CHAPTER XXI

Finite Free Resolutions

This chapter puts together specific computations of complexes and homology. Partly these provide examples for the general theory of Chapter XX, and partly they provide concrete results which have occupied algebraists for a century. They have one aspect in common: the computation of homology is done by means of a finite free resolution, i.e. a finite complex whose modules are finite free.

The first section shows a general technique (the mapping cylinder) whereby the homology arising from some complex can be computed by using another complex which is finite free. One application of such complexes has already been given in Chapter X, putting together Proposition 4.5 followed by Exercises 10–15 of that chapter.

Then we go to major theorems, going from Hilbert's Syzygy theorem, from a century ago, to Serre's theorem about finite free resolutions of modules over polynomial rings, and the Quillen-Suslin theorem. We also include a discussion of certain finite free resolutions obtained from the Koszul complex. These apply, among other things, to the Grothendieck Riemann-Roch theorem of algebraic geometry.

Bibliographical references refer to the list given at the end of Chapter XX.

§1. SPECIAL COMPLEXES

As in the preceding chapter, we work with the category of modules over a ring, but the reader will notice that the arguments hold quite generally in an abelian category.

In some applications one determines homology from a complex which is not suitable for other types of construction, like changing the base ring. In this section, we give a general procedure which constructs another complex with better properties than the first one, while giving the same homology. For an application to Noetherian modules, see Exercises 12–15 of Chapter X.

Let $f\colon K \to C$ be a morphism of complexes. We say that f is a **homology isomorphism** if the natural map

$$H(f): H(K) \to H(C)$$

is an isomorphism. The definition is valid in an abelian category, but the reader may think of modules over a ring, or abelian groups even. A family $\mathfrak{F}$ of objects will be called **sufficient** if given an object E there exists an element F in $\mathfrak{F}$ and an epimorphism

$$F \to E \to 0,$$

and if $\mathfrak{F}$ is closed under taking finite direct sums. For instance, we may use for $\mathfrak{F}$ the family of free modules. However, in important applications, we shall deal with finitely generated modules, in which case $\mathfrak{F}$ might be taken as the family of finite free modules. These are in fact the applications I have in mind, which resulted in having axiomatized the situation.

Proposition 1.1. *Let C be a complex such that $H^p(C) \neq 0$ only for $0 \leqq p \leqq n$. Let $\mathfrak{F}$ be a sufficient family of projectives. There exists a complex*

$$0 \to K^0 \to K^1 \to \cdots \to K^n \to 0$$

such that:

$$K^p \neq 0 \quad \text{only for} \quad 0 \leqq p \leqq n;$$

$$K^p \text{ is in } \mathfrak{F} \text{ for all } p \geqq 1;$$

and there exists a homomorphism of complexes

$$f: K \to C$$

which is a homology isomorphism.

Proof. We define f_m by descending induction on m:

$$\begin{array}{ccccccccc}
\longrightarrow & K^m & \longrightarrow & K^{m+1} & \xrightarrow{\delta_K^{m+1}} & K^{m+2} & \longrightarrow \\
 & \downarrow{\scriptstyle f_m} & & \downarrow{\scriptstyle f_{m+1}} & & \downarrow{\scriptstyle f_{m+2}} & \\
\longrightarrow & C^m & \longrightarrow & C^{m+1} & \xrightarrow[\delta_C^{m+1}]{} & C^{m+2} & \longrightarrow
\end{array}$$

We suppose that we have defined a morphism of complexes with $p \geqq m + 1$ such that $H^p(f)$ is an isomorphism for $p \geqq m + 2$, and

$$f_{m+1}: Z^{m+1}(K) \to H^{m+1}(C)$$

is an epimorphism, where Z denotes the cycles, that is Ker δ. We wish to construct K^m and f_m, thus propagating to the left. First let $m \geqq 0$. Let B^{m+1} be the kernel of

$$\text{Ker } \delta_K^{m+1} \to H^{m+1}(C).$$

Let K' be in $\mathfrak{F}$ with an epimorphism

$$\delta' : K' \to B^{m+1}.$$

Let $K'' \to H^m(C)$ be an epimorphism with K'' in $\mathfrak{F}$, and let

$$f'' : K'' \to Z^m(C)$$

be any lifting, which exists since K'' is projective. Let

$$K^m = K' \oplus K''$$

and define $\delta^m : K^m \to K^{m+1}$ to be δ' on K' and 0 on K''. Then

$$f_{m+1} \circ \delta'(K') \subset \delta_C(C_m),$$

and hence there exists $f' : K' \to C^m$ such that

$$\delta_C \circ f' = f_{m+1} \circ \delta'.$$

We now define $f_m : K^m \to C^m$ to be f' on K' and f'' on K''. Then we have defined a morphism of complexes truncated down to m as desired.

Finally, if $m = -1$, we have constructed down to K^0, δ^0, and f_0 with

$$K^0 \xrightarrow{f_0} H^0(C) \to 0$$

exact. The last square looks like this, defining $K^{-1} = 0$.

$$\begin{array}{ccccc} 0 & \longrightarrow & K' \oplus K'' & \xrightarrow{\delta_0 = \delta'} & \delta' K' \subset K^1 \\ & & f' \searrow \ \swarrow f'' & & \downarrow f_1 \\ 0 & \longrightarrow & C^0 & \longrightarrow & C^1 \end{array}$$

We replace K^0 by $K^0/(\text{Ker } \delta^0 \cap \text{Ker } f_0)$. Then $H^0(f)$ becomes an isomorphism, thus proving the proposition.

We want to say something more about K^0. For this purpose, we define a new concept. Let $\mathfrak{F}$ be a family of objects in the given abelian category (think of modules in first reading). We shall say that $\mathfrak{F}$ is **complete** if it is sufficient, and for any exact sequence

$$0 \to F' \to F \to F'' \to 0$$

with F'' and F in $\mathfrak{F}$ then F' is also in $\mathfrak{F}$.

Example. In Chapter XVI, Theorem 3.4 we proved that the family of finite flat modules in the category of finite modules over a Noetherian ring is complete. Similarly, the family of flat modules in the category of modules over a ring is complete. We cannot get away with just projectives or free modules, because in the statement of the proposition, K^0 is not necessarily free but we want to include it in the family as having especially nice properties. In practice, the family consists of the flat modules, or finite flat modules. Cf. Chaper X, Theorem 4.4, and Chapter XVI, Theorem 3.8.

Proposition 1.2. *Let $f: K \to C$ be a morphism of complexes, such that K^p, $H^p(C)$ are $\neq 0$ only for $p = 1, \dots, n$. Let $\mathfrak{F}$ be a complete family, and assume that K^p, C^p are in $\mathfrak{F}$ for all p, except possibly for K^0. If f is a homology isomorphism, then K^0 is also in $\mathfrak{F}$.*

Before giving the proof, we define a new complex called the **mapping cylinder** of an arbitrary morphism of complexes f by letting

$$M^p = K^p \oplus C^{p-1}$$

and defining $\delta_M : M^p \to M^{p+1}$ by

$$\delta_M(x, y) = (\delta x, fx - \delta y).$$

It is trivially verified that M is then a complex, i.e. $\delta \circ \delta = 0$. If C' is the complex obtained from C by shifting degrees by one (and making a sign change in δ_C), so $C'^p = C^{p-1}$, then we get an exact sequence of complexes

$$0 \to C' \to M \to K \to 0$$

and hence the **mapping cylinder exact cohomology sequence**

$$\begin{array}{ccccccccc} H^p(K) & \longrightarrow & H^{p+1}(C') & \longrightarrow & H^{p+1}(M) & \longrightarrow & H^{p+1}(K) & \longrightarrow & H^{p+2}(C') \\ & & \| & & & & & & \| \\ & & H^p(C) & & & & & & H^{p+1}(C) \end{array}$$

and one sees from the definitions that the cohomology maps

$$H^p(K) \to H^{p+1}(C') \approx H^p(C)$$

are the ones induced by $f: K \to C$.

We now return to the assumptions of Proposition 1.2, so that these maps are isomorphisms. We conclude that $H(M) = 0$. This implies that the sequence

$$0 \to K^0 \to M^1 \to M^2 \to \cdots \to M^{n+1} \to 0$$

is exact. Now each M^p is in $\mathfrak{F}$ by assumption. Inserting the kernels and cokernels at each step and using induction together with the definition of a complete family, we conclude that K^0 is in $\mathfrak{F}$, as was to be shown.

In the next proposition, we have axiomatized the situation so that it is applicable to the tensor product, discussed later, and to the case when the family $\mathfrak{F}$ consists of flat modules, as defined in Chapter XVI. No knowledge of this chapter is needed here, however, since the axiomatization uses just the general language of functors and exactness.

Let $\mathfrak{F}$ be a complete family again, and let T be a covariant additive functor on the given category. We say that $\mathfrak{F}$ is **exact for *T*** if given an exact sequence

$$0 \to F' \to F \to F'' \to 0$$

in $\mathfrak{F}$, then

$$0 \to T(F') \to T(F) \to T(F'') \to 0$$

is exact.

Proposition 1.3. *Let $\mathfrak{F}$ be a complete family which is exact for T. Let $f: K \to C$ be a morphism of complexes, such that K^p and C^p are in $\mathfrak{F}$ for all p, and K^p, $H^p(C)$ are zero for all but a finite number of p. Assume that f is a homology isomorphism. Then*

$$T(f): T(K) \to T(C)$$

is a homology isomorphism.

Proof. Construct the mapping cylinder M for f. As in the proof of Proposition 1.2, we get $H(M) = 0$ so M is exact. We then start inductively from the right with zeros. We let Z^p be the cycles in M^p and use the short exact sequences

$$0 \to Z^p \to M^p \to Z^{p+1} \to 0$$

together with the definition of a complete family to conclude that Z^p is in $\mathfrak{F}$ for all p. Hence the short sequences obtained by applying T are exact. But $T(M)$ is the mapping cylinder of the morphism

$$T(f): T(K) \to T(C),$$

which is therefore an isomorphism, as one sees from the homology sequence of the mapping cylinder. This concludes the proof.

§2. FINITE FREE RESOLUTIONS

The first part of this section develops the notion of resolutions for a case somewhat more subtle than projective resolutions, and gives a good example for the considerations of Chapter XX. Northcott in [No 76] pointed out that minor adjustments of standard proofs also applied to the non-Noetherian rings, only occasionally slightly less tractable than the Noetherian ones.

Let A be a ring. A module E is called **stably free** if there exists a finite free module F such that $E \oplus F$ is finite free, and thus isomorphic to $A^{(n)}$ for some positive integer n. In particular, E is projective and finitely generated.

We say that a module M has a **finite free resolution** if there exists a resolution

$$0 \to E_n \to \cdots \to E_0 \to M \to 0$$

such that each E_i is finite free.

Theorem 2.1. *Let M be a projective module. Then M is stably free if and only if M admits a finite free resolution.*

Proof. If M is stably free then it is trivial that M has a finite free resolution. Conversely assume the existence of the resolution with the above notation. We prove that M is stably free by induction on n. The assertion is obvious if $n = 0$. Assume $n \geqq 1$. Insert the kernels and cokernels at each step, in the manner of dimension shifting. Say

$$M_1 = \mathrm{Ker}(E_0 \to P),$$

giving rise to the exact sequence

$$0 \to M_1 \to E_0 \to M \to 0.$$

Since M is projective, this sequence splits, and $E_0 \approx M \oplus M_1$. But M_1 has a finite free resolution of length smaller than the resolution of M, so there exists a finite free module F such that $M_1 \oplus F$ is free. Since $E_0 \oplus F$ is also free, this concludes the proof of the theorem.

A resolution

$$0 \to E_n \to \cdots \to E_0 \to M \to 0$$

is called **stably free** if all the modules E_i $(i = 0, \ldots, n)$ are stably free.

Proposition 2.2. *Let M be an A-module. Then M has a finite free resolution of length $n \geqq 1$ if and only if M has a stably free resolution of length n.*

Proof. One direction is trivial, so we suppose given a stably free resolution with the above notation. Let $0 \leqq i < n$ be some integer, and let F_i, F_{i+1} be finite free such that $E_i \oplus F_i$ and $E_{i+1} \oplus F_{i+1}$ are free. Let $F = F_i \oplus F_{i+1}$. Then we can form an exact sequence

$$0 \to E_n \to \cdots \to E_{i+1} \oplus F \to E_i \oplus F \to \cdots \to E_0 \to M \to 0$$

in the obvious manner. In this way, we have changed two consecutive modules in the resolution to make them free. Proceeding by induction, we can then make E_0, E_1 free, then E_1, E_2 free, and so on to conclude the proof of the proposition.

The next lemma is designed to facilitate dimension shifting.

We say that two modules M_1, M_2 are **stably isomorphic** if there exist finite free modules F_1, F_2 such that $M_1 \oplus F_1 \approx M_2 \oplus F_2$.

Lemma 2.3. *Let M_1 be stably isomorphic to M_2. Let*

$$0 \to N_1 \to E_1 \to M_1 \to 0$$

$$0 \to N_2 \to E_2 \to M_2 \to 0$$

be exact sequences, where M_1 is stably isomorphic to M_2, and E_1, E_2 are stably free. Then N_1 is stably isomorphic to N_2.

Proof. By definition, there is an isomorphism $M_1 \oplus F_1 \approx M_2 \oplus F_2$. We have exact sequences

$$0 \to N_1 \to E_1 \oplus F_1 \to M_1 \oplus F_1 \to 0$$

$$0 \to N_2 \to E_2 \oplus F_2 \to M_2 \oplus F_2 \to 0$$

By Schanuel's lemma (see below) we conclude that

$$N_1 \oplus E_2 \oplus F_2 \approx N_2 \oplus E_1 \oplus F_1.$$

Since E_1, E_2, F_1, F_2 are stably free, we can add finite free modules to each side so that the summands of N_1 and N_2 become free, and by adding 1-dimensional free modules if necessary, we can preserve the isomorphism, which proves that N_1 is stably isomorphic to N_2.

We still have to take care of **Schanuel's lemma**:

Lemma 2.4. *Let*

$$0 \to K \to P \to M \to 0$$

$$0 \to K' \to P' \to M \to 0$$

be exact sequences where P, P' are projective. Then there is an isomorphism

$$K \oplus P' \approx K' \oplus P.$$

Proof. Since P is projective, there exists a homomorphism $P \to P'$ making the right square in the following diagram commute.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K & \xrightarrow{i} & P & \longrightarrow & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle w} & & \downarrow{\scriptstyle \mathrm{id}} & & \\
0 & \longrightarrow & K' & \xrightarrow[j]{} & P' & \longrightarrow & M & \longrightarrow & 0
\end{array}$$

Then one can find a homomorphism $K \to K'$ which makes the left square commute. Then we get an exact sequence

$$0 \to K \to P \oplus K' \to P' \to 0$$

by $x \mapsto (ix, ux)$ for $x \in K$ and $(y, z) \mapsto wy - jz$. We leave the verification of exactness to the reader. Since P' is projective, the sequence splits thus proving Schanuel's lemma. This also concludes the proof of Lemma 2.3.

The minimal length of a stably free resolution of a module is called its **stably free dimension**. To construct a stably free resolution of a finite module, we proceed inductively. The preceding lemmas allow us to carry out the induction, and also to stop the construction if a module is of finite stably free dimension.

Theorem 2.5. *Let M be a module which admits a stably free resolution of length n*

$$0 \to E_n \to \cdots \to E_0 \to M \to 0.$$

Let

$$F_m \to \cdots \to F_0 \to M \to 0$$

be an exact sequence with F_i stably free for $i = 0, \dots, m$.

(i) *If $m < n - 1$ then there exists a stably free F_{m+1} such that the exact sequence can be continued exactly to*

$$F_{m+1} \to \cdots \to F_0 \to M \to 0.$$

(ii) *If $m = n - 1$, let $F_n = \mathrm{Ker}(F_{n-1} \to F_{n-2})$. Then F_n is stably free and thus*

$$0 \to F_n \to F_{n-1} \to \cdots \to F_0 \to M \to 0$$

is a stably free resolution.

Remark. If A is Noetherian then of course (i) is trivial, and we can even pick F_{m+1} to be finite free.

Proof. Insert the kernels and cokernels in each sequence, say

$$K_m = \mathrm{Ker}(E_m \to E_{m-1}) \quad \text{if} \quad m \neq 0$$

$$K_0 = \mathrm{Ker}(E_0 \to M),$$

and define K'_m similarly. By Lemma 2.3, K_m is stably isomorphic to K'_m, say

$$K_m \oplus F \approx K'_m \oplus F'$$

with F, F' finite free.

If $m < n - 1$, then K_m is a homomorphic image of E_{m+1}; so both $K_m \oplus F$ and $K'_m \oplus F'$ are homomorphic images of $E_{m+1} \oplus F$. Therefore K'_m is a homomorphic image of $E_{m+1} \oplus F$ which is stably free. We let $F_{m+1} = E_{m+1} \oplus F$ to conclude the proof in this case.

If $m = n - 1$, then we can take $K_n = E_n$. Hence $K_m \oplus F$ is stably free, and so is $K'_m \oplus F'$ by the isomorphism in the first part of the proof. It follows trivially that K'_m is stably free, and by definition, $K'_m = F_{m+1}$ in this case. This concludes the proof of the theorem.

Corollary 2.6. *If $0 \to M_1 \to E \to M \to 0$ is exact, M has stably free dimension $\leqq n$, and E is stably free, then M_1 has stably free dimension $\leqq n - 1$.*

Theorem 2.7. *Let*

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

be an exact sequence. If any two of these modules have a finite free resolution, then so does the third.

Proof. Assume M' and M have finite free resolutions. Since M is finite, it follows that M'' is also finite. By essentially the same construction as Chapter XX, Lemma 3.8, we can construct an exact and commutative diagram where E', E, E'' are stably free:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & M'_1 & \to & M_1 & \to & M''_1 & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & E' & \to & E & \to & E'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & M' & \to & M & \to & M'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

We then argue by induction on the stably free dimension of M. We see that M_1 has stably free dimension $\leqq n - 1$ (actually $n - 1$, but we don't care), and M'_1 has finite stably free dimension. By induction we are reduced to the case when M has stably free dimension 0, which means that M is stably free. Since by assumption there is a finite free resolution of M', it follows that M'' also has a finite free resolution, thus concluding the proof of the first assertion.

Next assume that M', M'' have finite free resolutions. Then M is finite. If both M' and M'' have stably free dimension 0, then M', M'' are projective and $M \approx M' \oplus M''$ is also stably free and we are done. We now argue by induction on the maximum of their stably free dimension n, and we assume $n \geqq 1$. We can construct an exact and commutative diagram as in the previous case with E', E, E'' finite free (we leave the details to the reader). But the maximum of the stably free dimensions of M'_1 and M''_1 is at most $n - 1$, and so by induction it follows that M_1 has finite stably free dimension. This concludes the proof of the second case.

Observe that the third statement has been proved in Chapter XX, Lemma 3.8 when A is Noetherian, taking for $\mathfrak{A}$ the abelian category of finite modules, and for $\mathscr{C}$ the family of stably free modules. Mitchell Stokes pointed out to me that the statement is valid in general without Noetherian assumption, and can be proved as follows. We assume that M, M'' have finite free resolutions. We first show that M' is finitely generated. Indeed, suppose first that M is finite free. We have two exact sequences

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

$$0 \to K'' \to F'' \to M'' \to 0$$

where F'' is finite free, and K'' is finitely generated because of the assumption that M'' has a finite free resolution. That M' is finitely generated follows from Schanuel's lemma. If M is not free, one can reduce the finite generation of M' to the case when M is free by a pull-back, which we leave to the reader.

Now suppose that the stably free dimension of M'' is positive. We use the same exact commutative diagram as in the previous cases, with E', E, E'' finite free. The stably free dimension of M''_1 is one less than that of M'', and we are done by induction. This concludes the proof of Theorem 2.7.

This also concludes our general discussion of finite free resolutions. For more information cf. Northcott's book on the subject.

We now come to the second part of this section, which provides an application to polynomial rings.

Theorem 2.8. *Let R be a commutative Noetherian ring. Let x be a variable. If every finite R-module has a finite free resolution, then every finite $R[x]$-module has a finite free resolution.*

In other words, in the category of finite R-modules, if every object is of finite stably free dimension, then the same property applies to the category of finite $R[x]$-modules. Before proving the theorem, we state the application we have in mind.

Theorem 2.9. (Serre). *If k is a field and $x_1, \ldots, x_r$ independent variables, then every finite projective module over $k[x_1, \ldots, x_r]$ is stably free, or equivalently admits a finite free resolution.*

Proof. By induction and Theorem 2.8 we conclude that every finite module over $k[x_1, \ldots, x_r]$ is of finite stably free dimension. (We are using Theorem 2.1.) This concludes the proof.

The rest of this section is devoted to the proof of Theorem 2.8.

Let M be a finite $R[x]$-module. By Chapter X, Corollary 2.8, M has a finite filtration

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

such that each factor M_i/M_{i+1} is isomorphic to $R[x]/P_i$ for some prime P_i. In light of Theorem 2.7, it suffices to prove the theorem in case $M = R[x]/P$ where P is prime, which we now assume. In light of the exact sequence

$$0 \to P \to R[x] \to R[x]/P \to 0.$$

and Theorem 2.7, we note that M has a finite free resolution if and only if P does.

Let $\mathfrak{p} = P \cap R$. Then $\mathfrak{p}$ is prime in R. Suppose there is some $M = R[x]/P$ which does not admit a finite free resolution. Among all such M we select one for which the intersection $\mathfrak{p}$ is maximal in the family of prime ideals obtained as above. This is possible in light of one of the basic properties characterizing Noetherian rings.

Let $R_0 = R/\mathfrak{p}$ so R_0 is entire. Let $P_0 = P/\mathfrak{p}R[x]$. Then we may view M as an $R_0[x]$-module, equal to R_0/P_0. Let $f_1, \ldots, f_n$ be a finite set of generators for P_0, and let f be a polynomial of minimal degree in P_0. Let K_0 be the quotient field of R_0. By the euclidean algorithm, we can write

$$f_i = q_i f + r_i \quad \text{for} \quad i = 1, \ldots, n$$

with $q_i, r_i \in K_0[x]$ and $\deg r_i < \deg f$. Let d_0 be a common denominator for the coefficients of all q_i, r_i. Then $d_0 \neq 0$ and

$$d_0 f_i = q_i' f + r_i'$$

where $q_i' = d_0 q_i$ and $r_i' = d_0 r_i$ lie in $R_0[x]$. Since $\deg f$ is minimal in P_0 it follows that $r_i' = 0$ for all i, so

$$d_0 P_0 \subset R_0[x]f = (f).$$

Let $N_0 = P_0/(f)$, so N_0 is a module over $R_0[x]$, and we can also view N_0 as a module over $R[x]$. When so viewed, we denote N_0 by N. Let $d \in R$ be any element reducing to d_0 mod $\mathfrak{p}$. Then $d \notin \mathfrak{p}$ since $d_0 \neq 0$. The module N_0 has a finite filtration such that each factor module of the filtration is isomorphic to some $R_0[x]/Q_0$ where Q_0 is an associated prime of N_0. Let Q be the inverse image of Q_0 in $R[x]$. These prime ideals Q are precisely the associated primes of N in $R[x]$. Since d_0 kills N_0 it follows that d kills N and therefore d lies in every associated prime of N. By the maximality property in the selection of P, it follows that every one of the factor modules in the filtration of N has a finite free resolution, and by Theorem 2.7 it follows that N itself has a finite free resolution.

Now we view $R_0[x]$ as an $R[x]$-module, via the canonical homomorphism

$$R[x] \to R_0[x] = R[x]/\mathfrak{p}R[x].$$

By assumption, $\mathfrak{p}$ has a finite free resolution as R-module, say

$$0 \to E_n \to \cdots \to E_0 \to \mathfrak{p} \to 0.$$

Then we may simply form the modules $E_i[x]$ in the obvious sense to obtain a finite free resolution of $\mathfrak{p}[x] = \mathfrak{p}R[x]$. From the exact sequence

$$0 \to \mathfrak{p}R[x] \to R[x] \to R_0[x] \to 0$$

we conclude that $R_0[x]$ has a finite free resolution as $R[x]$-module.

Since R_0 is entire, it follows that the principal ideal (f) in $R_0[x]$ is $R[x]$-isomorphic to $R_0[x]$, and therefore has a finite free resolution as $R[x]$-module. Theorem 2.7 applied to the exact sequence of $R[x]$-modules

$$0 \to (f) \to P_0 \to N \to 0$$

shows that P_0 has a finite free resolution; and further applied to the exact sequence

$$0 \to \mathfrak{p}R[x] \to P \to P_0 \to 0$$

shows that P has a finite free resolution, thereby concluding the proof of Theorem 2.8.

§3. UNIMODULAR POLYNOMIAL VECTORS

Let A be a commutative ring. Let $(f_1, \ldots, f_n)$ be elements of A generating the unit ideal. We call such elements **unimodular**. We shall say that they have the **unimodular extension property** if there exists a matrix in $GL_n(A)$ with first column ${}^t(f_1, \ldots, f_n)$. If A is a principal entire ring, then it is a trivial exercise to prove that this is always the case. Serre originally asked the question whether it is true for a polynomial ring $k[x_1, \ldots, x_r]$ over a field k. The problem was solved by Quillen and Suslin. We give here a simplification of Suslin's proof by Vaserstein, also using a previous result of Horrocks. The method is by induction on the number of variables, in some fashion.

We shall write $f = {}^t(f_1, \ldots, f_n)$ for the column vector. We first remark that f has the unimodular extension property if and only if the vector obtained by a permutation of its components has this property. Similarly, we can make the usual row operations, adding a multiple gf_i to f_j ($j \neq i$), and f has the unimodular extension property if and only if any one of its transforms by row operations has the unimodular extension property.

We first prove the theorem in a context which allows the induction.

Theorem 3.1. (Horrocks). *Let* $(\mathfrak{o}, \mathfrak{m})$ *be a local ring and let* $A = \mathfrak{o}[x]$ *be the polynomial ring in one variable over* $\mathfrak{o}$. *Let* f *be a unimodular vector in* $A^{(n)}$ *such that some component has leading coefficient* 1. *Then* f *has the unimodular extension property.*

Proof. (Suslin). If $n = 1$ or 2 then the theorem is obvious even without assuming that $\mathfrak{o}$ is local. So we assume $n \geqq 3$ and do an induction of the smallest degree d of a component of f with leading coefficient 1. First we note that by the Euclidean algorithm and row operations, we may assume that f_1 has leading coefficient 1, degree d, and that $\deg f_i < d$ for $j \neq 1$. Since f is unimodular, a relation $\sum g_i f_i = 1$ shows that not all coefficients of $f_2, \ldots, f_n$ can lie in the maximal ideal $\mathfrak{m}$. Without loss of generality, we may assume that some coefficient of f_2 does not lie in $\mathfrak{m}$ and so is a unit since $\mathfrak{o}$ is local. Write

$$f_1(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \quad \text{with} \quad a_i \in \mathfrak{o},$$
$$f_2(x) = b_s x^s + \cdots + b_0 \quad \text{with} \quad b_i \in \mathfrak{o},\ s \leqq d - 1,$$

so that some b_i is a unit. Let $\mathfrak{a}$ be the ideal generated by all leading coefficients of polynomials $g_1 f_1 + g_2 f_2$ of degree $\leqq d - 1$. Then $\mathfrak{a}$ contains all the coefficients b_i, $i = 0, \ldots, s$. One sees this by descending induction, starting with b_s which is obvious, and then using a linear combination

$$x^{d-s} f_2(x) - b_s f_1(x).$$

Therefore $\mathfrak{a}$ is the unit ideal, and there exists a polynomial $g_1 f_1 + g_2 f_2$ of degree $\leqq d - 1$ and leading coefficient 1. By row operations, we may now get a polynomial of degree $\leqq d - 1$ and leading coefficient 1 as some component in the i-th place for some $i \neq 1, 2$. Thus ultimately, by induction, we may assume that $d = 0$ in which case the theorem is obvious. This concludes the proof.

Over any commutative ring A, for two column vectors f, g we write $f \sim g$ over A to mean that there exists $M \in GL_n(A)$ such that

$$f = Mg,$$

and we say that f is **equivalent to** g **over** A. Horrocks' theorem states that a unimodular vector f with one component having leading coefficient 1 is $\mathfrak{o}[x]$-equivalent to the first unit vector e^1. We are interested in getting a similar descent over non-local rings. We can write $f = f(x)$, and there is a natural "constant" vector $f(0)$ formed with the constant coefficients. As a corollary of Horrocks' theorem, we get:

Corollary 3.2. *Let $\mathfrak{o}$ be a local ring. Let f be a unimodular vector in $\mathfrak{o}[x]^{(n)}$ such that some component has leading coefficient 1. Then $f \sim f(0)$ over $\mathfrak{o}[x]$.*

Proof. Note that $f(0) \in \mathfrak{o}^{(n)}$ has one component which is a unit. It suffices to prove that over any commutative ring R any element $c \in R^{(n)}$ such that some component is a unit is equivalent over R to e^1, and this is obvious.

Lemma 3.3. *Let R be an entire ring, and let S be a multiplicative subset. Let x, y be independent variables. If $f(x) \sim f(0)$ over $S^{-1}R[x]$, then there exists $c \in S$ such that $f(x + cy) \sim f(x)$ over $R[x, y]$.*

Proof. Let $M \in GL_n(S^{-1}R[x])$ be such that $f(x) = M(x)f(0)$. Then $M(x)^{-1}f(x) = f(0)$ is constant, and thus invariant under translation $x \mapsto x + y$. Let

$$G(x, y) = M(x)M(x + y)^{-1}.$$

Then $G(x, y)f(x + y) = f(x)$. We have $G(x, 0) = I$ whence

$$G(x, y) = I + yH(x, y)$$

with $H(x, y) \in S^{-1}R[x, y]$. There exists $c \in S$ such that cH has coefficients in R. Then $G(x, cy)$ has coefficients in R. Since $\det M(x)$ is constant in $S^{-1}R$, it follows that $\det M(x + cy)$ is equal to this same constant and therefore that $\det G(x, cy) = 1$. This proves the lemma.

Theorem 3.4. *Let R be an entire ring, and let f be a unimodular vector in $R[x]^{(n)}$, such that one component has leading coefficient 1. Then $f(x) \sim f(0)$ over $R[x]$.*

Proof. Let J be the set of elements $c \in R$ such that $f(x + cy)$ is equivalent to $f(x)$ over $R[x, y]$. Then J is an ideal, for if $c \in J$ and $a \in R$ then replacing y by ay in the definition of equivalence shows that $f(x + cay)$ is equivalent to $f(x)$ over $R[x, ay]$, so over $R[x, y]$. Equally easily, one sees that if $c, c' \in J$ then $c + c' \in J$. Now let $\mathfrak{p}$ be a prime ideal of R. By Corollary 3.2 we know that $f(x)$ is equivalent to $f(0)$ over $R_{\mathfrak{p}}[x]$, and by Lemma 3.3 it follows that there exists $c \in R$ and $c \notin \mathfrak{p}$ such that $f(x + cy)$ is equivalent to $f(x)$ over $R[x, y]$. Hence J is not contained in $\mathfrak{p}$, and so J is unit ideal in R, so there exists an invertible matrix $M(x, y)$ over $R[x, y]$ such that

$$f(x + y) = M(x, y)f(x).$$

Since the homomorphic image of an invertible matrix is invertible, we substitute 0 for x in this last relation to conclude the proof of the theorem.

Theorem 3.5. (Quillen-Suslin). *Let k be a field and let f be a unimodular vector in $k[x_1, \ldots, x_r]^{(n)}$. Then f has the unimodular extension property.*

Proof. By induction on r. If $r = 1$ then $k[x_1]$ is a principal ring and the theorem is left to the reader. Assume the theorem for $r - 1$ variables with $r \geqq 2$, and put

$$R = k[x_1, \dots, x_{r-1}].$$

We view f as a vector of polynomials in the last variable x_r and want to apply Theorem 3.4. We can do so if some component of f has leading coefficient 1 in the variable x_r. We reduce the theorem to this case as follows. The proof of the Noether Normalization Theorem (Chapter VIII, Theorem 2.1) shows that if we let

$$y_r = x_r$$

$$y_i = x_i - x_r^{m_i}$$

then the polynomial vector

$$f(x_1, \dots, x_r) = g(y_1, \dots, y_r)$$

has one component with y_r-leading coefficient equal to 1. Hence there exists a matrix $N(y) = M(x)$ invertible over $R[x_r] = R[y_r]$ such that

$$g(y_1, \dots, y_r) = N(y_1, \dots, y_r)g(y_1, \dots, y_{r-1}, 0),$$

and $g(y_1, \dots, y_{r-1}, 0)$ is unimodular in $k[y_1, \dots, y_{r-1}]^{(n)}$. We can therefore conclude the proof by induction.

We now give other formulations of the theorem. First we recall that a module E over a commutative ring A is called **stably free** if there exists a finite free module F such that $E \oplus F$ is finite free.

We shall say that a commutative ring A has the **unimodular column extension property** if every unimodular vector $f \in A^{(n)}$ has the unimodular extension property, for all positive integers n.

Theorem 3.6. *Let A be a commutative ring which has the unimodular column extension property. Then every stably free module over A is free.*

Proof. Let E be stably free. We use induction on the rank of the free modules F such that $E \oplus F$ is free. By induction, it suffices to prove that if $E \oplus A$ is free then E is free. Let $E \oplus A = A^{(n)}$ and let

$$p : A^{(n)} \to A$$

be the projection. Let u^1 be a basis of A over itself. Viewing A as a direct summand in $E \oplus A = A^{(n)}$ we write

$$u^1 = {}^t(a_{11}, \dots, a_{n1}) \quad \text{with} \quad a_{i1} \in A.$$

Then u^1 is unimodular, and by assumption u^1 is the first column of a matrix $M = (a_{ij})$ whose determinant is a unit in A. Let

$$u^j = Me^j \quad \text{for} \quad j = 1, \ldots, n,$$

where e^j is the j-th unit column vector of $A^{(n)}$. Note that u^1 is the first column of M. By elementary column operations, we may change M so that $u^j \in E$ for $j = 2, \ldots, n$. Indeed, if $pe^j = cu^1$ for $j \geqq 2$ we need only replace e^j by $e^j - ce^1$. Without loss of generality we may therefore assume that $u^2, \ldots, u^n$ lie in E. Since M is invertible over A, it follows that M induces an automorphism of $A^{(n)}$ as A-module with itself by

$$X \mapsto MX.$$

It follows immediately from the construction and the fact that $A^{(n)} = E \oplus A$ that M maps the free module with basis $\{e^2, \ldots, e^n\}$ onto E. This concludes the proof.

If we now feed Serre's Theorem 2.9 into the present machinery consisting of the Quillen-Suslin theorem and Theorem 3.6, we obtain the alternative version of the Quillen-Suslin theorem:

Theorem 3.7. *Let k be a field. Then every finite projective module over the polynomial ring $k[x_1, \ldots, x_r]$ is free.*

§4. THE KOSZUL COMPLEX

In this section, we describe a finite complex built out of the alternating product of a free module. This gives an application of the alternating product, and also gives a fundamental construction used in algebraic geometry, both abstract and complex, as the reader can verify by looking at Griffiths-Harris [GrH 78], Chapter V, §3; Grothendieck's [SGA 6]; Hartshorne [Ha 77], Chapter III, §7; and Fulton-Lang [FuL 85], Chapter IV, §2.

We know from Chapter XX that a free resolution of a module allows us to compute certain homology or cohomology groups of a functor. We apply this now to Hom and also to the tensor product. Thus we also get examples of explicit computations of homology, illustrating Chapter XX, by means of the Koszul complex. We shall also obtain a classical application by deriving the so-called Hilbert Syzygy theorem.

Let A be a ring (always assumed commutative) and M a module. A sequence of elements $x_1, \ldots, x_r$ in A is called M-**regular** if $M/(x_1, \ldots, x_r)M \neq 0$, if x_1

is not divisor of zero in M, and for $i \geqq 2$, x_i is not divisor of 0 in

$$M/(x_1, \ldots, x_{i-1})M.$$

It is called **regular** when $M = A$.

Proposition 4.1. *Let $I = (x_1, \ldots, x_r)$ be generated by a regular sequence in A. Then I/I^2 is free of dimension r over A/I.*

Proof. Let $\bar{x}_i$ be the class of x_i mod I^2. It suffices to prove that $\bar{x}_1, \ldots, \bar{x}_r$ are linearly independent. We do this by induction on r. For $r = 1$, if $\bar{a}\bar{x} = 0$, then $ax = bx^2$ for some $b \in A$, so $x(a - bx) = 0$. Since x is not zero divisor in A, we have $a = bx$ so $\bar{a} = 0$.

Now suppose the proposition true for the regular sequence $x_1, \ldots, x_{r-1}$. Suppose

$$\sum_{i=1}^{r} \bar{a}_i \bar{x}_i = 0 \quad \text{in} \quad I/I^2.$$

We may assume that $\sum a_i x_i = 0$ in A; otherwise $\sum a_i x_i = \sum y_i x_i$ with $y_i \in I$ and we can replace a_i by $a_i - y_i$ without changing $\bar{a}_i$.

Since x_r is not zero divisor in $A/(x_1, \ldots, x_{r-1})$ there exist $b_i \in A$ such that

$$a_r x_r + \sum_{i=1}^{r-1} a_i x_i = 0 \Rightarrow a_r = \sum_{i=1}^{r-1} b_i x_i \Rightarrow \sum_{i=1}^{r-1} (a_i + b_i x_r) x_i = 0.$$

By induction,

$$a_j + b_j x_r \in \sum_{i=1}^{r-1} A x_i \qquad (j = 1, \ldots, r - 1)$$

so $a_j \in I$ for all j, so $\bar{a}_j = 0$ for all j, thus proving the proposition.

Let K, L be complexes, which we write as direct sums

$$K = \bigoplus K_p \quad \text{and} \quad L = \bigoplus L_q$$

with $p, q \in \mathbf{Z}$. Usually, $K_p = L_q = 0$ for $p, q < 0$. Then the **tensor product** $K \otimes L$ is the complex such that

$$(K \otimes L)_n = \bigoplus_{p+q=n} K_p \otimes L_q;$$

and for $u \in K_p$, $v \in L_q$ the differential is defined by

$$d(u \otimes v) = du \otimes v + (-1)^p u \otimes dv.$$

(Carry out the detailed verification, which is routine, that this gives a complex.)

Let A be a commutative ring and $x \in A$. We define the complex $K(x)$ to have $K_0(x) = A$, $K_1(x) = Ae_1$, where e_1 is a symbol, Ae_1 is the free module of rank 1 with basis $\{e_1\}$, and the boundary map is defined by $de_1 = x$, so the complex can be represented by the sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & Ae_1 & \xrightarrow{d} & A & \longrightarrow & 0 \\ & & \| & & \| & & \\ 0 & \longrightarrow & K_1(x) & \longrightarrow & K_0(x) & \longrightarrow & 0 \end{array}$$

More generally, for elements $x_1, \ldots, x_r \in A$ we define the **Koszul complex** $K(x) = K(x_1, \ldots, x_r)$ as follows. We put:

$K_0(x) = A$;

$K_1(x) =$ free module E with basis $\{e_1, \ldots, e_r\}$;

$K_p(x) =$ free module $\bigwedge^p E$ with basis $\{e_{i_1} \wedge \cdots \wedge e_{i_p}\}$, $i_1 < \cdots < i_p$;

$K_r(x) =$ free module $\bigwedge^r E$ of rank 1 with basis $e_1 \wedge \cdots \wedge e_r$.

We define the **boundary maps** by $de_i = x_i$ and in general

$$d : K_p(x) \to K_{p-1}(x)$$

by

$$d(e_{i_1} \wedge \cdots \wedge e_{i_p}) = \sum_{j=1}^{p} (-1)^{j-1} x_{i_j} e_{i_1} \wedge \cdots \wedge \widehat{e_{i_j}} \wedge \cdots \wedge e_{i_p}.$$

A direct verification shows that $d^2 = 0$, so we have a complex

$$0 \to K_r(x) \to \cdots \to K_p(x) \to \cdots \to K_1(x) \to A \to 0$$

The next lemma shows the extent to which the complex is independent of the ideal $I = (x_1, \ldots, x_r)$ generated by (x). Let

$$I = (x_1, \ldots, x_r) \supset I' = (y_1, \ldots, y_r)$$

be two ideals of A. We have a natural ring homomorphism

$$\text{can} : A/I' \to A/I.$$

Let $\{e'_1, \ldots, e'_r\}$ be a basis for $K_1(y)$, and let

$$y_i = \sum c_{ij} x_j \quad \text{with} \quad c_{ij} \in A.$$

We **define** $f_1 : K_1(y) \to K_1(x)$ by

$$f_1 e'_i = \sum c_{ij} e_j$$

and

$$f_p = f_1 \wedge \cdots \wedge f_1, \qquad \text{product taken } p \text{ times.}$$

Let $D = \det(c_{ij})$ be the determinant. Then for $p = r$ we get that

$$f_r : K_r(y) \to K_r(x) \text{ is multiplication by } D.$$

Lemma 4.2. *Notation as above, the homomorphisms f_p define a morphism of Koszul complexes:*

$$\begin{array}{ccccccccccccc} 0 & \to & K_r(y) & \to \cdots \to & K_p(y) & \to \cdots \to & K_1(y) & \to & A & \to & A/I' & \to & 0 \\ & & \downarrow{\scriptstyle f_r = D} & & \downarrow{\scriptstyle f_p} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{can}} & & \\ 0 & \to & K_r(x) & \to \cdots \to & K_p(x) & \to \cdots \to & K_1(x) & \to & A & \to & A/I & \to & 0 \end{array}$$

and define an isomorphism if D is a unit in A, for instance if (y) is a permutation of (x).

Proof. By definition

$$f(e'_{i_1} \wedge \cdots \wedge e'_{i_p}) = \left(\sum_{j=1}^{r} c_{i_1 j} e_j\right) \wedge \cdots \wedge \left(\sum_{j=1}^{r} c_{i_p j} e_j\right).$$

Then

$$\begin{aligned} fd(e'_{i_1} \wedge \cdots \wedge e'_{i_p}) &= f\left(\sum_k (-1)^{k-1} y_{i_k} e'_{i_1} \wedge \cdots \wedge \widehat{e'_{i_k}} \wedge \cdots \wedge e'_{i_p}\right) \\ &= \sum_k (-1)^{k-1} y_{i_k} \left(\sum_{j=1}^{r} c_{i_1 j} e_j\right) \wedge \cdots \wedge \widehat{\sum_k} \wedge \cdots \wedge \left(\sum_{j=1}^{r} c_{i_p j} e_j\right) \\ &= \sum (-1)^{k-1} \left(\sum_{j=1}^{r} c_{i_1 j} e_j\right) \wedge \cdots \wedge \underbrace{\left(\sum_{j=1}^{r} c_{i_k j} x_j e_j\right)}_{\text{omitted}} \wedge \cdots \wedge \left(\sum_{j=1}^{r} c_{i_p j} e_j\right) \\ &= df(e'_{i_1} \wedge \cdots \wedge e'_{i_p}) \end{aligned}$$

using $y_{i_k} = \sum c_{i_k j} x_j$. This concludes the proof that the f_p define a homomorphism of complexes.

In particular, if (x) and (y) generate the same ideal, and the determinant D is a unit (i.e. the linear transformation going from (x) to (y) is invertible over the ring), then the two Koszul complexes are isomorphic.

The next lemma gives us a useful way of making inductions later.

Proposition 4.3. *There is a natural isomorphism*

$$K(x_1, \dots, x_r) \approx K(x_1) \otimes \cdots \otimes K(x_r).$$

Proof. The proof will be left as an exercise.

Let $I = (x_1, \dots, x_r)$ be the ideal generated by $x_1, \dots, x_r$. Then directly from the definitions we see that the 0-th homology of the Koszul complex is simply A/IA.

More generally, let M be an A-module. Define the **Koszul complex of** M by

$$K(x; M) = K(x_1, \dots, x_r; M) = K(x_1, \dots, x_r) \otimes_A M$$

Then this complex looks like

$$0 \to K_r(x) \otimes M \to \cdots \to K_2(x) \otimes_A M \to M^{(r)} \to M \to 0.$$

We sometimes abbreviate $H_p(x; M)$ for $H_pK(x; M)$. The first and last homology groups are then obtained directly from the definition of boundary. We get

$$H_0(K(x; M)) \approx M/IM;$$

$$H_r(K(x); M) = \{v \in M \text{ such that } x_iv = 0 \text{ for all } i = 1, \dots, r\}.$$

In light of Proposition 4.3, we study generally what happens to a tensor product of any complex with $K(x)$, when x consists of a single element. Let $y \in A$ and let C be an arbitrary complex of A-modules. We have an exact sequence of complexes

$$(1) \qquad 0 \to C \to C \otimes K(y) \to (C \otimes K(y))/C \to 0$$

made explicit as follows.

$$\begin{array}{ccccccccc}
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & C_{n+1} & \to & (C_{n+1} \otimes A) \oplus (C_n \otimes K_1(y)) & \to & C_n \otimes K_1(y) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle d_n \otimes \mathrm{id}} & & \\
0 & \to & C_n & \to & (C_n \otimes A) \oplus (C_{n-1} \otimes K_1(y) & \to & C_{n-1} \otimes K_1(y)) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle d_{n-1} \otimes \mathrm{id}} & & \\
0 & \to & C_{n-1} & \to & (C_{n-1} \otimes A) \oplus (C_{n-2} \otimes K_1(y)) & \to & C_{n-2} \otimes K_1(y) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & &
\end{array}$$

We note that $C \otimes K_1(y)$ is just C with a dimension shift by one unit, in other words

(2) $$(C \otimes K_1(y))_{n+1} = C_n \otimes K_1(y).$$

In particular,

(3) $$H_{n+1}(C \otimes K(y)/C) \approx H_n(C).$$

Associated with an exact sequence of complexes, we have the homology sequence, which in this case yields the long exact sequence

$$\longrightarrow H_{n+1}(C) \longrightarrow H_{n+1}(C \otimes K_1(y))$$

$$\longrightarrow H_{n+1}(C \otimes K(y)/C) \xrightarrow{\partial} H_n(C)$$

$$H_{n+1}(C \otimes K(y)/C) \approx H_n(C)$$

which we write stacked up according to the index:

(4) $$\begin{gathered}\to H_{p+1}(C) \to H_{p+1}(C) \to H_{p+1}(C \otimes K(y)) \to \\ \to H_p(C) \to H_p(C) \to H_p(C \otimes K(y)) \to\end{gathered}$$

ending in lowest dimension with

(5) $$\to H_1(C) \to H_1(C \otimes K(y)) \to H_0(C) \to H_0(C).$$

Furthermore, a direct application of the definition of the boundary map and the tensor product of complexes yields:

The boundary map on $H_p(C)$ $(p \geqq 0)$ is induced by multiplication by $(-1)^p y$:

(6) $$\partial = (-1)^p m(y) : H_p(C) \to H_p(C).$$

Indeed, write

$$(C \otimes K(y))_p = (C_p \otimes A) \oplus (C_{p-1} \otimes K_1(y)) \approx C_p \oplus C_{p-1}.$$

Let $(v, w) \in C_p \oplus C_{p-1}$ with $v \in C_p$ and $w \in C_{p-1}$. Then directly from the definitions,

(7) $$d(v, w) = (dv + (-1)^{p-1}yw, dw).$$

To see (6), one merely follows up the definitions of the boundary, taking an element $w \in C_p \approx C_p \otimes K_1(y)$, lifting back to $(0, w)$, applying d, and lifting back to C_p. If we start with a cycle, i.e. $dw = 0$, then the map is well defined on the homology class, with values in the homology.

Lemma 4.4. *Let $y \in A$ and let C be a complex as above. Then $m(y)$ annihilates $H_p(C \otimes K(y))$ for all $p \geqq 0$.*

Proof. If (v, w) is a cycle, i.e. $d(v, w) = 0$, then from (7) we get at once that $(yv, yw) = d(0, (-1)^p v)$, which proves the lemma.

In the applications we have in mind, we let $y = x_r$ and

$$C = K(x_1, \ldots, x_{r-1}; M) = K(x_1, \ldots, x_{r-1}) \otimes M.$$

Then we obtain:

Theorem 4.5.(a) *There is an exact sequence with maps as above:*

$$\to H_pK(x_1, \ldots, x_{r-1}; M) \to H_pK(x_1, \ldots, x_{r-1}; M) \to H_pK(x_1, \ldots, x_r; M)$$

$$\cdots \to H_1(x_1, \ldots, x_r; M) \to H_0(x_1, \ldots, x_{r-1}; M) \xrightarrow{m(x_r)} H_0(x_1, \ldots, x_{r-1}; M).$$

(b) *Every element of $I = (x_1, \ldots, x_r)$ annihilates $H_p(x; M)$ for $p \geqq 0$.*
(c) *If $I = A$, then $H_p(x; M) = 0$ for all $p \geqq 0$.*

Proof. This is immediate from Proposition 4.3 and Lemma 4.4.

We define the **augmented Koszul complex** to be

$$0 \to K_r(x; M) \to \cdots \to K_1(x; M) = M^{(r)} \to M \to M/IM \to 0.$$

Theorem 4.6. *Let M be an A-module.*
(a) *Let $x_1, \ldots, x_r$ be a regular sequence for M. Then $H_pK(x; M) = 0$ for $p > 0$. (Of course, $H_0K(x; M) = M/IM$.) In other words, the augmented Koszul complex is exact.*
(b) *Conversely, suppose A is local, and $x_1, \ldots, x_r$ lie in the maximal ideal of A. Suppose M is finite over A, and also assume that $H_1K(x; M) = 0$. Then $(x_1, \ldots, x_r)$ is M-regular.*

Proof. We prove (a) by induction on r. If $r = 1$ then $H_1(x; M) = 0$ directly from the definition. Suppose $r > 1$. We use the exact sequence of Theorem 4.5(a). If $p > 1$ then $H_p(x; M)$ is between two homology groups which are 0, so $H_p(x; M) = 0$. If $p = 1$, we use the very end of the exact sequence of Theorem 4.5(a), noting that $m(x_r)$ is injective, so by induction we find $H_1(x; M) = 0$ also, thus proving (a).

As to (b), by Lemma 4.4 and the hypothesis, we get an exact sequence

$$H_1(x_1, \ldots, x_{r-1}; M) \xrightarrow{m(x_r)} H_1(x_1, \ldots, x_{r-1}; M) \to H_1(x; M) = 0,$$

so $m(x_r)$ is surjective. By Nakayama's lemma, it follows that

$$H_1(x_1, \ldots, x_{r-1}; M) = 0.$$

By induction $(x_1, \ldots, x_{r-1})$ is an M-regular sequence. Looking again at the tail end of the exact sequence as in (a) shows that x_r is $M/(x_1, \ldots, x_{r-1})M$-regular, whence proving (b) and the theorem.

We note that (b), which uses only the triviality of H_1 (and not all H_p) is due to Northcott [No 68], 8.5, Theorem 8. By (a), it follows that $H_p = 0$ for $p > 0$.

An important special case of Theorem 4.6(a) is when $M = A$, in which case we restate the theorem in the form:

Let $x_1, \ldots, x_r$ be a regular sequence in A. Then $K(x_1, \ldots, x_r)$ is a free resolution of A/I:

$$0 \to K_r(x) \to \cdots \to K_1(x) \to A \to A/I \to 0.$$

In particular, A/I has Tor-*dimension* $\leqq r$.

For the Hom functor, we have:

Theorem 4.7. *Let $x_1, \ldots, x_r$ be a regular sequence in A. Then there is an isomorphism*

$$\varphi_{x,M}: H^r(\mathrm{Hom}(K(x), M)) \to M/IM$$

to be described below.

Proof. The module $K_r(x)$ is 1-dimensional, with basis $e_1 \wedge \cdots \wedge e_r$. Depending on this basis, we have an isomorphism

$$\mathrm{Hom}(K_r(x), M) \approx M,$$

whereby a homomorphism is determined by its value at the basis element in M. Then directly from the definition of the boundary map d_r in the Koszul complex, which is

$$d_r : e_1 \wedge \cdots \wedge e_r \mapsto \sum_{j=1}^{r} (-1)^{j-1} x_j e_1 \wedge \cdots \wedge \hat{e}_j \wedge \cdots \wedge e_r$$

we see that

$$H^r(\mathrm{Hom}(K_r(x), M) \approx \mathrm{Hom}(K_r(x), M)/d^{r-1}\,\mathrm{Hom}(K_{r-1}(x), M)$$
$$\approx M/IM.$$

This proves the theorem.

The reader who has read Chapter XX knows that the i-th homology group of $\mathrm{Hom}(K(x), M)$ is called $\mathrm{Ext}^i(A/I, M)$, determined up to a unique isomorphism by the complex, since two resolutions of A/I differ by a morphism of complexes, and two such morphisms differ by a homotopy which induces a homology isomorphism. Thus Theorem 4.7 gives an isomorphism

$$\varphi_{x,M} : \mathrm{Ext}^r(A/I, M) \to M/IM.$$

In fact, we shall obtain morphisms of the Koszul complex from changing the sequence. We go back to the hypothesis of Lemma 4.2.

Lemma 4.8. *If $I = (x) = (y)$ where (x), (y) are two regular sequences, then we have a commutative diagram*

$$\begin{array}{ccc} & & M/IM \\ & \overset{\varphi_{x,M}}{\nearrow} & \\ \operatorname{Ext}^r(A/I, M) & & \Big\downarrow {\scriptstyle D = \det(c_{ij})} \\ & \underset{\varphi_{y,M}}{\searrow} & \\ & & M/IM \end{array}$$

where all the maps are isomorphisms of A/I-modules.

The fact that we are dealing with A/I-modules is immediate since multiplication by an element of A commutes with all homomorphisms in sight, and I annihilates A/I.

By Proposition 4.1, we know that I/I^2 is a free module of rank r over A/I. Hence

$$\bigwedge^r(I/I^2)$$

is a free module of rank 1, with basis $\bar{x}_1 \wedge \cdots \wedge \bar{x}_r$ (where the bar denotes residue class mod I^2). Taking the dual of this exterior product, we see that under a change of basis, it transforms according to the inverse of the determinant mod I^2. This allows us to get a canonical isomorphism as in the next theorem.

Theorem 4.9. *Let $x_1, \ldots, x_r$ be a regular sequence in A, and let $I = (x)$. Let M be an A-module. Let*

$$\psi_{x,M} : M/IM \to (M/IM) \otimes \bigwedge^r(I/I^2)^{\text{dual}}$$

be the embedding determined by the basis $(\bar{x}_1 \wedge \cdots \wedge \bar{x}_r)^{\text{dual}}$ of $\bigwedge^r(I/I^2)^{\text{dual}}$. Then the composite isomorphism

$$\operatorname{Ext}^r(A/I, M) \xrightarrow{\varphi_{x,M}} M/IM \xrightarrow{\psi_{x,M}} (M/IM) \otimes \bigwedge^r(I/I^2)^{\text{dual}}$$

is a functorial isomorphism, independent of the choice of regular generators for I.

We also have the analogue of Theorem 4.5 in intermediate dimensions.

Theorem 4.10. *Let $x_1, \ldots, x_r$ be an M-regular sequence in A. Let $I = (x)$. Then*

$$\operatorname{Ext}^i(A/I, M) = 0 \quad \textit{for} \quad i < r.$$

Proof. For the proof, we assume that the reader is acquainted with the exact homology sequence. Assume by induction that $\operatorname{Ext}^i(A/I, M) = 0$ for

$i < r - 1$. Then we have the exact sequence

$$0 = \mathrm{Ext}^{i-1}(A/I, M/x_1M) \to \mathrm{Ext}^i(A/I, M) \xrightarrow{x_1} \mathrm{Ext}^i(A/I, M)$$

for $i < r$. But $x_1 \in I$ so multiplication by x_1 induces 0 on the homology groups, which gives $\mathrm{Ext}^i(A/I, M) = 0$ as desired.

Let $L_N \to N \to 0$ be a free resolution of a module N. By definition,

$$\mathrm{Tor}_i^A(N, M) = i\text{-th homology of the complex } L \otimes M.$$

This is independent of the choice of L_N up to a unique isomorphism. We now want to do for Tor what we have just done for Ext.

Theorem 4.11. *Let $I = (x_1, \ldots, x_r)$ be an ideal of A generated by a regular sequence of length r.*

(i) *There is a natural isomorphism*

$$\mathrm{Tor}_i^A(A/I, A/I) \approx \textstyle\bigwedge_{A/I}^i(I/I^2), \quad \textit{for} \quad i \geqq 0.$$

(ii) *Let L be a free A/I-module, extended naturally to an A-module. Then*

$$\mathrm{Tor}_i^A(L, A/I) \approx L \otimes \textstyle\bigwedge_{A/I}^i(I/I^2), \quad \textit{for} \quad i \geqq 0.$$

These isomorphisms will follow from the next considerations.

First we use again that the residue classes $\bar{x}_1, \ldots, \bar{x}_r$ mod I^2 form a basis of I/I^2 over A/I. Therefore we have a unique isomorphism of complexes

$$\varphi_x : K(x) \otimes A/I \to \textstyle\bigwedge(I/I^2) = \bigoplus \bigwedge^i(I/I^2)$$

with zero differentials on the right-hand side, such that

$$e_{i_1} \wedge \cdots \wedge e_{i_p} \mapsto \bar{x}_{i_1} \wedge \cdots \wedge \bar{x}_{i_p}.$$

Lemma 4.12. *Let $I = (x) \supset I' = (y)$ be two ideals generated by regular sequences of length r. Let $f: K(y) \to K(x)$ be the morphism of Koszul complexes defined in Lemma 4.2. Then the following diagram is commutative:*

$$\begin{array}{ccc} K(y) \otimes A/I' & \xrightarrow{\varphi_y} & \bigwedge_{A/I'}(I'/I'^2) \\ \downarrow{\scriptstyle f \otimes \mathrm{can}} & & \downarrow{\scriptstyle \text{canonical hom}} \\ K(x) \otimes A/I & \xrightarrow[\varphi_x]{} & \bigwedge_{A/I}(I/I^2) \end{array}$$

Proof. We have

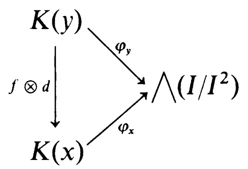
$$\varphi_x \circ (f \otimes \text{can})(e'_{i_1} \wedge \cdots \wedge e'_{i_p} \otimes 1)$$

$$= \sum_{j=2}^{r} c_{i_1 j}\bar{x}_j \wedge \cdots \wedge \sum_{j=1}^{r} c_{i_p j}\bar{x}_j$$

$$= \bar{y}_{i_1} \wedge \cdots \wedge \bar{y}_{i_p} = \text{can}(\varphi_y(e'_{i_1} \wedge \cdots \wedge e'_{i_p})).$$

This proves the lemma.

In particular, if $I' = I$ then we have the commutative diagram



which shows that the identification of $\text{Tor}_i(A/I, A/I)$ with $\bigwedge^i(I/I^2)$ via the choices of bases is compatible under one isomorphism of the Koszul complexes, which provide a resolution of A/I. Since any other homomorphism of Koszul complexes is homotopic to this one, it follows that this identification does not depend on the choices made and proves the first part of Theorem 4.11.

The second part follows at once, because we have

$$\text{Tor}_i^A(A/I, L) = H_i(K(x) \otimes L) = H_i((K(x) \otimes_A A/I) \otimes_{A/I} L$$
$$= \textstyle\bigwedge^i_{A/I}(I/I^2) \otimes L.$$

This concludes the proof of Theorem 4.11.

Example. Let k be a field and let $A = k[x_1, \dots, x_r]$ be the polynomial ring in r variables. Let $I = (x_1, \dots, x_r)$ be the ideal generated by the variables. Then $A/I = k$, and therefore Theorem 4.11 yields for $i \geqq 0$:

$$\text{Tor}_i^A(k, k) \approx \textstyle\bigwedge^i_k(I/I^2)$$

$$\text{Tor}_i^A(L, k) \approx L \otimes \textstyle\bigwedge^i_k(I/I^2)$$

Note that in the present case, we can think of I/I^2 as the vector space over k with basis $\bar{x}_1, \dots, \bar{x}_r$. Then A can be viewed as the symmetric algebra SE, where E is this vector space. We can give a specific example of the Koszul complex in this context as in the next theorem, given for a free module.

Theorem 4.13. *Let E be a finite free module of rank r over the ring R. For each $p = 1, \dots, r$ there is a unique homomorphism*

$$d_p : \bigwedge^p E \otimes SE \to \bigwedge^{p-1} E \otimes SE$$

such that

$$d_i((x_1 \wedge \cdots \wedge x_p) \otimes y)$$

$$= \sum_{i=1}^{p} (-1)^{i-1} (x_1 \wedge \cdots \wedge \widehat{x_i} \wedge \cdots \wedge x_p) \otimes (x_i \otimes y)$$

where $x_i \in E$ and $y \in SE$. This gives the resolution

$$0 \to \bigwedge^r E \otimes SE \to \bigwedge^{r-1} E \otimes SE \to \cdots \to \bigwedge^0 E \otimes SE \to R \to 0$$

Proof. The above definitions are merely examples of the Koszul complex for the symmetric algebra SE with respect to the regular sequence consisting of some basis of E.

Since d_p maps $\bigwedge^p E \otimes S^q E$ into $\bigwedge^{p-1} E \otimes S^{q+1} E$, we can decompose this complex into a direct sum corresponding to a given graded component, and hence:

Corollary 4.14. *For each integer $n \geqq 1$, we have an exact sequence*

$$0 \to \bigwedge^r E \otimes S^{n-r} E \to \cdots \to \bigwedge^1 E \otimes S^{n-1} E \to S^n E \to 0$$

where $S^j E = 0$ for $j < 0$.

Finally, we give an application to a classical theorem of Hilbert. The polynomial ring $A = k[x_1, \dots, x_r]$ is naturally graded, by the degrees of the homogeneous components. *We shall consider graded modules, where the grading is in dimensions $\geqq 0$, and we assume that homomorphisms are graded of degree* 0.

So suppose M is a graded module (and thus $M_i = 0$ for $i < 0$) and M is finite over A. Then we can find a graded surjective homomorphism

$$L_0 \to M \to 0$$

where L_0 is finite free. Indeed, let $w_1, \dots, w_n$ be homogeneous generators of M. Let $e_1, \dots, e_n$ be basis elements for a free module L_0 over A. We give L_0 the grading such that if $a \in A$ is homogeneous of degree d then ae_i is homogeneous of degree

$$\deg ae_i = \deg a + \deg w_i.$$

Then the homomorphism of L_0 onto M sending $e_i \mapsto w_i$ is graded as desired.

The kernel M_1 is a graded submodule of L_0. Repeating the process, we can find a surjective homomorphism

$$L_1 \to M_1 \to 0.$$

We continue in this way to obtain a graded resolution of M. We want this resolution to stop, and the possibility of its stopping is given by the next theorem.

Theorem 4.15. (Hilbert Syzygy Theorem). *Let k be a field and*

$$A = k[x_1, \ldots, x_r]$$

the polynomial ring in r variables. Let M be a graded module over A, and let

$$0 \to K \to L_{r-1} \to \cdots \to L_0 \to M \to 0$$

be an exact sequence of graded homomorphisms of graded modules, such that $L_0, \ldots, L_{r-1}$ are free. Then K is free. If M is in addition finite over A and $L_0, \ldots, L_{r-1}$ are finite free, then K is finite free.

Proof. From the Koszul complex we know that $\mathrm{Tor}_i(M, k) = 0$ for $i > r$ and all M. By dimension shifting, it follows that

$$\mathrm{Tor}_i(K, k) = 0 \quad \text{for} \quad i > 0.$$

The theorem is then a consequence of the next result.

Theorem 4.16. *Let F be a graded finite module over $A = k[x_1, \ldots, x_r]$. If $\mathrm{Tor}_1(F, k) = 0$ then F is free.*

Proof. The method is essentially to do a Nakayama type argument in the case of the non-local ring A. First note that

$$F \otimes k = F/IF$$

where $I = (x_1, \ldots, x_r)$. Thus $F \otimes k$ is naturally an $A/I = k$-module. Let $v_1, \ldots, v_n$ be homogeneous elements of F whose residue classes mod IF form a basis of F/IF over k. Let L be a free module with basis $e_1, \ldots, e_n$. Let

$$L \to F$$

be the graded homomorphism sending $e_i \mapsto v_i$ for $i = 1, \ldots, n$. It suffices to prove that this is an isomorphism. Let C be the cokernel, so we have the exact sequence

$$L \to F \to C \to 0.$$

Tensoring with k yields the exact sequence

$$L \otimes k \to F \otimes k \to C \otimes k \to 0.$$

Since by construction the map $L \otimes k \to F \otimes k$ is surjective, it follows that $C \otimes k = 0$. But C is graded, so the next lemma shows that $C = 0$.

Lemma 4.17. *Let N be a graded module over $A = k[x_1, \dots, x_r]$. Let $I = (x_1, \dots, x_r)$. If $N/IN = 0$ then $N = 0$.*

Proof. This is immediate by using the grading, looking at elements of N of smallest degree if they exist, and using the fact that elements of I have degree > 0.

We now get an exact sequence of graded modules

$$0 \to E \to L \to F \to 0$$

and we must show that $E = 0$. But the exact homology sequence and our assumption yields

$$0 = \mathrm{Tor}_1(F, k) \to E \otimes k \to L \otimes k \to F \otimes k \to 0.$$

By construction $L \otimes k \to F \otimes k$ is an isomorphism, and hence $E \otimes k = 0$. Lemma 4.17 now shows that $E = 0$. This concludes the proof of the syzygy theorem.

Remark. The only place in the proof where we used that k is a field is in the proof of Theorem 4.16 when we picked homogeneous elements $v_1, \dots, v_n$ in M whose residue classes mod IM form a basis of M/IM over A/IA. Hilbert's theorem can be generalized by making the appropriate hypothesis which allows us to carry out this step, as follows.

Theorem 4.18. *Let R be a commutative local ring and let $A = R[x_1, \dots, x_r]$ be the polynomial ring in r variables. Let M be a graded finite module over A, projective over R. Let*

$$0 \to K \to L_{r-1} \to \cdots \to L_0 \to M \to 0$$

be an exact sequence of graded homomorphisms of graded modules such that $L_0, \dots, L_{r-1}$ are finite free. Then K is finite free.

Proof. Replace k by R everywhere in the proof of the Hilbert syzygy theorem. We use the fact that a finite projective module over a local ring is free. Not a word needs to be changed in the above proof with the following exception. We note that the projectivity propagates to the kernels and cokernels in the given resolution. Thus F in the statement of Theorem 4.16 may be assumed projective, and each graded component is projective. Then F/IF is projective over $A/IA = R$, and so is each graded component. Since a finite projective module over a local ring is free, and one gets the freeness by lifting a basis from the residue class field, we may pick $v_1, \dots, v_n$ homogeneous exactly as we did in the proof of Theorem 4.16. This concludes the proof.

EXERCISES

For exercises 1 through 4 on the Koszul complex, see [No 68], Chapter 8.

1. Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of A-modules. Show that tensoring with the Koszul complex $K(x)$ one gets an exact sequence of complexes, and therefore an exact homology sequence

$$0 \to H_rK(x; M') \to H_rK(x; M) \to H_rK(x; M'') \to \cdots$$
$$\cdots \to H_pK(x; M') \to H_pK(x; M) \to H_pK(x; M'') \to \cdots$$
$$\cdots \to H_0K(x; M') \to H_0K(x; M) \to H_0K(x; M'') \to 0$$

2. (a) Show that there is a unique homomorphism of complexes

$$f: K(x; M) \to K(x_1, \dots, x_{r-1}; M)$$

such that for $v \in M$:

$$f_p(e_{i_1} \wedge \cdots \wedge e_{i_p} \otimes v) = \begin{cases} e_{i_1} \wedge \cdots \wedge e_{i_p} \otimes x_r v & \text{if } i_p = r \\ e_{i_1} \wedge \cdots \wedge e_{i_p} \otimes v & \text{if } i_p = r. \end{cases}$$

(b) Show that f is injective if x_r is not a divisor of zero in M.

(c) For a complex C, denote by $C(-1)$ the complex shifted by one place to the left, so $C(-1)_n = C_{n-1}$ for all n. Let $\overline{M} = M/x_rM$. Show that there is a unique homomorphism of complexes

$$g: K(x_1, \dots, x_{r-1}, 1; M) \to K(x_1, \dots, x_{r-1}; \overline{M})(-1)$$

such that for $v \in M$:

$$g_p(e_{i_1} \wedge \cdots \wedge c_{i_p} \otimes v) = \begin{cases} e_{i_1} \wedge \cdots \wedge e_{i_{p-1}} \otimes v & \text{if } i_p = r \\ 0 & \text{if } i_p < r. \end{cases}$$

(d) If x_r is not a divisor of 0 in M, show that the following sequence is exact:

$$0 \to K(x; M) \xrightarrow{f} K(x_1, \dots, x_{r-1}, 1; M) \xrightarrow{g} K(x_1, \dots, x_{r-1}; \overline{M})(-1) \to 0.$$

Using Theorem 4.5(c), conclude that for all $p \geqq 0$, there is an isomorphism

$$H_pK(x; M) \xrightarrow{\approx} H_pK(x_1, \dots, x_{r-1}; \overline{M}).$$

3. Assume A and M Noetherian. Let I be an ideal of A. Let $a_1, \dots, a_k$ be an M-regular sequence in I. Show that this sequence can be extended to a maximal M-regular sequence $a_1, \dots, a_q$ in I, in other words an M-regular sequence such that there is no M-regular sequence $a_1, \dots, a_{q+1}$ in I.

4. Again assume A and M Noetherian. Let $I = (x_1, \dots, x_r)$ and let $a_1, \dots, a_q$ be a maximal M-regular sequence in I. Assume $IM \neq M$. Prove that

$$H_{r-q}(x; M) \neq 0 \text{ but } H_p(x; M) = 0 \text{ for } p > r - q.$$

[See [No 68], 8.5 Theorem 6. The result is similar to the result in Exercise 5, and generalizes Theorem 4.5(a). See also [Mat 80], pp. 100-103. The result shows that all maximal M-regular sequences in M have the same length, which is called the I-**depth** of M and is denoted by $\operatorname{depth}_I(M)$. For the proof, let s be the maximal integer such that $H_s K(x; M) \neq 0$. By assumption, $H_0(x; M) = M/IM \neq 0$, so s exists. We have to prove that $q + s = r$. First note that if $q = 0$ then $s = r$. Indeed, if $q = 0$ then every element of I is zero divisor in M, whence I is contained in the union of the associated primes of M, whence in some associated prime of M. Hence $H_r(x; M) \neq 0$.

Next assume $q > 0$ and proceed by induction. Consider the exact sequence

$$0 \to M \xrightarrow{a_1} M \to M/a_1M \to 0$$

where the first map is $m(a_1)$. Since I annihilates $H_p(x; M)$ by Theorem 4.5(c), we get an exact sequence

$$0 \to H_p(x; M) \to H_p(x; M/a_1M) \to H_{p-1}(x; M) \to 0.$$

Hence $H_{s+1}(x; M/a_1M) \neq 0$, but $H_p(x; M/a_1M) = 0$ for $p \geqq s + 2$. From the hypothesis that $a_1, \ldots, a_q$ is a maximal M-regular sequence, it follows at once that $a_2, \ldots, a_q$ is maximal M/a_1M-regular in I, so by induction, $q - 1 = r - (s + 1)$ and hence $q + s = r$, as was to be shown.]

5. The following exercise combines some notions of Chapter XX on homology, and some notions covered in this chapter and in Chapter X, §5. Let M be an A-module.

Let A be Noetherian, M finite module over A, and I an ideal of A such that $IM \neq M$. Let r be an integer $\geqq 1$. Prove that the following conditions are equivalent:

(i) $\operatorname{Ext}^i(N, M) = 0$ for all $i < r$ and all finite modules N such that $\operatorname{supp}(N) \subset \mathfrak{X}(I)$.

(ii) $\operatorname{Ext}^i(A/I, M) = 0$ for all $i < r$.

(iii) There exists a finite module N with $\operatorname{supp}(N) = \mathfrak{X}(I)$ such that

$$\operatorname{Ext}^i(N, M) = 0 \quad \text{for all } i < r.$$

(iv) There exists an M-regular sequence $a_1, \ldots, a_r$ in I.

[*Hint*: (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) is clear. For (iii) $\Rightarrow$ (iv), first note that

$$0 = \operatorname{Ext}^0(N, M) = \operatorname{Hom}(N, M).$$

Assume $\operatorname{supp}(N) = \mathfrak{X}(I)$. Find an M-regular element in I. If there is no such element, then I is contained in the set of divisors of 0 of M in A, which is the union of the associated primes. Hence $I \subset P$ for some associated prime P. This yields an injection $A/P \subset M$, so

$$0 \neq \operatorname{Hom}_{A_P}(A_P/PA_P, M).$$

By hypothesis, $N_P \neq 0$ so $N_P/PN_P \neq 0$, and N_P/PN_P is a vector space over A_P/PA_P, so there exists a non-zero A_P/PA_P homomorphism

$$N_P/PN_P \to M_P,$$

so $\operatorname{Hom}_{A_P}(N_P, M_P) \neq 0$, whence $\operatorname{Hom}(N, M) \neq 0$, a contradiction. This proves the existence of one regular element a_1.

Now let $M_1 = M/a_1M$. The exact sequence

$$0 \to M \xrightarrow{a_1} M \to M/a_1M \to 0$$

yields the exact cohomology sequence

$$\to \operatorname{Ext}^i(N, M) \to \operatorname{Ext}^i(N, M/a_1M) \to \operatorname{Ext}^{i+1}(N, M) \to$$

so $\operatorname{Ext}^i(N, M/a_1M) = 0$ for $i < r - 1$. By induction there exists an M_1-regular sequence $a_2, \dots, a_r$ and we are done.

Last, (iv) $\Rightarrow$ (i). Assume the existence of the regular sequence. By induction, $\operatorname{Ext}^i(N, a_1M) = 0$ for $i < r - 1$. We have an exact sequence for $i < r$:

$$0 \to \operatorname{Ext}^i(N, M) \xrightarrow{a_1} \operatorname{Ext}^i(N, M)$$

But $\operatorname{supp}(N) = \mathfrak{X}(\operatorname{ann}(N)) \subset \mathfrak{X}(I)$, so $I \subset \operatorname{rad}(\operatorname{ann}(N))$, so a_1 is nilpotent on N. Hence a_1 is nilpotent on $\operatorname{Ext}^i(N, M)$, so $\operatorname{Ext}^i(N, M) = 0$. Done.] See Matsumura's [Mat 70], p. 100, Theorem 28. The result is useful in algebraic geometry, with for instance $M = A$ itself. One thinks of A as the affine coordinate ring of some variety, and one thinks of the equations $a_i = 0$ as defining hypersurface sections of this variety, and the simultaneous equations $a_1 = \cdots = a_r = 0$ as defining a complete intersection. The theorem gives a cohomological criterion in terms of Ext for the existence of such a complete intersection.