A THEOREM OF HOMOLOGICAL ALGEBRA: THE HILBERT-BURCH THEOREM

Maiyuran Arumugam

Supervisor: Dr. Daniel Chan

School of Mathematics,

The University of New South Wales.

November 2005

Submitted in partial fulfillment of the requirements of the degree of

Bachelor of Science with Honours

Abstract

In his 1956 paper 'A theorem of homological algebra', Rees introduced the grade or depth of an ideal to the world. In the decades since it has become a tool of great significance in homological algebra, spawning the development of a number of new areas of study.

This thesis aims to develop the basic homological theory leading to the idea of depth, and then to use this concept to prove the Hilbert-Burch theorem. A few of the numerous applications of this theorem are also briefly discussed.

Simplifying assumptions have been made along the way, so the treatment of material is for the most part played out in the setting of Noetherian rings and modules.

Acknowledgements

I would like to express my sincere gratitude to all those who have helped make the last four years a wonderful experience - I know I'll forget to mention someone who deserves credit below, so thank you one and all!

I would like to thank the UNSW School of Mathematics and Department of Actuarial Studies for all their support and assistance through the last four years. Special thanks must go to my supervisor, Dr. Daniel Chan, for all his guidance, support and patience throughout this year, giving up much of his time to help clarify matters. Thanks also to Dr. Ian Doust and Dr. Dennis Trenerry for their valuable advice and assistance in the course of my degree.

Thanks also to the many friends - particularly Alex, Dom, Doris, Han, Hing, Imanuel, Ishtiaq, Jack, Jacquie, Kenneth and my fellow Honours students - whose companionship has made this journey so enjoyable (and kept me out of a strait-jacket in the process)!

Finally, and most importantly, thanks to my parents and my sister for all their patience, understanding and support through this year and all the ones before it.

Maiyuran Arumugam, November 2005.

Preliminaries

Author's Note

At the beginning of this year, I set out to study the key results developed by David Buchsbaum and David Eisenbud in their paper [BE77] and look at how this related to the Hilbert-Burch theorem from homological algebra.

Little did I realize just how deep the mine of knowledge I was tapping into would prove to be, and in the end I have - unfortunately - been unable to reach this original goal, having struck out in different directions numerous times through the year.

What I have set out to do in writing this thesis, therefore, is to provide a concise account of the basics of homological algebra and to give some insight into the use of depth as a homological device, leading up to the Hilbert-Burch theorem.

Although for the most part the material here is an exposition of material from existing sources, I have at times attempted to present proofs which differ from those typically found in the literature, in order to emphasize particular ideas. Thus for example the proof of the Auslander-Buchsbaum Formula in Section 3.4 is done in a fashion (using the functor Ext) that I have not as yet seen elsewhere (though I do not doubt it has been done before).

There is a considerable amount of material in this thesis, but it barely scratches the surface of the possibilities available in homological algebra, and I have reluctantly omitted a number of potentially interesting topics, as will become evident from my concluding remarks.

It is generally assumed the reader is familiar with the notions of group and ring theory (to the level taught in third year at the University of New South Wales, for instance), and has at the least a vague grasp of what a module is and of some of basic properties of modules. This is sufficient to read Chapter 6, following which the reader should be ready to launch into the thesis proper.

The reader with more exposure to modules and rings may well be able to skim past Chapter 6, however it is recommended that all readers at the least skim Chapter 6, simply to ensure awareness of any conventions to be introduced in this chapter.

Finally, since no work of mathematics would be complete without an exercise for the reader, I have made the attempt to include one. A truly worthy exercise, however, is to *"Take any book on homological algebra, and prove all the theorems without looking at the proofs given in that book."* (This problem is supposed to have been posed by Serge Lang on p.105 of the 1965 edition of his textbook 'Algebra').

Structure of this Thesis

This section provides a brief guide to the contents - the chapters should be read in sequence to maintain coherence... after being reduced modulo 6.

Chapter 6 is mainly a chapter of preliminaries, introducing modules in a very speedy fashion and then adding some useful miscellaneous results (since once the brief introduction to modules is complete it is not expected the reader will need much more knowledge). It is recommended that all readers at least glance through this chapter before progressing any further, simply to get a feel for any restrictions/assumptions that may be imposed (e.g. that all rings are Noetherian and all modules finitely generated), though after this the reader will probably not find it necessary to refer to this chapter again.

Chapters 1 and 2 introduce the homological algebra needed for the results of this thesis. Chapter 1 focuses on the very basic terminology and ideas, leading up to the long exact sequence in homology, whilst Chapter 2 deals with the more advanced concepts of resolutions and functors. In particular we look at the functors Tor and Ext, and the chapter concludes by expressing the homological dimension of a module in terms of Tor and Ext.

Chapter 3 introduces regular sequences, and uses these to lead into the concept of the depth of an ideal. We then look at how depth relates to some other possibilities for measuring the size of an ideal, such as dimension and codimension, before concluding the chapter with a proof of the famous Auslander-Buchsbaum Formula.

In Chapter 4 we approach regular sequences from a different direction, based on the Koszul complex. We develop this as a homological tool by starting from simple examples and building up a more general theory using the concept of a mapping cone. The chapter is closed out by a section relating the homology of the Koszul complex to regular sequences.

Finally, in Chapter 5 we come to the Hilbert-Burch theorem of the title. We proceed to prove the Hilbert-Burch theorem and discuss some of its potential applications, making note of an important result on the characterization of free resolutions along the way.

Conventions and Notation

It often happens in mathematics that different sources use different notation for the same thing (or use the same notation to mean different things), but some conventions have been established:

- Throughout this thesis, $\mathbb{K}$ will denote a field.
- A 'ring' (usually denoted R) refers to a Noetherian commutative ring with identity
- A 'module' (usually denoted M) refers to a finitely generated R-module over a ring as above, though we will often omit the ring and refer simply to a 'module'.
- Given elements $m_1, m_2, \ldots$ in an R-module M as above, then $\langle m_1, m_2, \ldots \rangle$ denotes the submodule of M generated by these elements. This notation also denotes ideals of a ring, since these are submodules of the ring as a module over itself.
- Ideals of a ring R will usually be denoted I. Prime or maximal ideals will respectively be denoted by P or $\mathfrak{m}$.
- Given a module M over a ring R we write $M \xrightarrow{x} M$ (where $x \in R$) for the R-module homomorphism $\varphi : M \to M$ defined by $\varphi(m) = xm$ for all $m \in M$.
- In a quotient module of a module M, then $[m]$ will denote the coset of $m \in M$ in the quotient module.

At times we may have cause to explicitly disregard these conventions, and if doing so will state as much. We may also reiterate redundant points (such as rings being Noetherian) for emphasis.

Contents

Chapter 1

Basic Homological Algebra

Homological algebra has its origins in algebraic topology, however the usefulness of being able to access homological methods in commutative algebra has seen the field expand into most aspects of mainstream algebra, to the point where it is now an invaluable tool for the modern algebraist. Indeed, the rise of homological algebra is often considered to be one reason why modules have supplanted ideals as the most popular structures used in modern algebra, though there is still a significant interplay between the two.

In this chapter we begin by introducing the language of category theory, and then go on to introduce a few of the basic ideas of homological algebra, starting from complexes and working our way through homology groups to build up to the long exact sequence in homology.

We will then take advantage of the base established in this fashion in the next chapter, where we progress to developing some of the more advanced material that will recur somewhat more frequently in the course of this thesis.

The two chapters are essentially a pair, and should be treated as such. An excellent reference for the content of both chapters is [OSB00], whilst most of the ideas are introduced quite succintly (albeit from a somewhat more topological viewpoint than we will be taking) in [CC05], and are of a standard that is (hopefully) accessible to the reader.

1.1 Category Theory

There is a great deal of similarity between different areas of algebra, e.g. groups, rings and modules all possess homomorphisms, isomorphisms, isomorphism theorems, and the like. These similarities can be exploited using category theory, which brings these structures (and their characteristics) together under a single roof. Since its origins in the work of Eilenberg & Maclane in the 1940s, category theory has evolved in response to the needs of algebraic topology, homological algebra and most recently algebraic geometry.

The language of category theory is now widely used, but there are few specific results to do with category theory. This section, therefore, is primarily to provide concrete definitions of some key terms, together with a few examples. For the sake of simplicity we omit checking that the examples satisfy the definitions.

Definition 1.1. *A* ***category*** $\mathcal{C}$ *consists of a class of objects (denoted Obj* $\mathcal{C}$*) such that for any two objects* $X, Y \in Obj\, \mathcal{C}$ *there is a set of morphisms* $Mor_{\mathcal{C}}(X, Y)$ *and:*

- *For* $X, Y, Z \in Obj\, \mathcal{C}$ *the composition map* $Mor_{\mathcal{C}}(X, Y) \times Mor_{\mathcal{C}}(Y, Z) \to Mor_{\mathcal{C}}(X, Z)$ *taking* $(f, g) \mapsto g * f$ *is associative.*
- *For each* $X, Y \in Obj\, \mathcal{C}$ *there exists* $id_X \in Mor_{\mathcal{C}}(X, X)$ *such that* $f * id_X = f$ *and* $id_X * g = g$ *(for* $f \in Mor_{\mathcal{C}}(X, Y)$ *and* $g \in Mor_{\mathcal{C}}(Y, X)$*).*

Example 1.2. For any ring R, $R - Mod$ and $Mod - R$ denote the categories of left and right R-modules respectively (with morphisms and composition respectively defined as module homomorphisms and composition in the natural sense, i.e. $f * g = f \circ g$). □

Example 1.3. *Ab* denotes the category of abelian groups, with morphisms and composition defined naturally, as for the module categories. □

Example 1.4. Given any category $\mathcal{C}$, we can form the *opposite category* $\mathcal{C}^{op}$ where Obj $\mathcal{C}^{op}$ = Obj $\mathcal{C}$, $Mor_{\mathcal{C}^{op}}(X, Y) = Mor_{\mathcal{C}}(Y, X)$ and composition is defined by $f *^{op} g = g * f$. □

We can now define familiar ideas such as isomorphisms using this new terminology.

Definition 1.5. *An **isomorphism** between two objects X, Y in a category $\mathcal{C}$ is a morphism $f \in Mor_{\mathcal{C}}(X, Y)$ for which there exists $g \in Mor_{\mathcal{C}}(Y, X)$ with $f * g = id_Y$ and $g * f = id_X$.*

Hand-in-hand with the concept of a category is that of a *functor*, which is essentially a function between categories, and allows us to consider relationships between categories.

Definition 1.6. *A **(covariant) functor** F between categories $\mathcal{C}$ and $\mathcal{D}$ consists of:*

- *A function $F : Obj\,\mathcal{C} \to Obj\mathcal{D}$ taking $X \mapsto F(X)$.*
- *For any $X, Y \in Obj\,\mathcal{C}$ a function $F : Mor_{\mathcal{C}}(X, Y) \to Mor_{\mathcal{D}}(F(X), F(Y))$ such that $F(id_X) = id_{F(X)}$ and $F(g * f) = F(g) * F(f)$.*

*A **contravariant functor** F between two categories $\mathcal{C}$ and $\mathcal{D}$ is simply a covariant functor from $\mathcal{C} \to \mathcal{D}^{op}$.*

Example 1.7. Given some fixed $M \in R-Mod$ then $\mathrm{Hom}_R(M, -)$ is a (covariant) functor from $R - Mod$ to $R - Mod$, and $\mathrm{Hom}_R(-, M)$ is a (contravariant) functor from $Mod - R$ to $Mod - R$. □

Example 1.8. Given some fixed $M \in Mod-R$ then $M \otimes_R -$ is a (covariant) functor from $R-Mod$ to $R-Mod$ and $- \otimes_R M$ is a (covariant) functor from $Mod-R$ to $Mod-R$. □
(This is perhaps not the most significant of discrepancies, however, as we are working within a structure where we can treat any module as both a left and right R-module).

These two examples will be encountered again in more detail in Chapter 2.

1.2 Complexes

Of interest in the theory of homology are sequences of modules (over a particular ring) linked by homomorphisms (a topological approach to this is developed in [CC05]). In particular, those sequences where composition of homomorphisms gives zero are of interest, and lead to the definition of a complex.

Definition 1.9.

$$M_\bullet : \ldots \longrightarrow M_{i+1} \xrightarrow{\partial_i} M_i \xrightarrow{\partial_{i-1}} M_{i-1} \longrightarrow \cdots \tag{1.1}$$

A sequence of modules (as displayed above) is a ***(chain) complex*** *if any two consecutive morphisms compose to give* 0*, i.e. if* $\partial_{i-1}\partial_i = 0$ *for all* i*.*

Example 1.10. Over the ring $\mathbb{Z}$, consider the sequence $0 \longrightarrow \mathbb{Z} \xrightarrow{\varphi} \mathbb{Z} \xrightarrow{\psi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$, where φ is multiplication by 4, and ψ takes any $n \in \mathbb{Z}$ into the coset $n + 2\mathbb{Z}$ of $\mathbb{Z}/2\mathbb{Z}$. This is a complex of $\mathbb{Z}$-modules. □

Example 1.11. Given a ring R, the sequence $0 \longrightarrow R \xrightarrow{x} R \longrightarrow 0$ is a complex of R-modules. (Here the superscript x denotes multiplication by $x \in R$.) □

Equivalently, a complex is a sequence of modules with $\operatorname{im}(\partial_i) \subseteq \ker(\partial_{i-1})$ for all i. This naturally leads to questions about the case of equality, and about possible quotient groups.

Definition 1.12. *The* i^{th} ***homology group*** *(denoted* $H_i(M_\bullet)$*) of a complex* $M_\bullet$ *as in (4.1) is the quotient group* $ker(\partial_{i-1})/im(\partial_i)$*. We say* $M_\bullet$ *is* ***exact at*** M_i *if* $H_i(M_\bullet) = 0$*, and* $M_\bullet$ *is* ***exact*** *if it is exact at* M_i *for all* i*.*

Example 1.13. Over the ring $\mathbb{R}$, an example of an exact complex of $\mathbb{R}$-modules is (recall matrices act (multiply) on the left):

$$0 \longrightarrow \mathbb{R}^2 \xrightarrow{\begin{pmatrix} 1 & 1 \\ -1 & 0 \\ 0 & -1 \end{pmatrix}} \mathbb{R}^3 \xrightarrow{\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}} \mathbb{R} \longrightarrow 0$$

□

Example 1.14. In Example 1.11, the 0^{th} and 1^{st} homology groups are $R/\langle x\rangle$ and $\{r \in R \mid rx = 0\}$ respectively. □

The above example helps motivate for the study of complexes and exact sequences, as we are studying the kernel of the map $\begin{pmatrix}1 & 1 & 1\end{pmatrix}$ as a submodule (vector subspace) of $\mathbb{R}^3$ by mapping a copy of $\mathbb{R}^2$ onto it, which we can then manipulate as desired.

Remark 1.15. There is a corresponding theory for complexes where the indices are increasing, i.e. those of the form $M_\bullet : \ldots \longrightarrow M_{i-1} \xrightarrow{d^i} M_i \xrightarrow{d^{i+1}} M_{i+1} \longrightarrow \cdots$. Such complexes are called ***cochain complexes***, and the i^{th} homology group is called the i^{th} ***cohomology group*** of the complex, denoted $H^i(M_\bullet)$. We will typically refer to chain complexes simply as complexes - we will not be using cochain complexes, so no confusion should arise. □

Special cases of exact sequences include $0 \longrightarrow A \xrightarrow{f} B$ and $A \xrightarrow{g} B \longrightarrow 0$, which demonstrate that f is injective (its kernel is trivial) and g is surjective (has image B). Combining these gives one of the most important types of exact sequence, called the short exact sequence.

Example 1.16. A **short exact sequence** is an exact sequence of the form

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

□

Exactness is at once very simple and very powerful, and forms a key element of the technique known as the **diagram chase**, which is nicely illustrated by the next result.

Theorem 1.17 (The Short 5 lemma). *Consider the following commutative diagram of two short exact sequences. If φ and ρ are isomorphisms, then so is ψ.*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\rho} & & \\
0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0
\end{array}$$

Proof. Suppose $u \in \ker(\psi)$. Then commutativity of the diagram tells us $\rho(g(u)) = g'(\psi(u)) = g'(0) = 0$, and since ρ is an isomorphism, $g(u) = 0$. Exactness at B means that $u \in \ker(g) \Rightarrow u \in \mathrm{im}(f)$, so there exists $a \in A$ such that $f(a) = u$.

Commutativity of the diagram now gives $f'(\varphi(a)) = \psi(f(a)) = \psi(u) = 0$, meaning $\varphi(a) = 0$ (by injectivity of f' using exactness at A') and so $a = 0$ (since φ is an isomorphism), so that $u = f(0) = 0$. Hence $u \in \ker(\psi) \Rightarrow u = 0$, so ψ is injective.

Next, consider $b' \in B'$. Then $g'(b') \in C'$, so $\rho^{-1}(g'(b')) \in C$, and by surjectivity of g there exists $b \in B$ such that $g(b) = \rho^{-1}(g'(b'))$. By commutativity of the diagram, $g'(\psi(b)) = \rho(g(b)) = \rho(\rho^{-1}(g'(b'))) = g'(b')$, so $g'(b' - \psi(b)) = 0$.

This means $b' - \psi(b) \in \ker(g') = \mathrm{im}(f')$ (by exactness at B'), so there exists a' in A' with $f'(a') = b' - \psi(b)$. Since φ is an isomorphism, there exists $a \in A$ such that $\varphi(a) = a'$, and $b' - \psi(b) = f'(\varphi(a)) = \psi(f(a))$ by commutativity of the diagram. Hence $b' = \psi(b) + \psi(f(a)) = \psi(b + f(a))$, so $b' \in B' \Rightarrow b' \in \mathrm{im}(\psi)$, showing that ψ is surjective and thus completing the proof of the short 5 lemma. □

In the short 5 lemma, we linked two complexes via a series of morphisms to produce a commutative diagram. This leads to the definition of a chain map between complexes.

Definition 1.18. *A **chain map** between two chain complexes $M_\bullet$ and $M'_\bullet$ is a collection of maps $\psi_\bullet := \{\psi_i\}_{i \in \mathbb{Z}}$ such that for each i $\psi_i : M_i \to M'_i$ is a module homomorphism and the following diagram commutes:*

$$\begin{CD}
\cdots @>>> M_{i+1} @>\partial_{i+1}>> M_i @>\partial_i>> M_{i-1} @>>> \cdots \\
@. @VV\psi_{i+1}V @VV\psi_iV @VV\psi_{i-1}V @. \\
\cdots @>>> M'_{i+1} @>\partial'_{i+1}>> M'_i @>\partial'_i>> M_{i-1} @>>> \cdots
\end{CD}$$

This notion of a chain map gives some structure to the class of complexes - we can now consider complexes as we do modules, with for instance a zero complex $0_\bullet$ being a sequence of zero modules. Such a complex can be linked to other complexes via the trivial chain map, consisting of a series of zero homomorphisms.

Remark 1.19. Following on from this, it should come as no surprise to discover that there is a category of complexes, where the objects are the chain complexes and morphisms are the chain maps between complexes. □

1.3 Homology

In this section we briefly outline some important properties of the homology groups of a complex, which we will study primarily for the information they provide about the extent to which the complex 'deviates' from exactness. This in turn lets us make statements about the modules in the complex.

It is straightforward to show the homology groups obtained from a complex of R-modules are themselves R-modules, using the properties of the R-module homomorphisms between the modules in the sequence (namely, that their kernels and images are also R-modules, and hence the quotients are also R-modules).

The introduction of chain maps in the previous section adds another tool to our kit for studying these groups, since a chain map between two complexes naturally induces a series of homomorphisms between the homology groups of these complexes, as we now prove.

Proposition 1.20. *Given a chain map $\psi_\bullet$ between two complexes $M_\bullet$ and $M'_\bullet$, as shown*

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & M_{i+1} & \xrightarrow{\partial_{i+1}} & M_i & \xrightarrow{\partial_i} & M_{i-1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle \psi_{i+1}} & & \downarrow{\scriptstyle \psi_i} & & \downarrow{\scriptstyle \psi_{i-1}} & & \\
\cdots & \longrightarrow & M'_{i+1} & \xrightarrow{\partial'_{i+1}} & M'_i & \xrightarrow{\partial'_i} & M_{i-1} & \longrightarrow & \cdots
\end{array}$$

then for each i there is a homomorphism $H_i(\psi_\bullet) : H_i(M_\bullet) \to H_i(M'_\bullet)$ induced by ψ_i and defined by $(H_i(\psi_\bullet))([m]) = [\psi_i(m)]$ for all $m \in ker(\partial_i)$ ($[m]$ denotes the coset $m + im(\partial_{i+1})$ in the homology group $H_i(M_\bullet)$). A common convention (which we will adopt) is to write $(\psi_*)_i := H_i(\psi_\bullet)$.

Proof. We must show that $(\psi_*)_i$ is well-defined for each i, which has two components:

- Given $m \in \ker(\partial_i)$, we need $\psi_i(m) \in \ker(\partial'_i)$. Here if $m \in \ker(\partial_i)$ then $\psi_{i-1}(\partial_i(m)) = \psi_{i-1}(0) = 0$ (homomorphisms take 0 to 0), but commutativity of the diagram means $\partial'_i(\psi_i(m)) = \psi_{i-1}(\partial_i(m)) = 0$, confirming $\psi_i(m) \in \ker(\partial'_i)$, as desired.
- Given $n \in \mathrm{im}(\partial_{i+1})$, we need $\psi_i(n) \in \mathrm{im}(\partial_{i+1})$ (to ensure different coset representatives in $H_i(M_\bullet)$ give the same coset in $H_i(M'_\bullet)$). Here if $n \in \mathrm{im}(\partial_{i+1})$ there exists $u \in M_{i+1}$ with $\partial_{i+1}(u) = n$. By commutativity of the diagram, we see $\psi_i(n) = \psi_i(\partial_{i+1}(u)) = \partial'_{i+1}(\psi_{i-1}(u)) \in \mathrm{im}(\partial'_{i+1})$, as desired.

Showing $(\psi_*)_i)$ is a module homomorphism is straightforward, so is omitted. ☐

Whilst chain maps provide a tool for studying homology groups, there is a question over when two chain maps between the same complexes might induce the same maps on homology. This question is answered through the definition of an equivalence relation.

Definition 1.21. *Given a ring R, two complexes $M_\bullet$ and $M'_\bullet$ of R-modules, and two chain maps $\varphi_\bullet, \tilde{\varphi}_\bullet : M_\bullet \to M'_\bullet$ as below:*

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & M_{n+1} & \xrightarrow{\partial_{n+1}} & M_n & \xrightarrow{\partial_n} & M_{n-1} & \xrightarrow{\partial_{n-1}} & \cdots \\
 & & {\scriptstyle\tilde{\varphi}_{n+1}}\Downarrow\Downarrow{\scriptstyle\varphi_{n+1}} & & {\scriptstyle\tilde{\varphi}_{n}}\Downarrow\Downarrow{\scriptstyle\varphi_{n}} & & {\scriptstyle\tilde{\varphi}_{n-1}}\Downarrow\Downarrow{\scriptstyle\varphi_{n-1}} & & \\
\cdots & \longrightarrow & M'_{n+1} & \xrightarrow{\partial'_{n+1}} & M'_n & \xrightarrow{\partial'_n} & M'_{n-1} & \xrightarrow{\partial'_{n-1}} & \cdots
\end{array}$$

then we say $\varphi_\bullet$ and $\tilde{\varphi}_\bullet$ are ***homotopy equivalent*** *if there exists a collection of module homomorphisms $s_\bullet$ with $s_i : M_i \to M'_{i+1}$ defined such that $\varphi_i - \tilde{\varphi}_i = \partial'_{i+1} \circ s_i + s_{i-1} \circ \partial_i$ for all i. The map $s_\bullet$ is called a* ***homotopy****.*

This notion of homotopy plays a significant role in topology, and defines an equivalence relation on chain maps - two chain maps are equivalent iff there is a homotopy between them. The use of this equivalence relation is that two homotopic chain maps induce the same map on homology, so the equivalence classes of chain maps now give the induced maps on homology. We refer the reader to [CC05] for the details.

1.4 The Long Exact Sequence in homology

In this section we will introduce the long exact sequence in homology, which is one of the most useful gadgets available in the field of homological algebra, and is a key component of actually computing homology groups, in most cases.

But first, having been equipped with the notion of chain maps between complexes, we can now consider the notion of exact sequences of complexes.

Definition 1.22. *Given complexes $M_\bullet$, $M'_\bullet$ and $M''_\bullet$ and chain maps $f_\bullet : M'_\bullet \to M_\bullet$, $g_\bullet : M_\bullet \to M''_\bullet$ then we have a* ***short exact sequence of complexes*** *given by*

$$0_\bullet \longrightarrow M'_\bullet \xrightarrow{f_\bullet} M_\bullet \xrightarrow{g_\bullet} M''_\bullet \longrightarrow 0_\bullet$$

if for each i there is an exact sequence given by:

$$0 \longrightarrow M'_i \xrightarrow{f_i} M_i \xrightarrow{g_i} M''_i \longrightarrow 0$$

Here the 'short exact sequence of complexes' is actually a structure of the form below, where the rows are short exact sequences and columns are complexes:

$$\begin{array}{ccccccccc}
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M'_{i+1} & \xrightarrow{f_{i+1}} & M_{i+1} & \xrightarrow{g_{i+1}} & M''_{i+1} & \longrightarrow & 0 \\
 & & \downarrow \partial'_{i+1} & & \downarrow \partial_{i+1} & & \downarrow \partial''_{i+1} & & \\
0 & \longrightarrow & M'_i & \xrightarrow{f_i} & M_i & \xrightarrow{g_i} & M''_i & \longrightarrow & 0 \\
 & & \downarrow \partial'_i & & \downarrow \partial_i & & \downarrow \partial''_i & & \\
0 & \longrightarrow & M'_{i-1} & \xrightarrow{f_{i-1}} & M_{i-1} & \xrightarrow{g_{i-1}} & M''_{i-1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & &
\end{array}$$

(for simplicity we omit the homomorphisms in the two zero complexes!)

We now proceed to the the long exact sequence in homology.

Theorem 1.23 (Long Exact Sequence in homology). *Suppose we have a short exact sequence of chain complexes described as below:*

$$0_\bullet \longrightarrow M'_\bullet \xrightarrow{f_\bullet} M_\bullet \xrightarrow{g_\bullet} M''_\bullet \longrightarrow 0_\bullet$$

This induces a long exact sequence of maps in homology as below:

$$\longrightarrow H_n(M'_\bullet) \xrightarrow{(f_*)_n} H_n(M_\bullet) \xrightarrow{(g_*)_n} H_n(M''_\bullet) \xrightarrow{\delta_n} H_{n-1}(M'_\bullet) \xrightarrow{(f_*)_{n-1}} \cdots \tag{1.2}$$

The maps $\delta_n : H_n(M''_\bullet) \to H_{n-1}(M'_\bullet)$ are called ***connecting homomorphisms****.*

Proof. Proposition (1.20) gives us well-defined maps $(f_*)_n$ and $(g_*)_n$ for all n. It remains, therefore, to define δ_n and check it is a module homomorphism for all n, and following this, to check exactness at all points. We begin by defining δ_n.

We will keep track of the algebra using the following commutative diagram:

$$\begin{array}{ccccc}
 & & y & \overset{g_n}{\longmapsto} & x \\
 & & \downarrow{\scriptstyle \partial_n} & & \downarrow{\scriptstyle \partial''_n} \\
z & \overset{f_{n-1}}{\longmapsto} & \partial_n(y) & \overset{g_{n-1}}{\longmapsto} & 0 \\
\downarrow{\scriptstyle \partial'_{n-1}} & & \downarrow{\scriptstyle \partial_{n-1}} & & \\
0 & \overset{f_{n-2}}{\longmapsto} & 0 & &
\end{array}$$

Consider $x \in \ker(\partial''_n) \subseteq M''_n$. Since g_n is surjective (the rows are short exact sequences) there exists $y \in M_n$ with $g_n(y) = x$, and so $0 = \partial''_n(x) = \partial''_n(g_n(y)) = g_{n-1}(\partial_n(y))$. Thus $\partial_n(y) \in \ker(g_{n-1}) = \text{im}(f_{n-1})$, so there exists $z \in M'_n$ with $f_{n-1}(z) = \partial_n(y)$ (as f_{n-1} injective means y uniquely determines z).

Further, $f_{n-2}(\partial'_{n-1}(z)) = \partial_{n-1}(f_{n-1}(z)) = \partial_{n-1}(\partial_{n-2}(y)) = 0$ (using commutativity of the diagram and the fact $M_\bullet$ is a complex), and since f_{n-2} is injective we find $\partial'_{n-1}(z) = 0$, i.e. $z \in \ker(\partial'_{n-1})$. Thus any given $x \in \ker(\partial''_n)$ leads to $z \in \ker(\partial'_{n-1})$, so we define δ_n by $\delta_n([x]) = [z]$. We check below that δ_n is well-defined, using the diagrams:

$$\begin{array}{ccccc} w & \xmapsto{f_n} & y-\hat{y} & \xmapsto{g_n} & 0 \\ \downarrow{\scriptstyle \partial'_n} & & \downarrow{\scriptstyle \partial_n} & & \downarrow{\scriptstyle \partial''_n} \\ z-\hat{z} & \xmapsto{f_{n-1}} & \partial_n(y-\hat{y}) & \xmapsto{g_{n-1}} & 0 \end{array} \qquad \text{and} \qquad \begin{array}{ccccc} & & u & \xmapsto{g_{n+1}} & v \\ & & \downarrow{\scriptstyle \partial_{n+1}} & & \downarrow{\scriptstyle \partial''_{n+1}} \\ & & y & \xmapsto{g_n} & x \\ & & \downarrow{\scriptstyle \partial_n} & & \\ z & \xmapsto{f_{n-1}} & 0 & & \end{array}$$

- Our choice of $[z]$ is independent of the choice of $y \in g_n^{-1}(x)$. Given another $\hat{y} \in g_n^{-1}(x)$ there is a unique $\hat{z} \in \ker(\partial'_{n-1})$ with $f_{n-1}(\hat{z}) = \partial_n(\hat{y})$. Then $g_n(y - \hat{y}) = x - x = 0$, so $y - \hat{y} \in \ker(g_n) = \operatorname{im}(f_n)$ and there exists a unique $w \in M'_n$ with $f_n(w) = y - \hat{y}$. It is easy to see that $f_{n-1}(\partial'_n(w)) = \partial_n(f_n(w)) = \partial_n(y - \hat{y}) = \partial_n(y) - \partial_n(\hat{y}) = f_{n-1}(z) - f_{n-1}(\hat{z}) = f_{n-1}(z - \hat{z})$, and injectivity of f_{n-1} forces $z - \hat{z} = \partial'_n(w)$. Thus $[z] = [\hat{z}]$, giving independence of z under choice of y.
- Choice of $[z]$ is independent of which coset representative of $[x]$ we began with, or equivalently, $x \in \operatorname{im}(\partial''_{n+1}) \Rightarrow z \in \operatorname{im}(\partial'_n)$. Suppose that $x = \partial''_{n+1}(v)$ for $v \in M''_{n+1}$. Then $v = g_{n+1}(u)$ for some $u \in M_{n+1}$ and $x = \partial''_{n+1}(g_{n+1}(u)) = g_n(\partial_{n+1}(u))$. Thus we can choose $y \in g_n^{-1}(x)$ to be $\partial_{n+1}(u)$, giving $\partial_n(y) = \partial_n(\partial_{n+1}(u)) = 0$, so our choice of $z \in \ker(f_{n-1})$ is in fact forced to be $z = 0 \in \operatorname{im}(\partial'_n)$. Since choice of y does not affect the coset $[z]$ for a given x, then $x \in \operatorname{im}(\partial''_{n+1}) \Rightarrow [z] = \operatorname{im}(\partial'_n)$.

Thus δ_n is well-defined for all n, and it is easily checked that δ_n is always a module homomorphism, so we omit this. It remains only to check exactness:

- *Exactness at* $H_n(M_\bullet)$. Given $[w] \in H_n(M'_\bullet)$, then exactness of rows lets us state $(g_*)_n((f_*)_n([w])) = (g_*)_n([f_n(w)]) = [g_n(f_n(w))] = [0]$, so $\ker((g_*)_n) \supseteq \operatorname{im}((f_*)_n)$.

For the converse, suppose $[y] \in \ker((g_*)_n)$, so $g_n(y) \in \operatorname{im}(\partial''_{n+1})$. Then for some $v \in M''_{n+1}$ we have $g_n(y) = \partial''_{n+1}(v)$, and by surjectivity of g_{n+1} for some $u \in M_{n+1}$ we have $v = g_{n+1}(u)$. Hence $g_n(y) = \partial''_{n+1}(g_{n+1}(v)) = g_n(\partial_{n+1}(u))$, and so $y - \partial_{n+1}(u) \in \ker(g_n)$ (as g_n is a homomorphism).

Exactness of rows ensures $y - \partial_{n+1}(u) = f_n(w)$ for some $w \in M'_{n+1}$, and so provided $w \in \ker(\partial'_n)$ then $(f_*)_n([w]) = [y]$. Thus to show $\partial'_n(w) = 0$ it suffices to show $f_{n-1}(\partial'_n(w)) = 0$ (by injectivity of f_{n-1}). Since the diagram commutes, it is equivalent to get $0 = \partial_n(f_n(w)) = \partial_n(y - \partial_{n+1}(u)) = \partial_n(y) = 0$ (as $y \in \ker(\partial_n)$ is part of the definition of $[y] \in H_n(M_\bullet)$).

- *Exactness at $H_n(M'_\bullet)$ and $H_n(M''_\bullet)$* follow similarly by diagram chase, so are omitted.

This completes the proof, giving us the long exact sequence in homology, as desired. □

Chapter 2

Resolutions and Functors

Having established some of the basic ideas underpinning homological algebra, we now move to more advanced notions, namely those of forming resolutions of a module and of producing a 'derived functor' based on a given functor. In particular, we consider the functors Ext and Tor, which were introduced by Cartan and Eilenberg in [CE56] to unify the cohomology theories of groups, Lie algebras and associative algebras.

This chapter can essentially be considered an extension of the previous one, so the same remarks apply, and as with the previous chapter, the recommended references for the subject matter are [OSB00] and [CC05].

2.1 Resolutions

Definition 2.1. *Given a ring R and an R-module M, then a* ***resolution of*** *M is an exact complex of R-modules of the form:*

$$\cdots \longrightarrow M_2 \xrightarrow{\varphi_2} M_1 \xrightarrow{\varphi_1} M_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

If there exists some $n \geq 0$ such that $M_k = 0$ for all $k > n$ (and $M_n \neq 0$), then the resolution is said to be ***finite*** *of length n.*

This concept of a resolution of an R-module does not at first appear to be one of particular interest, and indeed, might seem to complicate the situation by introducing more modules. It is precisely this introduction of new modules that makes resolutions so useful, when we restrict the types of modules to be introduced.

Definition 2.2. *Given a ring R and an R-module M, then a* ***projective resolution*** *of M is an exact complex of R-modules of the form:*

$$\cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

where P_0, P_1, $\ldots$ are all projective modules. If $P_0, P_1, \ldots$ are all free modules, then the resolution is a ***free resolution*** *of M.*

Remark 2.3. Sometimes a resolution of M is written in the form:

$$\cdots \longrightarrow M_2 \xrightarrow{\varphi_2} M_1 \xrightarrow{\varphi_1} M_0 \longrightarrow 0$$

so the complex is exact everywhere except at M_0, with the homology at M_0 being:

$$M_0/\mathrm{im}(\varphi_1) = M_0/\ker(\varphi_0) \simeq \mathrm{im}(\varphi_0) = M$$

Note that although not explicitly provided, we are implicitly defining φ_0.

This is done mainly to ensure every explicitly stated module in a projective (or free) resolution is projective (or free), and the choice of notation is a matter of personal preference. At times we will use both in the chapters to come. □

Example 2.4. The complex $0 \longrightarrow R \xrightarrow{x} R \longrightarrow 0$ of Example 1.11 is a free resolution of $R/\langle x\rangle$ when x is not a zero divisor (written as in the above remark). In the notation of Definition 2.2 this would be:

$$0 \longrightarrow R \xrightarrow{x} R \longrightarrow R/\langle x\rangle \longrightarrow 0$$

where $R \to R/\langle x\rangle$ is the canonical quotient homomorphism. □

This example has now been used three times, and will be brought up again in the next few chapters - this complex is actually one of the simplest examples of the complex known as the *Koszul Complex*, which will be studied in detail in Chapter 4.

Example 2.5. In a ring R containing two elements x, y then a free resolution of $\langle x, y \rangle$ is given by the complex $0 \longrightarrow R \longrightarrow R^2 \longrightarrow \langle x, y \rangle \longrightarrow 0$, where the map $R \to R^2$ takes $r \mapsto \binom{ry}{-rx}$ and the map $R^2 \to \langle x, y \rangle$ takes $\binom{a}{b} \mapsto ax + by$. □

The usefulness of free resolutions is of course a moot point if we have no knowledge regarding their existence, but it turns out it is always possible to find a free (and hence projective) resolution of any module.

Proposition 2.6. *Any*[1] *module M over a given ring R possesses a free resolution.*

Proof. Firstly, we can choose a free module F_0 and map a set of generators of F_0 to a set of generators for M, giving a surjective map $\varphi_0 : F_0 \to M$. By the first isomorphism theorem (6.6), $F_0/\ker(\varphi_0) \simeq M$.

Now the 'obstruction to exactness' of the sequence $0 \longrightarrow F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$ is that the homology at F_0 is $\ker(\varphi_0)$, rather than 0, so it is of interest to look at this submodule of F_0.

As for M, we can choose a free module F_1 and a homomorphism φ_1 which maps a set of generators of F_1 to a set of generators of $\ker(\varphi_0)$. Continuing in this fashion, we construct the free resolution:

$$\cdots \longrightarrow F_{n+1} \xrightarrow{\varphi_{n+1}} F_n \xrightarrow{\varphi_n} F_{n-1} \longrightarrow \cdots \longrightarrow F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

where each φ_n surjectively maps F_n onto $\ker(\varphi_{n-1})$ (for $n > 0$) and φ_0 surjectively maps F_0 onto M. □

[1] Note that this includes modules which are not necessarily finitely generated!

Definition 2.7. *Given a ring R, the* ***projective dimension*** *(or* ***homological dimension****) of an R-module M (denoted $\mathrm{pd}_R(M)$) is the smallest non-negative integer n for which there exists a projective resolution of M of length n, i.e. the minimal n such that projective modules P_0, ..., P_n exist to make the following is an exact complex:*

$$0 \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

Projective resolutions offer a means to construct a complex (which happens to be exact) from any given module over a ring. Similarly, given a module homomorphism $\varphi : M \to N$ (for some modules M, N) and projective resolutions of M and N, we can construct a chain map $\tilde{\varphi}$ between them. We will prove this as a special case of a stronger result.

Theorem 2.8. *Given a ring R, suppose we have two complexes as below (of R-modules and R-module homomorphisms):*

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & P_1 & \xrightarrow{\partial_1} & P_0 & \xrightarrow{\partial_0} & N & \longrightarrow & 0 \\ & & & & & & \downarrow{\scriptstyle\varphi} & & \\ \cdots & \longrightarrow & M_1 & \xrightarrow{\partial'_1} & M_0 & \xrightarrow{\partial'_0} & N' & \longrightarrow & 0 \end{array}$$

where $P_0, P_1, \ldots$ are projective modules, and the lower row is an exact complex.

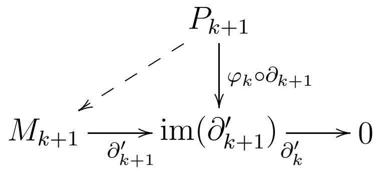
Then there is a chain map $\varphi_\bullet$ induced from the first complex to the second by φ, with $\varphi_i : P_i \to M_i$ and $\varphi_{-1} = \varphi$ (using negative indices because they are notationally nice).

([CC05] contains a version of this theorem for free modules, though of course all free modules are projective, and in the rings most interesting to us, vice versa).

Proof. Firstly, note that $\varphi \circ \partial_0 : P_0 \to N$ is an R-module homomorphism and that $\partial'_0 : M_0 \to N'$ is surjective (since the second complex is exact). Since P_0 is projective, there exists an R-module homomorphism $\varphi_0 : P_0 \to M_0$ such that $\partial'_0 \circ \varphi_0 = \varphi \circ \partial_0$.

We now proceed inductively - suppose we have constructed appropriate (commuting) module homomorphisms φ_j for all $j \leq k$. Then $\partial'_k \circ \varphi_k \circ \partial_{k+1} = \varphi_{k-1} \circ \partial_k \circ \partial_{k+1} = 0$, so $\mathrm{im}(\varphi_k \circ \partial_{k+1}) \subseteq \ker(\partial'_k) = \mathrm{im}(\partial'_{k+1})$.

As a result, we can form the commutative diagram below:



and the fact P_{k+1} is projective and ∂'_{k+1} surjective (onto $\mathrm{im}(\partial'_{k+1})$ lets us define a homomorphism $\varphi_{k+1} : P_{k+1} \to M_{k+1}$ such that $\partial'_{k+1} \circ \varphi_{k+1} = \varphi_k \circ \partial_{k+1}$. (The use of $\mathrm{im}(\partial'_{k+1})$ rather than M_k is of course valid as $\mathrm{im}(\partial'_{k+1})$ is a submodule of M_k).

This completes the inductive step, and with our base case, completes the proof. □

Whilst this construction does not guarantee uniqueness of the homomorphisms (and hence of the chain maps), it is possible to prove that all chain maps formed between two complexes in this fashion are homotopy equivalent.

Remark 2.9. Thus far we have been referring to projective resolutions, but as noted previously the cases of most interest to us tend to be local rings and polynomial rings, where projective modules are free modules. Hence in these situations we can and will refer to the projective dimension of a module as the minimal length of any *free* resolution of that module. □

Aside from minimality of length, there is another sense in which we can logically talk about minimality of a free resolution, namely when each free module has minimal rank (i.e. choosing each free module with the smallest possible number of generators).

Definition 2.10. *Given a local ring $(R, \mathfrak{m})$, then a complex of R-modules (such as below) is* ***minimal*** *if $im(\partial_n) \subseteq \mathfrak{m}M_{n-1}$ for all n.*

$$\cdots \longrightarrow M_{n+1} \xrightarrow{\partial_{n+1}} M_n \xrightarrow{\partial_n} M_{n-1} \xrightarrow{\partial_{n-1}} \cdots$$

If all modules in the complex are free and of finite rank, the homomorphisms ∂_n can be represented by matrices over R, and minimality means all entries of such matrices are contained in $\mathfrak{m}$. For a free resolution, this definition turns out to be equivalent to every free module posessing the smallest possible number of generators.

It turns out that in a local ring $(R, \mathfrak{m})$, any free resolution of a finitely generated R-module M is isomorphic to the direct sum of a minimal free resolution with a resolution of the trivial R-module 0. (The direct sum is defined with i^{th} module being the direct sum of the i^{th} module in each complex). In particular, this argument can be used to show the minimal free resolution is unique up to isomorphism (the details are on pp.490-491 of [EIS95]).

Remark 2.11. [Injective Resolutions] Thus far we have only commented on the use of projective (and free) resolutions, without making reference to the dual[2] concept - that of an injective resolution. An injective resolution of a module M over a ring R is found by constructing a sequence of injective modules Q_0, Q_1, ..., such that there is an exact sequence:

$$0 \longrightarrow M \longrightarrow Q_0 \longrightarrow Q_1 \longrightarrow Q_2 \longrightarrow \cdots$$

This result of course hinges on the ability to embed M in an injective module Q_0 to begin with, and this is a result proved (twice) in [CE56]. The first proof is by Baer (who was the person responsible for defining the notion of an injective module) and the other is by Eckmann and Schöpf.

[2]The term 'dual' is somewhat of a misnomer - whilst the definitions are certainly dual, this is not true of all the theory!

In fact there is a stronger result possible - any module M over any ring R is contained in a unique (up to isomorphism) injective R-module E such that every non-zero R-submodule of E intersects M non-trivially. The module E is called the **injective hull** of M, and it is this result that lets us embed the cokernel of each map into the next module. This defines a unique minimal injective resolution for any module M over any ring R! $\square$

One might question why, in light of the above remark, people have studied projective resolutions rather than concentrating on injective resolutions. There are several reasons for this, but perhaps the most significant is that injective modules are rarely finitely generated, which forces everything to be done in the setting of non-Noetherian modules. This is not the most pleasant of experiences for the algebraist.

2.2 Derived Functors

In Section 1.1 we introduced the notions of categories and of functors between categories, and we now look at functors between categories of modules. More specifically, we will consider modules over some given ring R, so will work within the categories $R - Mod$ and (less often) $Mod - R$, though it is possible to generalize some of the ideas.

In particular, we will define what it means for a functor to be exact and how to measure the departure from exactness of functors, using the so-called derived functors. To illustrate the points made in the discussion, two main examples will be used leading to the derived functors Ext and Tor, both of which are amongst the most useful devices available in homological algebra.

In this section, all functors $F : R - Mod \to R - Mod$ are assumed[3] to satisfy the condition $F(0) = 0$ for both the R-module $0 \in R - Mod$ and the zero morphism between any two modules in $R - Mod$ (essentially to ensure that F takes complexes in $R - Mod$ to complexes in $R - Mod$).

We begin by defining what it means for a functor to be exact.

[3]This is not normally an assumption, as the left-exact and right-exact functors under consideration always satisfy it, but we will list it as such to make it explicit here.

Definition 2.12. *A (covariant) functor* $F : R - Mod \to R - Mod$ *is said to be* ***exact*** *if for any objects* A, B, C *in* $R - Mod$ *(and morphisms* $\varphi : A \to B$*,* $\psi : B \to C$ *such that* $0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$ *is a short exact sequence (for some morphisms in* $Hom_R(A, B)$ *and* $Hom_R(B, C)$*, then the sequence*

$$0 \longrightarrow F(A) \xrightarrow{F(\varphi)} F(B) \xrightarrow{F(\psi)} F(C) \longrightarrow 0$$

is always an exact sequence. We will also say the functor F *is:*

- ***Right exact*** *if* $F(A) \xrightarrow{F(\varphi)} F(B) \xrightarrow{F(\psi)} F(C) \longrightarrow 0$ *is always an exact sequence.*
- ***Left exact*** *if* $0 \longrightarrow F(A) \xrightarrow{F(\varphi)} F(B) \xrightarrow{F(\psi)} F(C)$ *is always an exact sequence.*

(The same definitions apply if F *is a contravariant functor, with the positions of* $F(C)$ *and* $F(A)$ *interchanged).*

Remark 2.13. [Exact Functors and Splicing]

It may seem odd that we define a functor to be exact based on what it does to short exact sequences rather than all exact sequences. It turns out that under Definition 2.12 then if F is a covariant exact functor, then F takes any exact sequence $A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ into a sequence $F(A) \xrightarrow{F(\varphi)} F(B) \xrightarrow{F(\psi)} F(C)$ which is also exact, and this lets us prove that an exact functor maps arbitrary exact sequences to exact sequences. (A similar result holds for contravariant functors).

This seems the most natural way to define an exact functor, and that it suffices only to check the case of short exact sequences is a nice result, which serves to reinforce the importance of these sequences in the theory of homological algebra.

A proof that short exact sequences are sufficient is based on the fact that any exact sequence can be decomposed into short exact sequences using the technique of 'splicing' which is covered[4] in [CC05] (Lecture 22).

[4] Although not included at the time of writing, the author has assured us that it will shortly be there.

The essential idea of splicing is that given an exact sequence of the form

$$\cdots \longrightarrow M_{i+1} \xrightarrow{\partial_{i+1}} M_i \xrightarrow{\partial_i} M_{i-1} \longrightarrow \cdots$$

then we can write it out in full as a sequence of modules (though not a complex!):

$$\longrightarrow M_{i+1} \xrightarrow{\partial_{i+1}} \mathrm{im}(\partial_{i+1}) = \ker(\partial_i) \hookrightarrow M_i \xrightarrow{\partial_i} \mathrm{im}(\partial_i) = \ker(\partial_{i-1}) \hookrightarrow M_{i-1} \longrightarrow$$

and for each i get the short exact sequence $0 \longrightarrow \ker(\partial_i) \hookrightarrow M_i \longrightarrow \mathrm{im}(\partial_i) \longrightarrow 0$.

Thus any exact sequence may be spliced into short exact sequences, which are sent to other short exact sequences by the exact functor. These can then be recomposed to give an exact sequence, which turns out to be the sequence obtained by applying the functor to the original exact sequence. □

Exact functors are useful in the study of homology precisely because they preserve exactness. More commonly found, however, are left exact and right exact functors, which are in a sense 'almost exact'. Some common examples of these are given below.

Example 2.14. Given any module $M \in R-Mod$, then the functor $\mathrm{Hom}_R(M, \cdot)$ (which takes any module $N \in R-Mod$ to the module $\mathrm{Hom}_R(M, N) \in R-Mod$) is left exact. □

Example 2.15. Given any module $M \in R-Mod$, then the functor $\mathrm{Hom}_R(\cdot, M)$ is left exact (note that this is an example of a *contravariant* functor). □

Example 2.16. Given any module $M \in Mod-R$, consider the functor $M \otimes_R -$, which takes any $N \in R-Mod$ to the module $M \otimes_R N \in R-Mod$. This functor is right exact. □

Remark 2.17. When these functors are exact, it turns out we can make certain assertions regarding the modules involved, such as:

(a) Suppose $M \in R-Mod$. If $\mathrm{Hom}_R(M, \cdot)$ is an exact functor, then M is projective.

(b) Suppose $M \in R-Mod$. If $\mathrm{hom}_R(\cdot, M)$ is an exact functor, then M is injective.

Proof. We provide a proof of (a), with the proof of (b) being fairly similar.

Suppose we have a short exact sequence $0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$.

Because $\mathrm{Hom}_R(M, \cdot)$ is always left exact, we already know that the sequence

$$0 \longrightarrow \mathrm{Hom}_R(M, A) \xrightarrow{\varphi_*} \mathrm{Hom}_R(M, B) \xrightarrow{\psi_*} \mathrm{Hom}_R(M, C)$$

is exact, so exactness of $\mathrm{Hom}_R(M, \cdot)$ only tells us that ψ_* is surjective, i.e. for any homomorphism $f \in \mathrm{Hom}_R(M, C)$ there exists $g \in \mathrm{Hom}_R(M, B)$ such that $\psi_*(g) = f$ (that is, $\psi \circ g = f$).

In other words, ψ is surjective and for any homomorphism $f : M \to C$ there exists a filler homomorphism $g : M \to B$ such that the following diagram commutes:

$$\begin{array}{ccccc} & & M & & \\ & \overset{g}{\swarrow} & \downarrow f & & \\ B & \xrightarrow{\psi} & C & \longrightarrow & 0 \end{array}$$

But this is precisely the definition of a projective module, so M is projective, as desired. ☐

The tensor product also induces a particular type of module when exact, and if $M \otimes_R -$ is an exact functor for $M \in Mod - R$ then M is called a **flat** module. We will not be making direct use of flat modules, but note that any projective module is flat (though the converse is not true in general). ☐

Left exact and right exact functors are in some sense 'almost exact'. The extent to which they differ from being exact is measured by the so-called derived functors.

Definition 2.18. *Let R be a ring, F a right exact (covariant) functor from $R - Mod$ to $R - Mod$, and M an R-module (i.e. in $R - Mod$). Suppose first that we have a projective resolution $P_\bullet$ of M, which we write as follows:*

$$\cdots \longrightarrow P_{i+1} \xrightarrow{\partial_{i+1}} P_i \xrightarrow{\partial_i} P_{i-1} \longrightarrow \cdots \longrightarrow P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\partial_0} M \longrightarrow 0$$

Applying the functor F to this gives the complex $F(P_\bullet)$ defined to be

$$\cdots \longrightarrow F(P_{i+1}) \xrightarrow{F(\partial_{i+1})} F(P_i) \xrightarrow{F(\partial_i)} F(P_{i-1}) \longrightarrow \cdots \longrightarrow F(P_0) \xrightarrow{F(\partial_0)} F(M) \longrightarrow 0$$

*and we define the i^{th} **left-derived functor** of F at M to be $(L_iF)(M) = H_i(F(P_\bullet))$, the homology group at $F(P_i)$ of the above complex.*

We can similarly define right-derived functors (which result from left exact functors) and can make definitions for contravariant functors along the same lines. (Although not specified, it should be clear the action of L_iF on morphisms is to send them to the induced maps on homology of the complex $F(P_\bullet)$).

One of the most useful gadgets in computing homology is the long exact sequence in homology (of Section 1.4). A similar construction exists for derived functors, as we note in the following proposition (stated for the left-derived functors of a right exact covariant functor - the corresponding definitions are fairly clear for right-derived functors and the derived functors of contravariant functors).

Proposition 2.19. *Let R be a ring, $F : R - Mod \to R - Mod$ a right exact covariant functor and M an R-module. Then the left-derived functors of F at any R-module M are independent of the projective resolution of M used in the definition, and further:*

(a) $(L_0F)(M) = F(M)$ *(for all $M \in R - Mod$)*

(b) Every short exact sequence of complexes $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ *induces a long exact sequence in the functor, of the form:*

$$\longrightarrow (L_{i+1}F)(A) \longrightarrow (L_{i+1}F)(B) \longrightarrow (L_{i+1}F)(C) \xrightarrow{\delta_{i+1}} (L_iF)(A) \longrightarrow (L_iF)(B) \longrightarrow \cdots \tag{2.1}$$

(Note that for right-derived functors the arrows progress from lower indices to higher ones, rather than from higher to lower).

The proof is omitted to avoid the complications[5].

It is worth mentioning, however, that the proof of (b) entails constructing a short exact sequence of complexes using projective resolutions of A, B, C (with chain maps induced by Theorem 2.8), whereupon the long exact sequence in F is just a special case of the long exact sequence in homology.

2.3 Tor and Ext

Two of the most important derived functors in homological algebra are the functors Tor and Ext. In this section we will briefly define Tor and Ext and remark on some of their properties, before showing how they may be used to compute the projective dimension of modules in local rings, to illustrate their usefulness in homological computations.

Definition 2.20. *Given a ring R and an R-module M, then the functor $Tor_i^R(M, -)$ is defined to be the i^{th} left-derived functor of the right exact functor $M \otimes_R -$.*

Example 2.21. Given a ring R and an R-module M, if $x \in R$ is not a zero divisor then $\mathrm{Tor}_1^R(R/\langle x\rangle, M) = \{m \in M \big| xm = 0\}$, $\mathrm{Tor}_0^R(R/\langle x\rangle M) = M/\langle x\rangle M$ and $\mathrm{Tor}_i^R(R/\langle x\rangle, M) = 0$ for all other i. □

(We deliberately omit the actual computation, since we will do essentially the same example for Ext, and this particular example may be found in [CC05]. It is left as an exercise for the interested reader.)

The other major derived functor in homological algebra is the functor Ext, which is a right-derived functor of the left exact functor Hom. In this case, however, we can define Ext in either of two ways, using either of the left exact functors $\mathrm{Hom}_R(M, -)$ or $\mathrm{Hom}_R(-, M)$.

The definition we provide will be the standard one, which is based on the use of injective resolutions.

[5] Such as, for example, the use of a three-dimensional commutative diagram in [OSB00] to prove independence of the projective resolution!

Definition 2.22. *Given a ring R and two R-modules M, N, we can take an injective resolution of N, of the form* $0 \longrightarrow N \longrightarrow Q_0 \longrightarrow Q_1 \longrightarrow \cdots$ *and on applying the left exact functor $Hom_R(M, -)$ to this get the complex:*

$$0 \longrightarrow Hom_R(M, Q_0) \longrightarrow Hom_R(M, Q_1) \longrightarrow Hom_R(M, Q_2) \longrightarrow \cdots \tag{2.2}$$

(we suppress writing $Hom_R(M, N)$ because it will be the homology at $Hom_R(M, Q_0)$).

We now define $Ext^i_R(M, N)$ to be the i^{th} right-derived functor of $Hom_R(M, \cdot)$ at N, which is the homology of the complex (2.2) at $Hom_R(M, Q_i)$.

Remark 2.23. [About Ext] Although the above definition is the standard way to define Ext, it is not a method conducive to computation, as injective resolutions are, as noted, not the most friendly of devices.

There is another method for computing Ext, which takes advantage of the fact the left exact functor $\mathrm{Hom}_R(-, M)$ is contravariant. This method begins wih a projective resolution of M, of the form $\cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$.

Applying the functor $\mathrm{Hom}_R(\cdot, N)$ to this resolution gives the complex

$$\cdots \longleftarrow \mathrm{Hom}_R(P_2, N) \longleftarrow \mathrm{Hom}_R(P_1, N) \longleftarrow \mathrm{Hom}_R(P_0, N) \longleftarrow 0$$

As before $\mathrm{Ext}^i_R(M, N)$ is defined to be the homology group of the complex (2.23) at $\mathrm{Hom}_R(P_i, N)$. (We have deliberately chosen the orientation of this sequence to highlight the contravariant nature of the functor used).

We will be using both methods in later chapters, although typically this latter method will be our preferred option. □

We now turn to the computation of an example of Ext (from which it will hopefully be apparent why we neglected the example of Tor above, owing to the similarities).

Example 2.24. Our example of Ext will compute $\text{Ext}^i_R(R/\langle x\rangle, M)$ when $x \in R$ is not a zero divisor and M is some R-module, using the projective (in fact free) resolution of $R/\langle x\rangle$ given in Example 2.4, namely $\cdots \longrightarrow 0 \longrightarrow R \xrightarrow{x} R \longrightarrow R/\langle x\rangle \longrightarrow 0$.

Applying $\text{Hom}_R(\cdot, M)$ to this resolution gives us:

$$0 \longrightarrow \text{Hom}_R(R, M) \xrightarrow{x^*} \text{Hom}_R(R, M) \longrightarrow 0 \longrightarrow \cdots$$

(since $\text{Hom}_R(0, M) \simeq 0$ for any R-module M).

Recall that $\text{Hom}_R(R, M) \simeq M$ via the canonical isomorphism $f \mapsto f(1)$, and observe that the induced map x^* acts by $(x^*(f))(r) = f(xr) = x(f(r))$ for all $r \in R$, so is just multiplication by x. Thus the above complex is isomorphic to:

$$0 \longrightarrow M \xrightarrow{x} M \longrightarrow 0 \longrightarrow \cdots$$

Upon taking the homology we easily find that $\text{Ext}^1_R(R, M) \simeq M/\langle x\rangle M$, $\text{Ext}^0_R(R, M) \simeq \{m \in M \big| xm = 0\}$ and $\text{Ext}^i_R(R, M) = 0$ for all other values of i.

□

We also prove a result about Ext that will be needed in the next chapter.

Proposition 2.25. *Ext commutes with finite direct sums in the second variable, so for any $i \geq 0$ and modules $A, B_1, \ldots, B_n$ over a ring R:*

$$Ext^i_R(A, \oplus_{j=1}^n B_j) \simeq \oplus_{j=1}^n Ext^i_R(A, B_j)$$

Comparable results exist for the first variable and for Tor, but we will not need those, so do not provide them here.

Proof. The proof is an easy inductive argument on n once we establish the base case $n = 2$, so we will only prove the result for this base case.

It is clear that $\mathrm{Hom}_R(A, B_1 \oplus B_2) \simeq \mathrm{Hom}_R(A, B_1) \oplus \mathrm{Hom}_R(A, B_2)$ (we identify any $(f_1, f_2) \in \mathrm{Hom}_R(A, B_1) \oplus \mathrm{Hom}_R(A, B_2)$ with $f \in \mathrm{Hom}_R(A, B_1 \oplus B_2)$ by letting $f(a) = (f_1(a), f_2(a))$ for all $a \in A$).

We now refer to Definition 18.1 of [CC05], which defines the direct sum of two complexes of R-modules $M_\bullet$ and $M'_\bullet$ as being the complex $(M \oplus M')_\bullet$ with $(M \oplus M')_i = M_i \oplus M'_i$ for all i. This definition further goes on to note $H_i((M \oplus M')_\bullet) \simeq H_i(M_\bullet) \oplus H_i(M'_\bullet)$ for all i.

Consider a projective resolution $P_\bullet$ of A in the form used in Remark 2.3:

$$\cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow 0$$

We can apply the functors $\mathrm{Hom}_R(-, B_1)$ and $\mathrm{Hom}_R(-, B_2)$ to $P_\bullet$ to get two complexes $\mathrm{Hom}_R(P_\bullet, B_1)$ and $\mathrm{Hom}_R(P_\bullet, B_2)$ of the form:

$$\mathrm{Hom}_R(P_\bullet, B_1) : 0 \longrightarrow \mathrm{Hom}_R(P_0, B_1) \longrightarrow \mathrm{Hom}_R(P_1, B_1) \longrightarrow \mathrm{Hom}_R(P_2, B_1) \longrightarrow \cdots$$

$$\mathrm{Hom}_R(P_\bullet, B_2) : 0 \longrightarrow \mathrm{Hom}_R(P_0, B_2) \longrightarrow \mathrm{Hom}_R(P_1, B_2) \longrightarrow \mathrm{Hom}_R(P_2, B_2) \longrightarrow \cdots$$

and can define $\mathrm{Hom}_R(P_\bullet, B_1) \oplus \mathrm{Hom}_R(P_\bullet, B_2)$ to be the complex such that:

$$\begin{aligned}(\mathrm{Hom}_R(P_\bullet, B_1) \oplus \mathrm{Hom}_R(P_\bullet, B_2))_{-i} &= (\mathrm{Hom}_R(P_\bullet, B_1))_{-i} \oplus (\mathrm{Hom}_R(P_\bullet, B_2))_{-i} \\ &= \mathrm{Hom}_R(P_i, B_1) \oplus \mathrm{Hom}_R(P_i, B_2) \\ &\simeq \mathrm{Hom}_R(P_i, B_1 \oplus B_2)\end{aligned}$$

NB. Recall that we are only working over chain complexes, so the indices should be decreasing as we progress rightwards along the maps. In this context - particularly given the indices used on the $\{P_j\}$, it makes sense to assign the modules negative indices as members of the complex.

By using the definition of Ext and using the result on homology we obtained above from [CC05], we now find:

$$\begin{aligned}\mathrm{Ext}^i_R(A, B_1 \oplus B_2) &= H_{-i}(\mathrm{Hom}_R(P_\bullet, B_1) \oplus \mathrm{Hom}_R(P_\bullet, B_2)) \\ &= H_{-i}(\mathrm{Hom}_R(P_\bullet, B_1)) \oplus H_{-i}(\mathrm{Hom}_R(P_\bullet, B_2)) \\ &= \mathrm{Ext}^i_R(A, B_1) \oplus \mathrm{Ext}^i_R(A, B_2)\end{aligned}$$

Thus we have established our base case, so the inductive argument shows that Ext commutes with finite direct sums in the second variable. □

We now have these derived functors Ext and Tor, but as yet have not seen any use for them. To dispel any concerns that this is merely an esoteric line of thought with little real value, we illustrate how Tor may be used to compute projective dimension in a local ring.

Theorem 2.26. *Given a local ring $(R, \mathfrak{m})$ and finitely generated R-module M, any minimal free resolution of M has length equal to $pd_R(M)$. In addition, we have the relation $pd_R(M) = min\{i \big| Tor^R_{i+1}(R/\mathfrak{m}, M) = 0\}$.*

Proof. Consider a minimal free resolution of M, of the form:

$$0 \longrightarrow F_{\mathrm{pd}_R(M)} \longrightarrow \cdots \longrightarrow F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\partial_0} M \longrightarrow 0$$

Clearly if $i > \mathrm{pd}_R(M)$ then $F_i = 0$ means $\mathrm{Tor}^R_i(R/\mathfrak{m}, M) = 0$ (since the tensor product $R/\mathfrak{m} \otimes_R F_i = 0$, so its homology is also 0). Hence $\mathrm{Tor}^R_{i+1}(R/\mathfrak{m}, M) = 0$ for any $i \geq \mathrm{pd}_R(M)$, so $\mathrm{pd}_R(M) \geq \min\{i \big| \mathrm{Tor}^R_{i+1}(R/\mathfrak{m}, M) = 0\}$.

Now suppose we have a minimal free resolution of M with length n (so $n \geq \mathrm{pd}_R(M)$). It follows from Definition 2.10 that the tensor product of $R/\mathfrak{m}$ with this minimal free resolution is a complex in which every differential is 0 (as for any j the homomorphism $R/\mathfrak{m} \otimes_R \partial_j : R/\mathfrak{m} \otimes_R F_j \to R/\mathfrak{m} \otimes_R F_{j-1}$ is induced by a map taking $F_n \to \mathfrak{m}F_{j-1}$, so $\mathrm{im}(R/\mathfrak{m} \otimes_R \partial_j) \subseteq R/\mathfrak{m} \otimes \mathfrak{m}F_{j-1} = 0$).

Thus $\operatorname{Tor}_i^R(R/\mathfrak{m}, M) = \ker(R/\mathfrak{m} \otimes_R \partial_i)/\operatorname{im}(R/\mathfrak{m} \otimes_R \partial_{i+1}) \simeq R/\mathfrak{m} \otimes_R F_i$ for each i (from the definition of Tor). This means $\operatorname{Tor}_{i+1}^R(R/\mathfrak{m}, M) = 0$ iff $R/\mathfrak{m} \otimes_R F_{i+1} = 0$, which in turn is true iff $F_{i+1} = 0$ (else F_{i+1} free and finitely generated means there is an element $(1, 1, \ldots, 1) \in F_{i+1}$, and we would require $(1 + \mathfrak{m}) \otimes (1, 1, \ldots, 1) = 0$).

Hence we find $\inf\{i \big| \operatorname{Tor}_{i+1}^R(R/\mathfrak{m}, M) = 0\} = \inf\{i \big| F_{i+1} = 0\} \geq n \geq \operatorname{pd}_R(M)$. Together with the reverse inequality (above), this means $\operatorname{pd}_R(M) = \inf\{i \big| \operatorname{Tor}_{i+1}^R(R/\mathfrak{m}, M) = 0\}$ as desired (and simultaneously shows $n = \operatorname{pd}_R(M)$ to give the first part of the theorem). □

Remark 2.27. There is a similar characterization of projective dimension using the functor Ext, which was provided by Rees as Lemma 5.1 of his paper [REE57]. Rees proved that a finitely generated module M over a local ring $(R, \mathfrak{m})$ has projective dimension $\operatorname{pd}_R(M) = \inf\{i \big| \operatorname{Ext}_R^i(M, R/\mathfrak{m}) \neq 0\}$. □

Chapter 3

Depth

Measuring the size of an ideal in a ring is a problem that has been considered numerous times through the years, with the options including geometric notions such as Krull dimension and codimension (or height) as well as homological notions such as projective dimension. Another idea is that of the *depth* of an ideal, which was introduced by Rees in 1956[1] (in [REE56]) and developed further in [REE57], and it is this idea we consider here.

We will develop depth based on the notion of a regular sequence, and formulate a precise definition in terms of the functor Ext to emphasize the homological nature of depth (which has also been called 'homological codimension'). We reiterate that all rings are assumed to be Noetherian, though a treatment in the non-Noetherian case can be developed without too much difficulty (for such a treatment, see [NOR76]).

After defining depth, we will take a look at how it relates to some other notions that can be used to measure the size of an ideal - in particular projective dimension, Krull dimension and codimension, and at some of the connections between these ideas and depth - before concluding the chapter with a proof of the famous Auslander-Buchsbaum Formula, relating depth to projective dimension.

[1]This statement may mislead. In fact Auslander and Buchsbaum devised a very similar notion at around the same time, and published several papers on the matter, including the paper [AB57] which we refer to later. It is Rees, however, who is generally credited with the discovery. Auslander and Buchsbaum called it 'codimension', which (in view of the issues with nomenclature that we will touch on in Remark 3.19) may have contributed to Rees' getting the plaudits!

3.1 Regular Sequences

Definition 3.1. *Given a ring R and an R-module M, then a sequence $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$ is called a* ***regular sequence*** *on M (or an M*-***sequence****) if*

(i) $\langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle M \neq M$.

(ii) For $i = 1, 2, \ldots, n$, then α_i is a nonzerodivisor on $M/\langle \alpha_1, \alpha_2, \ldots, \alpha_{i-1} \rangle M$ (which when $i = 1$ is simply M).

If condition (ii) holds, the sequence is said to be ***weakly regular*** *(on M).*

We say x is a nonzerodivisor on M if $xm = 0 \Rightarrow m = 0$ for all $m \in M$.

In the particular case $M = R$, then we call $\alpha_1, \ldots, \alpha_n$ an R-sequence.

At times we may simply refer to a 'regular sequence' without specifying either ring or module. This is done when it is immaterial - beyond our standard assumptions of a Noetherian ring, etc. - what the ring and module are.

Example 3.2. In the polynomial ring $R = \mathbb{K}[x_1, x_2, \ldots, x_n]$, the sequence of indeterminates $x_1, x_2, \ldots, x_n$ forms an R-sequence. $\square$

Example 3.3. In the polynomial ring $R = \mathbb{K}[x_1, x_2]$ the sequence x_1^2, x_1 does *NOT* form an R-sequence, since x_1 is a zero divisor on $R/\langle x_1^2 \rangle$. $\square$

It is clear that the first s terms of an M-sequence (where $1 \leq s \leq n$) also form an M-sequence, and we can develop this further to consider the other terms in the sequence.

Proposition 3.4. *The following are equivalent about M-sequences:*

(a) $x_1, \ldots, x_n$ *is an M-sequence.*

(b) $x_1, \ldots, x_s$ *is an M-sequence and* $x_{s+1}, \ldots, x_n$ *is an* $M/\langle x_1, \ldots, x_s \rangle M$*-sequence for any integer* $0 < s < n$.

Proof. Suppose (a) holds, i.e. $x_1, \ldots, x_n$ is an M-sequence. Since $x_1, \ldots, x_s$ is obviously an M-sequence, we only need check that $x_{s+1}, \ldots, x_n$ is an $M/\langle x_1, \ldots, x_s \rangle M$ sequence.

Checking the first condition of Definition 3.1 is straightforward, since we note that $\langle x_{s+1},\dots,x_n\rangle(M/\langle x_1,\dots,x_s\rangle M) = M/\langle x_1,\dots,x_s\rangle M$ means if $m \in M \setminus \langle x_{s+1},\dots,x_n\rangle M$, then $m + \langle x_1,\dots,x_s\rangle M = \langle x_1,\dots,x_s\rangle M$ in the quotient ring. Hence $m \in \langle x_1,\dots,x_s\rangle M$, so $M \subseteq \langle x_{s+1},\dots,x_n\rangle M \cup \langle x_1,\dots,x_s\rangle M \subseteq \langle x_1,\dots,x_n\rangle M \subseteq M$, i.e. $M = \langle x_1,\dots,x_n\rangle M$. Since $x_1,\dots,x_n$ is an M-sequence, condition (i) of the definition prevents this, and therefore $\langle x_{s+1},\dots,x_n\rangle(M/\langle x_1,\dots,x_s\rangle M) \neq M/\langle x_1,\dots,x_s\rangle M$ as desired.

In checking condition (ii) of Definition 3.1, we know that x_{s+1} is not a zero divisor on $M/\langle x_1,\dots,x_s\rangle M$, and that x_k is not a zero divisor on $M/\langle x_1,\dots,x_{k-1}\rangle M$ for every $k = s+2,\dots,n$. Thus to show $(a) \Rightarrow (b)$ it suffices to show $M/\langle x_1,\dots,x_{k-1}\rangle M \simeq (M/\langle x_1,\dots,x_s\rangle M)/\langle x_{s+1},\dots,x_{k-1}\rangle(M/\langle x_1,\dots,x_s\rangle M)$ for all $s+2 \leq k \leq n$.

This is a straightforward application[2] of Theorem 6.6 to the homomorphism ψ obtained by composing the quotient maps $\varphi_1 : M \to M/\langle x_1,\dots,x_s\rangle M$ and $\varphi_2 : M/\langle x_1,\dots,x_s\rangle M \to (M/\langle x_1,\dots,x_s\rangle M)/\langle x_{s+1},\dots,x_{k-1}\rangle(M/\langle x_1,\dots,x_s\rangle M)$. (Since quotient homomorphisms are surjective, ψ is surjective, and it is easy to check $\ker(\psi) = \langle x_1,\dots,x_{k-1}\rangle$, giving the desired result).

Conversely, if (b) holds then x_{s+1} is not a zero divisor on $M/\langle x_1,\dots,x_s\rangle M$ and x_k is not a zero divisor on $(M/\langle x_1,\dots,x_s\rangle M)/\langle x_{s+1},\dots,x_{k-1}\rangle(M/\langle x_1,\dots,x_s\rangle M)$ for $s+2 \leq k \leq n$. From above this means x_k is not a zero divisor on $M/\langle x_1,\dots,x_{k-1}\rangle M$, and so condition (ii) of Definition 3.1 holds for the sequence $x_1,\dots,x_n$. Condition (i) follows easily, so $x_1,\dots,x_n$ is an M-sequence, completing the equivalence. □

This result enables us to prove in some special cases that any M-sequence may be permuted. That this is not true in general is seen by examples such as the next one (a modified form of the example on page 422 of [EIS95]).

[2]That the first isomorphism theorem for modules should be involved should not come as any surprise when quotient maps are involved!

Example 3.5. In the ring $R = \mathbb{K}[x, y, z]$, then $(x-1)z, x, (x-1)y$ (in that order)is an R-sequence, but when in the order $(x-1)z, (x-1)y, x$ is not an R-sequence (as $(x-1)y$ is a zero divisor on $R/\langle (x-1)z \rangle$). □

Although not true in general, it is true that in a Noetherian local ring any permutation of a regular sequence on a module gives another regular sequence on that module.

Proposition 3.6. *If $(R, \mathfrak{m})$ is a Noetherian local ring and M is an R-module, then any permutation of an M-sequence is also an M-sequence.*

Proof. First consider the case where the M-sequence is of length 2.

Lemma 3.7. *If x_1, x_2 is an M-sequence, then x_2, x_1 is an M-sequence iff x_2 is not a zero divisor on M. This is always true in the case of a Noetherian local ring.*

Proof. With x_1, x_2 an M-sequence then $\langle x_2, x_1 \rangle M = \langle x_1, x_2 \rangle M \neq M$, so it suffices to prove that x_1 is not a zero divisor on $M/\langle x_2 \rangle M$ when x_1, x_2 is an M-sequence to prove the 'if' in the first statement (the 'only if' is trivial, so we omit it).

Suppose x_1 is a zero divisor on $M/\langle x_2 \rangle M$, so there exists $n \in M \setminus \langle x_2 \rangle M, m \in M$ with $x_1 n = x_2 m$. If $m \in \langle x_1 \rangle M$ then $m = x_1 m'$ for some $m' \in M$, and then $x_1(n - x_2 m') = 0$, so either x_1 is a zero divisor on M or $n = x_2 m' \in \langle x_2 \rangle M$. Both scenarios are contradictions, so $m \in M \setminus \langle x_1 \rangle M$. Then $x_2 m \in \langle x_1 \rangle M$ implies $x_2(m + \langle x_1 \rangle M) = \langle x_1 \rangle M$, making x_2 a zero divisor on $M/\langle x_1 \rangle M$. But this now contradicts x_1, x_2 being an M-sequence. Thus x_1 cannot be a zero divisor on $M/\langle x_2 \rangle M$ (else we get a contradiction), so x_2, x_1 is an M-sequence iff x_2 is not a zero divisor on M, as desired.

Now suppose we are in a Noetherian local ring $(R, \mathfrak{m})$, and suppose $x_2 m = 0$ for some $m \in M$. Then $m \in \langle x_1 \rangle M$ (since x_2 is not a zero divisor on $M/\langle x_1 \rangle M$), so $m = x_1 m'$ for some $m' \in M$. This gives $0 = x_2(x_1 m') = x_1(x_2 m')$, which forces $x_2 m' = 0$ (as x_1 is not a zero divisor on M). Letting $L = \{m \in M : x_2 m = 0\}$, then clearly L is a submodule of M and we have shown $L \subseteq \langle x_1 \rangle L$, meaning $L = \langle x_1 \rangle L$ (as the reverse inclusion is automatic).

Here $x_1 \in \langle x_1 \rangle \subseteq \mathfrak{m}$ (since any proper ideal is contained in a maximal ideal), so that $L = \langle x_1 \rangle L \subseteq \mathfrak{m}L \subseteq L$, giving $L = \mathfrak{m}L$. Since L is a submodule of M it must be finitely generated (by Proposition 6.14 M is Noetherian) and by Nakayama's Lemma (6.33), we get $L = 0$. Thus x_2 is not a zero divisor on M if R is a Noetherian local ring. $\square$

Now consider a general M-sequence $x_1, \ldots, x_n$. Since any permutation is a product of transpositions of consecutive elements, we only need check that all transpositions of the form $(i, i+1)$ applied to $x_1, \ldots, x_n$ give M-sequences (for $1 \leq i \leq n-1$).

Using Proposition 3.4 twice then $x_1, \ldots, x_{i-1}, x_{i+1}, x_i, x_{i+2}, \ldots, x_n$ is an M-sequence iff $x_1, \ldots, x_{i-1}$ is an M-sequence, x_{i+1}, x_i is an $M/\langle x_1, \ldots, x_{i-1} \rangle M$-sequence and $x_{i+2}, \ldots, x_n$ is an $M/\langle x_1, \ldots x_{i+1} \rangle M$-sequence (truncating after first the $(i+1)^{th}$ element, and then after the $(i-1)^{th}$ element of the M-sequence $x_1, \ldots, x_{i-1}, x_{i+1}, x_i$).

But $x_1, \ldots, x_n$ is an M-sequence, so using Proposition 3.4 twice more and combining this with Lemma 3.7 we find that $x_1, \ldots, x_{i-1}, x_{i+1}, x_i, x_{i+2}, \ldots, x_n$ is an M-sequence iff x_{i+1} is not a zero divisor on $M/\langle x_1, \ldots, x_{i-1} \rangle M$, which holds for a Noetherian local ring. $\square$

3.2 Maximal Regular Sequences

To date we have only considered finite regular sequences, without heed to the possibility of infinite regular sequences. This is because in a Noetherian ring all regular sequences must be finite, as we prove in our next result (note that in a non-Noetherian ring it **is** possible to have infinite regular sequences).

Proposition 3.8. *Given a Noetherian ring R and any R-module M, any regular sequence on M is finite.*

Proof. Consider an infinite M-sequence $x_1, x_2, \ldots$ in R.

Then in the sequence of ideals (ordered by inclusion) with the n^{th} ideal generated by the first n elements of our M-sequence (as below), all inclusions are proper inclusions.

$$\langle x_1 \rangle \subseteq \langle x_1, x_2 \rangle \subseteq \langle x_1, x_2, x_3 \rangle \subseteq \dots \tag{3.1}$$

To see this, suppose that there is an inclusion that is not proper, i.e. $\langle x_1, \dots, x_k \rangle = \langle x_1, \dots, x_{k+1} \rangle$ for some $k \in \mathbb{Z}^+$. Then $x_{k+1} \in \langle x_1, \dots, x_k \rangle$, so for any $m \in M$ we see $x_{k+1}m \in \langle x_1, \dots, x_k \rangle M$.

Hence $x_{k+1}(m + \langle x_1, \dots, x_k \rangle M) = \langle x_1, \dots, x_k \rangle M$ for all $m \in M$, meaning x_{k+1} is a zero divisor on $M/\langle x_1, \dots, x_k \rangle M$ unless $M/\langle x_1, \dots, x_k \rangle M = 0$, i.e. unless $M = \langle x_1, \dots, x_k \rangle M$. In the former instance, the requirement that $x_1, \dots, x_{k+1}$ be the beginning of an (infinite) M-sequence (and hence an M-sequence itself) is violated, whilst in the latter case the requirement that $x_1, \dots, x_k$ be the beginning of an M-sequence (and so an M-sequence itself) is failed.

Thus in the chain (3.1) all inclusions are proper, giving an ascending chain of ideals in the Noetherian ring R. By the Ascending Chain Condition, this chain must terminate, so for some k we must have $\langle x_1, \dots, x_k \rangle = \langle x_1, \dots, x_{k+1} \rangle$, giving a contradiction as before.

Since regardless of our approach we get a contradiction, we conclude that no infinite M-sequences exist in a Noetherian ring, i.e. any regular sequence in a Noetherian ring is finite, as desired. □

Because we can truncate any regular sequence to get another regular sequence, it makes sense in light of this result to be particularly concerned with those regular sequences that are maximal, in the sense that they cannot be extended by another element to form a regular sequence.

Definition 3.9. *Given a ring R and an R-module M, then a **maximal regular sequence** on M is an M-sequence $x_1, x_2, \dots, x_n$ contained in R such that for any $y \in R$ the sequence $x_1, \dots, x_n, y$ is* not *an M-sequence.*

The next theorem is one of the most critical of this chapter, and will allow us to define the concept of depth.

Theorem 3.10. *Given a ring R, a finitely generated R-module M and a proper ideal $I \subset R$ such that $IM \neq M$, then all maximal regular sequences on M that are contained in I have the same length, which is equal to* $\inf\{i \big| Ext^i_R(R/I, M) \neq 0\}$.

There are many possible proofs - Kaplansky provides a non-homological proof on page 87 of [KAP74], Eisenbud proves it using the Koszul complex in [EIS95], and Rees proves it in essentially the form we have here, though the method varies slightly[3].

Proof. Suppose we have a maximal M-sequence in I of length n, namely $x_1, \dots, x_n$. Let $I_k = \langle x_1, \dots, x_k \rangle$ and $M_k = M/I_kM$ for all $k = 1, \dots, n$ (and $M_0 = M$). We will at times use the fact $M_k \simeq M_{k-1}/\langle x_k \rangle M_{k-1}$ without stating it (this was proved back when coming up with Proposition 3.4).

We first prove that $\mathrm{Ext}^k_R(R/I, M) = 0$ if $k < n$, and then that $\mathrm{Ext}^n_R(R/I, M) \neq 0$.

Firstly, for any $f \in \mathrm{Hom}_R(R/I, M_{k-1})$ then $x_k f(1+I) = f(x_k+I) = f(I) = 0$, using the definition of a module homomorphism. Since x_k is not a zero divisor on M_{k-1} (by definition of a regular sequence), this means $f(1 + I) = 0$ and so $f(r + I) = rf(1 + I) = 0$ for every $r+I \in R/I$, i.e. $f = 0$. This holds for any $f \in \mathrm{Hom}_R(R/I, M_{k-1})$ so $\mathrm{Hom}_R(R/I, M_{k-1}) = 0$ for all $1 \leq k \leq n$.

We now introduce a useful lemma relating Ext to this result.

Lemma 3.11. *Given a ring R, an ideal I of R, an R-module M and an M-sequence of length k contained in I, then $Ext^k_R(R/I, M) \simeq Hom_R(R/I, M_k)$ (where M_k is defined as above for each k, and $0 \leq k \leq n$).*

Proof. $\mathrm{Ext}^0_R(R/I, M) \simeq \mathrm{Hom}_R(R/I, M) = \mathrm{Hom}_R(R/I, M_0)$, so the result holds for $k = 0$. This establishes a base case, and we proceed inductively.

[3] This proof was originally constructed as an independent exercise, but has since been cleaned up using ideas from [SIM01], [BH93] and [KAP74].

Suppose the result holds for $k = j$ $(0 \leq j < n)$, so $\text{Ext}^j_R(R/I, M) \simeq \text{Hom}_R(R/I, M_j)$ (and from above $\text{Ext}^j_R(R/I, M) = 0$). Then for $k = j+1$ we begin with an M-sequence of length $j+1$ in I (note that $j+1 \geq 1$).

Because x_1 is not a zero divisor on M, we have a short exact sequence:

$$0 \longrightarrow M \xrightarrow{x_1} M \longrightarrow M_1 \longrightarrow 0$$

where the map from $M \to M_1$ is the canonical quotient homomorphism.

We now form the long exact sequence in Ext to get:

$$\to \text{Ext}^j_R(R/I, M) \to \text{Ext}^j_R(R/I, M_1) \xrightarrow{\delta_j} \text{Ext}^{j+1}_R(R/I, M) \xrightarrow{x_1} \text{Ext}^{j+1}_R(R/I, M) \to$$

where $\text{Ext}^j_R(R/I, M) = 0$, and x_1 (the homomorphism) is the map induced by multiplication by x_1 ($\in R$) taking $\text{Ext}^{j+1}_R(R/I, M) \to \text{Ext}^{j+1}_R(R/I, M)$).

Since $x_1 \in I$, then x_1 annihilates the R-module R/I, and in fact we claim this means x_1 annihilates $\text{Ext}^{j+1}_R(R/I, M)$. The easiest way to see this is to take an *injective* resolution of M, which we write as:

$$0 \longrightarrow M \xrightarrow{\psi_0} I_0 \xrightarrow{\psi_1} I_1 \xrightarrow{\psi_2} \cdots$$

Applying the functor $\text{Hom}_R(R/I, -)$ to this resolution gives the complex:

$$0 \longrightarrow \text{Hom}_R(R/I, I_0) \xrightarrow{(\psi^*)_0} \text{Hom}_R(R/I, I_1) \xrightarrow{(\psi^*)_1} \cdots$$

Since x_1 annihilates R/I, it annihilates any R-module homomorphism in $\text{Hom}_R(R/I, I_j)$ for any $j > 0$. As a result, it annihilates $\ker((\psi^*)_{j+1}) \subseteq \text{Hom}_R(R/I, I_{j+1})$ so annihilates $\text{Ext}^{j+1}_R(R/I, I_{j+1})$.

The long exact sequence is now $0 \to \mathrm{Ext}^j_R(R/I, M_1) \to \mathrm{Ext}^{j+1}_R(R/I, M) \to 0$. The homomorphism between $\mathrm{Ext}^j_R(R/I, M_1)$ and $\mathrm{Ext}^{j+1}_R(R/I, M)$ is thus both injective and surjective, so is an isomorphism.

Thus $\mathrm{Ext}^{j+1}_R(R/I, M) \simeq \mathrm{Ext}^j_R(R/I, M_1)$, and applying the inductive hypothesis we see $\mathrm{Ext}^j_R(R/I, M_1) \simeq \mathrm{Hom}_R(R/I, M_1/\langle x_2, \ldots, x_{j+1}\rangle M_1)$, since by Proposition 3.4 we know $x_2, \ldots, x_{j+1}$ is an M_1-sequence. But $M_1/\langle x_2, \ldots, x_{j+1}\rangle M_1 \simeq M_{j+1}$ (this was noted in the proof of Proposition 3.4), and so:

$$\mathrm{Ext}^{j+1}_R(R/I, M) \simeq \mathrm{Ext}^j_R(R/I, M_1) \simeq \mathrm{Hom}_R(R/I, M_1/\langle x_2, \ldots, x_{j+1}\rangle M_1) \simeq \mathrm{Hom}_R(R/I, M_{j+1})$$

This completes the inductive step, and together with our base case proves the lemma.

□

We now use Lemma 3.11 to assert that for any $1 \leq k \leq n$, then:

$$\mathrm{Ext}^{k-1}_R(R/I, M) \simeq \mathrm{Hom}_R(R/I, M_{k-1}) = 0$$

proving that $\mathrm{Ext}^k_R(R/I, M) = 0$ for $k < n$.

It remains only to prove that $\mathrm{Ext}^n_R(R/I, M) \neq 0$, which by our Lemma is equivalent to proving $\mathrm{Hom}_R(R/I, M_n) \neq 0$. Suppose the contrary, i.e. suppose $\mathrm{Hom}_R(R/I, M_n) = 0$. Then we claim there exists $y \in I$ such that y is an M_n-sequence.

This is proved by Bruns and Herzog in [BH93] (as Lemma 1.2.3(b)). The proof combines ideas from the theory of associated primes with ideas on localization, but is somewhat more involved than we have built up to in this thesis, so is omitted. □

An immediate corollary is that any M-sequence in a ring can be completed to a maximal M-sequence. This is clearly a very nice result, as without it the computation of maximal M-sequences would require us not just to try and find an M-sequence, but to try and find a *particular* M-sequence! This would mean both choosing the right elements and doing so in the right order - a process that could very quickly become absolutely horrific!

Corollary 3.12. *Given a ring R and an R-module M, then any M-sequence in R can be completed to a maximal M-sequence.*

Proof. Suppose the length of any maximal M-sequence in R is n. Then consider an M-sequence of the form $x_1, x_2, \ldots, x_p$ for some $p < n$. Since $p \neq n$, this M-sequence cannot be maximal, so there exists some $y_1 \in R$ such that $x_1, x_2, \ldots, x_p, y_1$ is an M-sequence.

Similarly, we can find y_2, y_3, $\ldots$, y_{n-p} such that $x_1, x_2, \ldots, x_p, y_1, y_2, \ldots, y_{n-p}$ is an M-sequence in R, and since this has length n it is maximal. Thus we have completed the M-sequence $x_1, \ldots, x_p$ to a maximal M-sequence, as desired. □

Definition 3.13. *Given a ring R, an R-module M and a proper ideal $I \subset R$, then the **depth of** I **on** M, denoted depth(I,M), is defined to be the maximum length of any M-sequence contained in the ideal I.*

Remark 3.14. Notice that in the particular case of $(R, \mathfrak{m})$ a local ring, then we will have $\operatorname{depth}(\mathfrak{m}, R) = \inf\{i \big| \operatorname{Ext}^i_R(R/\mathfrak{m}, M) \neq 0\}$. This invites comparison with $\operatorname{pd}_R(M)$, which we saw in the previous chapter was $\inf\{i \big| \operatorname{Ext}^i_R(M, R/\mathfrak{m}) \neq 0\}$. Relating these two notions will be done in Section 3.4 via the Auslander-Buchsbaum Formula. □

Some peculiarities of notation relating to depth are that:

- The depth of an ideal I on the ring R as an R-module is often written $\operatorname{depth}(I)$ rather than $\operatorname{depth}(I, R)$.
- In a local ring $(R, \mathfrak{m})$, the depth of the maximal ideal $\mathfrak{m}$ on an R-module M is often written $\operatorname{depth}(M)$ rather than $\operatorname{depth}(\mathfrak{m}, M)$.

Although these appear to create confusion if using $\operatorname{depth}(I)$ in a local ring, for instance, it is usually apparent from the context which meaning is intended. In addition, if considering $\operatorname{depth}(\mathfrak{m}, R)$ in a local ring $(R, \mathfrak{m})$, this is usually written as $\operatorname{depth}(R)$.

Remark 3.15. The depth of an ideal is a particular instance of what Rees originally defined to be 'grade', but is very closely related in that what Rees defined (in [REE57]) to be the grade of an R-module M is what we define to be the depth of $\text{Ann}(M)$, the annihilator of M in R. This, however, is generally regarded as a very minor difference in the grand scheme of things. □

3.3 Depth versus Codimension

We remarked at the beginning of this chapter that depth could be related to other numerical invariants of ideals, including the projective dimension, the Krull dimension and the codimension (which we will soon meet).

In this section we will focus primarily on the codimension, since the major relationship between projective dimension and depth will be characterized by the Auslander-Buchsbaum Formula in the next section, and there are not really any notable relationships between Krull dimension and depth.

The first step in such a comparison is to define codimension.

Definition 3.16. *Let R be a ring and let I be an ideal in R. The* ***codimension*** *of I in R (denoted $\text{codim}(I)$) is defined to be the supremum of the lengths of chains of prime ideals of R that are contained in I (ordering by inclusion).*

Remark 3.17. There is a more formal definition in terms of localization, however we omit this as it is not significantly more useful for our purposes. □

Example 3.18. The simplest example is in a field $\mathbb{K}$, where the ideal (0) has codimension 0 and the ideal $\mathbb{K}$ has codimension 1! □

Remark 3.19. One always needs to be cautious when using terms such as 'codimension', since over the years this particular idea has also been called 'height', 'rank' and even 'depth'! This variability in nomenclature does not all go one way - Auslander and Buchsbaum used the term 'codimension' to refer to what we have here introduced as 'depth'.

As a result, we reiterate the importance of knowing just what definition is being used by any given author (and refer the reader to Definitions 3.13 and 3.16 to ensure no confusion arises in this thesis). □

One of the key theorems in the theory of codimension (which can potentially be related to any of a number of results for depth) is the Principal Ideal Theorem of Krull, which is one of the major results in dimension theory. Because of its importance, we provide a statement of the theorem here, though the proof is omitted:

Theorem 3.20. *Given a ring R and elements $x_1, \ldots, x_n \in R$, then any prime ideal P which is minimal amongst prime ideals of R containing $x_1, \ldots, x_n$ must have codimension at most n.*

There is also a converse to this, which asserts that given any prime ideal P of codimension n in a ring, there exists an ideal I generated by n elements such that P is minimal amongst prime ideals containing I.

Remark 3.21. A useful inequality to know about codimension is due to Macaulay, and states that if M is a $p \times q$ matrix with entries in a (Noetherian) ring R, and $I_k(M)$ is the ideal generated by the determinants of the $k \times k$ submatrices of M, then any prime P which is minimal over $I_k(M)$ has codimension bounded above by $(p-k+1)(q-k+1)$. We will make use of this in a later chapter, so remark upon it now. □

Remark 3.22. In [EIS95] there is reference on page 449 to a result which it is claimed 'plays a role in the theory of depth something like the one played by the principal ideal theorem in the theory of codimension'. Although this analogy is not really obvious, the result is reproduced here for the benefit of the interested reader, without the proof.

Lemma 3.23. *If M is a finitely generated module over a local ring $(R, \mathfrak{m})$, I is an ideal in R and $y \in \mathfrak{m}$ then depth$(\langle I, y\rangle, M) \leq$ depth$(I, M) + 1$.*

□

The result in the aforementioned remark was intended for use in putting an upper bound on depth(I, M) (for an ideal I in a ring R with an R-module M) using maximal chains of prime ideals. When taking depth(I, R), we obtain a nice relationship that holds in any Noetherian ring.

Theorem 3.24. *Given any ideal I in a Noetherian ring R, then:*

$$\textit{depth}(I, R) \leq \textit{codim}(I)$$

Proof. We prove this by induction on depth(I, R).

Suppose depth$(I, R) = 0$. Then codim$(I, R) \geq 0$, so the inequality is valid when depth$(I, R) = 0$.

Now suppose depth$(I, R) \leq$ codim(I) if depth$(I, R) \leq n$ (for any ring R and any ideal $I \subset R$). Consider the case where depth$(I, R) = n + 1$, and let $x_1, \ldots, x_{n+1}$ be a maximal R-sequence of length $n + 1$ in I. Here x_1 is not a zero divisor over R, so is not contained in any minimal prime ideal of R (by Proposition 6.32).

Consider the ideal $I/\langle x_1 \rangle$ in the ring $R/\langle x_1 \rangle$. Because the prime ideals of $R/\langle x_1 \rangle$ are in one-to-one correspondence with the prime ideals of R containing $\langle x_1 \rangle$ (this is a standard result in ring theory), any chain of prime ideals in $R/\langle x_1 \rangle$ descending from $I/\langle x_1 \rangle$ can be 'raised' to a chain of prime ideals in R descending from I, all of which contain $\langle x_1 \rangle$.

But $\langle x_1 \rangle$ is not contained in any minimal prime ideal of R, so given any such 'raised' chain of prime ideals in R then we can find (at least) one more prime to be added onto this chain. Hence the supremum of the lengths of chains of prime ideals in the ideal I in R is at least one more than the supremum of the lengths of chains of prime ideals in the ideal $I/\langle x_1 \rangle$ in $R/\langle x_1 \rangle$, and so codim$(I/\langle x_1 \rangle) <$ codim(I).

Then depth$(I/\langle x_1 \rangle, R/\langle x_1 \rangle) = n$ (else we contradict maximality of the R-sequence $x_1, \ldots, x_{n+1}$), so by the inductive hypothesis $n \leq$ codim$(I/\langle x_1 \rangle) <$ codim(I), which means depth$(I, R) = n + 1 \leq$ codim(I). □

The case when the inequality of Theorem 3.24 is an equality is one of particular interest, as it defines a very special class of ring.

Definition 3.25. *A ring R in which every ideal I satisfies depth$(I, R) =$ codim(I) is called a **Cohen-Macaulay ring**.*

To date we have (intentionally) concentrated our attention on the links between depth and codimension of ideals, since codimension is the 'geometric' idea that seems to come closest to fitting the role played by the 'algebraic' idea of depth of an ideal. We will now briefly mention the links between depth and Krull dimension, and between depth and projective dimension.

Depth is not really related to Krull dimension in any meaningful sense of the word, since the main inequality linking the two is that in the case of a local ring $(R, \mathfrak{m})$ then $\mathrm{depth}(\mathfrak{m}, R) \leq \dim(R)$.

In actual fact, however, note that $\dim(R)$ is the number of inclusions in any maximal chain of prime ideals contained in R (ordered by inclusion). In fact, such a chain is also a maximal chain of prime ideals contained in $\mathfrak{m}$, using the fact that any proper ideal of a ring is contained in a maximal ideal, so $\dim(R) = \mathrm{codim}(\mathfrak{m})$. Hence our 'inequality' is just a special case of the inequality linking depth and codimension.

We omit the major relationship (in a local ring) between depth and projective dimension (fundamental as it is) since it will form the central plank of our next section, on the Auslander-Buchsbaum Formula.

3.4 The Auslander-Buchsbaum Formula

We have already remarked on the apparent similarities between the formulae used to compute the depth and projective dimension of modules in local rings (in terms of the vanishing of Ext), suggesting that these notions should - at least in local rings - complement one another.

In fact, Zariski and Samuel (in [ZS60]) refer to the depth [4] of an ideal as its 'homological codimension', which reinforces the idea that it complements the projective (or homological) dimension, in much the same way that codimension complements Krull dimension.

In the case of a (Noetherian) local ring, it turns out the Auslander-Buchsbaum Formula (proved in [AB57]) provides a direct link between the projective dimension of a module and its depth (when the former quantity is finite).

Theorem 3.26 (Auslander-Buchsbaum Formula). *Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$ and let $M \neq 0$ be a finitely generated R-module with finite projective dimension. Then*

$$pd_R(M) = depth(R) \text{ - } depth(M) \tag{3.2}$$

There are a number of ways to prove this, including induction on the depth of $\mathfrak{m}$ (first upon R and then in a secondary induction on M), and induction on $\mathrm{pd}_R(M)$ using the homology of the Koszul complex. Our approach will be to induct on $\mathrm{pd}_R(M)$, but since we will only meet the Koszul complex in Chapter 4, we will use the functor Ext to achieve the same purpose[5].

Proof. We first establish the result when $\mathrm{pd}_R(M) = 0$ as a separate lemma.

Lemma 3.27. *Given a local ring $(R, \mathfrak{m})$ then depth(R) = depth(F) for any finitely generated free R-module F.*

Proof. Since F is finitely generated and free, $F \simeq R^n$ for some non-negative integer n, so it is more than sufficient to show that $\mathrm{Ext}^i_R(R/\mathfrak{m}, R^n) = 0$ iff $\mathrm{Ext}^i_R(R/\mathfrak{m}, R) = 0$ for any i, as then it is clear that:

$$\mathrm{depth}(R^n) = \inf\{i \big| \mathrm{Ext}^i_R(R/I, R^n) \neq 0\} = \inf\{i \big| \mathrm{Ext}^i_R(R/I, R) \neq 0\} = \mathrm{depth}(R)$$

[4]In another indication of how variable notation is, they refer to it as 'grade', and use the term 'depth' to refer to what we call 'codimension'!

[5]I have not as yet come across a proof using this method, which suggests that it may not be the standard approach. It is nonetheless a good exercise that once again conveys the power of Ext.

But $R^n = \oplus_{j=1}^n R$, so using Proposition 2.25 we find that

$$\mathrm{Ext}_R^i(R/\mathfrak{m}, R^n) \simeq \oplus_{j=1}^n(\mathrm{Ext}_R^i(R/\mathfrak{m}, R)) = (\mathrm{Ext}_R^i(R/\mathfrak{m}, R))^n$$

from which it immediately follows that $\mathrm{Ext}_R^i(R/\mathfrak{m}, R^n) = 0$ iff $\mathrm{Ext}_R^i(R/\mathfrak{m}, R) = 0$.

This completes our proof, so that the Auslander-Buchsbaum Formula holds for any finitely generated free module over a local ring (i.e. when $\mathrm{pd}_R(M) = 0$). □

Now suppose (3.2) holds for all finitely generated R-modules with projective dimension less than k and consider a minimal free resolution of an R-module M which satisfies $\mathrm{pd}_R(M) = k$, such as:

$$0 \longrightarrow F_k \longrightarrow \cdots \xrightarrow{\varphi_3} F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

In particular, consider the first step of this resolution:

$$0 \longrightarrow N \xrightarrow{\iota} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0 \tag{3.3}$$

where $N = \ker(\varphi_0)$ and ι is the inclusion into the free module F_0.

Since this is a free resolution of M it is exact at F_0, and $N = \ker(\varphi_0) = \mathrm{im}(\varphi_1)$ means a free resolution of N is:

$$0 \longrightarrow F_k \longrightarrow \cdots \xrightarrow{\varphi_3} F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} N \longrightarrow 0$$

Hence N has a free resolution of length $k-1$, so $\mathrm{pd}_R(N) \leq k-1 = \mathrm{pd}_R(M) - 1$ (as any free resolution is also a projective resolution).

Suppose $\mathrm{pd}_R(N) = j < k-1$ (for some non-negative integer j), i.e. suppose we can find free modules F'_j, F'_{j-1}, $\ldots$, F'_1, F'_0 such that there exists a free resolution of N

given by $0 \longrightarrow F'_j \longrightarrow \cdots \longrightarrow F'_1 \xrightarrow{\varphi'_1} F'_0 \xrightarrow{\varphi'_0} N \longrightarrow 0$. This in turn gives another free resolution for M, namely:

$$0 \longrightarrow F'_j \longrightarrow \cdots \longrightarrow F'_1 \xrightarrow{\varphi'_1} F'_0 \xrightarrow{\iota\circ\varphi'_0} F_0 \longrightarrow M \longrightarrow 0$$

But now we have a projective resolution of M with length $j+1 < k = \mathrm{pd}_R(M)$, contradicting the definition of projective dimension. Hence $\mathrm{pd}_R(N) \not< k-1$, so $\mathrm{pd}_R(N) = k-1 = \mathrm{pd}_R(M) - 1$.

By our inductive hypothesis $\mathrm{pd}_R(N) = \mathrm{depth}(R) - \mathrm{depth}(N)$, so we have shown that $\mathrm{pd}_R(M) = \mathrm{depth}(R) - \mathrm{depth}(N) + 1$ and proving the Auslander-Buchsbaum formula is now equivalent to proving $\mathrm{depth}(M) = \mathrm{depth}(N) - 1$.

For this we apply the functor $\mathrm{Hom}_R(R/\mathfrak{m}, -)$ to the short exact sequence (3.3) above and then form a long exact sequence in Ext to get:

$$\to \mathrm{Ext}^j_R(R/\mathfrak{m}, F_0) \longrightarrow \mathrm{Ext}^j_R(R/\mathfrak{m}, M) \longrightarrow \mathrm{Ext}^{j+1}_R(R/\mathfrak{m}, N) \longrightarrow \mathrm{Ext}^{j+1}_R(R/\mathfrak{m}, F_0) \to$$

(since Ext is a right-derived functor, the indices should be increasing in this sequence as the arrows progress).

Since $\mathrm{pd}_R(N) \geq 0$, then by the inductive hypothesis $\mathrm{depth}(R) - \mathrm{depth}(N) \geq 0$, so $\mathrm{depth}(N) \leq \mathrm{depth}(R) = \mathrm{depth}(F_0)$ (with the equality following from Lemma 3.27, as F_0 is finitely generated and free).

Thus if $j+1 < \mathrm{depth}(N)$, then using the definition of depth via the vanishing of Ext the first three terms of the long exact sequence above become:

$$\to 0 \longrightarrow \mathrm{Ext}^j_R(R/\mathfrak{m}, M) \longrightarrow 0 \to$$

and so $\mathrm{Ext}^j_R(R/\mathfrak{m}, M) = 0$ (by exactness).

Thus $\mathrm{Ext}^j_R(R/\mathfrak{m}, M) = 0$ for all $j < \mathrm{depth}(N) - 1$, so $\mathrm{depth}(M) \geq \mathrm{depth}(N) - 1$.

Ignoring the trivial modules, then the long exact sequence in Ext can be written as follows (writing $d = \text{depth}(N)$ for convenience):

$$0 \longrightarrow \text{Ext}^{d-1}(R/\mathfrak{m}, M) \longrightarrow \text{Ext}^{d}(R/\mathfrak{m}, N) \longrightarrow \text{Ext}^{d}(R/\mathfrak{m}, F_0) \longrightarrow \cdots$$

If $\text{pd}_R(N) > 0$, then $\text{depth}(F_0) = \text{depth}(R) > d$ so the long exact sequence begins:

$$0 \to \text{Ext}^{d-1}(R/\mathfrak{m}, M) \longrightarrow \text{Ext}^{d}(R/\mathfrak{m}, N) \to 0$$

Thus $\text{Ext}^{d-1}(R/\mathfrak{m}, M) \simeq \text{Ext}^{d}(R/\mathfrak{m}, N)$ (the constraints of exactness force the map between these two to be injective and surjective), so $\text{Ext}^{d-1}(R/\mathfrak{m}, M) \neq 0$, from the definition of $d = \text{depth}(N)$.

Because $\text{Ext}^{j}(R/\mathfrak{m}, M) = 0$ for all $j < d - 1$, we find that $\text{depth}(M) = \text{depth}(N) - 1$, completing the proof of the Auslander-Buchsbaum Formula when $\text{pd}_R(N) > 0$.

If $\text{pd}_R(N) = 0$, then N is projective, and hence free (since $(R, \mathfrak{m})$ is local). The minimal free resolution of M is thus:

$$0 \longrightarrow N \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

where N is a finitely generated free R-module (finite generation comes from Propositions 6.14 and 6.13, since N is a submodule of the finitely generated free R-module F_0).

The main consequence of this is that $\varphi_1 : N \to F_0$ can be represented by a matrix over R with every entry contained in $\mathfrak{m}$.

We now revisit our long exact sequence in Ext, which has the form:

$$0 \longrightarrow \text{Ext}^{d-1}(R/\mathfrak{m}, M) \longrightarrow \text{Ext}^{d}(R/\mathfrak{m}, N) \xrightarrow{(\varphi_1)_*} \text{Ext}^{d}(R/\mathfrak{m}, F_0) \longrightarrow \cdots$$

We wish to show that $\operatorname{Ext}^{d-1}(R/\mathfrak{m}, M) \neq 0$, which will demonstrate that $\operatorname{depth}(M) \leq d-1 = \operatorname{depth}(N) - 1$, and together with our earlier inequality will prove the Auslander-Buchsbaum Formula when $\operatorname{pd}_R(M) = 1$.

Now by exactness at $\operatorname{Ext}^{d-1}(R/\mathfrak{m}, M)$ and at $\operatorname{Ext}^d(R/\mathfrak{m}, N)$, we find:

$$\operatorname{Ext}^{d-1}(R/\mathfrak{m}, M)/0 \simeq \ker((\varphi_1)_*)$$

so to show $\operatorname{Ext}^{d-1}(R/\mathfrak{m}, M) \neq 0$ we will show $\ker((\varphi_1)_*) \neq 0$. Because we know that $\operatorname{Ext}^d(R/\mathfrak{m}, N) \neq 0$ (as $d = \operatorname{depth}(N)$) it is more than sufficient to show that the induced map on homology $(\varphi_1)_* : \operatorname{Ext}^d(R/\mathfrak{m}, N) \to \operatorname{Ext}^d(R/\mathfrak{m}, F_0)$ is the zero map.

Since N and F_0 are both finitely generated free modules, we can write $N \simeq R^p$ and $F_0 \simeq R^q$ for some non-negative integers p, q. Thus we are seeking to show the map $(\varphi_1)_* : \operatorname{Ext}^d(R/\mathfrak{m}, R^p) \to \operatorname{Ext}^d(R/\mathfrak{m}, R^q)$ induced by $\varphi_1 : R^p \to R^q$ is the zero map (here we have essentially chosen some fixed generating sets for N and F_0). Using the property that Ext commutes with direct sums in the second variable, then we can represent $(\varphi_1)_*$ as being a map from $(\operatorname{Ext}^d(R/\mathfrak{m}, R))^p \to (\operatorname{Ext}^d(R/\mathfrak{m}, R))^q$.

Now, since N and F_0 form modules in a minimal free resolution of M, then φ_1 can be represented by a matrix with all coefficients in the maximal ideal $\mathfrak{m}$. This is the critical step, as now an arguement very similar to that used in Lemma 3.11 enables us to assert that $(\varphi_1)_*$ is indeed the zero map, as desired.

□

The Auslander-Buchsbaum Formula has many consequences, and it is worth our discussing some of these in a few remarks:

Remark 3.28. The Auslander-Buchsbaum Formula resembles the relationship $\dim(I) + \operatorname{codim}(I) = \dim(R)$ on Krull dimension and codimension in affine domains, which weakens to the inequality $\dim(I) + \operatorname{codim}(I) \leq \dim(R)$ over all rings.

The corresponding homological inequality (proved by Rees in [REE57]) is that if I is an ideal in a Noetherian ring R and M is a module with projective dimension less than $\operatorname{depth}(I, R)$, then $\operatorname{pd}_R(M) + \operatorname{depth}(I, M) \geq \operatorname{depth}(I, R)$. □

Remark 3.29. A consequence of the Auslander-Buchsbaum Formula is that in a local ring $(R, \mathfrak{m})$ then $\operatorname{depth}(R) \geq \operatorname{depth}(M)$ for any finitely generated module M with $\operatorname{pd}_R(M)$ finite, which leads us to suspect existence of some link between M-sequences and R-sequences (e.g. that any M-sequence is also an R-sequence).

In fact one of the great open problems of homological algebra (as listed by Hochster[6] in the series of talks [HOC75]) is the so-called **Zero divisor conjecture**, which postulates that if $x \in R$ is an M-sequence of length 1, then x is an R-sequence of length 1.

Although proved in some special cases (such as when the local ring R contains a field of characteristic $p > 0$), the general case of this conjecture remains unresolved. □

The Auslander-Buchsbaum Formula is a powerful result in homological algebra, and seems to be an appropriate place for us to pause our introduction to depth, and introduce another significant homological tool - the Koszul complex.

[6] Whilst Hochster did not explicitly identify these as the key conjectures of homological algebra, his list is considered definitive by many.

Chapter 4

The Koszul Complex

An alternate approach to regular sequences and the notion of depth can be developed via the Koszul complex, which is one of the major tools relating regular sequences back to homological algebra, and has also been developed into a construction of some significance in algebraic geometry (though we do not consider the geometric implications of it here).

The name 'Koszul complex' derives from Jean-Louis Koszul, who used this complex to study Lie algebra cohomology, though it had been studied before his time by Hilbert (as a free resolution of the field $\mathbb{K}$ as a $\mathbb{K}[x_1, \ldots, x_n]$-module, as well as by Cayley. The usefulness of the Koszul complex as more than just an exact complex was developed by Auslander, Buchsbaum and Serre in the 1950s, and in the years since, generalizations have been devloped by Eagon & Northcott and by Buchsbaum & Rim.

In studying the Koszul complex, we will begin with the simplest examples (as recorded by Eisenbud[1]), before discussing the more general cases. Although the construction of the Koszul complex usually involves exterior algebra (and this was the historical approach), we will use mapping cones to provide a more elementary approach. To conclude the chapter we place the Koszul complex within the framework of depth established in Chapter 3.

Much of the material is based on [EIS95] Chapter 17, but the fact that we avoid the exterior algebra and make some simplifications to provide a more elementary treatment mean that Section 4.2 in particular is not similar to the treatment of the Koszul complex in most references.

[1]Although Eisenbud was the one to record this treatment, it was Buchsbaum who introduced it to him.

4.1 The Basic Koszul Complex

The simplest Koszul complex (as seen in Example 1.11) is the complex $K(x)$ defined (on a ring R) by a single element $x \in R$ as:

$$0 \longrightarrow R \xrightarrow{x} R \longrightarrow 0 \tag{4.1}$$

Here $H_0(K(x)) = R/\langle x \rangle$ and $H_1(K(x)) = \{r \in R : rx = 0\}$ (ignoring quotients by zero). Note that $H_0(K(x)) = 0$ iff x generates R, whilst $H_1(K(x)) = 0$ iff x is not a zero divisor on R, so that x is an R-sequence iff $H_0(K(x)) \neq 0$ (this is the first condition of Definition 3.1) and $H_1(K(x)) = 0$ (this is the second condition of Definition 3.1).

This indicates a connection between regular sequences and the homology of the Koszul complex generated by one element. We now turn to the Koszul complex on two elements, formed by including a second element $y \in R$ as shown (note that all matrices are assumed to multiply on the left):

$$K(x, y): \ 0 \longrightarrow R \xrightarrow{\binom{y}{-x}} R^2 \xrightarrow{(x,y)} R \longrightarrow 0 \tag{4.2}$$

Here $H_0(K(x, y)) = R/\langle x, y \rangle$, so $H_0(K(x, y)) = 0$ iff $\langle x, y \rangle$ generate R (i.e. the first condition in Definition 3.1 is equivalent to $H_0(K(x, y)) \neq 0$). The other homology groups are $H_2(K(x, y)) = \{r \in R : ry = 0, rx = 0\}$ (which is 0 iff either x or y is not a zero divisor on R), and $H_1(K(x, y)) = \{(a, b) \in R^2 : ax + by = 0\}/\{(ry, -rx) \in R^2 : r \in R\}$.

If x is not a zero divisor, then any pair $(a, b) \in R^2$ with $ax + by = 0$ can be defined by b alone (if there were another pair (a', b) with $a'x + by = 0$ then $x(a - a') = 0$, so $a = a'$). Hence we find $by = -ax \in \langle x \rangle$, so $y(b + \langle x \rangle) = 0_{R/\langle x \rangle}$. Thus x, y is an R-sequence (given $H_0(K(x, y)) \neq 0$ and x not a zero divisor in R) iff y is not a zero divisor on $R/\langle x \rangle$, which occurs iff $b = -rx$ for some $r \in R$. In turn this forces $a = ry$, so $(a, b) \in \{(ry, -rx) \in R^2 : r \in R\}$.

Thus given $H_0(K(x,y)) \neq 0$, then if x is not a zero divisor on R then x, y is an R-sequence iff $H_1(K(x,y)) = 0$, and similarly if y is not a zero divisor on R then y, x is an R-sequence iff $H_1(K(x,y)) = 0$.

In short, the existence of a Koszul complex $K(x,y)$ such that both $H_0(K(x,y)) \neq 0$ and $H_1(K(x,y)) = 0 = H_2(K(x,y))$ is equivalent to either x, y or y, x being an R-sequence.

The Koszul complex $K(x,y)$ can also be presented via a commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & R & \xrightarrow{x} & R & \longrightarrow & 0 \\ & & \big\downarrow{\scriptstyle y} & & \big\downarrow{\scriptstyle y} & & \\ 0 & \longrightarrow & R & \xrightarrow{x} & R & \longrightarrow & 0 \end{array}$$

which relates $K(x,y)$ to the map of complexes $K(x) \xrightarrow{y} K(x)$.

This map of complexes is related to the construction of the general Koszul complex via the mapping cone (which we discuss in the next section) and involves the presentation:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R & \xrightarrow{-x} & R & \longrightarrow & 0 & & \\ & & & \searrow^{y} & \oplus & \searrow^{y} & & & \\ & & 0 & \longrightarrow & R & \xrightarrow{x} & R & \longrightarrow & 0 \end{array}$$

Such a diagram also demonstrates that the lower row $K(x)$ is a subcomplex of $K(x,y)$ and the upper row (isomorphic to $K(x)$) is the quotient of $K(x,y)$ by $K(x)$. The diagram below presents this as $K(x) \to K(x,y) \to K(-x)$, where $K(-x) \simeq K(x,y)/K(x)$):

$$\begin{array}{rccccccccc} K(x): & 0 & \longrightarrow & 0 & \longrightarrow & R & \xrightarrow{x} & R & \longrightarrow & 0 \\ & & & \big\downarrow & & \big\downarrow{\scriptstyle \binom{1}{0}} & & \big\downarrow{\scriptstyle id} & & \\ K(x,y): & 0 & \longrightarrow & R & \xrightarrow{\binom{y}{-x}} & R^2 & \xrightarrow{(x,y)} & R & \longrightarrow & 0 \\ & & & \big\downarrow{\scriptstyle id} & & \big\downarrow{\scriptstyle (0,1)} & & \big\downarrow & & \\ K(-x): & 0 & \longrightarrow & R & \xrightarrow{-x} & R & \longrightarrow & 0 & \longrightarrow & 0 \end{array} \tag{4.3}$$

This short exact sequence of complexes induces the long exact sequence in homology below (some straightforward diagram chasing shows the connecting homomorphism is multiplication by y):

$$0 \longrightarrow H_2(K(x,y)) \longrightarrow H_1(K(-x)) \xrightarrow{y} H_1(K(x)) \longrightarrow H_1(K(x,y)) \longrightarrow H_0(K(-x))$$

In the special case of a local ring $(R, \mathfrak{m})$, $H_0(K(x,y)) \neq 0$ iff $x, y \in \mathfrak{m}$. This is because if $x, y \in \mathfrak{m}$ then $\langle x, y \rangle \subseteq \mathfrak{m} \neq R$, so $H_0(K(x,y)) = R/\langle x, y \rangle \neq 0$. Conversely, if either x or y is not in $\mathfrak{m}$ then $\langle x, y \rangle \not\subseteq \mathfrak{m}$, so $\langle x, y \rangle = R$ (as any proper ideal would be contained in the maximal ideal) and $H_0(K(x,y)) = 0$.

Hence $H_1(K(x,y)) = 0$ implies $0 = H_1(K(x))/yH_1(K(-x)) \simeq H_1(K(x))/yH_1(K(x))$ (using exactness at $H_1(K(x))$ in the long exact sequence above). But now $H_1(K(x)) = yH_1(K(x)) \subseteq \mathfrak{m}H_1(K(x)) \subseteq H_1(K(x))$, so $\mathfrak{m}H_1(K(x)) = H_1(K(x))$. By Nakayama's lemma, $H_1(K(x)) = 0$, so x is not a zero divisor and in turn $H_2(K(x,y)) = 0$.

Thus in a (Noetherian) local ring, x, y forms a regular sequence iff both $H_0(K(x,y)) \neq 0$ and $H_1(K(x,y)) = 0$. An identical argument shows that in such a situation y, x is also a regular sequence. In fact if $(R, \mathfrak{m})$ is a local ring, x, y an R-sequence implies $ax+by, cx+dy$ is an R-sequence whenever $ad - bc$ is a unit in R.

This is presented as Exercise 17.1 in [EIS95], with the method being to display that $K(x,y)$ and $K(ax+by, cx+dy)$ are isomorphic. A quick computation shows that the isomorphism is:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & R & \xrightarrow{\binom{y}{-x}} & R^2 & \xrightarrow{(x,y)} & R & \longrightarrow & 0 \\
\downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle (ad-bc)\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}^T\right)^{-1}} & & \downarrow{\scriptstyle ad-bc} & & \downarrow{\scriptstyle 1} \\
0 & \longrightarrow & R & \xrightarrow[\binom{cx+dy}{-ax-by}]{} & R^2 & \xrightarrow[(ax+by,cx+dy)]{} & R & \longrightarrow & 0
\end{array}$$

where we know 1 is invertible, and the fact $ad - bc$ is invertible gives invertibility of the other two maps. Another proof of Lemma 3.7 is an immediate consequence.

4.2 Koszul complexes in general

When building the Koszul complex for two elements, we remarked it was possible to get a more general construction via mapping cones, an idea which we explore further in this section.

Definition 4.1. *Consider two complexes $M_\bullet, M'_\bullet$ and a chain map $\psi_\bullet$ between them, as in the commutative diagram shown.*

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & M_{n+1} & \xrightarrow{\partial_{n+1}} & M_n & \xrightarrow{\partial_n} & M_{n-1} & \longrightarrow & \cdots \\ && \downarrow{\scriptstyle \psi_{n+1}} && \downarrow{\scriptstyle \psi_n} && \downarrow{\scriptstyle \psi_{n-1}} && \\ \cdots & \longrightarrow & M'_{n+1} & \xrightarrow{\partial'_{n+1}} & M'_n & \xrightarrow{\partial'_n} & M'_{n-1} & \longrightarrow & \cdots \end{array}$$

*The **mapping cone** of $\psi_\bullet$ is the complex $M^\psi_\bullet$ such that $M^\psi_n = M_{n-1} \oplus M'_n$ and $\partial^\psi_n : M^\psi_n \to M^\psi_{n-1}$ acts on $M_{n-1} \oplus M'_n$ to give $\partial^\psi_n(m, m') = (-\partial_{n-1}(m), \psi_{n-1}(m) + \partial'_n(m'))$. (We require the negative sign to ensure $\partial^\psi_n \circ \partial^\psi_{n-1} = 0$, making the commutativity of the original diagram work for us).*

A more appropriate diagram to illustrate this is the schematic presentation we saw in our second diagram for the basic Koszul complex, which in the definition above would be:

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & M_{n+1} & \xrightarrow{-\partial_{n+1}} & M_n & \xrightarrow{-\partial_n} & M_{n-1} & \longrightarrow & \cdots \\ & \searrow & \oplus & \searrow^{\psi_{n+1}} & \oplus & \searrow^{\psi_n} & \oplus & \searrow & \\ \cdots & \longrightarrow & M'_{n+2} & \xrightarrow{\partial'_{n+2}} & M'_{n+1} & \xrightarrow{\partial'_{n+1}} & M'_n & \longrightarrow & \cdots \end{array}$$

The second diagram for the Koszul complex on two variables (from the previous section) illustrates the mapping cone of the homomorphism $K(x) \xrightarrow{y} K(x)$.

Extending this, we construct the Koszul complex $K(x_1, x_2, \ldots, x_n)$ on n variables as the mapping cone of the chain map $K(x_1, \ldots, x_{n-1}) \xrightarrow{x_n} K(x_1, \ldots, x_{n-1})$ taking the Koszul complex on $n-1$ variables to itself (where every map is multiplication by x_n).

Note that every non-trivial module in the Koszul complex is free, and their ranks are the binomial coefficients taken from the n^{th} row of Pascal's Triangle. (For example, in the Koszul complex generated by 1 element, there are two non-trivial modules, which are free with ranks 1 and 1. Similarly, in the Koszul complex generated by two elements the three non-trivial modules are free with ranks $1, 2, 1$, and so forth). Proving this is a near-trivial induction, so is omitted.

As an example, we construct the Koszul complex on three variables.

Example 4.2. Consider the mapping cone $K(x, y) \xrightarrow{z} K(x, y)$ for three elements x, y, z of a ring R, as below:

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & R & \xrightarrow{\binom{-y}{x}} & R^2 & \xrightarrow{(-x,-y)} & R & \longrightarrow & 0 & \longrightarrow & 0 \\
\oplus & \searrow^{z} & \oplus & \searrow^{z} & \oplus & \searrow^{z} & \oplus & \searrow^{z} & \oplus & \searrow^{z} & \oplus \\
0 & \longrightarrow & 0 & \longrightarrow & R & \xrightarrow{\binom{y}{-x}} & R^2 & \xrightarrow{(x,y)} & R & \longrightarrow & 0
\end{array}$$

Here $0 \oplus 0 \simeq 0$, $R \oplus 0 \simeq R$, $R^2 \oplus R \simeq R^3$, $R \oplus R^2 \simeq R^3$ and $0 \oplus R \simeq R$, so we can write this as a single complex:

$$0 \longrightarrow R \xrightarrow{\begin{pmatrix} -y \\ x \\ z \end{pmatrix}} R^3 \xrightarrow{\begin{pmatrix} z & 0 & y \\ 0 & z & -x \\ -x & -y & 0 \end{pmatrix}} R^3 \xrightarrow{\begin{pmatrix} x & y & z \end{pmatrix}} R \longrightarrow 0$$

The single complex follows directly from the mapping cone - the 3×3 matrix just reflects the relation of Definition 4.1 that $\partial_n^{\psi}(m, m') = (-\partial_n(m), \psi_{n-1}(m) + \partial'_{n-1}(m'))$ (albeit with the variables reordered to give us a complex that looks nicer). □

Whilst constructing the Koszul complex using mapping cones is straightforward, the usual approach to meet the Koszul complex is based on via exterior algebra, and a discussion of this method can be found in any of [BH93], [EIS95], [JAC80] or [LAN02].

Unfortunately, to maintain our focus on the real goal - of using the Koszul complex in the context of depth - we have reluctantly been forced to jettison this approach. In practical terms, however, we do not lose much by focusing on the construction via mapping cones instead, as we are about to see.

4.3 The Koszul complex and depth

There is a very natural link between the Koszul complex and the notion of R-sequences in a ring, and in fact the Koszul complex of a sequence of elements in a ring can be used to determine the depth of the ideal generated by those elements. In this section we will explore some of these links in greater detail.

Theorem 4.3. *If $x_1, \ldots, x_n$ is an R-sequence in the ring R then the Koszul complex $K(x_1, \ldots, x_n)$ provides a free resolution of the ideal $R/\langle x_1, \ldots, x_n\rangle$.*

Proof. The proof is a straightforward induction on n using mapping cones, so is omitted. All modules are finite and free, so it is only necessary to check that the homology groups take the desired values (in this case, $H_0(K(x_1, \ldots, x_{j+1})) = R/\langle x_1, \ldots, x_{j+1}\rangle$ and $H_i(K(x_1, \ldots, x_{j+1})) = 0$ elsewhere), which follows easily after some diagram chasing. □

Note that because of the way we write the Koszul complex, it is a free resolution in the alternate form described in Remark 2.3, rather than that of Definition 2.2, which is why we wish the 0^{th} homology group to be non-trivial.

In a local ring, this result can be strengthened to an if and only if result.

Theorem 4.4. *A sequence $x_1, \ldots, x_n$ of elements in the maximal ideal $\mathfrak{m}$ of a local ring $(R, \mathfrak{m})$ is an R-sequence iff $H_1(K(x_1, \ldots, x_n)) = 0$.*

Proof. For the 'only if' statement, note that from Theorem 4.3 if $x_1, \ldots, x_n$ is an R-sequence then $K(x_1, \ldots, x_n)$ is a free resolution of $R/\langle x_1, \ldots, x_n\rangle$, so $H_1(K(x_1, \ldots, x_n)) = 0$ as desired.

There is more work involved in the 'if' statement, and we require the following lemma.

Lemma 4.5. *If $H_i(K(x_1, \ldots, x_n)) = 0$ for some $i \geq 1$ (where $x_1, \ldots, x_n$ are elements in the maximal ideal of a local ring), then $H_k(K(x_1, \ldots, x_n)) = 0$ for all $k \geq i$.*

Proof. We induct on n, the number of elements generating the Koszul complex.

When $n = 1$ the result is clearly true, as for $k \geq 1$ the homology group is a quotient of 0. Suppose the result holds when $n = j$, i.e. for any sequence of j elements $y_1, \ldots, y_j$ in $\mathfrak{m}$, if $H_i(K(y_1, \ldots, y_j)) = 0$ for some i then $H_k(K(y_1, \ldots, y_j)) = 0$ for all $k \geq i$.

Now consider a sequence of elements $z_1, \ldots, z_{j+1} \in \mathfrak{m}$ such that $H_i(K(z_1, \ldots, z_{j+1})) = 0$ for some i. Since $K(z_1, \ldots, z_{j+1})$ is the mapping cone of $K(z_1, \ldots, z_j) \xrightarrow{z_{j+1}} K(z_1, \ldots, z_j)$, we form a short exact sequence of complexes (such as (4.3) for the two variable case):

$$0 \longrightarrow K(z_1, \ldots, z_j) \longrightarrow K(z_1, \ldots, z_{j+1}) \longrightarrow K(z_1, \ldots, z_j) \longrightarrow 0$$

The long exact sequence in homology induced by this short exact sequence now includes a number of subsequences of the form:

$$H_k(K(z_1, \ldots, z_j)) \xrightarrow{z_{j+1}} H_k(K(z_1, \ldots, z_j)) \longrightarrow H_k(K(z_1, \ldots, z_{j+1})) \longrightarrow H_{k-1}(K(z_1, \ldots, z_j)) \tag{4.4}$$

where all connecting homomorphisms are multiplication by z_{j+1}, with $k \geq 1$.

Then $H_i(K(z_1, \ldots, z_{j+1})) = 0$ implies that $H_i(K(z_1, \ldots, z_j) \xrightarrow{z_{j+1}} H_i(K(z_1, \ldots, z_j))$ is a surjective homomorphism, so:

$$H_i(K(z_1, \ldots, z_j)) = z_{j+1} H_i(K(z_1, \ldots, z_j)) \subseteq \langle z_{j+1} \rangle H_i(K(z_1, \ldots, z_j))$$

Since $H_i(K(z_1, \ldots, z_j))$ is an R-module, the reverse inclusion also holds, which gives $H_i(K(z_1, \ldots, z_j)) = \langle z_{j+1} \rangle H_i(K(z_1, \ldots, z_j))$. Use of Nakayama's Lemma (Theorem 6.33) immediately lets us see $H_i(K(z_1, \ldots, z_j)) = 0$. It follows that $H_k(K(z_1, \ldots, z_j)) = 0$ for all $k \geq i$ by the inductive hypothesis.

Checking the subsequences shown in the sequence (4.4) for each $k \geq i$, we now find that $k \geq i$ implies $H_k(K(z_1, \ldots, z_{j+1})) = 0$ (these homology groups all map injectively to 0), which gives $H_k(K(z_1, \ldots, z_{j+1})) = 0$ for all $k \geq i$ as desired.

This completes the inductive step, so if $H_i(K(x_1, \ldots, x_n)) = 0$ for some $i \geq 1$ then $H_k(K(x_1, \ldots, x_n)) = 0$ for all $k \geq i$. □

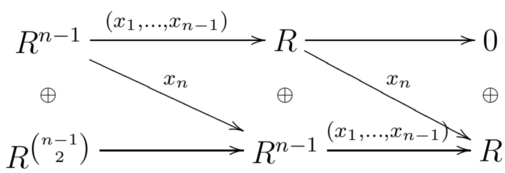
Using the lemma, if $H_1(K(x_1, \ldots, x_n)) = 0$, then $H_k(K(x_1, \ldots, x_n)) = 0$ for all $k \geq 1$ (and so $K(x_1, \ldots, x_n)$ is a free resolution of $R/\langle x_1, \ldots, x_n\rangle$).

Another inductive argument on n is now sufficient to demonstrate the desired result, since if $H_1(K(x_1, \ldots, x_n)) = 0$ then $H_1(K(x_1, \ldots, x_{n-1}) = 0$ (from the proof of the lemma), which in the inductive step shows $x_1, \ldots, x_{n-1}$ was an R-sequence. Because $x_1, \ldots, x_n \in \mathfrak{m}$ then $\langle x_1, \ldots, x_n\rangle \subseteq \mathfrak{m} \subset R$, so the only thing to check is that x_n is not a zero divisor on $R/\langle x_1, \ldots, x_{n-1}\rangle$.

This turns out to be true because it can be shown (without much difficulty) that:

$$H_1(K(x_1, \ldots, x_n)) = \{r \in R : rx_n \in \langle x_1, \ldots, x_{n-1}\rangle\}/\langle x_1, \ldots, x_{n-1}\rangle$$

by considering the first homology group of $K(x_1, \ldots, x_n)$ as part of a mapping cone:



We skim over the details of this proof, as it is quite straightforward and consequently achieves little more than to take up space. □

Remark 4.6. Under the conditions of the previous theorem, then if $x_1, \ldots, x_n \in \mathfrak{m}$ is an R-sequence, then the Koszul complex is the unique (up to isomorphism) minimal free resolution of $R/\langle x_1, \ldots, x_n\rangle$. □

Theorems 4.3 and 4.4 establish the Koszul complex as a device that can be used to work with R-sequences, though outside of local rings we cannot use the Koszul complex generated by n elements of a ring to identify whether those elements form an R-sequence.

What we *can* do, however, is to determine the common length of all maximal R-sequences contained within the ideal generated by those n elements (simultaneously demonstrating that all maximal R-sequences contained in the ideal *do* have the same length). This is encapsulated in the following result, which we provide without proof:

Theorem 4.7. *Given elements $x_1, \ldots, x_n$ in a ring R, then every maximal R-sequence contained in the ideal $I = \langle x_1, \ldots, x_n \rangle \subset R$ has length $\inf\{k \big| H_{n-k}(K(x_1, \ldots, x_n)) \neq 0\}$.*

This would appear to provide us with a mechanism for defining the depth of an ideal on a ring (recall that the ring is Noetherian, so every ideal must be finitely generated). Recall, however, that in the previous chapter our definition of depth of an ideal was broader than this, applying to modules over a ring as well as the ring itself.

The trick in defining depth more generally via the Koszul complex is to consider the tensor product $M \otimes_R K(x_1, \ldots, x_n)$. We consider the $n = 1$ case below as an example.

Example 4.8. The Koszul complex generated by a single element x becomes (in this more general setting):

$$M \otimes_R K(x):\ 0 \longrightarrow M \otimes_R R \xrightarrow{id \otimes_R x} M \otimes_R R \longrightarrow 0$$

Using the isomorphism $M \otimes_R R \simeq M$ we can write this as $0 \longrightarrow M \xrightarrow{x} M \longrightarrow 0$, from which it follows that $H_0(K(x)) = M/\langle x \rangle M$ and $H_1(K(x)) = \{m \in M : xm = 0\}$, so x is an M-sequence iff $H_0(M \otimes_R K(x)) \neq 0$ and $H_1(M \otimes_R K(x)) = 0$, in the same fashion as before. □

We can now reformulate our results in terms of M-sequences, as below (proofs are omitted, but can be found in Chapter 17 of [EIS95] if desired, as well as in some of the other references previously mentioned for this section).

Since our main purpose is to introduce the reader to the Koszul complex and its relationship with depth, and the situation for M-sequences closely resembles that for R-sequences, we omit discussing the details.

Theorem 4.9 (Theorem 4.4 revisited). *Let $(R, \mathfrak{m})$ be a local ring and M a finitely generated R-module. A sequence $x_1, \ldots, x_n$ of elements in $\mathfrak{m}$ is an M-sequence if and only if $H_1(M \otimes_R K(x_1, \ldots, x_n)) = 0$.*

Theorem 4.10 (Theorem 4.7 revisited). *Given elements $x_1, \ldots, x_n$ in a ring R and a finitely generated R-module M, then every maximal M-sequence contained in the ideal $I = \langle x_1, \ldots, x_n \rangle \subset R$ has length equal to $\inf\{k \big| H_{n-k}(M \otimes_R K(x_1, \ldots, x_n)) \neq 0\}$.*

This last result is used by Eisenbud to define depth(I, M) as the length of any maximal M-sequence in an ideal I provided $IM \neq M$. (If $IM = M$, then he defines depth(I, M) to be infinite).

Theorem 4.7 (and its generalization Theorem 4.10) imply that if in a ring R a proper ideal I is generated by n elements, then depth$(I, R) \leq n$, since we know the 0^{th} homology group of the Koszul complex is non-trivial when $I \neq R$. This is analogous to the Principal Ideal Theorem we mentioned in the last chapter, once again suggesting the existence of connections between depth and codimension in ideals.

In summary, the Koszul complex is a powerful homological tool that is closely related to the notion of depth, and has many attractive properties for use in this study. When fully treated using the theory of exterior algebra, it also possesses some nice duality properties, and has uses in algebraic geometry (in the study of tangent bundles on projective n-space).

Chapter 5

The Hilbert-Burch Theorem

Having studied the theory of depth, we are now ready to set about the proof of the Hilbert-Burch theorem mentioned in the title of this thesis. A special case of this theorem was originally proved by David Hilbert in his 1890 paper *Über die Theorie von algebraischen Formen* in order to give an example of a free resolution, and it was extended to a more general form by Lindsay Burch in 1968.

In her paper [BUR56], Burch stated the theorem as follows:

Theorem 5.1 (The Hilbert-Burch Theorem - Burch). *Let $(R, \mathfrak{m})$ be a Noetherian local ring, and I an ideal in R with projective dimension 1. Then for some $n > 1$ the ideal I is the set of all determinants of matrices obtained by adjoining to a certain $(n-1) \times n$ matrix with elements in $\mathfrak{m}$ another row of elements arbitrarily chosen in R.*

Burch's motivation in proving this theorem was to find an upper bound on the minimal number of generators of the ideal $I(X)$ induced by a set X of points known to lie on a curve of given degree in projective space. Although such an upper bound had been already been derived, Burch was hoping to develop a generalization.

In this chapter we will first provide an exposition of the proof of the Hilbert-Burch theorem (following the method of [EIS00]) and then discuss some of its applications in the wider theory of commutative algebra.

5.1 Proof of the Hilbert-Burch Theorem

The form of the Hilbert-Burch theorem that we will be using in this section is taken from [EIS00] as Theorem 3.2 (and is also given in [EIS95] as Theorem 20.15, though with some minor differences). In this form it is actually a special case of the first structure theorem (Theorem 3.1) of [BE74], though as previously noted we avoid the exterior algebra needed for such a proof.

Almost all of the results in [BE74] were underpinned by the following result, which lets us identify precisely when a complex of free modules is exact:

Theorem 5.2 (Characterization of Free Resolutions). *Let R be a Noetherian ring. Then the complex of finitely generated free modules:*

$$0 \longrightarrow F_n \xrightarrow{\varphi_n} F_{n-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0$$

is an exact complex (so describes a free resolution of $F_0/im(\varphi_1)$) if and only if both the following conditions hold:

- *$rank(F_k) = rank(\varphi_k) + rank(\varphi_{k-1})$ for all $k = 1, \ldots, n-1$ and $rank(F_n) = rank(\varphi_n)$.*
- *$depth(I(\varphi_k), R) \geq k$ for all $k = 1, \ldots, n$.*

We do not as yet have all the terminology necessary to comprehend this theorem as yet, since whilst we can logically take the *rank* of a finitely generated free module $F \simeq R^n$ to be n, it is not so clear how to define the rank of a module homomorphism, and so we must impose a definition.

Definition 5.3 (Rank of a homomorphism of free modules). *Let R be a ring and $G_1 \simeq R^p$, $G_2 \simeq R^q$ be finitely generated free R-modules. Any module homomorphism $\theta : G_1 \to G_2$ with respect to fixed bases of G_1, G_2 can be represented by a $q \times p$ matrix with entries in R, and we define the* ***rank*** *of θ to be $rank(\theta) = \max\{r \,|\, I_r(\theta) \neq 0\}$, where $I_r(\theta)$ is the ideal generated by the determinants of all $r \times r$ submatrices of θ.*

This definition may seem slightly odd, but consideration of the situation for linear maps between finite-dimensional vector spaces over the same field (as covered in a basic linear algebra course) shows it is the correct one.

To see this, consider such a linear map in reduced row echelon form, so that at most one term in any row and any column is non-zero. The rank is then the number of leading columns, which is just the number of non-zero entries, and these non-zero entries form the diagonal of the submatrix of largest size with non-zero determinant.

Definition 5.4. *In the situation of Definition 5.3, we denote the ideal $I_{rank(\theta)}(\theta)$ by $I(\theta)$.*

We omit the proof of Theorem 5.2, since it would require aspects of the theory that we have elected to omit in this thesis, but it may be found on pages 498–499 of [EIS95].

As an application of 5.2, we prove a result of Auslander and Buchsbaum.

Corollary 5.5. *Let R be a Noetherian ring. Any non-trivial ideal I of R that has a finite free resolution contains an element a that is not a zero divisor.*

Proof. Suppose we take a finite free resolution of I, of the form:

$$0 \longrightarrow F_n \xrightarrow{\varphi_n} F_{n-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{\varphi_1} I$$

We can obtain a finite free resolution of the quotient R/I by embedding I in R as follows:

$$0 \longrightarrow F_n \xrightarrow{\varphi_n} F_{n-1} \longrightarrow \cdots \longrightarrow F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} R \xrightarrow{\psi} R/I \longrightarrow 0$$

(observing that $\varphi_1 : F_1 \to R$ simply maps F_1 onto the subset $I \subseteq R$).

Here φ_1 is a homomorphism of free R-modules, so can be represented by a matrix with entries in R. Since $\text{im}(\varphi_1) = I \neq 0$, we know φ_1 is not the zero map and so the matrix has at least one non-zero entry, i.e. $\text{rank}(\varphi_1) \geq 1$.

Because the image of φ_1 is a submodule of R, we also find $\text{rank}(\varphi_1) \leq 1$ (as there is precisely one row, so there are no $r \times r$ submatrices when $r > 1$).

Thus $\text{rank}(\varphi_1) = 1$, so $I(\varphi_1)$ is the ideal of R generated by the elements of the matrix representing φ_1, which turns out to be precisely $\text{im}(\varphi_1) = I$. Hence $I(\varphi_1) = I$.

Applying Theorem 5.2 applied to the resolution of R/I, we now find $\text{depth}(I) = \text{depth}(I(\varphi_1)) \geq 1$, so I must contain an element which is not a zero divisor, as desired. □

Remark 5.6. In fact Auslander and Buchsbaum only *proved* this corollary with the added condition that the ideal had non-zero codimension, and merely remarked in [AB57] that this extra condition could be dropped. Burch noted this in [BUR56] - and also noted that she could not actually find a proof in the literature - so proved it herself using the theory of associated primes. □

We are now ready to set about considering the proof of the Hilbert-Burch theorem to be found in [EIS00]. We begin with a statement of the theorem as it will be proved (though we have inserted some modifications to simplify the notation).

Theorem 5.7 (The Hilbert-Burch Theorem - Eisenbud). *Let R be a Noetherian ring and I a non-trivial proper ideal of R with a free resolution of length 1, as follows:*

$$0 \longrightarrow F \xrightarrow{\varphi} G \xrightarrow{\psi} I \longrightarrow 0$$

If the rank of the free module F is t, then the rank of the free module G is $t+1$, and if we fix bases (generating sets) for F and G then φ may be represented by a $(t+1) \times t$ matrix. Letting d_i be $(-1)^i$ times the determinant of the $t \times t$ matrix formed by deleting the i^{th} row of φ, then $I_t(\varphi) = \langle d_1, \ldots, d_{t+1} \rangle$, and we find that $I = aI_t(\varphi)$ for some $a \in R$ not a zero divisor. The i^{th} element of the matrix for ψ will turn out to be $d_i a$. Moreover, depth$(I_t(\varphi)) = 2$.

Conversely, given $a \in R$ not a zero divisor and a $(t+1) \times t$ matrix φ with entries in R such that depth$(I_t(\varphi)) \geq 2$, then the ideal $I = aI_t(\varphi)$ has a free resolution of length 1 as above.

That this statement encompasses Burch's statement of the theorem is not hard to see - the conditions hold almost trivially, and the only potential difficulty (that the elements of the matrix used must be in $\mathfrak{m}$) is overcome by any element of I being a multiple of a, which in a local ring would be in $\mathfrak{m}$).

Proof. Firstly, we can obtain a free resolution of R/I of the form:

$$0 \longrightarrow F \xrightarrow{\varphi} G \xrightarrow{\psi} R \longrightarrow R/I \longrightarrow 0 \tag{5.1}$$

Because φ and ψ are homomorphisms of finitely generated free modules (the finite generation follows easily from the fact the ring is Noetherian, so that ideals and quotients are finitely generated), they can be represented by matrices with entries in R.

Since ψ maps G onto $I \neq 0$ then $\psi \neq 0$, so at least one element of ψ is non-zero, meaning $\text{rank}(\psi) \geq 1$. Thus $\text{rank}(\psi) = 1$ (as ψ is a $1 \times (t+1)$ matrix, so $I_r(\psi) = 0$ for $r > 1$).

Applying Theorem 5.2 to first the free resolution of I and then the free resolution of R/I (as given in (5.1)), we find that $\text{rank}(\varphi) = \text{rank}(F) = t$, and then $\text{rank}(G) = \text{rank}(\varphi) + \text{rank}(\psi) = t + 1$.

This also shows that $\text{depth}(I(\varphi)) = \text{depth}(I_t(\varphi)) \geq 2$, and from Section 3.3 we know $\text{depth}(I_t(\varphi)) \leq \text{codim}(I_t(\varphi)) \leq ((t+1)-t+1)(t-t+1) = 2$ (using Macaulay's inequality). Combining these proves that $\text{depth}(I(\varphi)) = 2$, as desired.

Now let Δ be the $1 \times (t+1)$ matrix with $\Delta_i = d_i$ for $i = 1, \ldots, t+1$. The matrix Δ represents a module homomorphism from $R^{t+1} \to R$, and in fact we claim it defines a complex:

$$0 \longrightarrow F \xrightarrow{\varphi} G \xrightarrow{\Delta} R \tag{5.2}$$

Clearly $\varphi \circ 0 = 0$, so we only need check $\Delta \circ \varphi = 0$, i.e. as matrices $\Delta\varphi = 0$. Here $(\Delta\varphi)_i = \sum_{j=1}^{t+1} d_j \varphi_{ji}$, which is just the determinant of the $(t+1) \times (t+1)$ matrix formed by augmenting φ with its i^{th} column and expanding the determinant down this augmented column. (This follows from the definition of d_i). Because this matrix has two identical columns, its determinant is 0 so $\Delta\varphi = 0$ as desired.

We now have two complexes, namely:

$$0 \longrightarrow F \xrightarrow{\varphi} G \xrightarrow{\psi} R$$

$$0 \longrightarrow F \xrightarrow{\varphi} G \xrightarrow{\Delta} R$$

Applying the contravariant functor $\mathrm{Hom}_R(-, R)$ to these gives the complexes:

$$0 \longrightarrow R^* \xrightarrow{\psi^*} G^* \xrightarrow{\varphi^*} F^*$$

$$0 \longrightarrow R^* \xrightarrow{\Delta^*} G^* \xrightarrow{\varphi^*} F^*$$

where we write M^* to denote $\mathrm{Hom}_R(M, R)$ for $M = R, F, G$ (and place the $*$ as a superscript on the homomorphisms as well for consistency).

Now, given any $f \in F^* = \mathrm{Hom}_R(F, R)$, we can describe the action of f on F as multiplication of the coordinate vector (with respect to the fixed generating set for F) by the unique $1 \times \mathrm{rank}(F)$ matrix whose i^{th} element is the image under f of the i^{th} element of the generating set. Similarly any $1 \times \mathrm{rank}(F)$ matrix with entries in R defines a unique module homomorphism in F^*.

This establishes a correspondence between elements of F^* and elements of $R^{\mathrm{rank}(F)} \simeq F$, and it is easy to check that this correspondence is in fact a module isomorphism, so $F^* \simeq F$, and similarly $G^* \simeq G$.

(We obtain these matrices using the finite generation of F and G).

We now prove the next result as a lemma.

Lemma 5.8. *Let R be a ring and F, G be finitely generated free R-modules. Fix bases of F and G, and suppose $\theta : F \to G$ is a module homomorphism, with matrix also denoted by θ. Then we claim the map $\theta_* : G^* \to F^*$ induced by θ can be represented by the matrix θ^T.*

Proof. Observe that θ_* induces an R-module homomorphism α from $G \to F$, by commutativity of the following diagram:

$$\begin{array}{ccc} G & \simeq & G^* \\ \downarrow \alpha & & \downarrow \theta_* \\ F & \simeq & F^* \end{array}$$

Since α is a homomorphism of finitely generated free modules, it can be represented by a matrix with elements in R, and it is now a straightforward process of checking what occurs to the basis elements of G when going around the square (via G^* and F^*) to show that the matrix for α is indeed the matrix θ^T. □

Using this lemma twice in each complex, then our complexes become:

$$0 \longrightarrow R \xrightarrow{\psi^T} G \xrightarrow{\varphi^T} F \qquad \text{and}$$

$$0 \longrightarrow R \xrightarrow{\Delta^T} G \xrightarrow{\varphi^T} F$$

Now, observe that the $r \times r$ submatrices of φ^T are precisely the transposes of the $r \times r$ submatrices of φ, and since determinants are invariant under transpose, this means that $I_r(\varphi^T) = I_r(\varphi)$for any non-negative integer r.

Immediate consequences of this are that $\text{rank}(\varphi)^T = \text{rank}(\varphi) = t$, and $\text{depth}(I(\varphi^T)) = \text{depth}(I(\varphi)) \geq 2 > 1$. Because $\text{rank}(\varphi) = t$, then we know that there exists at least one $t \times t$ submatrix of φ with non-zero determinant, so that at least one of the d_i is non-zero.

Thus $\text{rank}(\Delta^T) = 1$, and in fact $I(\Delta^T) = I_1(\Delta^T) = I_t(\varphi)$ (since the 1×1 submatrices of Δ^T are its elements, which are (up to sign) precisely the determinants of the $t \times t$ submatrices of φ, so generate the same ideal). Consequently $\text{depth}(I(\Delta^T)) = \text{depth}(I(\varphi)) \geq 2$.

Combining the results of the previous two paragraphs, we find $\operatorname{depth}(I(\Delta^T)) \geq 2$, $\operatorname{depth}(I(\varphi^T)) \geq 1$, $\operatorname{rank}(\Delta^T) = 1 = \operatorname{rank}(R)$ and $\operatorname{rank}(\varphi^T) + \operatorname{rank}(\Delta^T) = t + 1 = \operatorname{rank}(G)$.

But now these are precisely the conditions of Theorem 5.2, so that the complex of free modules $0 \longrightarrow R \xrightarrow{\Delta^T} G \xrightarrow{\varphi^T} F$ is exact. We have a complex $0 \longrightarrow R \xrightarrow{\psi^T} G \xrightarrow{\varphi^T} F$ of projective modules, and can now utilize Theorem 2.8 (on inducing chain maps).

The homomorphism $id : F \to F$, which induces a chain map of complexes as below:

$$\begin{array}{ccccccc}
F & \xleftarrow{\varphi^T} & G & \xleftarrow{\psi^T} & R & \longleftarrow & 0 \\
\downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\
F & \xleftarrow{\varphi^T} & G & \xleftarrow{\Delta^T} & R & \longleftarrow & 0
\end{array}$$

Clearly the induced map from $G \to G$ must be the identity (for the leftmost square to commute) whilst the induced homomorphism from $R \to R$ can be represented as multiplication by some $a \in R$ (where a is the image of the identity). This makes our diagram:

$$\begin{array}{ccccccc}
F & \xleftarrow{\varphi^T} & G & \xleftarrow{\psi^T} & R & \longleftarrow & 0 \\
\downarrow{\scriptstyle id} & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle a} & & \\
F & \xleftarrow{\varphi^T} & G & \xleftarrow{\Delta^T} & R & \longleftarrow & 0
\end{array}$$

Commutativity of the rightmost square now gives $id \cdot \psi^T = \Delta^T \cdot a$, which tells us that $\psi_i = d_i a$ for each $i = 1, \ldots, t+1$. Consequently we can represent our original ideal I by $I = \operatorname{im}(\psi) = \langle \psi_1, \ldots, \psi_{t+1} \rangle = \langle d_1 a, \ldots, d_{t+1} a \rangle = a \langle d_1, \ldots, d_{t+1} \rangle = a I_t(\varphi)$.

Now $I = a I_t(\varphi) \subseteq \langle a \rangle$, but because I has a finite free resolution (as part of the statement of the theorem), then Corollary 5.5 means I must contain an element $r \in R$ which is not a zero divisor.

Here $r \in \langle a \rangle$, so $r = as$ for some $s \in R$, and if a is a zero divisor (say $au = 0$ for some $u \in R$), then $ur = uas = 0$, making r a zero divisor. Since this is clearly not possible, then a cannot be a zero divisor.

This completes the proof of one direction of the Hilbert-Burch theorem, and we now turn to the converse. Suppose we have a $(t+1) \times t$ matrix φ with entries in R such that $\text{depth}(I_t(\varphi)) \geq 2$ and an element $a \in R$ which is not a zero divisor.

It follows that $I_t(\varphi)) \neq 0$ (since it has non-zero depth), so $\text{rank}(\varphi) \geq t$, and since the rank is bounded by the dimensions of the matrix, we find $\text{rank}(\varphi) = t$, so $I(\varphi) = I_t(\varphi)$.

If we now induce the map $a\Delta$ represented by a $1 \times (t+1)$ matrix whose i^{th} element is $d_i a$ (which is based on the determinants of the $t \times t$ submatrices of φ), then we find $I_1(a\Delta) = aI_1(\Delta) \neq 0$ (since $I_1(\Delta) = I_t(\varphi) \neq 0$, and a is not a zero divisor, so will not annihilate the non-zero elements of $I_1(\Delta)$). Thus $\text{rank}(a\Delta) \geq 1$ and hence $\text{rank}(a\Delta) = 1$ (since again the dimensions of the matrix bound the rank).

Notice that $I(a\Delta) = I_1(a\Delta) = aI_1(\Delta) = aI(\varphi)$, so $\text{depth}(I(a\Delta)) = \text{depth}(aI(\varphi)) \geq 1$ (since $I(\varphi) \geq 2$ means there exists an element in $I(\varphi)$ which is not a zero divisor, and multiplying this element by $a \in R$ cannot give a zero divisor).

Using the characterization of free resolutions, we thus find that a free resolution of $R/(aI(\varphi))$ of length 2 is provided by the maps φ and $a\Delta$, and since φ is $(t+1) \times t$ and $a\Delta$ is $1 \times (t+1)$ this resolution must be:

$$0 \longrightarrow R^t \xrightarrow{\varphi} R^{t+1} \xrightarrow{a\Delta} R \longrightarrow R/(aI(\varphi)) \longrightarrow 0$$

which in turn demonstrates that the free resolution of $I = aI(\varphi)$ must be:

$$0 \longrightarrow F \xrightarrow{\varphi} G \longrightarrow I \longrightarrow 0$$

using the isomorphisms of generating sets of F and G with R^t and R^{t+1}.

This completes the proof of the Hilbert-Burch theorem presented by Eisenbud and its converse, as desired. $\square$

Remark 5.9. This proof is somewhat involved - the proof provided (as an exercise) in [KAP74] is regarded as one of the shortest proofs available of this theorem, and is valid even in the non-Noetherian case (according to Buchsbaum & Eisenbud). For our purposes, however, it does not provide nearly as nice an illustration of the role played by depth in the development of the proof, since here most steps involved using the depth to check the characterization of free resolutions. □

5.2 Applications of the Hilbert-Burch Theorem

As has been remarked, Hilbert originally proved the Hilbert-Burch theorem to give an example of a free resolution (though Meyer had conjectured something similar several years earlier) in a very particular case. In the eighty years following his discovery, the theorem would be rediscovered several times - and even published on occasion - before Burch proved it in the more general case we saw here.

The Hilbert-Burch theorem was essentially the first significant result in the study of the structure of finite free resolutions, classifying free resolutions of length 2 that begin with a free module of rank 1. Buchsbaum & Eisenbud generalized it in the paper [BE74] to determine structure theorems for arbitrary free resolutions, and Hochster has since attempted to develop a theory to further generalize this.

From a practical point of view, the Hilbert-Burch theorem has been put to use in a number of settings, several of which we consider below.

The study of Grothendieck's lifting problem

This problem posed by Grothendieck works in the setting of a regular local ring $(R, \mathfrak{m})$ - a local ring is said to be *regular* if the maximal ideal $\mathfrak{m}$ is generated by an R-sequence.

Suppose $x \in \mathfrak{m} \setminus \mathfrak{m}^2$. Let B be a finitely generated $R/\langle x\rangle$-module. Grothendieck's lifting problem is to determine whether there exists an R-module A such that x is not a zero divisor on A and $A/\langle x\rangle A \simeq B$.

(If such a module A exists, it is called a *lifting* of B to R).

The Hilbert-Burch theorem essentially resolves the special case where S is also a local ring and $B = S/I$ for some ideal I of S such that S/I has projective dimension 2, by showing that a lifting does exist in this case. The structure theorems Buchsbaum and Eisenbud developed from the Hilbert-Burch theorem in [BE74] can be used to prove that if S/I has finite projective dimension and I can be generated by 3 (or fewer) elements then a lifting of S/I exists.

Computing invariants of sets of points in $\mathbb{P}^2$

As mentioned, Burch's original purpose in proving her version of the theorem was to try and generalize some known results related to the generators of ideals in projective space. More specifically, the Hilbert-Burch theorem has as a consequence that if a set of points $X \in \mathbb{P}^2$ corresponds to an ideal $I(X)$ with many generators, then the degree of all generators must be quite high. (A classical example is provided on page 503 of Eisenbud).

Determining conditions of factoriality for certain hypersurface rings

There are a number of results on when a ring of the form $R/\langle f \rangle$ is a unique factorization domain (particularly when R is either a regular local ring or a polynomial ring). One such result is a theorem of Andreotti and Salmon (proved in 1957, which obviously predates Burch's work on the Hilbert-Burch theorem).

Theorem 5.10 (Andreotti-Salmon Theorem). *Let* $(R, \mathfrak{m})$ *be a regular local ring of dimension three and* $0 \neq f$ *be an element of* $\mathfrak{m}$*. Then the ring* $R/\langle f \rangle$ *is a unique factorization domain iff* f *cannot be expressed as the determinant of an* $n \times n$ *matrix with entries in* $\mathfrak{m}$ *for* $n > 1$.

This theorem can be proved using the Hilbert-Burch theorem, with the approach provided as Exercise 20.17 on page 516 of [EIS95], and this is quite a nice result to go through.

These are just a few of the many potential applications of the Hilbert-Burch theorem, which is a device that continues to attract attention and study in the present day.

Closing Remarks

Homological algebra is one of the most significant branches of commutative algebra, having played a critical role in the rise of modules as a major area of study. One of the most powerful notions in homological algebra is that of depth, which offers significant scope in many computations.

In particular, we have seen that depth enables us to identify precisely when a finite complex of free modules is exact, classifying finite free resolutions in a manner that leads to a proof of the Hilbert-Burch theorem, as well as its generalizations.

One drawback of working in so rich and diverse a field, however, is that many ideas of considerable merit must be omitted from any discussion. Two such areas that we reluctantly did not discuss in this thesis, for instance, are:

- The theory of *associated primes* - a prime ideal in a ring is associated to a module over that ring if it annihilates some element of the module. The theory of such ideals played a significant role in Burch's proof of the Hilbert-Burch Theorem, and holds the key to formulating a geometric interpretation of depth.
- Development of the *exterior algebra* - this allows the full beauty of the Koszul complex to shine through by removing the need to build it inductively, and can also be used to study the structure theorems of Buchsbaum & Eisenbud.

These of course are just two of an almost limitless set of possibilities for advancing from the material in this thesis, and in writing this thesis it is hoped the reader is both equipped with the tools to start down these paths and given the motivation to do so.

Thank you for reading my thesis.

Chapter 6

Background Material

In this chapter we treat the basics of module theory and some of the fundamental ring theory necessary to progress to the later material. We begin with a quick summary of basic module theory and in particular what it means for a module (or ring) to be Noetherian, and follow this up with some basic definitions that are necessary for the rest of this thesis.

Having done this, then the reader should have virtually all the background material necessary to progress through the thesis, aside from a few odds and ends which we provide as the section entitled 'Miscellany'.

It is expected that the reader will at least have a vague notion regarding much of the content of this chapter, so we are somewhat more prepared to go through the material fairly quickly than we have been in other circumstances.

Useful references for this material include just about any introductory work to commutative algebra and/or algebraic geometry, and include (from the references list here) [AM69], [JAC80], [KAP74] and [LAN02]. [Author's Note: Although not directly used for this thesis, the books 'Undergraduate commutative algebra' and 'Undergraduate algebraic geometry' by Miles Reid are also good for a basic introduction to this material.]

6.1 Noetherian Rings and Modules

The simplest concept of a module is as a vector space over a ring of scalars (rather than a field) - indeed, in this context a module satisfies all axioms of a vector space. For the sake of completeness, we provide some formal definitions related to modules below, though the reader may well have seen these already, so we omit the extended discussions.

Definition 6.1. *Let R be a ring. An abelian group M is an R-**module** (or **module over** R) if there exists a map $\mu : R \times M \to M$ (called the **action of** R **on** M) taking $(r, m) \mapsto rm := \mu(r, m)$ such that*

- *For any $m \in M$ the identity $1 \in R$ acts via $1m = m$.*
- *For any $r, s \in R$ and $m \in M$ then $r(sm) = (rs)m$.*
- *For any $r, s \in R$ and $m \in M$ then $(r + s)m = rm + sm$.*
- *For any $r \in R$ and $m, n \in M$ then $r(m + n) = rm + rn$.*

where we use the standard additive notation for the group operation on M and standard conventions for the ring operations on R (whether addition denotes addition in the the ring or in the module is thus determined by the context).

This definition is of a left R-module, since the action of R on M is on the left. Right R-modules are similarly defined.

Example 6.2. Any ring R is a module over itself, with the action of R on R being multiplication in the ring. □

Remark 6.3. For convenience, we often abuse notation and simply refer to a 'module' without specifying the ring, since there is rarely any risk of confusing the ring being used. □

We have noted that modules are essentially a more general type of vector space, and can also define what amounts to a more general concept of a linear map, which is the module homomorphism.

Definition 6.4. *Let R be a ring and M, N be R-modules. A **homomorphism of** R**-modules** (or R**-module homomorphism**) is a group homomorphism $\varphi : M \to N$ such that $\varphi(rm) = r\varphi(m)$ for all $r \in R, m \in M$.*

Remark 6.5. Note that monomorphisms, epimorphisms and isomorphisms of R-modules (over some ring R), can all be defined in a similar fashion. We will often refer to a homomorphism of R-modules as simply a 'homomorphism', or a 'map', particularly when no ambiguity exists.

Unless explicitly stated otherwise, both these terms refer to an appropriate module homomorphism over the ring R (or whichever ring we are working over). □

Observe that our definition made use of the fact all modules are abelian groups. The ideas of group theory often provide useful definitions for module theory. For example given a module M over a ring R we define an R-submodule of M to be a subgroup of M that is an R-module under the action of R on M, and a quotient R-module as the quotient group of M with the canonical induced action of R.

The major results in group theory - such as the isomorphism theorems - also carry across, and we now state the first isomorphism theorem for modules (for future use):

Theorem 6.6 (First Isomorphism Theorem for Modules). *Given two modules M and N over a ring R and an R-module homomorphism $\varphi : M \to N$, then $ker(\varphi)$ and $im(\varphi)$ are R-submodules of M and N respectively, and $M/ker(\varphi) \simeq im(\varphi)$ as R-modules.*

Proof. Straightforward, so omitted. See for example [AM69] page 19. □

Given a module M over a ring R, we define the R-submodule of M generated by some $m \in M$ as $\langle m \rangle := \{rm \big| r \in R\} = Rm$, which is the smallest submodule of M that contains M (ordering by inclusion). The R-submodule of M generated by any subset of elements of M can be similarly defined.

Of particular interest in considering submodules generated by elements is the case where M has a finite set of generators, corresponding to the case of a finite-dimensional vector space.

Definition 6.7. *A module M over a ring R is **finitely generated** if there exists a finite subset $\{m_1, \ldots, m_n\}$ of M such that $\langle m_1, \ldots, m_n \rangle = M$, i.e. any element $m \in M$ can be written in the form $\sum_{i=1}^{n} r_i m_i$ for some $r_1, r_2, \ldots, r_n \in R$. (Some books write this $M = Rm_1 + \cdots + Rm_n$).*

Remark 6.8. The reader should bear in mind that unlike in a vector space, the number of generators in any minimal generating set of elements for a module (that is, a set which generates the module but contains no proper subset generating the module) is not constant. For example, the $\mathbb{Z}$-module $\mathbb{Z}$ is finitely generated by either of the minimal generating sets $\{1\}$ and $\{2, 3\}$. □

For this thesis, we assume all modules are finitely generated.

In the 1920s Emmy Noether demonstrated that many significant steps could be made in the theory of rings and modules by the imposition of a single condition on these modules, called the ascending chain condition.

Definition 6.9 (Ascending Chain Condition). *Let R be a ring and M an R-module. M satisfies the **Ascending Chain Condition (a.c.c)** if any increasing sequence of R-submodules $M_1 \subseteq M_2 \subseteq \ldots$ of M (ordered by inclusion) becomes stationary after a finite number of steps (i.e. there exists some $n \geq 1$ such that $M_j = M_n$ for all $j \geq n$).*

In honour of Noether's work, the term Noetherian was introduced for such rings and modules.

Definition 6.10 (Noetherian). *Let R be a ring and M an R-module. M is **Noetherian** if either fo the following equivalent conditions hold:*

- *M satisfies the ascending chain condition.*
- *Every R-submodule of M is finitely generated.*

It is the equivalence of the ascending chain condition with finite generation of every submodule of M in the above definition that makes it so important. A special case of this is when $M = R$, in which case the R-submodules are the ideals in R.

Some obvious examples of Noetherian rings include fields, and principal ideal domains. These can be used to build up less trivial examples of Noetherian rings.

Example 6.11. [Hilbert Basis Theorem] If R is any Noetherian ring, then the polynomial ring $R[x]$ is Noetherian.

By induction the polynomial ring $R[x_1, \ldots, x_n]$ with n indeterminates is Noetherian. □

The case of a polynomial ring can be used to demonstrate that non-Noetherian rings exist.

Example 6.12. The polynomial ring $R = \mathbb{K}[x_1, \ldots]$ with an infinite number of indeterminates is not Noetherian, as the ideal $\langle x_1, \ldots, \rangle$ generated by the indeterminates is not finitely generated. (R itself, however, is finitely generated by 1). □

Thus we see that the ascending chain condition strengthens the notion of finite generation of a module. There is also a theory obtained from imposing a *descending chain condition* on the ring/module, and such rings/modules are called Artinian.

It turns out that any Artinian ring is Noetherian, but that the converse is not true, so in general one studies Noetherian rings as a matter of course.

For this thesis, we assume all rings are Noetherian.

(We may often state this result, despite the redundancy, simply to reinforce the point).

We have now assumed all rings are Noetherian and all modules finitely generated. In fact, over a Noetherian ring any finitely generated module is Noetherian, so our assumptions are essentially that all rings and modules are Noetherian.

In order to prove this, however we first need to know that modules derived from Noetherian modules (i.e. submodules and quotient modules) are Noetherian.

Proposition 6.13. *If M is a Noetherian module M over a ring R, then all submodules and quotient modules of M are Noetherian.*

Proof. (This is an example of our abusing the notation - clearly all modules are over R).

Any R-submodule of an R-submodule of M is also an R-submodule of M, so must be finitely generated, which by the second condition of Definition 6.10 proves that any submodule of M is Noetherian.

The submodules of any quotient module of M are in one-to-one correspondence with the submodules of M (linked by the canonical quotient homomorphism), so any ascending chain of submodules of the quotient can be 'pulled back' to an ascending chain of submodules of M. Since M is Noetherian, this chain must become stationary (by the a.c.c), and applying the quotient homomorphism to return to the quotient module, we find that the original chain becomes stationary. Hence any quotient of a Noetherian module satisfies the a.c.c, so is Noetherian. □

Having proven this, we outline the proof that finitely generated modules over a Noetherian ring are Noetherian.

Proposition 6.14. *If R is a Noetherian ring, then the Noetherian R-modules are precisely the finitely generated R-modules.*

Proof. (Sketch - see [LAN02] or [AM69] for a full proof)

Any Noetherian module is finitely generated (being a submodule of itself), and any finitely generated module is a quotient (by some relations) of a finite direct sum of copies of R. Now any finite direct sum of Noetherian modules is Noetherian (proof omitted here), so the finite direct sum of copies of R is Noetherian and hence the quotient is Noetherian by Proposition 6.13, completing the proof. □

6.2 Modules

In the chapters to follow[1], some special modules assume great importance, namely free, projective and injective modules. In this section we define these modules, and also look at the basic properties of Hom and of the tensor product $\otimes$, both of which will be significant in what follows.

We begin by defining free modules.

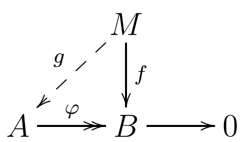
Definition 6.15 (Free Modules). *Let R be a ring and M an R-module. M is a **free module** over R if M is a direct sum of copies of R.*

This direct sum may be finite, in which case $M \simeq R^n$ for some $n \in \mathbb{N}$ or infinite, in which case any element of M may be represented by a sequence of elements of R, only finitely many of which are non-zero.

We next define the projective modules, which in a sense generalize free modules.

Definition 6.16 (Projective Modules). *Let R be a ring and M an R-module. M is a **projective module** if given any R-modules A, B together with a surjective homomorphism $\varphi : A \to B$ and a homomorphism $f : M \to B$ then there exists a homomorphism $g : M \to A$ such that $\varphi \circ g = f$.*

Remark 6.17. [Commutative Diagrams] This can also be defined using a commutative diagram, which we introduce in this remark for the benefit of readers not familiar with the notion.



A diagram of modules connected by module homomorphisms (such as the one above) is said to be *commutative* if composing the homomorphisms along any path from one module to another in the diagram will always give the same result.

[1]Author's Note: Having recommended this chapter be the first read, I will assume that this is indeed the case!

For example, in the diagram here we can go from M to B either directly or indirectly (via A), and the diagram commutes since $\varphi \circ g : M \to A \to B$ will always give the same result as $f : M \to B$.

(The role of the 0 is actually a consequence we will develop in Chapter 1).

□

Remark 6.18. Projective modules generalize free modules in the sense that any projective module is a direct summand of a free module. Thus any free module is projective, though in general the converse is false (for example $\mathbb{Z}/2\mathbb{Z}$ is a module of $\mathbb{Z}/6\mathbb{Z}$, but the direct sum decomposition of $\mathbb{Z}/6\mathbb{Z}$ is $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$).

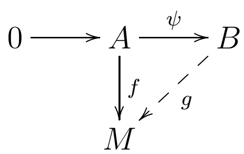
In some special cases, however, all projective modules are free, and in particular:

- Any projective module over a local ring (to be defined in Section 6.3) is free over that ring - this was proved by Irving Kaplansky in 1957.
- Any projective module over a polynomial ring (over a field) is free - this was conjectured by Serre in 1957 and independently proved by Quillen and Suslin in 1976. It is now known as the *Quillen-Suslin Theorem.*

□

Dual to the concept of a projective module is that of an injective module.

Definition 6.19. *Let R be a ring and M an R-module. M is an* ***injective module*** *if given any R-modules A, B together with an injective homomorphism $\psi : A \to B$ and a homomorphism $f : A \to M$ then there exists a homomorphism $g : B \to M$ such that $g \circ \psi = f$. Alternately, g makes the following diagram commute:*



Remark 6.20. We will see that some of the properties of projective and injective modules are also dual when we meet them again in Chapter 2. For example, any (finitely generated) module can be expressed as the image of a module homomorphism from a projective module, and any module can be embedded into an injective module. □

Having defined these modules, we now leave their actual use until 2, and turn to two functors (to be defined in Section 1.1) which are critical to the study of modules in homological algebra. The first of these is Hom.

Definition 6.21 (Hom). *Let R be a ring and M, N be two R-modules. The set of all R-module homomorphisms from $M \to N$ is denoted $Hom_R(M, N)$.*

Remark 6.22. $\mathrm{Hom}_R(M, N)$ is itself an R-module, with the action of $r \in R$ on $f \in \mathrm{Hom}_R(M, N)$ taking it to $rf \in \mathrm{Hom}_R(M, N)$, where rf is defined by $(rf)(m) = r(f(m)) = f(rm)$ for each $m \in M$. □

Example 6.23. Let R be a ring and M an R-module. Then $\mathrm{Hom}_R(R, M) \simeq M$, via the canonical isomorphism $f \leftrightarrow f(1)$.

This is because given $m \in M$, we can define $f : R \to M$ by $f(r) = rm$, and conversely, given any $f \in \mathrm{Hom}_R(R, M)$ we can define $m = f(1) \in M$. It is easy to verify that this is a valid isomorphism, so we omit the details. □

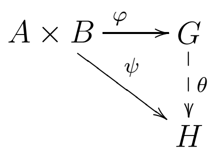
Remark 6.24. Let R be a ring and M, N be finitely generated free R-modules (with $M \simeq R^p$ and $N \simeq R^q$). Then any module homomorphism $\varphi : M \to N$ can be expressed as multiplication by a $q \times p$ matrix with elements in R. In such a situation, then we will often abuse terminology and simply refer to both the matrix and the homomorphism as φ. Although poor nomenclature, this is more convenient than repeatedly interchanging between the two! □

The other device of great importance is the tensor product $\otimes$ of two R-modules. This can be defined in either of two ways, and we take our cue from the approach used in [JAC80] and [OSB00].

Definition 6.25 (Tensor product). *Let R be a ring and M, N be two R-modules. A* bilinear map *from $M \times N$ to an abelian group G is a map $\varphi : M \times N \to G$ such that for any $m, m' \in M$, $n, n' \in N$ and $r \in R$ we have:*

- $\varphi(m, n + n') = \varphi(m, n) + \varphi(m, n')$
- $\varphi(m + m', n) = \varphi(m, n) + \varphi(m', n)$
- $\varphi(rm, n) = \varphi(m, rn)$

A pair (G, φ) of this form is called a balanced product*, and is called a* ***tensor product*** *of M and N if for any other balanced product (H, ψ) of M and N there is a unique group homomorphism $\theta : G \to H$ such that the following diagram commutes:*



(Note that although the standard definition of a tensor product is in terms of a right R-module with a left R-module, we are assuming commutativity in the sense that we can forcibly impose the action of R on a left R-module on any right R-module as well. This saves us effort with our definitions).

Remark 6.26. [About tensor products] Although tensor products when defined in this way are not guaranteed to exist, there is a means of constructing a tensor product of M and N that both demonstrates tensor products exist and enables us to talk about 'the' tensor product of M and N.

This construction takes place by constructing the free abelian group F with basis $\{(m, n) : m \in M, n \in N\}$ and taking the quotient of F by the subgroup generated by all elements of the form $(m + m', n) - (m, n) - (m', n)$, $(m, n + n') - (m, n) - (m, n')$ and $(rm, n) - (m, rn)$ for any $m, m' \in M$, $n, n' \in N$ and $r \in R$.

The quotient group is denoted $M \otimes_R N$ and the coset of an element (m, n) of $M \times N$ in this quotient group is denoted $m \otimes n$ (we drop the subscript for simplicity). The tensor product is then the balanced product $(M \otimes_R N, \varphi)$ where $\varphi(m,n) = m \otimes n$. We usually abuse notation and just call $M \otimes_R N$ the tensor product.

The condition in our definition that made a balanced product a tensor product is called the universal property of tensor products, and can be used to show that:

- $M \otimes_R N \simeq N \otimes_R M$ for any R-modules M, N.
- $M \otimes_R R \simeq M$ for any R-module M (via the isomorphism $m \otimes r \leftrightarrow rm$)
- The tensor product $\otimes$ commutes with finite direct sums.

□

Having developed some of the more important ideas related to module theory, we are essentially done with the preliminaries, so will simply collate a few more miscellaneous results together to complete the preparations.

6.3 Miscellany

We deliberately aim to keep this section sparse, since the level of assumed ring theory for this thesis should be sufficient for the reader to go through the vast majority of the material unimpeded. Hence we merely provide a few definitions that the reader may not have seen before - the two actual results are given without proof, since in the first case the proof is virtually trivial and in the second case (the NAK Lemma) it is worthwhile reading a full development of the theory to comprehend the proof.

The book by [AM69] is recommended as a resource for the reader who is genuinely uncomfortable with this notion and wishes to develop their commutative algebra further (which is certainly not a bad thing by any means!)

The first definition we introduce will be that of a local ring.

Definition 6.27. *A* ***local ring*** *is a ring R for which there is only one maximal ideal, denoted $\mathfrak{m}$. Frequently we simply write $(R, \mathfrak{m})$ to introduce the local ring and its maximal ideal at the same time.*

Example 6.28. If $\mathbb{K}$ is a field, then the power series ring $\mathbb{K}[[x_1, \ldots, x_n]]$ over some number of indeterminates is a local ring, with the maximal ideal being the ideal generated by the indeterminates. □

We next introduce the definition of the Krull dimension of a ring and/or an ideal, which can be used to measure the size of an ideal.

Definition 6.29. *The* ***Krull dimension of a ring*** *R (denoted dim(R)) is the supremum of the lengths of chains of prime ideals in R (where the length of a chain is the number of proper inclusions in it, so for example the chain $P_0 \subset P_1 \subset \cdots \subset P_n$ has length n).*

The ***Krull dimension of an ideal*** *I in R (denoted dim(I)) is equal to dim(R/I), and is the supremum of the lengths of chains of prime ideals in R which contain I.*

Some special types of rings are particularly easy to characterise in this fashion.

Example 6.30. Any principal ideal domain R has dimension at most 1.

To see this, let (p_0) and (p_1) be two prime ideals in R with $(p_0) \subset (p_1)$. Since (p_0) is prime $p_0 = ab$ means either $p_0 \big| a$ (making b a unit) or $p_0 \big| b$ (making a a unit). Here, $p_0 \in (p_1)$ so $p_0 = p_1 r$ for some $r \in R$. Since (p_1) is prime, p_1 is not a unit (else $(p_1) = R$ cannot be prime), which means $p_0 \big| p_1$, i.e. $(p_1) \subseteq (p_0)$ as well. Thus the longest chain of proper inclusions of prime ideals is $(0) \subseteq (p_0)$. □

We make brief mention of a minimal prime ideal at one stage, so will introduce the definition here:

Definition 6.31. *A prime ideal P in a ring R is a* ***minimal prime ideal*** *of R if P does not properly contain any prime ideal of R.*

This definition is actually only provided to let us use the following proposition:

Proposition 6.32. *If P is a minimal prime ideal of a ring R, and $x_1 \in R$ is not a zero divisor, then $x_1 \notin P$.*

Finally, we provide a statement of the famous NAK Lemma (more commonly known as Nakayama's Lemma). The proof may be found in any introductory textbook on commutative algebra, and more to the point, it is *particularly* worthwhile the reader who is not aware of the proof picking up such a textbook (e.g. [AM69]), so we omit it here!

Theorem 6.33. *Let M be a finitely generated module over a ring R and I be an ideal contained in the Jacobson radical of R (that is, I is contained in every maximal ideal of R). Then $IM = M$ iff $M = 0$.*

References

[AB57] Auslander, M., Buchsbaum, D.A., Homological Dimension in Local Rings, *Transactions of the American Mathematical Society*, **Vol. 85**(2) (1957) 390–405.

[AM69] Atiyah, M.F., Macdonald, I.G., *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, Inc. : Reading, Massachusetts, 1969.

[BE74] Buchsbaum, D.A., Eisenbud, D., Some structure theorems for finite free resolutions, *Advances in Mathematics* **12**(1) (1974), 84–139.

[BE77] [2]Buchsbaum, D.A., Eisenbud, D., Algebra Structures for Finite Free Resolutions, and Some Structure Theorems for Ideals of Codimension 3, *American Journal of Mathematics* **99**(3) (1977), 447–485.

[BH93] Bruns, W., Herzog, J., *Cohen-Macaulay Rings*, Cambridge Studies in Advanced Mathematics no. 39, Cambridge University Press : Cambridge, 1993.

[BUR56] Burch, L. On ideals of finite homological dimension in local rings, *Proceedings of the Cambridge Philosophical Society*, **Vol. 64**(4) (1968) 941–948.

[CE56] Cartan, H., Eilenberg, S., *Homological Algebra*, Princeton University Press : Princeton, New Jersey, 1956.

[CC05] Chan, D., Homology and Homological Algebra, *Notes typeset by Kenneth Chan* (2005). http://www.maths.unsw.edu.au/ danielch/homology05b/halec.pdf

[EIS95] Eisenbud, D., *Commutative Algebra with a view toward Algebraic Geometry*, Graduate Texts in Mathematics no. 150, Springer-Verlag: New York, 1995.

[2]Although I did not end up using this paper as an actual reference, for a large part of the year it served as a motivating guide on my path of study, and so I include it.

[EIS00] Eisenbud, D., *The Geometry of Syzygies*, Graduate Texts in Mathematics no. 292, Springer: New York, 2000.

[HOC75] Hochster, M., *Topics in the homological theory of modules over commutative rings* (Expository lectures from the CBMS Regional Conference held at the University of Nebraska, Lincoln, Neb., June 24–28, 1974; Conference Board of the Mathematical Sciences Regional Conference Series in Mathematics, No. 24), Published for the Conference Board of the Mathematical Sciences by the American Mathematical Society, Providence, R.I., 1975.

[JAC80] Jacobson, N., *Basic Algebra II*, W.H. Freeman and Company, 1980.

[KAP59] Kaplansky, I., *Homological Dimension of Rings and Modules*, (Published as a Technical Report under the auspices of the US Army's Office of Ordnance in 1959, by the University of Chicago.)

[KAP74] Kaplansky, I., *Commutative Rings*, The University of Chicago Press: Chicago, 1974.

[LAD96] Lady, E.L., Notes from a course on Homological Algebra (May, 1996). URL is http://www.math.hawaii.edu/ lee/homolog/index.html

[LAN02] Lang, S., *Algebra (Revised* 3^{rd} *edition*, Graduate Texts in Mathematics no. 211, Springer: New York, 2002.

[NOR76] Northcott, D.G., *Finite Free Resolutions* Cambridge Tracts in Mathematics no. 71, Cambridge University Press: Cambridge, 1976.

[OSB00] Osborne, M.S., *Basic Homological Algebra*, Graduate Texts in Mathematics no. 196, Springer-Verlag: New York, 2000.

[REE56] Rees, D., A theorem of homological algebra, *Proceedings of the Cambridge Philosophical Society*, **Vol. 52**(4) (1956) 605–610.

[REE57] Rees, D., The grade of an ideal or module, *Proceedings of the Cambridge Philosophical Society*, **Vol. 53**(1) (1957) 28–42.

[SIM01] Simon, J., *The Formula of Auslander and Buchsbaum*, Lecture given at the 2001 Summer School : 'Homological conjectures for finite dimensional algebras' (held in Nordfjordeid, Norway). URL is http://www.math.ntnu.edu/ oyvinso/Nordfjordeid/Transparencies/simontalk.ps

[WEI–] Weibel, C.A., *History of Homological Algebra*, Web Article (first accessed on 24/5/2005 and available as of 2/11/2005 – Year of creation not specified). URL is http://math.rutgers.edu/ weibel/history.dvi

[ZS60] Zariski, O., Samuel, P. *Commutative Algebra (Vol. II)*, Graduate Texts in Mathematics no. 29, Springer-Verlag: New York, 1960