom}_R(C, N)$ that maps to g via γ. Let

$$K = \frac{N \oplus F}{\{(h(c), -\alpha(c)) : c \in C\}}$$

(pushout). Then

$$\begin{array}{ccc} C & \xrightarrow{h} & N \\ \downarrow\alpha & & \downarrow\alpha' \\ F & \xrightarrow{h'} & K \end{array}$$

commutes, and we have a well-defined homomorphism $p : K \to M$ given as $p(a, b) = \beta(b)$. Note that this is surjective. The natural map $i : N \to K$ is injective, as $(n, 0) = (h(c), -\alpha(c)) \in N \oplus F$ means that $\alpha(c) = 0$, whence $c = 0$. The image of N in K is in the kernel of p, and if $(a, b) \in \ker p$, then $p(b) = 0$, 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:

$$\begin{array}{ccccccc} 0 \to & C & \xrightarrow{\alpha} & F & \xrightarrow{\beta} & M & \to 0 \\ & \downarrow h & & \downarrow h' & & || & \\ 0 \to & N & \to & K & \to & M & \to 0 \end{array}$$

and from it we get the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 \to & \mathrm{Hom}_R(M, N) & \to & \mathrm{Hom}_R(F, N) & \to & \mathrm{Hom}_R(C, N) & \xrightarrow{\gamma} & \mathrm{Ext}^1_R(M, N) \\ & || & & \uparrow h' & & \uparrow h & & || \\ 0 \to & \mathrm{Hom}_R(M, N) & \to & \mathrm{Hom}_R(K, N) & \to & \mathrm{Hom}_R(N, N) & \xrightarrow{\delta} & \mathrm{Ext}^1_R(M, N) \end{array}$$

which proves that $\delta(\mathrm{id}_N) = \gamma(h)$, so that $g \in \mathrm{Ext}^1(M, N)$ corresponds to an extension.

It remains to prove that φ is injective. Let $0 \to N \to K \to M \to 0$ be an extension of M by N. Since F is projective, we get a commutative diagram

$$\begin{array}{ccccccc} 0 \to & C & \to & F & \to & M & \to 0 \\ & \downarrow & & \downarrow & & || & \\ 0 \to & N & \to & K & \to & M & \to 0 \end{array}$$

I leave it as a straightforward exercise that the pushout of $C \to F$ and $C \to N$ above is isomorphic to K, and that the short exact sequence with the pushout and the one with K are equivalent. Thus if any two extensions of M by N give the same element of $\mathrm{Ext}^1_R(M, N)$, they are equivalent. $\square$

Definition 19.3 *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'). Note that the diagonal $\Delta = \{(i(n), i'(n)) : n \in N\}$ is a submodule of X. The* **Baer sum** *of e and e' is $e : 0 \to N \to Y \to M \to 0$, where $Y = X/\Delta$, the map $j : N \to Y$ is $j(n) = (i(n), 0) = (0, -i'(n))$, and $p : Y \to M$ takes (x, x') to $p(x) = p'(x')$.*

Exercise 19.4 Prove that the Baer sum of two extensions of M by N is an extension of M by N.

Exercise 19.5 Prove that the set of Baer sums of equivalence classes of extensions of M by N is an abelian group under Baer sums, with the split extensions forming the zero.

Exercise 19.6 Prove that the map $e \mapsto \delta(\mathrm{id}_N)$ is an isomorphism of the group of extensions of M by N to $\mathrm{Ext}^1_R(M, N)$.

Let's look at Ext and extensions in another way. But really, the rest of this section is REDUNDANT!

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 $\delta(\mathrm{id}_M)$. I think that it is a lot harder to prove that this map induces an isomorphism of the group of extensions of M by N to $\mathrm{Ext}^1_R(M, N)$.

Lemma 19.7 *Suppose that e and e' are equivalent extensions of M by N. Then $\delta(\mathrm{id}_M)$ is the same in both cases.*

Proof. (Can this proof be shortened??) Let

$$\begin{array}{ccccccccccc}
e: & 0 & \to & N & \xrightarrow{i} & K & \xrightarrow{p} & M & \to & 0 \\
& & & || & & \downarrow \varphi & & || & & \\
e': & 0 & \to & N & \xrightarrow{i'} & K' & \xrightarrow{p'} & M & \to & 0
\end{array}$$

where φ is an isomorphism. Naturally, $i' = \varphi \circ i$ and $p' = p \circ \varphi^{-1}$. Let $(I^\bullet, d)$ be an injective resolution of N and $(J^\bullet, \delta)$ an injective resolution of M. As in Proposition 15.7, $I^\bullet \oplus J^\bullet$ is an injective resolution of K and hence also of K' with some modified maps as follows. From

$$\begin{array}{cccccccccc}
0 \to & N & \xrightarrow{i} & K & \xrightarrow{\delta^{-1} \circ p} & J^0 & \xrightarrow{\delta^0} & J^1 & \to \cdots \\
& || & & \downarrow f^0 & & \downarrow f^1 & & \downarrow f^2 & \\
0 \to & N & \xrightarrow{d^{-1}} & I^0 & \xrightarrow{d^0} & I^1 & \to & I^2 & \to \cdots
\end{array}$$

we get

$$\begin{array}{cccccccccc}
0 \to & N & \xrightarrow{\varphi \circ i} & K' & \xrightarrow{\delta^{-1} \circ p \circ \varphi^{-1}} & J^0 & \xrightarrow{\delta^0} & J^1 & \to \cdots \\
& || & & \downarrow f^0 \circ \varphi^{-1} & & \downarrow f^1 & & \downarrow f^2 & \\
0 \to & N & \xrightarrow{d^{-1}} & I^0 & \xrightarrow{d^0} & I^1 & \to & I^2 & \to \cdots
\end{array}$$

and we also get the map $K \to I^0 \oplus J^0$ as $k \mapsto (-f^0(k), \delta \circ p(k))$, the map $K' \to I^0 \oplus J^0$ as $k \mapsto (-f^0 \circ \varphi^{-1}(k), \delta \circ p \circ \varphi^{-1}(k))$, and the map $I^0 \oplus J^0 \to I^1 \oplus J^1$ as $(a, b) \mapsto (d^0(a) + f^1(b), \delta^0(b))$.

We get exact rows and columns in the following:

$$\begin{array}{ccccccc}
 & 0 & & 0 & & 0 & \\
 & \downarrow & & \downarrow & & \downarrow & \\
0 \to & \mathrm{Hom}_R(M,N) & \to & \mathrm{Hom}_R(M,K) & \to & \mathrm{Hom}_R(M,M) & \\
 & \downarrow & & \downarrow & & \downarrow & \\
0 \to & \mathrm{Hom}_R(M,I^0) & \to & \mathrm{Hom}_R(M,I^0 \oplus J^0) & \to & \mathrm{Hom}_R(M,J^0) & \to 0 \\
 & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & \\
0 \to & \mathrm{Hom}_R(M,I^1) & \to & \mathrm{Hom}_R(M,I^1 \oplus J^1) & \to & \mathrm{Hom}_R(M,J^1) & \to 0
\end{array}$$

We apply the Snake Lemma (on α, β, γ). Here $\mathrm{id}_M \in \mathrm{Hom}_R(M,M) \subseteq \mathrm{Hom}_R(M,J^0)$ is in the kernel of γ, or more precisely, $\delta^{-1} \in \mathrm{Hom}_R(M,J^0)$ is in the kernel, and so maps to $\operatorname{coker}\alpha$ as follows. First of all, $\delta^{-1} \in \mathrm{Hom}_R(M,J^0)$ is the image of $(0,\delta^{-1}) : M \to I^0 \oplus J^0$. The image of $(0,\delta^{-1})$ in $\mathrm{Hom}_R(M,I^1 \oplus J^1)$ is $(f^1 \circ \delta^{-1}, 0)$, and its preimage in $\mathrm{Hom}_R(M,I^1)$ is $f^1 \circ \delta^{-1}$. Let $m \in M$. Write $m = p(k)$ for some $k \in K$. Then $d^1 \circ f^1 \circ \delta^{-1}(m) = d^1 \circ d^0 \circ f^0(m) = 0$, so that $f^1 \circ \delta^{-1}$ is in the kernel of the map $\mathrm{Hom}_R(M,I^1) \to \mathrm{Hom}_R(M,I^2)$, or in other words, id_M maps to the image of $f^1 \circ \delta^{-1}$ in $\mathrm{Ext}^1(M,N)$.

We have all the information to say what happens with the extension e': id_M maps to the same element $f^1 \circ \delta^{-1}$ as the id_M arising from the extension e. □

Exercise 19.8 (Which I am not able to solve right now.) Now let M and N be R-modules, let $g \in \mathrm{Ext}^1_R(M,N)$. Let F be a free R-module mapping onto M, and let C be the kernel. Then the short exact sequence $0 \to C \xrightarrow{\alpha} F \xrightarrow{\beta} M \to 0$ 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 onto g via γ. Let

$$K = \frac{N \oplus F}{\{(h(c), -\alpha(c)) : c \in C\}}$$

(pushout). Then

$$\begin{array}{ccc}
C & \xrightarrow{h} & N \\
\downarrow \alpha & & \downarrow \alpha' \\
F & \xrightarrow{h'} & K
\end{array}$$

commutes, and we have a well-defined homomorphism $p : K \to M$ given as $p(a,b) = \beta(b)$. Note that this is surjective. The natural map $i : N \to K$ is injective, as $(n,0) = (h(c), -\alpha(c)) \in N \oplus F$ means that $\alpha(c) = 0$, whence $c = 0$. The image of N in K is in the kernel of p, and if $(a,b) \in \ker p$, then $p(b) = 0$, 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. Show that this extension yields the original $g \in \mathrm{Ext}^1_R(M,N)$.

20 Essential extensions

In this section we look more closely at the structure of injective modules.

Definition 20.1 *An extension $M \subseteq N$ of R-modules is said to be* **essential** *(over R) if for every non-zero submodule K of N, $K \cap M$ is non-zero.*

Remark 20.2

(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 such that $S^{-1}M \neq 0$, then $S^{-1}M \subseteq S^{-1}N$ is essential over $S^{-1}R$.

Lemma 20.3 *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 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 Remark 20.2, every chain has an upper bound. Thus by Zorn's lemma the existence conclusion follows. □

Proposition 20.4 *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 14.3, $N \cong E \oplus M$ 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 14.3 it suffices to prove that any injective homomorphism $f : E \to M$ splits. Without loss of generality M is different from E. By assumption for every $x \in M \setminus E$, $Rx \cap E = 0$. Let Λ be the set of all submodules K of M such that $K \cap E = 0$. We just proved that Λ is not empty. We can 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. □

Now we can make Lemma 20.3 more precise under an additional assumption:

Lemma 20.5 *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 20.3 there exists a submodule L of N that is maximal among all essential extensions of M in N. Suppose for contradiction that L is not injective. Then by Proposition 20.4, L has a proper essential extension E (which is not necessarily a submodule of N). Since N is injective, by definition we have

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

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 (Remark 20.2), 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 20.4, L is injective. $\square$

Theorem 20.6 *Let M be an R-module. Then there exists an overmodule that is injective and essential over M. Any two such overmodules are isomorphic.*

Proof. By Theorem 14.14 there exists an injective R-module N containing M, and Lemma 20.5 finishes the proof of existence.

Suppose that E and E' are injective modules that are essential over M. Then

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

and h has to be injective as E is essential over M and M embeds in E'. Since h and E are injective, it 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 20.7 *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 20.8 *Let $M \subseteq E$ be R-modules. The following are equivalent:*

(1) E is a maximal essential extension of M.

(2) E is injective, $M \subseteq E$ 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. Assume (1). Clearly $M \subseteq E$ is essential. Let F be an essential extension of E. Then by one of the remarks, F is an essential extension of M, and by the maximality assumption in (1), $E = F$, so by Proposition 20.4, E is injective. This proves (2).

(2) and (3) are equivalent by definition.

Assume (2). Let E' be an injective module such that $M \subseteq E' \subseteq E$. By Theorem 14.3, $E \cong E' \oplus E''$ for some submodule E'' of E. Then $E'' \cap M = 0$, so by assumption (2), $E'' = 0$. This proves (4).

Assume (4). By Lemma 20.5 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 as 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 20.9 *If E is an injective R-module, then $E_R(E) = E$.* $\square$

Proposition 20.10 *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 imbedding. $\square$

Definition 20.11 *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**.

Proposition 20.12 *Let $(R, \mathfrak{m})$ be a Noetherian ring and let M be an R-module. Prove that* $\mathrm{Hom}_R(R/\mathfrak{m}, M) \cong \mathrm{Hom}_R(R/\mathfrak{m}, E_R(M))$.

Proof. Define $\varphi : \mathrm{Hom}_R(R/\mathfrak{m}, M) \to \mathrm{Hom}_R(R/\mathfrak{m}, E_R(M))$ via the standard inclusion $M \subseteq E_R(M)$. Clearly φ is injective. Now let $f \in \mathrm{Hom}_R(R/\mathfrak{m}, E_R(M))$. This f is uniquely determined by $f(1) \in E_R(M)$. Since $M \to E_R(M)$ is essential, if $f(1) \neq 0$ there exists $r \in R$ such that $rf(1)$ is non-zero in M. If $r \in \mathfrak{m}$, then $0 = f(0) = f(r) = rf(1)$, so necessarily r is a unit in R. But then the image of f is in M, so that $\mathrm{Hom}_R(R/\mathfrak{m}, E_R(M)) \subseteq \mathrm{Hom}_R(R/\mathfrak{m}, M)$. □

Theorem 20.13 *Let $I^\bullet$ be a minimal injective resolution of an R-module M. Then for all $P \in \mathrm{Spec}\,(R)$ and all $i \geq 0$, $\mathrm{Hom}_{R_P}(R_P/PR_P, (I^i)_P) \to \mathrm{Hom}_{R_P}(R_P/PR_P, (I^{i+1})_P)$ is the zero map.*

Proof. By Exercise 20.14, $(I^\bullet)_P$ is an injective resolution of M_P, and by Remark 20.2, it is a minimal injective resolution of M_P.

Let Q^i be the kernel of $I^i \to I^{i+1}$ (i.e., the cokernel of $I^{i-2} \to I_{i-1}$). Then $0 \to Q^i \to I^i \to I^{i+1} \to I^{i+2} \to \cdots$ is exact. Since localization and Hom are left-exact (see Exercise 1.7), it follows that

$$0 \to \mathrm{Hom}_{R_P}(R_P/PR_P, Q^i) \xrightarrow{f} \mathrm{Hom}_{R_P}(R_P/PR_P, I^i) \xrightarrow{g} \mathrm{Hom}_{R_P}(R_P/PR_P, I^{i+1})$$

is exact. Since $I^\bullet$ is minimal, I^i is an essential extension of Q^i, so that by Proposition 20.12, $\mathrm{Hom}_{R_P}(R_P/PR_P, Q^i) \xrightarrow{f} \mathrm{Hom}_{R_P}(R_P/PR_P, I^i)$ is an isomorphism. Thus g is zero. □

Exercise 20.14 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 20.15 Prove that a localization of an injective module over a Noetherian ring is injective.

Exercise 20.16 Let P and Q be prime ideals in a Noetherian ring R with $Q \not\subseteq P$. Prove that $(E_R(R/Q))_P = 0$.

Exercise 20.17 Let P and Q be distinct prime ideals in a Noetherian ring R. Prove that $E_R(R/P) \ncong E_R(R/Q)$.

Exercise 20.18 Let R be a Noetherian ring and let $P \in \mathrm{Spec}\, R$. Prove that $E_R(R/P) \cong E_{R_P}(R_P/PR_P)$ as R_P-modules. Conclude 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 20.19 Let $P \subsetneq Q$ be distinct prime ideals in a Noetherian ring R. Prove that $\mathrm{Hom}_R(E_R(R/P), E_R(R/Q)) \neq 0$, and that $\mathrm{Hom}_R(E_R(R/Q), E_R(R/P)) = 0$.

Exercise 20.20 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 $R/(I_1 \cap I_2) \to (R/I_1) \oplus (R/I_2)$.)

Exercise 20.21 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.

Exercise 20.22 Prove that any two minimal injective resolutions of a module are isomorphic.

21 Structure of injective modules

Theorem 21.1 *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 the 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 20.5, there exists an injective submodule E' of E that is essential over R/P. By Theorem 20.8, $E' \cong E_R(R/P)$, and by Theorem 14.3, $E_R(R/P)$ is a direct summand of E.

Consider the submodules

$$\Lambda = \big\{ \sum_{\alpha \in S} E_R(R/P_\alpha) = \oplus_{\alpha \in S} E_R(R/P_\alpha) : S \big\}.$$

Then $\Lambda \neq 0$ by the previous paragraph. Order Λ by inclusion, etc – Zornify. Let $I = \sum E_R(R/P_\alpha) = \oplus E_R(R/P_\alpha)$ be a maximal element. 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 work of the previous argument, and by maximality of I, necessarily $I' = 0$. $\square$

Theorem 21.2 *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 21.3 *Let (R, m) be a Noetherian local ring. Then every element of $E_R(R/m)$ is annihilated by a power of the maximal ideal.*

Proof. Let x be a non-zero element of $E_R(R/m)$. If $P \in \mathrm{Ass}(Rx)$, then $R/P \subseteq Rx \subseteq E_R(R/m)$, and by Proposition 20.10, $E_R(R/P) \subseteq E_R(E_R(R/m)) = E_R(R/m)$, and by indecomposability established in Theorem 21.2, $E_R(R/P) = E_R(R/m)$. Then by Exercise 20.17, $P = m$.

It follows that m is the only associated prime of the finitely generated module Rx, so that some power of m annihilates x. $\square$

Definition 21.4 *Let (R, m) be a Noetherian local ring and let M be an R-module. The* **socle** *of M is $\mathrm{soc}\,(M) = 0_M :_M m = \mathrm{ann}_M(m)$.*

Proposition 21.5 *Let (R, m) be a Noetherian local ring. For any R-module M, $\mathrm{soc}\,(M)$ is a vector space over R/m.*

(1) If M is Artinian, then $\mathrm{soc}\, M \subseteq M$ is essential.
(2) If M is finitely generated, then $\mathrm{soc}\,(M)$ is a finite dimensional vector space.
(3) $\mathrm{soc}\,(E_R(R/m))$ is a one-dimensional vector space.

Proof. We only prove the last part. We know that R/m is a submodule of $E_R(R/m)$. Let $x \in E_R(R/m)$ be the image of $1 \in R/m$. Let $y \in \mathrm{soc}\,(E_R(R/m))$. By the property of essential modules, $Rx \cap Ry$ is a non-zero submodule of $E_R(R/m)$. Let z be a non-zero element of the intersection. Since both x and y are annihilated by m, necessarily $Rx = Rz = Ry$. $\square$

Exercise 21.6 Let (R, m) be a Noetherian local ring. Show that an R-module M is Artinian if and only if the following two conditions hold:

(1) $\mathrm{soc}\, M$ is a finite-dimensional vector space over R/m,
(2) every element of M is annihilated by a power of m.

Corollary 21.7 *If (R, m) is a Noetherian local ring, then $E_R(R/m)$ is Artinian.*

Proof. Use Exercise 21.6 and the previous two results. (We will give another proof in Corollary 22.6.) $\square$

Exercise 21.8 Let R be a Noetherian ring and let M be a finitely generated R-module. Write $E_R(M) \cong \oplus_{p \in \mathrm{Spec}\, R} E_R(R/p)^{\mu(p,M)}$. Prove that $\mu(p, M) = \dim_{\kappa(p)} \mathrm{Hom}_{R_p}(\kappa(p), M_p)$, 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.

Exercise 21.9 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 21.10__ Let k be a field, 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 21.11 Let R be a Noetherian ring, I an ideal in R, and P a prime ideal containing I. Prove that

$$\operatorname{Hom}_R(R/I, E_R(R/P)) \cong E_{R/I}(R/P).$$

Exercise 21.12 Let R be a Noetherian ring and let M be a finitely generated R-module. Let $I^\bullet$ be an injective resolution of M as in Definition 20.11. Write $I^i = \oplus_{P \in S_i} E_R(R/P)$. Prove that for every $P \in S_{i+1}$ there exists $Q \in S_i$ such that P contains Q.

Exercise 21.13 Let (R, m) be a Noetherian local ring. Let I be an m-primary ideal, and let $E = E_R(R/m)$. Prove that $\operatorname{ann}_E(I)$ is a finitely generated R-module.

22 Duality and injective hulls

Proposition 22.1 *Let (R, m) be a Noetherian local ring. Write $\_^\nu = \operatorname{Hom}_R(\_, E_R(R/m))$. 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 $M \cong R/m$ and $\mathrm{M}^\nu \cong (\mathrm{R/m})^\nu = \operatorname{Hom}_R(R/m, E_R(R/m)) = \operatorname{soc}(E_R(R/m))$ which is a one-dimensional vector space by Proposition 21.5.

Now let $\ell(M) > 1$. There exists an exact sequence $0 \to R/m \to M \to N \to 0$, and $\ell(N) = \ell(M) - 1$. Since $E_R(R/m)$ is injective, $0 \to \mathrm{N}^\nu \to \mathrm{M}^\nu \to (\mathrm{R/m})^\nu \to 0$ is exact, so by induction $\ell(\mathrm{M}^\nu) = \ell(\mathrm{N}^\nu) + 1 = \ell(N) + 1 = \ell(M)$. $\square$

Proposition 22.2 *Let (R, m) be a zero-dimensional Noetherian local ring. Then $\operatorname{Hom}_R(E_R(R/m), E_R(R/m)) \cong R$.*

Proof. Let $E = E_R(R/m)$. 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 again by the previous result, $\ell(\mathrm{E}^\nu) = \ell(R)$, 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 21.11, $E_{R/rR}(R/m) \cong E$. By Proposition 22.1 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. $\square$

Proposition 22.3 *Let (R, m) be a Noetherian local ring. Let $E = E_R(R/m)$. Then*

$$\mathrm{Hom}_R(E, E) \cong \widehat{R} = \lim_{\leftarrow} R/m^n.$$

Proof. Let $E_n = \{x \in E : m^n x = 0\}$.

Observe:

(1) $E_1 \subseteq E_2 \subseteq E_3 \subseteq \cdots \subseteq E$, and by Proposition 21.3, $\cup_n E_n = E$.

(2) If $f \in \mathrm{Hom}_R(E, E)$, 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) $\{\mathrm{Hom}_R(E_n, E_n)\}$ form an inverse system as any $g \in \mathrm{Hom}_R(E_{n+1}, E_{n+1})$ maps to $\mathrm{Hom}_R(E_n, E_n)$ by restriction.

(4) Claim: $\mathrm{Hom}_R(E, E) \cong \lim_{\leftarrow} \mathrm{Hom}_R(E_n, E_n)$. Certainly any $f \in \mathrm{Hom}_R(E, E)$ 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 $\{f_n\} \in \lim_{\leftarrow} \mathrm{Hom}_R(E_n, E_n)$, we can define $f : E \to E$ in the obvious way. This proves the claim.

Observe that $E_n = \{x \in E : m^n x = 0\} = \mathrm{Hom}_R(R/m^n, E)$. By Exercise 21.11, $E_n \cong E_{R/m^n}(R/m)$. By Proposition 22.2, $\mathrm{Hom}_R(E_n, E_n) = \mathrm{Hom}_{R/m^n}(E_n, E_n) \cong R/m^n$. Finally,

$$\mathrm{Hom}_R(E, E) \cong \lim_{\leftarrow} \mathrm{Hom}_R(E_n, E_n) \cong \lim_{\leftarrow} R/m^n \cong \widehat{R}.$$

(Well, we need to check that the following square commutes:

$$\begin{array}{ccc} \mathrm{Hom}_R(E_{n+1}, E_{n+1}) & \to & \mathrm{Hom}_R(E_n, E_n) \\ \downarrow & & \downarrow \\ R/m^{n+1} & \to & R/m^n \end{array}$$

But all we need to check is that the identiy of $\mathrm{Hom}_R(E_{n+1}, E_{n+1})$ comes to the same end either way, but this is easy.) □

Remark 22.4 $E_R(R/m)$ is a module over $\widehat{R}$.

Proof. Let $\{r_n\}$ be a Cauchy sequence in R, with $r_n - r_{n+1} \in m^n$ for all n. Let $x \in E$. By Proposition 21.3, there exists $l \in \mathbb{N}$ such that $m^l x = 0$. Thus we define $\{r_n\}x = r_l x$, and this works. □

Proposition 22.5 *Let (R, m) be a Noetherian local ring and let M be an R-module. Then $M = 0$ if and only if* $\mathrm{M}^\nu = 0$.

Proof. 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 $(\mathrm{Rx})^\nu = 0$. So by possibly replacing M by Rx, it suffices to prove the proposition in case M is generated by one element. But then $M/mM \cong R/m$, whence $(\mathrm{R/m})^\nu \cong \mathrm{M}^\nu$, so that Proposition 22.1, R/m embeds in M^ν, so M^ν is non-zero. □

The following was already proved in Corollary 21.7:

Corollary 22.6 *Let (R, m) be a Noetherian local ring. Then $E_R(R/m)$ is Artinian.*

Proof. Let $M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$ be a descending chain of submodules of $E = E_R(R/m)$. Then $\widehat{R} \cong \mathrm{E}^\nu \twoheadrightarrow \mathrm{M}_0^\nu \twoheadrightarrow \mathrm{M}_1^\nu \twoheadrightarrow \cdots$, so that $\mathrm{M}_\mathrm{i}^\nu = \widehat{R}/I_n$ 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 $n \geq l$. It follows that $\mathrm{M_l}/\mathrm{M}_\mathrm{n}^\nu = 0$, so that by the proposition above, $M_l = M_n$ for all $n \geq l$. $\square$

Exercise 22.7 Let (R, m) be a Noetherian local ring. Prove that $E_R(R/m) \otimes_R \widehat{R} \cong E_R(R/m)$.

This exercise enables us to formulate and prove Matlis duality next.

Theorem 22.8 (Matlis duality) *Let (R, m) be a Noetherian local ring. 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 $\mathrm{Hom}_{\widehat{R}}(M, E_R(R/m)) = \mathrm{M}^\nu$ is an Artinian R-module.

(2) If N is an Artinian R-module, then $\mathrm{Hom}_R(N, E_R(R/m)) = \mathrm{N}^\nu$ 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 21.5, N embeds in E^n. Then $\widehat{R}^n \cong (\mathrm{N}^\nu)^n$ 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 $a, b \in \mathbb{N}$, and similar reasoning as in the previous paragraph shows that $N = \mathrm{N}^{\nu\nu}$. $\square$

Exercise 22.9 Let (R, m) be a Noetherian local ring. Show that $\operatorname{ann}(E_R(R/m)) = 0$. (Hint: consider $R/\operatorname{ann} E \to \operatorname{Hom}_R(E_R(R/m), E_R(R/m)) \to \widehat{R}$.)

Exercise 22.10 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 22.11 Let (R, m) be a Noetherian local ring, let $E = E_R(R/m)$, and let M be an R-module of finite length. Show that $\mu(M) = \dim_{R/m} \operatorname{soc}(\operatorname{Hom}_R(M, E))$.

Exercise 22.12 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.

23 More on injective resolutions

We have seen that any left R-module has an injective resolution.

Definition 23.1 *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.*

The following two Schanuel-lemma type results for injectives have proofs essential dual to those of Theorem 3.4 and Theorem 3.5:

Theorem 23.2 (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 $I \oplus L \cong E \oplus K$.* □

Theorem 23.3 (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, $K \oplus E_{odd} \oplus I_{even} \cong L \oplus E_{even} \oplus I_{odd}$. □

Theorem 23.4 *Let (R,m) be a Noetherian local ring, and let $E = E_R(R/m)$. Then any Artinian R-module M has an injective resolution in which each injective module is a finite direct sum of copies of E, and if M has finite injective dimension, then M has an injective resolution of the form*

$$0 \to M \to E^{b_0} \to E^{b_1} \to E^{b_2} \to \cdots \to E^{b_{n-1}} \to E^{b_n} \to 0$$

for some $b_i \in \mathbb{N}$.

Proof. By Proposition 21.5, $\operatorname{soc} M \subseteq M$ is essential. Since M is Artinian, by Exercise 21.6, $\operatorname{soc} M$ is a finite-dimensional module over R/m, so that $\operatorname{soc} M$ has a maximal essential extension E^n for some $n \in \mathbb{N}$, whence the essential extension M of $\operatorname{soc} M$ embeds in E^n, and 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 n. Let $0 \to M \to I^0 \to \cdots \to I^n \to 0$ 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 $E^{b_{n-2}} \to E^{b_{n-1}}$. Then $0 \to M \to E^{b_0} \to E^{b_1} \to \cdots \to E^{b_{n-2}} \to E^{b_{n-1}} \to C \to 0$ is exact. By Schanuel's lemma (Theorem 23.3), 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 $b_{n+1} = 0$. □

Proposition 23.5 *Let (R,m) be a Noetherian ring, let $E = E_R(R/m)$, 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 free resolution of M^ν over $\widehat{R}$, where $\_^\nu = \operatorname{Hom}_R(\_, E)$.*

In particular, by Matlis duality, $\operatorname{injdim}_R(M) = \operatorname{pd}_{\widehat{R}}(\mathrm{M}^\nu)$.

Proof. By Theorem 23.4, each I^i is a direct sum of copies of $E_R(R/m)$. Since E is injective, $(\mathrm{I}^\bullet)^\nu \to \mathrm{M}^\nu \to 0$ is exact. prime ideals of R. By Exercise 20.19, $(\mathrm{I}^\mathrm{i})^\nu$ is a direct sum of copies of $\mathrm{E_R(R/m)}^\nu = \widehat{R}$, hence a free $\widehat{R}$-module, so that M^ν has finite projective dimension, and furthermore $\operatorname{pd}_{\widehat{R}} \mathrm{M}^\nu \leq \operatorname{injdim}_R M$. 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 23.6 *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 $J^i = \operatorname{Hom}_R(R/xR, I^{i+1})$ 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 $\operatorname{injdim}_{R/xR}(M/xM) \leq \operatorname{injdim}_R M - 1$.*

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 $\operatorname{Hom}_R(R/xR, \_)$ to the injective part to get

$$0 \to \operatorname{Hom}_R(R/xR, I^0) \to \operatorname{Hom}_R(R/xR, I^1) \to \cdots.$$

By Proposition 14.4, each $\operatorname{Hom}_R(R/xR, I^i)$ is an injective module over R/xR. The ith cohomology of the displayed cocomplex is $\operatorname{Ext}^i_R(R/xR, M)$. As a projective resolution of the R-module R/xR is $0 \to R \xrightarrow{x} R \to 0$, it follows that $\operatorname{Ext}^i_R(R/xR, M) = 0$ for $i \geq 2$, that $\operatorname{Ext}^1_R(R/xR, M) = \operatorname{Hom}_R(R, M)/x \operatorname{Hom}_R(R, M) \cong M/xM$, and that $\operatorname{Ext}^0_R(R/xR, M) = \operatorname{Hom}_R(R/xR, M) = 0$. In particular, in the cocomplex above, $\operatorname{Hom}_R(R/xR, I^0)$ injects into $\operatorname{Hom}_R(R/xR, I^1)$, so that $\operatorname{Hom}_R(R/xR, I^1) \cong \operatorname{Hom}_R(R/xR, I^0) \oplus E$ for some necessarily injective (R/xR)-module E, so that the displayed cocomplex yields the following cocomplex with the same cohomology:

$$0 \to E \xrightarrow{d_2|_E} \operatorname{Hom}_R(R/xR, I^2) \to \cdots.$$

In particular, the cohomology at E is $M/xM = \ker(d_2|_E)$, and the cohomology elsewhere is 0. Thus $0 \to M/xM \to J^\bullet$ is an exact cocomplex of (R/xR)-modules, which finishes the proof. $\square$

Corollary 23.7 (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 $i \geq 0$,*

$$\operatorname{Ext}^{i+1}_R(N, M) \cong \operatorname{Ext}^i_{R/xR}(N, M/xM).$$

Proof. Let $I^\bullet$ and $J^\bullet$ be as in Proposition 23.6. Then for $i \geq 0$,

$$\begin{aligned}
\operatorname{Ext}^{i+1}_R(N, M) &= \frac{\ker(\operatorname{Hom}_R(N, I^{i+1}) \to \operatorname{Hom}_R(N, I^{i+2}))}{\operatorname{im}(\operatorname{Hom}_R(N, I^i) \to \operatorname{Hom}_R(N, I^{i+1}))} \\
&\cong \frac{\ker(\operatorname{Hom}_R(N \otimes_R (R/xR), I^{i+1}) \to \operatorname{Hom}_R(N \otimes_R (R/xR), I^{i+2}))}{\operatorname{im}(\operatorname{Hom}_R(N \otimes_R (R/xR), I^i) \to \operatorname{Hom}_R(N \otimes_R (R/xR), I^{i+1}))} \\
&\cong \frac{\ker(\operatorname{Hom}_{R/xR}(N, \operatorname{Hom}_R(R/xR, I^{i+1})) \to \operatorname{Hom}_{R/xR}(N, \operatorname{Hom}_R(R/xR, I^{i+2})))}{\operatorname{im}(\operatorname{Hom}_{R/xR}(N, \operatorname{Hom}_R(R/xR, I^i)) \to \operatorname{Hom}_{R/xR}(N, \operatorname{Hom}_R(R/xR, I^{i+1})))} \\
&= \frac{\ker(\operatorname{Hom}_{R/xR}(N, J^i) \to \operatorname{Hom}_{R/xR}(N, J^{i+1}))}{\operatorname{im}(\operatorname{Hom}_{R/xR}(N, J^{i-1}) \to \operatorname{Hom}_{R/xR}(N, J^i))} \\
&\cong \operatorname{Ext}^i_{R/xR}(N, M/xM),
\end{aligned}$$

where the third equality is due to the tensor-hom adjointness. $\square$

Proposition 23.8 *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

$$\cdots \to \operatorname{Ext}_R^n(R/I, M) \xrightarrow{x} \operatorname{Ext}_R^n(R/I, M) \to \operatorname{Ext}_R^n(R/I, M/xM) \to \operatorname{Ext}_R^{n+1}(R/I, M) \xrightarrow{x} \operatorname{Ext}_R^{n+1}(R/I, M)$$

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. □

Corollary 23.9 *If M is a finitely generated module over a Noetherian local ring (R, m), then for any ideal I in R, $\operatorname{injdim}_R(M) \geq \operatorname{depth}_I(M)$.* □

Proposition 23.10 *If M is a finitely generated module over a Noetherian local ring (R, m), then $\operatorname{depth} R \leq \operatorname{injdim}_R(M)$.*

Proof. Let $x_1, \ldots, x_d \in m$ be a maximal regular sequence on R. Then

$$\operatorname{Ext}_R^d(R/(x_1, \ldots, x_d), M) = H^d(\operatorname{Hom}_R(K_\bullet(x_1, \ldots, x_d; R), M)) \cong M/(x_1, \ldots, x_d)M \neq 0,$$

so that $\operatorname{injdim}_R(M) \geq d = \operatorname{depth} R$. □

Lemma 23.11 *Let (R, m) be a Noetherian local ring, let N be a finitely generated R-module, and let $n \in \mathbb{N}$. Then $\operatorname{injdim}_R(N) \leq n$ if and only if $\operatorname{Ext}_R^j(M, N) = 0$ 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 16.3, $\operatorname{Ext}_R^j(M, C) \cong \operatorname{Ext}_R^{j+n}(M, N)$ for all $j \geq 1$. From the assumption we then get that $\operatorname{Ext}_R^j(M, C) = 0$ 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:

$$0 \to \operatorname{Hom}_R(M'', C) \to \operatorname{Hom}_R(M, C) \to \operatorname{Hom}_R(M', C) \to 0 = \operatorname{Ext}_R^1(M'', C),$$

so that $\operatorname{Hom}_R(\_, C)$ is exact on finitely generated R-modules, sot that by Baer's criterion Theorem 14.6, C is injective. It follows that $\operatorname{injdim} N \leq n$. $\square$

Theorem 23.12 *Let (R, m) be a Noetherian local ring, let N be a finitely generated R-module. Then $\operatorname{injdim}_R(N) = \sup\{l : \operatorname{Ext}_R^l(R/m, N) \neq 0\}$.*

Proof. Clearly $\operatorname{injdim}_R(N) \geq \sup\{l : \operatorname{Ext}_R^l(R/m, N) \neq 0\}$, so if the latter is infinity, N must not have finite injective dimension. So we may assume that $n = \sup\{l : \operatorname{Ext}_R^l(R/m, N) \neq 0\} \in \mathbb{N}$.

Claim: $\operatorname{Ext}_R^j(M, N) = 0$ for all $j > n$ and all finitely generated R-modules. Proof of the claim: If $M = R/m$, 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 $0 \to R/m \to M \to C \to 0$. 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 $\operatorname{Ext}_R^j(R/P, N) = 0$ 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:

$$\operatorname{Ext}_R^{n+j}(L, N) \to \operatorname{Ext}_R^{n+j}(R/P, N) \xrightarrow{s} \operatorname{Ext}_R^{n+j}(R/P, N) \to \operatorname{Ext}_R^{n+j+1}(L, N).$$

By induction on the dimension of the module in the first entry, $\operatorname{Ext}_R^{n+j}(L, N)$ and $\operatorname{Ext}_R^{n+j+1}(L, N)$ are zero. Hence $\operatorname{Ext}_R^{n+j}(R/P, N) = s \operatorname{Ext}_R^{n+j}(R/P, N)$, and $\operatorname{Ext}_R^{n+j}(R/P, N)$ is a finitely generated R-module, so by Nakayama's lemma, $\operatorname{Ext}_R^{n+j}(R/P, N) = 0$. This proves the claim.

But then by Lemma 23.11, N has injective dimension at most n. $\square$

Theorem 23.13 *Let (R, 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 $s \in m \setminus P$ and let $x \in N$ be the image of $1 \in R/P$. Then by Exercise 20.18, $x/s, x/s^2, x/s^3, \dots$ 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 $(1-rs)x = 0 \in E_R(R/P)$, so that $1 - rs \in P \subseteq m$, which is a contradiction. Thus $N = E_R(R/m)^n$ 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 $x_1, \dots, x_n \in m$ be a maximal regular sequence on R. Then we have a short exact sequence $0 \to R/m \to R/(x_1, \dots, x_n) \to R/I \to 0$ for some ideal I, whence by Theorem 23.12 we get a long exact sequence

$$\cdots \to \operatorname{Ext}^l_R(R/I, N) \to \operatorname{Ext}^l_R(R, N) \to \operatorname{Ext}^l_R(R/m, N) \to 0,$$

where $\operatorname{Ext}^l_R(R/m, N) \neq 0$, but $\operatorname{Ext}^l_R(R, N) = 0$, which gives a contradiction. Thus $\operatorname{depth} R \geq \operatorname{injdim}_R N$. Proposition 23.10 proves the other inequality. □

Exercise 23.14 (Ischebeck) Let (R, m) be a Noetherian local ring, and let M and N be finitely generated R-module such that N has finite injective dimension. Prove that $\operatorname{depth} R - \dim M = \sup \{l : Ext^l_R(M, N) \neq 0\}$.

Exercise 23.15 Let (R, m) be a Noetherian local ring. Suppose that R/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 23.16 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 $IM'' \neq M''$. Prove some I-depth inequalities on these modules. Note to self: HERE be explicit.

24 Gorenstein rings

Definition 24.1 *A Noetherian local ring (R, m) is* **Gorenstein** *if* $\operatorname{id}_R(R) < \infty$. *A Noetherian ring R is* **Gorenstein** *if for any maximal ideal m of R, R_m is Gorenstein.*

Proposition 24.2 *If R is a Gorenstein ring, then for any non-zerodivisor $x \in R$, R/xR is Gorenstein.*

Proof. This follows from Proposition 23.6. □

Theorem 24.3 *Every regular ring is Gorenstein.*

Proof. It suffices to prove that any regular local ring (R, m) is Gorenstein. By Theorem 13.2, 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 23.11, $\mathrm{injdim}_R(R) \le \dim R$. $\square$

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 23.13 we even know that for a complete intersection ring R, $\mathrm{injdim}_R R = \mathrm{depth}\, R = \dim R$.

Theorem 24.4 *Let (R, m) be a 0-dimensional Noetherian local ring. The following are equivalent:*

(1) $R \cong E_R(R/m)$.
(2) *R is Gorenstein.*
(3) $\dim_{R/m}(\mathrm{soc}\, R) = 1$.
(4) (0) *is an irreducible ideal in R (cannot be written as an intersection of two strictly larger ideals).*

Proof. Let $E = E_R(R/m)$.

Certainly (1) implies (2) and (3) (the latter by Proposition 21.5).

Assume (3). Let $\mathrm{soc}\,(R) = (x)$. Let I be a non-zero ideal in R. Since R is Artinian, $m^l = 0$ for some l, and in particular, we may choose a least integer l such that $m^l I = 0$. Then $0 \ne m^{l-1} I \subseteq \mathrm{soc}\, R$. Necessarily $x \in m^{l-1} I \subseteq I$, and similarly $x \in J$. Thus the intersection of two non-zero ideals cannot be zero. Thus (4) holds.

If (4) holds and $\dim_{R/m}(\mathrm{soc}\, R) > 1$, 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 21.5, $\mathrm{soc}\, R \subseteq R$ is an essential extension. If $\mathrm{soc}\, R$ is one-dimensional, this says that R is essential over a homomorphic image of R/m, so that the essential extension R of R/m injects in the maximal essential extension E of R/m. But R has finite length, so by Proposition 22.1, $\ell(R) = \ell(\mathrm{R}^\nu) = \ell(E)$, whence $R \cong E$. This proves (1).

Now assume (2). By Theorem 23.4, 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 $b_i \in \mathbb{N}$. Apply the dual $\_^\nu = \mathrm{Hom}_R(\_, E)$ to get the exact sequence

$$0 \to (\mathrm{E^{b_n}})^\nu \to \cdots \to (\mathrm{E^{b_1}})^\nu \to (\mathrm{E^{b_0}})^\nu \to \mathrm{R}^\nu \to 0,$$

and so by Proposition 22.2,

$$0 \to R^{b_n} \to \cdots \to R^{b_1} \to R^{b_0} \to E \to 0$$

is exact, so that E is finitely generated and has finite projective dimension over R. Thus by the Auslander–Buchsbaum formula, $\operatorname{pd}_R E + \operatorname{depth} E = \operatorname{depth} R = 0$, whence $\operatorname{pd}_R E = 0$, so E is projective and hence free over R. Thus $E \cong R^l$ for some l, but by Proposition 22.1, $\ell(E) = \ell(\mathrm{R}^\nu) = \mathrm{R}^\nu$, necessarily $l = 1$. This proves (1), and finishes the proof of the theorem. □

Theorem 24.5 *Let (R, 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/m)-vector space $((x_1, \ldots, x_d) : m)/(x_1, \ldots, x_d)$ 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 23.13, R is Artinian, so (2) and (3) hold by the previous theorem. So assume that $\operatorname{injdim}_R R > 0$. Then by Theorem 23.13, $\operatorname{depth} R > 0$. Let $x \in m$ be a non-zerodivisor. Then by Proposition 23.6, R/xR is a Gorenstein ring, so by induction on $\operatorname{depth} R$, 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 12.2, every system of parameters in R is a regular sequence, and by Proposition 23.6, (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 $j > d$, $\operatorname{Ext}^j_R(R/m, R) \cong \operatorname{Ext}^{j-d}_{R/(x_1,\ldots,x_d)}(R/m, R/(x_1, \ldots, x_d))$ by Corollary 23.7. Since by assumption $R/(x_1, \ldots, x_d)$ is Gorenstein and so an injective module over itself, $\operatorname{Ext}^{j-d}_{R/(x_1,\ldots,x_d)}(R/m, R/(x_1, \ldots, x_d)) = 0$. Since this holds for all $j > d$, by Theorem 23.12 says that $\operatorname{id}_R(R) \le d$, so that R is Gorenstein. □

Proposition 24.6 *Let (S, n) be a regular local ring, and let $R = S/I$ be a zero-dimensional quotient of S, with minimal free S-resolution*

$$0 \to F_d \to F_{d-1} \to \cdots \to F_0 \to R.$$

Then R is Gorenstein if and only if $F_d \cong S$.

Proof. By the Auslander–Buchsbaum formula, $d = \operatorname{pd}_S(R) = \operatorname{depth} S - \operatorname{depth} R = \operatorname{depth} S = \dim S$. By Exercise 7.8, $\operatorname{rank} F_d = \dim_{S/n} \operatorname{Tor}^S_d(R, S/n)$. But $\operatorname{Tor}^S_d(R/S/n) \cong H_d(S/I \otimes_S K_\bullet(y_1, \ldots, y_d; S))$, where $n = (y_1, \ldots, y_d)$. 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 24.5:

Theorem 24.7 *Every Gorenstein ring is Cohen–Macaulay.* □

Example 24.8 If (S, 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 24.9 Let (S, n) be a regular local ring of dimension d, and let $n = (y_1, \ldots, y_d)$. 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 24.10 Let (R, m) be a Cohen–Macaulay local ring. Let $x_1, \ldots, x_d$ be a system of parameters. Prove that $\dim \operatorname{soc}(\frac{R}{(x_1,\ldots,x_d)}) = \dim_{R/m} \operatorname{Ext}^d_R(R/m, R)$, and hence is independent of the system of parameters. This number is called the **Cohen–Macaulay type** of R.

Exercise 24.11 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 $\dim \operatorname{soc}(\frac{R}{(x_1,\ldots,x_d)}) \neq \dim \operatorname{soc}(\frac{R}{(y_1,\ldots,y_d)})$.

Exercise 24.12 Let (R, m) be a Gorenstein local ring. Prove that $\operatorname{injdim}_R(R) = \dim R = \operatorname{depth} R$.

25 Bass numbers

This section lacks details.

Definition 25.1 *Let M be a finitely generated module over a Noetherian ring R. Let $I^\bullet$ be any minimal injective resolution of M (recall Definition 20.11). 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 20.22 and possibly more work, Bass numbers are well-defined.

Proposition 25.2 $\mu_i(P, M) = \dim_{R_P/PR_P} \operatorname{Ext}^i_{R_P}(R_P/PR_P, I^i_P)$.

Proof. Let $I^\bullet$ be a minimal injective resolution of M. By Exercise 20.15, $(I^\bullet)_P$ is an injective resolution of M_P. By Remark 20.2 (and the definition of injective resolutions), $(I^\bullet)_P$ is a minimal injective resolution of M_P.

By Theorem 21.2, I^j is a direct sum of indecomposable injective modules of the form $E_R(R/Q)$ with Q prime ideals. By Exercises 20.16 and 20.18, $(I_j)_P$ 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 20.13 all the maps in the complex $\mathrm{Hom}_R(R/\mathfrak{m}, I^\bullet)$ are 0. Thus $\mu_i(\mathfrak{m}, M) = \dim_{R/\mathfrak{m}} \mathrm{Ext}^i_R(R/\mathfrak{m}, M)$. $\square$

The proof above shows the following:

Corollary 25.3 *If R is Noetherian local with maximal ideal m, then* $\mathrm{Ext}^i_R(R/m, M) = H^i(\mathrm{Hom}_R(R/m, I^\bullet)) \cong \mathrm{Hom}_R(R/m, I^i) = \mu_i(m, M)$. $\square$

Corollary 25.4 *If (R, m) is a Noetherian ring and M a finitely generated R-module, then $\mu_i(P, M) < \infty$ for all i and all $P \in \mathrm{Spec}\, R$.* $\square$

Exercise 25.5 Prove that the following are equivalent for a Noetherian local ring (R, m):

(1) R is Gorenstein.
(2) R is Cohen–Macaulay and of type 1.
(3) R is Cohen–Macaulay and $\mu_{\dim R}(m, R) = 1$.

Exercise 25.6 Let (R, m) be a Cohen–Macaulay local ring. Prove that $\mu_i(m, R) = 0$ for all $i \neq \dim R$.

Exercise 25.7 Let (R, m) be Gorenstein local ring of dimension d.

(1) Prove that for all $P \in \mathrm{Spec}\, R$, $\mu_i(P, R) = 0$ for all $i \neq \mathrm{ht}\, P$.
(2) Prove that a minimal injective resolution of R looks like:

$$0 \to R \to \oplus_{\mathrm{ht}\, P=0} E_R(R/P) \to \oplus_{\mathrm{ht}\, P=1} E_R(R/P) \to \cdots \to \oplus_{\mathrm{ht}\, P=d} E_R(R/P) \to 0.$$

(The maps are not easy to understand.)

Definition 25.8 *The* **injective type** *of a Noetherian local ring (R, m) of dimension d is $\mu_d(m, R)$.*

Remark 25.9 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.

26 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 26.1 *Let $\varphi : R^n \to R^m$ be a module homomorphism, and let M be an R-module. By the* **rank** *of φ we mean the largest integer r such that $I_r(\varphi) \notin \operatorname{ann} M$. We denote this number* $\operatorname{rank}(\varphi, M)$. *Note that by convention* $\operatorname{rank}(\varphi, M) \geq 0$. *Furthermore, 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 26.2 *If I is an ideal in R and M is an R-module, we set* $\operatorname{depth}_I(M) = \inf\{l \in \mathbb{N} : \operatorname{Ext}^l_R(R/I, M) \neq 0\}$. *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 23.8.

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 26.8) that the same equality also holds for general M.

Theorem 26.3 (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 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 an $d \times d$ submatrix of A such that m times its minor 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.

If $(x_1, \ldots, x_n) \in M^n$ is 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 $n < d$. $\square$

Theorem 26.4 (Acyclicity lemma, due to Peskine and Szpiro, ‘’) *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 26.5 *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

$F \overset{\alpha}{\to} \ker\beta$ 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 26.6 (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*

$$F_\bullet : \quad 0 \to F_n \overset{\delta_n}{\to} F_{n-1} \overset{\delta_{n-1}}{\longrightarrow} \cdots \to F_2 \overset{\delta_2}{\to} F_1 \overset{\delta_1}{\to} F_0,$$

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 26.5 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 26.4) to get that $F_\bullet \otimes M$ is exact.

Now suppose that $F_\bullet \otimes_R M$ is exact. By Theorem 26.3, $0 :_M (I_{\operatorname{rank} F_n}(\delta_n)) = 0$, 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 26.5, 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 $M/(x_1, \ldots, x_l)M$. 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 $M/(x_1, \ldots, x_l)M$. 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 $0 \to F_n \xrightarrow{\delta_n} F_{n-1} \to 0$ 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 $\mathrm{Ext}^l(R/m, M)$, we have that the last map in the display above is not injective. Thus $\mathrm{depth}_m(\mathrm{im}\,\delta_{n-1} \otimes M) = l - 1$.

By exactness assumption, $\ker(\delta_{n-i} \otimes \mathrm{id}_M) = \mathrm{im}(\delta_{n-i+1} \otimes \mathrm{id}_M)$. The short exact sequences $0 \to \mathrm{im}(\delta_{n-i+1} \otimes \mathrm{id}_M) \to F_{n-i} \otimes M \to \mathrm{im}(\delta_{n-i} \otimes \mathrm{id}_M) \to 0$ for $i = 2, \ldots, l$ and the long exact sequences on cohomology then give that for all $\mathrm{depth}_m(\mathrm{im}\,\delta_{n-i} \otimes M) = l - i$. In particular, $\mathrm{depth}_m(\mathrm{im}\,\delta_{n-l} \otimes M) = 0$. 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 26.7 (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 26.8 Let R be a Noetherian ring, and let I be an ideal in R. Prove or disprove the following (using Definition 26.2):

(1) If $I \subseteq J$, then $\mathrm{depth}_I(M) \le \mathrm{depth}_J(M)$.
(2) $\mathrm{depth}_I(M) = \mathrm{depth}_{I+\mathrm{ann}(M)}(M)$.
(3) $\mathrm{depth}_I(M) = \mathrm{depth}_{I(R/\mathrm{ann}\,M)}(M)$.
(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 26.9 Use Theorem 26.6 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

$$F_\bullet : \qquad 0 \to R \xrightarrow{x} R \xrightarrow{y} R \xrightarrow{x} R \xrightarrow{y} R \xrightarrow{x} R.$$

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. 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`.