An Introduction to Homological Algebra, with a View Towards the Syzygy Theorem

Anton Farmar, supervised by Dr Simon Crawford

Submitted 22nd of May 2022

Abstract

In an 1890 paper, David Hilbert proved the syzygy theorem alongside his two other fundamental theorems of polynomial rings: his Basissatz and Nullstellensatz. The approach Hilbert took has since been generalised as part of the field of homological algebra, which places the syzygy and related theorems in a wider context. In this project, we cover the results necessary to state and prove the syzygy theorem in its modern form.

Contents

1 Introduction

1.1 Background

When attempting to describe a module M over some ring R, it is a natural impulse to present it in terms of generators and relations between those generators. Seeing these relations as particular members of a free R-module, in turn we may wish to describe this submodule of relations – also known as **syzygies**, after the astronomical term referring to the alignment of celestial objects – in turn as a set of generators and relations.

In the world of group theory, where any subgroup of a free group is also free, we would have a complete description of a group in one step, since there are no syzygies of the generators of a free group – indeed for Abelian groups this also holds. However modules over a general ring R may be considerably more wild, and there is no reason to believe that this process of taking syzygies will terminate after any given number of steps. The process of taking successive generators and syzygies produces a **free resolution** for a module.

In the late 19th century, David Hilbert studied this situation for polynomial rings over fields in a seminal paper [Hil90] which laid the first stones of commutative algebra. Two theorems he proved in this paper are staples of the undergraduate algebra curriculum: the basis theorem, and the Nullstellensatz. Another theorem, now known as **Hilbert's Syzygy Theorem**, characterises the behaviour of free resolutions of modules over a polynomial ring.

At the time Hilbert was investigating polynomial invariants of such modules – now known as Hilbert polynomials – which are comparable to the Betti numbers of algebraic topology. Realising that these invariants could be calculated in the presence of a free resolution of finite length, Hilbert was motivated to demonstrate that finite resolutions always existed. He proved the following:

Theorem (Hilbert's Syzygy Theorem)**.** *Every ideal of the ring* $\Bbbk[x_1, \ldots, x_n]$ *over a field* $\Bbbk$ *has a free resolution of length at most* n*.*

Efforts to generalise the syzygy theorem and related results have lead to the development of homological algebra: a field of study which places Hilbert's work inside a much wider context. For example, the syzygy theorem has been generalised enormously, now stating a result that works for all polynomial rings rather than only those over a field. The more natural context of **projective** and **injective** modules, rather than free modules, not only leads to a theory that generalises to objects other than rings, but also provides slick category-theoretic results involving dual arguments. The presence of **derived functors** such as Ext provides us a sharp computational tool to explore homological properties in a stunningly direct way.

Remarkably the thrust of these techniques comes from a topological root, rather than a strictly algebraic one. Homology first appeared in an attempt to distinguish topological spaces by measuring the number of 'holes' they have. Noether was the first to observe that homology can be interpreted via Abelian groups, which was the start of the incorporation of algebra into homology, although the book entitled 'Homological Algebra', by Cartan and Eilenberg [CE56], is the source of the majority of the concepts introduced in this project.

The strength of these homological arguments is apparent not only in its striking results, but also its top-down perspective on ring theory, not to mention its remarkable computational tractability. The author hopes readers will appreciate the insight provided by the homological algebra presented in this project.

1.2 Structure

The author aims to introduce the homological perspective at an undergraduate level, with the principal goal of proving Hilbert's syzygy theorem in its more modern and general form.

Throughout the project we use results that are well-known in the literature and can be found in any book on homological algebra worth its salt. One such book by Rotman [Rot09] is followed closely, and some additional proofs come from Kaplansky [Kap72] and Nastacescu–van Oystaeyen [NvO87]. This paper attempts to find within these dense sources the skeleton that supports the syzygy theorem, and inserts useful original examples to support it.

Section 2 covers some prerequisite understanding of category theory that readers ought to be comfortable with. The author has endeavoured not to rely on too much categorical arcana, and hopes that the reader will not be overwhelmed by new definitions.

Section 3 introduces various foundational results involving Hom groups, and in particular the tensor product of modules, and the strong relationship that Hom and tensor have – the adjunction.

Section 4 discusses a core concept of homological algebra, namely that of an exact sequence. It also introduces the partial exactness of the Hom and tensor functors previously discussed, alongside a handful of convenient results.

Section 5 defines several fundamental kinds of modules, namely projective, injective, and flat modules. We also demonstrate that these modules are what allow Hom and tensor to preserve exact sequences entirely, rather than only partially. The results here provide the principal objects we use to build our homological machinery.

Section 6 introduces the general construction of homology groups in the general case, and makes note of the important concept of an Abelian category which has become standard in the field of homological algebra. Although its name may make it sound like the culmination of this paper, in fact this section provides the last tool we require in order to tackle the theory surrounding the syzygy theorem.

Section 7 constructs the derived functor Ext, and demonstrates some of its capabilities as a tool in module theory. Although this section does not define derived functors in general, it introduces Ext in a way that would allow an interested reader to observe the more general pattern.

Section 8 reaches the apex by introducing homological dimensions of modules and rings, and finally proving Hilbert's Syzygy Theorem.

Section 9 concludes the project by reflecting upon the previous material, and looking further into the depths of homological algebra that this project might have explored if time were more permissive.

In order to avoid cluttering the relevant chapters, Appendix A contains a few long calculations which provide examples of interesting objects.

2 Prerequisite Category Theory

Much of what we will explore will involve various category-theoretic ideas at a basic level. For this purpose, we briefly define the concepts required in a way that we hope will not obstruct the way to the more interesting results.

Definition 2.1. A **category** $\mathcal{C}$ consists of:
(1) A collection of **objects**,
(2) A collection of **morphisms** $\mathrm{Hom}(A, B)$ for any objects $A, B \in \mathcal{C}$,
for which the following stipulations hold:
(a) For any morphisms $f \in \mathrm{Hom}(A, B)$ and $g \in \mathrm{Hom}(B, C)$ there is a morphism $g \circ f \in \mathrm{Hom}(A, C)$,
(b) For appropriate[1]morphisms f, g, and h, we have $f \circ (g \circ h) = (f \circ g) \circ h$,
(c) For any object A, there is a morphism $1_A \in \mathrm{Hom}(A, A)$ such that $f \circ 1_A = f$ and $1_A \circ g = g$ for any appropriate morphisms f and g.

In the above definition, we used the weasel word 'collection' in order to sidestep set-theoretic worries. There is no particular reason that the objects of a category should form a set, or even that $\mathrm{Hom}(A, B)$ should form a set. That being said, the categories that we will consider in this project will have this property, whereas the collection of their objects will almost always form a proper class.

Remark. Categories with additional restrictions on the size of their collection of objects or morphisms are frequently studied. A category whose collections of objects and morphisms are sets is known as a **small category**, and a category for which only $\mathrm{Hom}(A, B)$ is a set for all objects A, B is known as **locally small**. Some authors use the term category to refer to locally small categories, but this definition is quite restrictive.

Lemma 2.2. *For any object A of a category $\mathcal{A}$, the identity morphism 1_A is unique with the property that $f \circ 1_A = f$ and $1_A \circ g$ for all appropriate morphisms f and g.*

Proof. Suppose $f \in \mathrm{Hom}(A, A)$ is another possible identity morphism. Then $1_A = f \circ 1_A = f$, so we are done. ☐

Examples 2.3. A category can be thought of as a context for studying a collection of interesting or important objects, and there are many examples of this kind:
- The category **Set**, whose objects are all sets, whose morphisms are functions between sets, and whose composition is function composition.
- The category **Top**, whose objects are topological spaces, whose morphisms are continuous maps, and whose composition is function composition.
- The categories ${}_R\mathbf{Mod}$ and $\mathbf{Mod}_R$ for some ring R, whose objects are left and right R-modules respectively, whose morphisms are R-maps, and whose composition is function composition.

Example 2.4. All of the above examples consist of sets and functions between them, but this need not be the case. For example, if we have a poset A we may construct a category $\mathcal{A}$ whose structure reflects the poset as follows:
- Let the objects of $\mathcal{A}$ be elements of A.
- Let $\mathrm{Hom}(a, b) = \{1\}$ if $a \leq b$, and $\emptyset$ otherwise. The choice of element – here 1 – is irrelevant as anything will do.
- The composition law is then necessarily defined by $1 \circ 1 = 1$.

This is a category, since $1_a = 1$ is the identity map, composition is associative, and composites exist due to the transitivity of the poset's order relation.

[1] By 'appropriate,' we mean that, in particular, $h \in \mathrm{Hom}(A, B)$, $g \in \mathrm{Hom}(B, C)$, and $f \in \mathrm{Hom}(C, D)$ for some objects A, B, C, D – this is to say that the composition exists since the 'target' of the previous morphism aligns with the 'source' of the next.

We now introduce a useful tool in describing properties of certain collections of objects and maps within a category.

Definition 2.5. A **commutative diagram** is a collection of objects and morphisms between those objects in a category such that the composition of all morphisms in a path between two objects is equal to the composition of all morphism in any other path with the same endpoints.

Of course, a diagram need not commute in general – we will refer to such things simply as 'diagrams' and point out when they do commute.

This definition is long-winded and much better shown through example, though there are much more sophisticated definitions in the literature. The simplest kind of commutative diagram simply describes equality of two morphisms f and g, as in the following:

$$\begin{tikzcd} A \arrow[r, bend left, "f"] \arrow[r, bend right, "g"'] & B \end{tikzcd}$$

We may observe in the above diagram that there are two paths from A to B – namely f and g – and if the diagram is commutative then this means that $f = g$.

Note that we can easily describe what it means for two morphisms to commute via a commutative diagram:

$$\begin{array}{ccc} A & \xrightarrow{f} & A \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{f} & A \end{array}$$

The above diagram is commutative if and only if $f \circ g = g \circ f$.

Similarly to how categories might generally be thought of as objects and maps between them, we would like to consider maps between categories.

Definition 2.6. A (covariant) **functor** $F\colon \mathcal{A} \to \mathcal{B}$ from a category $\mathcal{A}$ to a category $\mathcal{B}$ consists of:

(1) For every object A of $\mathcal{A}$, there is an object $F(A)$ of $\mathcal{B}$,
(2) For every morphism $g \in \mathrm{Hom}(A, A')$ in $\mathcal{A}$, there is a morphism $F(g)$ belonging to $\mathrm{Hom}(F(A), F(A'))$ in $\mathcal{B}$.

Furthermore the additional restrictions must be satisfied:

(a) For appropriate morphisms f, g within $\mathcal{A}$, we have $F(f \circ g) = F(f) \circ F(g)$,
(b) For any object A of $\mathcal{A}$, $F(1_A) = 1_{F(B)}$.

The above definition may again be quite wordy, but it can be summarised as saying that functors are maps that respect the structure of categories. We will soon see an example that shows it is a natural definition.

Remark. It might be tempting to define a category of categories, whose objects are categories and whose morphisms are functors. However this runs into an uncomfortable situation in which it is a member of its own collection of objects, which we are wont to avoid. Typically, authors restrict their attention on small categories to avoid a self-referential paradox – indeed there is a category of small categories.

Definition 2.7. Within a category $\mathcal{A}$, a morphism $f \in \mathrm{Hom}(A, B)$ is an **isomorphism** if there exists a morphism $g \in \mathrm{Hom}(B, A)$ with $g \circ f = 1_A$ and $f \circ g = 1_B$.

Definition 2.8. Two objects in a category are **isomorphic** if there exists an isomorphism between them.

Proposition 2.9. *Being isomorphic is an equivalence relation.*

Proof. It is clear that the identity map is an isomorphism, and since there is a two-sided inverse to any isomorphism, the relation is both reflexive and symmetric. Similarly if $f \in \mathrm{Hom}(A, B)$ and $g \in \mathrm{Hom}(B, C)$ are isomorphism with inverses f' and g' respectively, then:

$$(g \circ f) \circ (f' \circ g') = g \circ (f \circ f') \circ g' = g \circ 1_B \circ g' = g \circ g' = 1_C$$

and similarly $(f' \circ g') \circ (g \circ f) = 1_A$, so the relation is transitive. □

Remark. We could define isomorphisms using a commutative diagram. A morphism f is an isomorphism if there exists a morphism g such that the following diagram commutes (we use a dashed arrow for existentially hypothesised morphisms):

$$\begin{tikzcd} A \arrow[loop left, "1_A"] \arrow[r, bend left, "f"] & B \arrow[l, bend left, dashed, "g"] \arrow[loop right, "1_B"] \end{tikzcd}$$

Examples 2.10. Isomorphisms have well-established meanings within the categories we have seen previously:

- In **Set**, isomorphisms are bijections and two sets are isomorphic if and only if their cardinalities are equal.
- In ${}_R\mathbf{Mod}$ and $\mathbf{Mod}_R$, the meaning of category-theoretic isomorphisms are the same as in the usual algebraic definition.
- In **Top**, a continuous map is an isomorphism if and only if it is a homeomorphism, and two spaces are isomorphic if and only if they are homeomorphic.
- If A is a poset and $\mathcal{A}$ is the category defined in Example 2.4, then two objects are isomorphic if and only if they are equal.

Proposition 2.11. *If $F : \mathcal{A} \to \mathcal{B}$ is a functor, and $A, B \in \mathcal{A}$ are isomorphic, then $F(A)$ and $F(B)$ are isomorphic in $\mathcal{B}$.*

Proof. Let f be an isomorphism from A to B, with inverse f' Then:

$$F(f) \circ F(f') = F(f \circ f') = F(1_B) = 1_{F(B)},$$

and similarly $F(f') \circ F(f) = 1_{F(A)}$, so we are done. □

Example 2.12. We may define a group as a one-object category wherein every morphism is an isomorphism. This works since, if A is the unique object, we may identify the elements of the group as $\mathrm{Hom}(A, A)$, where the operation is composition. The identity of the group is then 1_A, and since every morphism has an inverse (they are all isomorphisms) this is indeed a group. Furthermore, if we have two such categories, it is easy to see that a functor between them is exactly a homomorphism of groups – it simply respects the group operation.

There are more distinguished kinds of morphisms in categories that we would like to bring to the reader's attention.

Definitions 2.13. A **monomorphism** or **monic morphism** is a morphism f belonging to $\mathrm{Hom}(A, B)$ that is left cancellable – that is, for morphisms $p, q \in \mathrm{Hom}(X, A)$, if we have $f \circ p = f \circ q$, then $p = q$.

Similarly, an **epimorphism** or **epic morphism** is a morphism $f \in \mathrm{Hom}(A, B)$ that is right cancellable – for $s, t \in \mathrm{Hom}(B, Y)$, if $s \circ f = t \circ f$, then $s = t$.

Example 2.14. In many situations, we may think of monomorphisms as being injections, and epimorphisms as being surjections, as this is true in **Set** for example. However whilst this is a useful intuition, it is not always totally correct. For example, we will consider the category **Ring** of unital rings and ring homomorphisms, wherein we claim that the inclusion map $\iota : \mathbb{Z} \to \mathbb{Q}$ is an epimorphism despite not being surjective.

We prove this claim now. Supposing that $f, g\colon \mathbb{Q} \to R$ for some ring R agree on the integers, then since $f(1) = g(1) = 1$, we have that $f(m)$ is a unit since $1 = f(m)f(1/m)$ and so $f(1/m) = f(m)^{-1}$ for all $0 \neq m \in \mathbb{Z}$, and similarly for g. Hence $f(1/m) = g(1/m)$, and since homomorphisms respect multiplication, $f(n/m) = g(n/m)$ for all $n/m \in \mathbb{Q}$. Hence $f = g$ – so the inclusion is an epimorphism despite not being surjective.

Another useful notion is that of a natural transformation, which broadly may be thought of as a homotopy-like relationship between two functors.

Definition 2.15. Given two functors F, G from $\mathcal{A}$ to $\mathcal{B}$, a **natural transformation** η from F to G consists of a map $\eta_A \in \mathrm{Hom}(F(A), G(A))$ corresponding to each object $A \in \mathcal{A}$, such that the following diagram commutes for all objects $A, B \in \mathcal{A}$ and maps $f \in \mathrm{Hom}(A, B)$:

$$\begin{tikzcd} F(A) \arrow[r, "\eta_A"] \arrow[d, "F(f)"] & G(A) \arrow[d, "G(f)"] \\ F(B) \arrow[r, "\eta_B"] & G(B) \end{tikzcd}$$

A **natural isomorphism** is a natural transformation between two functors where η_A is an isomorphism for every object A. We call two functors **naturally isomorphic** if there is a natural isomorphism between them.

Example 2.16. The category **Grp** of groups and group homomorphisms has a functor on it known as the opposite group, sending a group $(G, *)$ to its opposite $(G^{\mathrm{op}}, *^{\mathrm{op}})$, where $G^{\mathrm{op}} = G$ and $a *^{\mathrm{op}} b = b * a$. It turns out that this functor is naturally isomorphic to the identity functor (the functor that leaves a group unchanged) via the natural transformation defined by $\eta_G(g) = g^{-1}$.

From this point onwards, we assume that the reader is familiar enough with the concept of morphisms, functors, and natural transformations, so we will write $f\colon A \to B$ to denote a morphism $f \in \mathrm{Hom}(A, B)$, as well as $F\colon \mathcal{A} \to \mathcal{B}$ for a functor, and $\eta\colon F \to G$ for a natural transformation.

A lot of the explanatory power of category theory comes from the ability to pick out instances of the same fundamental concept within different categories. One example is the concept of the product. This idea comes up naturally in group theory and topology – to name just two examples – and the category-theoretic perspective elucidates their common thread.

Definition 2.17. Let A, B be objects in some category $\mathcal{A}$. A **product** of A and B is an object $A \sqcap B$ equipped with morphisms $\pi_A\colon A \sqcap B \to A$, $\pi_B\colon A \sqcap B \to B$, such that for any object C and morphism $f_A\colon C \to A$ and $f_B\colon C \to B$, there is a *unique* morphism $f\colon C \to A \sqcap B$ such that the following diagram commutes:

$$\begin{tikzcd} & C \arrow[dl, "f_A"'] \arrow[d, dashed, "f"] \arrow[dr, "f_B"] & \\ A & A \sqcap B \arrow[l, "\pi_A"] \arrow[r, "\pi_B"'] & B \end{tikzcd}$$

Proposition 2.18. *If it exists, the product of two objects in a category is unique up to isomorphism.*

Proof. Let P, P' be two products for A and B, with maps π_A, π_B and π'_A, π'_B respectively. Now by the definition above, there must exist morphisms f, f' such that the following diagram commutes:

$$\begin{tikzcd}
 & P \arrow[ddl, "\pi_A"'] \arrow[ddr, "\pi_B"] \arrow[d, "f"] & \\
 & P' \arrow[dl, "\pi'_A"] \arrow[dr, "\pi'_B"'] \arrow[d, "f'"] & \\
A & P \arrow[l, "\pi_A"] \arrow[r, "\pi_B"'] & B
\end{tikzcd}$$

Why must it be that $f \circ f' = 1_P$ and $f' \circ f = 1_{P'}$? Since the morphism $P \to P$ that commutes with the projections is unique, it must be equal to 1_P, and similarly for $1_{P'}$. Hence we are done. ☐

Examples 2.19. There is no guarantee that the product of two objects exists in an arbitrary category, though in the categories we have already seen it often exists and has special meaning:

- In **Set**, the product of two sets is isomorphic to the Cartesian product.
- In ${}_R$**Mod** and **Mod**$_R$, the product of two modules is the direct sum of modules. We will discuss the apparent conflict in terminology later.
- If A is a poset and $\mathcal{A}$ is the category defined in Example 2.4, then if a product of two elements exists, it is the infimum of those elements.

Definition 2.20. A **terminal object** in a category $\mathcal{A}$ is an object T such that, for all objects $A \in \mathcal{A}$, there is a *unique* morphism $A \to T$.

Proposition 2.21. *If it exists, the terminal object of a category is unique up to isomorphism.*

Proof. Suppose T, T' are two terminal objects. Then there exist unique morphisms $f \colon T' \to T$ and $f' \colon T \to T'$, and furthermore we have $f \circ f' \colon T \to T$ and $f' \circ f \colon T' \to T'$. However, 1_T and $1_{T'}$ already exist, so since the morphisms are unique, we have $f \circ f' = 1_T$, and likewise for T'. ☐

Examples 2.22.

- In **Set**, the terminal object is the set with one element.
- In ${}_R$**Mod** and **Mod**$_R$, the terminal object is the zero module.
- If A is a poset and $\mathcal{A}$ is the category defined in Example 2.4, then if it exists, the terminal object is the maximum of the poset.

There is a natural way to obtain more interesting definitions by reversing the definitions above. We present a rigorous way to define this now.

Definition 2.23. Given a category $\mathcal{A}$, the **opposite category** $\mathcal{A}^{\mathrm{op}}$ consists of the same objects as $\mathcal{A}$, but consists of the formal morphisms f^{op} for every morphism f of $\mathcal{A}$, where $f^{\mathrm{op}} \circ g^{\mathrm{op}} = (g \circ f)^{\mathrm{op}}$, so that $f^{\mathrm{op}} \in \mathrm{Hom}_{\mathcal{A}^{\mathrm{op}}}(B, A)$ given $f \in \mathrm{Hom}_{\mathcal{A}}(A, B)$.

Intuitively, this may be thought of as a category with the arrows reversed. A common thread in category theory is to consider the same definition of an object in the opposite category. This is known as dualisation.

Definition 2.24. Given a category $\mathcal{A}$ and objects A, B therein, a **coproduct** of A and B, denoted $A \sqcup B$, is an object $A \sqcup B$ equipped with morphisms $\iota_A \colon A \to A \sqcup B$ and $\iota_B \colon B \to A \sqcup B$ such that, for all objects C and maps $f_A \colon A \to C$, $f_B \colon B \to C$, there is a unique map $f \colon A \sqcup B \to C$ such that the following diagram commutes:

$$\begin{tikzcd}
 & C & \\
A \arrow[ur, "f_A"] \arrow[r, "\iota_A"] & A \sqcup B \arrow[u, dashed, "f"] & B \arrow[ul, "f_B"'] \arrow[l, "\iota_B"']
\end{tikzcd}$$

Equivalently, it is a product object in $\mathcal{A}^{\mathrm{op}}$.

Note that the above definition is simply the definition of a product with every arrow reversed! We say therefore that the notion of a coproduct is dual to that of a product. A consequence of this is that we obtain for free that the coproduct is unique up to isomorphism, as it is unique up to isomorphism in the opposite category, and it is easy to see that objects are isomorphic in the opposite category exactly when they are isomorphic ordinarily.

Examples 2.25.

- In **Set**, the coproduct of two sets is the disjoint union.
- In ${}_R\mathbf{Mod}$ and $\mathbf{Mod}_R$, the coproduct of two modules is the direct sum of modules – surprisingly, exactly the same as the product!
- If A is a poset and $\mathcal{A}$ is the category defined in Example 2.4, then if a coproduct of two elements exists, it is the supremum of those elements.

Definition 2.26. Given a category $\mathcal{A}$ an **initial object** is an object $I \in \mathcal{A}$ such that, for any object $A \in \mathcal{A}$, there is a unique morphism from I to A.

Equivalently, it is a terminal object in $\mathcal{A}^{\mathrm{op}}$.

Examples 2.27.

- In **Set**, the initial object is the empty set, provided that we think it possible to have a function from an empty set (although this is not controversial).
- In ${}_R\mathbf{Mod}$ and $\mathbf{Mod}_R$, the initial object is the zero module – exactly the same as the terminal object.
- If A is a poset and $\mathcal{A}$ is the category defined in Example 2.4, then if it exists, the initial object is the minimum of the poset.

There is another kind of functor that we might care about. Instead of respecting composition – that is, instead of having $F(f \circ g) = F(f) \circ F(g)$, we may have F reverse the composition, so that we have $F(f \circ g) = F(g) \circ F(f)$ instead. This is what it means to be contravariant, as opposed to an ordinary covariant functor whose definition we have seen previously.

Definition 2.28. A **contravariant functor** F wherein $F(f \circ g) = F(g) \circ F(f)$ replaces the restriction in the definition of a covariant functor.

Equivalently, it is a covariant functor $F\colon \mathcal{A}^{\mathrm{op}} \to \mathcal{B}$.

We will often say that $F\colon \mathcal{A} \to \mathcal{B}$ is a contravariant functor rather than saying that $F\colon \mathcal{A}^{\mathrm{op}} \to \mathcal{B}$ is a (covariant) functor.

In the remainder of this document, we will usually omit $\circ$ when composing morphisms in a category, and simply write fg instead of $f \circ g$ for the sake of brevity.

Instead of writing $\mathbf{Mod}_{\mathbb{Z}}$, we will typically refer to this category as **Ab**, the category of Abelian groups. We also assume that the reader is familiar with the construction of the free module $R^(X)$ with basis X, and that this may be seen as a functor $\mathbf{Set} \to {}_R\mathbf{Mod}$. Explicitly, the module $R^(X)$ consists of functions $f\colon X \to R$ for which $f(x) = 0$ for all but finitely many $x \in X$, and both addition and scalar multiplication are defined pointwise.

3 Hom, Tensor, and the Adjunction

The categories that we will be focusing on most – namely ${}_R\mathbf{Mod}$ and $\mathbf{Mod}_R$ for some ring R – inherit the core of the hom functor entirely from **Set**, as the following proposition shows.

Proposition 3.1. *If* $\mathrm{Hom}_{\mathcal{C}}(A, B)$ *is a set for all objects* A *and* B *in a category* $\mathcal{C}$*, then* $\mathrm{Hom}_{\mathcal{C}}(A, \Box)\colon \mathcal{C} \to \mathbf{Set}$ *and* $\mathrm{Hom}_{\mathcal{C}}(\Box, B)\colon \mathcal{C} \to \mathbf{Set}$ *are respectively covariant and contravariant functors.*

Proof. As a matter of notation, given morphisms $f\colon B \to B'$ and $i\colon A' \to A$, we will write f_* instead of $\mathrm{Hom}(A, f)$, and i^* instead of $\mathrm{Hom}(i, B)$. We now define $f_*\colon h \mapsto fh$ and $i^*\colon h \mapsto hi$, that is 'post-composition' and 'pre-composition' respectively.

We now see $(1_B)_*(h) = 1_B h = h$ so that $(1_B)_* = 1_{\mathrm{Hom}(A,B)}$, and $(g_* f_*)(h) = g(fh) = (gf)h = (gf)_*(h)$, so $\mathrm{Hom}(A, \Box)$ is a covariant functor. The proof is entirely similar for $\mathrm{Hom}(\Box, B)$, except that $i^* j^* = (ji)^*$. $\Box$

In this way, since the objects and morphisms of ${}_R\mathbf{Mod}$ and $\mathbf{Mod}_R$ are ultimately sets and certain functions between them, both forms of hom will be functors into **Set** in the way described above. For convenience, we will write the hom functors both in ${}_R\mathbf{Mod}$ and $\mathbf{Mod}_R$ simply as $\mathrm{Hom}_R(A, B)$, or even simply Hom when the context is clear – for instance when we have defined A and B to be right R-modules.

Seeing hom as a functor into **Set** is correct, of course, but it ignores the particular structure that modules have. It turns out that under certain conditions we can find a lot more structure in $\mathrm{Hom}_R(A, B)$. We proceed by elucidating some of this structure.

3.1 The Hom Functor

The first and most obvious structure is that $\mathrm{Hom}_R(A, B)$ is an Abelian group, with the operations defined pointwise. That is, if A, B are left or right R-modules, and $f, g \in \mathrm{Hom}_R(A, B)$ we may define $f + g$ as the function sending $a \in A$ to $f(a) + g(a)$. The identity of this Abelian group will be the constant zero function, which we will simply denote as 0.

We can do better, as $\mathrm{Hom}_R(A, B)$ being an Abelian group only relies on B being an Abelian group rather than an R-module. Naïvely, we may be tempted say that $\mathrm{Hom}_R(A, B)$ will also be an R-module, with scalar multiplication defined pointwise.

However this structure may not form a left module: supposing we are working in ${}_R\mathbf{Mod}$, given $a \in R$ and $f \in {}_R\mathrm{Hom}_R(A, B)$, we have that af is a homomorphism. Given $b \in R$, then this means in particular that $af(bx) = b \cdot af(x) = ba \cdot f(x)$, but since f is also a homomorphism, $a \cdot f(bx) = ab \cdot f(x)$ for all x. The equality $ab \cdot f(x) = ba \cdot f(x)$ simply does not hold in general – in particular in rings that do not commute.

There is a compromise that makes this work in a natural way.

Definition 3.2. The **centre** $Z(R)$ of a ring R is the subring of all elements that commute with all other elements of R. That is, $Z(R) = \{r \in R \mid \forall s \in R, rs = sr\}$.

Proof that $Z(R)$ *is a subring of* R. Note that $0 \in Z(R)$ and $1 \in Z(R)$.

Suppose $a, b \in Z(R)$. Then given some $s \in R$, we have $s(a - b) = sa - sb = as - bs = (a - b)s$, so $a - b \in Z(R)$. Similarly, $(ab)s = a(bs) = a(sb) = (as)b = (sa)b = s(ab)$, so $ab \in Z(R)$ as well. $\Box$

Proposition 3.3. *Both* $\mathrm{Hom}_R(A, \Box)$ *and* $\mathrm{Hom}_R(\Box, B)$ *may be seen as functors* ${}_R\mathbf{Mod} \to \mathbf{Ab}$ *and* ${}_R\mathbf{Mod} \to {}_{Z(R)}\mathbf{Mod}$*. The reverse holds for right* R*-modules.*

Proof. We have seen that $\mathrm{Hom}(A, B)$ is an Abelian group, so it remains only to show that f_* and f^* are group homomorphisms. Indeed, for any $a \in A$ and $g, h \in \mathrm{Hom}(A, B)$:

$$\begin{aligned} f_*(g+h)(a) &= f(g(a)+h(a)) \\ &= fg(a) + fh(a) \\ &= (f_*(g) + f_*(h))(a), \end{aligned}$$

and similarly for precomposition:

$$\begin{aligned} f^*(g+h)(a) &= g(f(a)) + h(f(a)) \\ &= gf(a) + hf(a) \\ &= (f^*(g) + f^*(h))(a), \end{aligned}$$

So indeed f_* and f^* are homomorphisms of Abelian groups.

To show the second part of the theorem, we need to show not only that $\mathrm{Hom}(A, B)$ is a left $Z(R)$-module, but also that f_* and f^* respect scalar multiplication.

Firstly, given $r \in Z(R)$ and $g \in \mathrm{Hom}(A, B)$, we define $(rf)(a) = rf(a)$, which evidently distributes over addition and is associative.

We confirm that rf is still a member of $\mathrm{Hom}(A, B)$. It respects addition since:

$$(rf)(a+b) = rf(a+b) = r(f(a) + f(b)) = rf(a) + rf(b).$$

Similarly it respects scalar multiplication since $(rf)(sa) = rf(sa) = rsf(a)$, and since $r \in Z(R)$ we have $rsf(a) = srf(a)$.

It remains only to show that f_* and f^* are $Z(R)$-homomorphisms. By our previous observations, they respect addition, so our last task is to show that they respect scalar multiplication.

Indeed $f_*(rg)(a) = f(rg(a)) = rf(g(a)) = (rf_*(g))(a)$, and for precomposition, $f^*(rg)(a) = rg(f(a)) = r(g(f(a))) = (rf^*(g))(a)$.

The proof for right R-modules is entirely similar, so we omit it here. $\square$

Unhappy though this $Z(R)$-module compromise may seem, our investigations into Abelian categories will reveal that $\mathrm{Hom}_R(A, B)$ being in **Ab** lends us more than enough power.

The previous proposition's core lay in showing that f_* and f^* are homomorphisms of Abelian groups. Observe that, writing $FB = \mathrm{Hom}_R(A, B)$, the map $f \mapsto f_*$ is itself a function $\mathrm{Hom}_R(X, Y) \to \mathrm{Hom}_{Z(R)}(FX, FY)$ – this is nothing special as this occurs for all covariant functors F. A natural question to ask is whether or not this map $f \mapsto f_*$ and its contravariant sibling $f \mapsto f^*$ are homomorphisms, rather than merely functions.

Though this property may seem very natural, not all functors $F\colon {}_R\mathbf{Mod} \to \mathbf{Ab}$ have it. For example, consider $\mathbb{Z}^(\square)$ – the free Abelian group on the underlying set of a given module. This functor does not even respect the 0 map, since the element 0 of M now corresponds to a nonzero basis element of $\mathbb{Z}^(M)$.

Since it is not universal, we give this phenomenon of preserving addition a suitable name.

Definition 3.4. A functor $F\colon {}_R\mathbf{Mod} \to \mathbf{Ab}$ is called **additive** if for all f, g belonging to $\mathrm{Hom}_R(A, B)$, we have $F(f+g) = Ff + Fg$. Note that this definition makes sense for both covariant and contravariant functors.

Proposition 3.5. *Both the functors* $\mathrm{Hom}_R(A, \square)$ *and* $\mathrm{Hom}_R(\square, B)$ *are additive.*

Proof. We will only show this holds for left R-modules, since the proof is entirely similar for right R-modules.

Suppose $f, g \in \mathrm{Hom}_R(A, B)$ so that $f_*, g_* \colon \mathrm{Hom}_R(M, A) \to \mathrm{Hom}_R(M, B)$. Then for any $k \in \mathrm{Hom}_R(M, A)$ we see that:

$$\begin{aligned}(f_* + g_*)(k) &= fk + gk \\ &= k^*(f) + k^*(g) \\ &= k^*(f + g) \\ &= (f + g)_*(k).\end{aligned}$$

Similarly given $f, g \in \mathrm{Hom}_R(A, B)$ so that we have

$$f^*, g^* \colon \mathrm{Hom}_R(B, M) \to \mathrm{Hom}_R(A, M),$$

we see that for any $k \in \mathrm{Hom}_R(B, M)$:

$$\begin{aligned}(f^* + g^*)(k) &= kf + kg \\ &= k_*(f) + k_*(g) \\ &= k_*(f + g) \\ &= (f + g)^*(k).\end{aligned}$$

Note that this proof relies on the observation that $f_*(g) = g^*(f)$. □

Example 3.6. The dual of a $\Bbbk$-vector space V is defined as $\mathrm{Hom}_\Bbbk(V, \Bbbk)$. The above results show that this is a contravariant, additive functor.

The Hom functor plays with direct sums and products of modules in an interesting way. We recapitulate the precise definitions for the sake of completeness.

Definition 3.7. Let $(A_i)_{i \in I}$ be some collection of R-modules. Then the **direct product**

$$P = \prod_{i \in I} A_i$$

is defined as all functions (not necessarily R-linear maps) $p \colon I \to \bigcup_{i \in I} A_i$ with $p(i) \in A_i$. This is an R-module with addition defined as $(p + q)(i) = p(i) + q(i)$, and the action of the scalars defined as $(rp)(i) = rp(i)$.

The **direct sum**

$$\bigoplus_{i \in I} A_i$$

is the submodule of P consisting of functions $p \in P$ such that $p(i) = 0$ for all but finitely many $i \in I$ (that is, for cofinitely many $i \in I$).

There is then a collection of injections $\iota_j \colon A_j \to \bigoplus_{i \in I} A_i$ sending $a \in A_j$ to the p, where $p(j) = a$ and is zero elsewhere. Similarly there is a collection of surjections $\pi_j \colon \prod_{i \in I} A_i \to A_j$ which sends p to $p(j)$. We use these R-linear maps in the following proposition.

Proposition 3.8. *For some collection of modules $(A_i)_{i \in I}$ and any module M, we have:*

$$\mathrm{Hom}\left(M, \prod_{i \in I} A_i\right) \cong \prod_{i \in I} \mathrm{Hom}(M, A_i) \quad \textit{and} \quad \mathrm{Hom}\left(\bigoplus_{i \in I} A_i, M\right) \cong \prod_{i \in I} \mathrm{Hom}(A_i, M)$$

Proof. We define a map $\phi_1 \colon \mathrm{Hom}\left(M, \prod_{i \in I} A_i\right) \to \prod_{i \in I} \mathrm{Hom}(M, A_i)$ by sending f to g, where $g(i)(m) = \pi_i f(m) = f(m)(i)$ – essentially exchanging the order of the arguments. We claim that it has an inverse in the map ϕ_2 defined by sending g to f, where $f(m)(i) =$

$g(i)(m)$, again reversing the arguments. It is evident that these are mutually inverse since they both reverse the arguments.

The former isomorphism requires a slightly subtler argument. We define the first map simply enough: $\psi_1 \colon \operatorname{Hom}\left(\bigoplus_{i \in I} A_i, M\right) \to \prod_{i \in I} \operatorname{Hom}(A_i, M)$ by sending f to g, where $g(i)(a) = f(\iota_i(a))$. Its mutual inverse is less easy. We define ψ_2 as sending g to f, where:

$$f(p) = \sum_{p(i) \neq 0} g(i)(p(i)).$$

Why is this well-defined? Since p is a member of the direct sum rather than a direct product, $p(i) = 0$ for all but finitely many $i \in I$, so we are summing finitely many elements. If p were an arbitrary element of the direct product, this would not be possible – a general module does not come equipped with a way to sum infinitely many elements.

Now why are these mutual inverses? It comes down to noticing that, if $p \in \bigoplus_{i \in I} A_i$, then $p = \sum_{p(i) \neq 0} \iota_i(p(i))$, which shows that $\psi_2 \psi_1$ is the identity, since:

$$\sum_{p(i) \neq 0} f \iota_i(p(i)) = f\left(\sum_{p(i) \neq 0} \iota_i(p(i))\right) = f(p).$$

As for $\psi_1 \psi_2$, we have for all $j \in I$ and $a \in A_j$:

$$\sum_{\iota_j(a)(i) \neq 0} g(i)(\iota_j(a)(i)) = g(j)(a).$$

This shows that the two are mutual inverses. $\square$

Remark. If the index set I is finite, it is immediate from Definition 3.7 that the direct sum and product are equal. In particular, though we shall not prove it here, for an index set $I = \{1, 2\}$, the direct sum (and equally, the product) is the ordinary direct sum $A_1 \oplus A_2$ that we are familiar with, and hence Hom distributes over the direct sum of two modules.

3.2 The Tensor Product

Linear maps are familiar as they are homomorphisms of R-modules. However, linear maps are limited by only having a single argument. If we want to have multiple variables, we need the notion of a *multi*-linear map. To explore how to do this, let us firstly work in a commutative ring R, and try to make a two-argument linear map in a natural way.

We are familiar with defining functions with many variables in **Set**: we simply see it as a function $A \times B \to C$. However via a technique called currying, we may see it as a function $A \to \operatorname{Hom}_{\mathbf{Set}}(B, C)$.

These two approaches are equivalent for functions between sets, but what about functions between R-modules? By replacing $A \times B$ with $A \oplus B$ and $\operatorname{Hom}_{\mathbf{Set}}(B, C)$ with $\operatorname{Hom}_R(B, C)$, we may work in the category of R-modules (by Proposition 3.3), and therefore see these maps of two variables as ordinary linear maps.

Given two R-maps $f_1 \colon A \oplus B \to C$ and $f_2 \colon A \to \operatorname{Hom}_R(B, C)$, we may view them as ordinary functions $\phi_1, \phi_2 \colon A \times B \to C$ by setting $\phi_1(a, b) = f_1((a, b))$ and $\phi_2(a, b) = f_2(a)(b)$. We then ask: what conditions on ϕ_1 and ϕ_2 must hold to make the corresponding functions f_1 and f_2 linear?

These requirements are routine to calculate, and we list them here, where $a, b \in A$, $x, y \in B$, and $r \in R$ are arbitrary:

For $f_1 \colon A \oplus B \to C$ to be linear:	For $f_2 \colon A \to \mathrm{Hom}_R(B, C)$ to be linear:
• $\phi_1(a+b, x+y) = \phi_1(a, x) + \phi_1(b, y)$, • $\phi_1(ra, rx) = r\phi_1(a, x)$.	• $\phi_2(a+b, x) = \phi_2(a, x) + \phi_2(b, x)$, • $\phi_2(a, x+y) = \phi_2(a, x) + \phi_2(a, y)$, • $\phi_2(ra, x) = \phi_2(a, rx) = r\phi_2(a, x)$.

By inspecting the above conditions, we see that unlike in the category of sets, creating a morphism of two variables via products and creating one by currying are distinct! The latter notion is what we will be scrutinising in the coming investigations.

Before we continue, we must talk about commutativity. We have been working in the whole world of rings until now, but multilinearity lives only amongst commutative rings. In the spirit of continuing our commutative ambivalence (and in the spirit of [Rot09]), we will restrict our attention to a specific kind of map that works better with arbitrary rings.

Definition 3.9. Given a (not necessarily commutative) ring R, a right R-module A, a left R-module B, and an Abelian group C, a function $f \colon A \times B \to C$ is ***R*-biadditive** if the following conditions hold for all $a, a' \in A$, $b, b' \in B$, and $r \in R$:

(1) $f(a + a', b) = f(a, b) + f(a', b)$,
(2) $f(a, b + b') = f(a, b) + f(a, b')$,
(3) $f(ar, b) = f(a, rb)$.

It is worth pausing on this definition momentarily, as it may at first appear somewhat arbitrary. Note the differences to the characterisation of linear maps $A \to \mathrm{Hom}_R(B, C)$ above. Why did we require A and B to be opposite-sided R-modules? Because if not, given $r, s \in R$ we get $f(rsa, x) = f(sa, rx) = f(a, srx) = f(sra, x)$, which does not mesh well with noncommutativity. Why did we require C only to be an Abelian group, and not require scalar multiplication to commute with the function? Again, since A and B are right and left R-modules respectively, this would not work well with noncommutative rings.

A goal we might aspire to is to encode these biadditive functions as ordinary additive functions – that is, homomorphisms of Abelian groups. Neither of the methods we suggested above are appropriate here, so we will develop a new construction, so that a biadditive functions are then additive functions from this object into C.

We will achieve this goal as follows. First, take $\mathbb{Z}^{(A \times B)}$ to be the free Abelian group with basis elements the set (not the module) $A \times B$. We then define the following subgroup, each generator of which corresponds to part of the definition of additivity:

$$H = \left\langle \begin{matrix} (a + a', b) - (a, b) - (a', b), \\ (a, b + b') - (a, b) - (a, b'), \\ (ar, b) - (a, rb) \end{matrix} \;\middle|\; \begin{matrix} a, a' \in A, \\ b, b' \in B, \\ r \in R \end{matrix} \right\rangle$$

We then take the quotient $\mathbb{Z}^{(A \times B)}/H$, which we give the following name.

Definition 3.10. The **tensor product over** R of a right R-module A and left R-module B is the Abelian group $A \otimes_R B = \mathbb{Z}^{(A \times B)}/H$ as defined above.

To denote the coset $(a, x) + H \in A \otimes_R B$, we will write $a \otimes x$, as is the convention. Note that these elements generate the entirety of $A \otimes_R B$, so that a general element of the tensor product is some sum of elements of the form $a \otimes x$.

Clearly the tensor product has *something* to do with biadditivity, but it is not yet clear what exactly this connection is. In the next few results, we will show that it encapsulates biadditive functions entirely.

Proposition 3.11. *The function $\eta \colon A \times B \to A \otimes_R B; (a, b) \mapsto a \otimes b$ is R-biadditive.*

Proof. Each of the generators of H corresponds to one of the stipulations in the definition of a biadditive function:

(1) $(a+a')\otimes b = (a+a',b)+H = (a+a',b)-(a+a',b)+(a,b)+(a',b)+H = (a\otimes b)+(a'\otimes b)$,
(2) $a\otimes(b+b') = (a,b+b')+H = (a,b+b')-(a,b+b')+(a,b)+(a,b')+H = (a\otimes b)+(a\otimes b')$,
(3) $ar\otimes b = (ar,b)+H = (ar,b)-(ar,b)+(a,rb)+H = a\otimes rb$. $\square$

This proposition shows that the tensor product exhibits biadditivity, but the next shows that in fact they are one and the same.

Proposition 3.12. *If $f\colon A\times B\to C$ is an R-biadditive function, then there exists an additive function $\phi\colon A\otimes_R B\to C$ such that $f=\phi\eta$, where $\eta\colon A\times B\to A\otimes_R B$ is the biadditive function defined in Proposition 3.11.*

Proof. We will define the map $\phi\colon A\otimes_R B\to C$ by $\phi(a\otimes b)=f(a,b)$, and extend linearly, which leaves us to show that this is well-defined. If we have two representatives of the same element in $A\otimes_R B$, then they differ in $\mathbb{Z}^{(A\times B)}$ by some sum of generators of H. It then follows that we need only show that our definition sends the generators of H to zero for ϕ to be well-defined. We check each one:
(1) $f(a+a',b)-f(a,b)-f(a',b) = f(a+a',b)-f(a+a',b)=0$,
(2) $f(a,b+b')-f(a,b)-f(a,b') = f(a,b+b')-f(a,b+b')=0$,
(3) $f(ar,b)-f(a,rb) = f(ar,b)-f(ar,b)=0$. $\square$

Corollary 3.13. *Given appropriate R-modules A,B and an Abelian group C, there is a bijection:*

$$\{R\text{-biadditive functions } A\times B\to C\}\leftrightarrow\{\text{Additive functions } A\otimes_R B\to C\}.$$
$$f\mapsto\phi,$$

where ϕ is as defined in Proposition 3.12.

Proof. Proposition 3.12 shows existence of ϕ, and uniqueness follows by noting $f(a,b)=\phi(a\otimes b)$, ergo ϕ is uniquely determined by f. $\square$

A natural question to now ask is that, given that this is a construction that takes in R-modules and produces Abelian group, does this form a functor? Indeed it does, and we will show this in a strong way.

Proposition 3.14. *Given $f\colon A\to A'$ and $g\colon B\to B'$ – maps of right and left R-modules respectively – there is a map $f\otimes g\colon A\otimes_R B\to A'\otimes_R B'$ such that, for appropriate maps, we have:*
(1) $(f\otimes g)(f'\otimes g')=(ff'\otimes gg')$, *and*
(2) $1_A\otimes 1_B=1_{A\otimes B}$.

In the language of category theory, we would say that the tensor product is a bifunctor.

Proof. We will show that, given $f\colon A\to A'$ and $g\colon B\to B'$, the map $\phi(a\otimes b)=f(a)\otimes g(b)$ is well-defined, after which the two identities follow easily.

By Proposition 3.12, we need only show that the map $\phi'(a,b)=f(a)\otimes g(b)$ is biadditive. Indeed:
(1) $f(a+b)\otimes g(x) = (f(a)+f(b))\otimes g(x) = f(a)\otimes g(x)+f(b)\otimes g(x)$,
(2) $f(a)\otimes g(x+y) = f(a)\otimes(g(x)+g(y)) = f(a)\otimes g(x)+f(a)\otimes g(y)$,
(3) $f(ar)\otimes g(x) = f(a)r\otimes g(x) = f(a)\otimes rg(x) = f(a)\otimes g(rx)$.
So $f\otimes g=\phi$ is well-defined and, as stated, the two identities follow easily from the definition:
(1) $(f\otimes g)(f'\otimes g')(\sum a_i\otimes b_i) = \sum ff'(a_i)\otimes gg'(b_i) = (ff'\otimes gg')(\sum a_i\otimes b_i)$, and
(2) $(1_A\otimes 1_B)(\sum a_i\otimes b_i) = \sum a_i\otimes b_i$. $\square$

Corollary 3.15. *Both $A\otimes_R\square\colon {}_R\mathbf{Mod}\to\mathbf{Ab}$ and $\square\otimes_R B\colon \mathbf{Mod}_R\to\mathbf{Ab}$ are covariant functors.*

Not only are these both functors, but indeed they are also additive functors.

Proposition 3.16. *Both $A \otimes_R \Box$ and $\Box \otimes_R B$ are additive functors.*

Proof. We show this only for $A \otimes_R \Box$ as the proof in the second case is entirely similar. Supposing that $f, g\colon {}_RB \to {}_RB'$ are given, we observe:

$$\begin{aligned}(1_A \otimes_R (f+g))(a \otimes b) &= a \otimes (f(b) + g(b)) \\ &= a \otimes f(b) + a \otimes g(b) \\ &= (1_A \otimes_R f)(a \otimes b) + (1_A \otimes_R g)(a \otimes b).\end{aligned}$$

This is what was required, since this holds by linearity for all elements of $A \otimes_R B$. $\Box$

We prove a parting result that might justify our calling the tensor a *product* – we see that it is linear in the sense that it distributes over sums.

Proposition 3.17. *If M is a right R-module and $(N_i)_{i \in I}$ is a family of left R-modules, then:*

$$M \otimes_R \bigoplus_{i \in I} N_i \cong \bigoplus_{i \in I} (M \otimes_R N_i).$$

Proof. We claim the map defined by the following is an isomorphism:

$$\phi\colon m \otimes \sum_i n_i \mapsto \sum_i m \otimes n_i.$$

This map is well-defined since it is evidently bilinear.

Letting $\iota_j\colon N_j \to \bigoplus_{i \in I} N_i$ be the inclusion, note that we have a map:

$$1_M \otimes \iota_j\colon M \otimes_R N_j \to M \otimes_R \bigoplus_{i \in I} N_j.$$

Taking the sum of these, we obtain a well-defined map $\bigoplus_{i \in I}(M \otimes_R N_i) \to M \otimes_R \bigoplus_{i \in I} N_i$:

$$\psi\colon m \otimes n_j \mapsto m \otimes \iota_j(n_j).$$

We claim that ψ and ϕ are mutual inverses. Indeed:

$$\begin{aligned}(\psi \circ \phi)\left(m \otimes \sum_i n_i\right) &= \psi\left(\sum_i m \otimes n_i\right) \\ &= \sum_i (m \otimes \iota_j(n_i)) \\ &= m \otimes \sum_i \iota_i(n_i) = m \otimes \sum_i n_i.\end{aligned}$$

Conversely, we see that:

$$\begin{aligned}(\phi \circ \psi)\left(\sum_i m_i \otimes n_i\right) &= \phi\left(\sum_i (m_i \otimes \iota_i(n_i))\right) \\ &= \sum_i (m_i \otimes n_i).\end{aligned}$$

This finishes the proof. $\Box$

3.3 Bimodules in Hom and Tensor

Often a module may be acted upon by two different rings, in a way that is compatible, and this has important effects on the structure of the two functors we have discussed.

For the rest of this section, let S be a ring, which may be distinct from R.

Definition 3.18. An (R, S)-bimodule M (written ${}_RM_S$ for brevity), is a left R-module and a right S module, such that a sort of associative law holds: for any $m \in M$, $r \in R$, and $s \in S$, we have $r(ms) = (rm)s$

Remark. Every left R-module ${}_RM$ is in fact an $(R, \mathbb{Z})$-bimodule ${}_RM_{\mathbb{Z}}$. To see this, first recall that the right $\mathbb{Z}$-action can only occur in one way: if $m \in M$ and $0 < z \in \mathbb{Z}$, then $mz = m + \cdots + m$, where the sum is repeated z times. If then $r \in R$, we have $(rm)z = rm + \cdots + rm = r(m + \cdots + m) = r(mz)$. This extends to negative and zero z, and hence the associative law holds. Naturally, a similar fact holds for right R-modules.

In the case that we have a bimodule, the Hom set is not only an Abelian group, but has the additional structure of a module. We first cover the contravariant case.

Proposition 3.19.
(1) $\operatorname{Hom}_R({}_RM, {}_RN_S)$ *is a right* S*-module, where* $(fs)(m) = f(m)s$ *and*
(2) $\operatorname{Hom}_R(M_R, {}_SN_R)$ *is a left* S*-module, where* $(sf)(m) = sf(m)$*.*

Proof. Since the second part is the mirror image of the first, we will only prove the first. Let $s, r \in S$, and let $f, g \in \operatorname{Hom}_R(M, N)$.

Firstly we show that the action is properly defined. If $m, n \in M$ and $x \in R$ then $(fs)(m + n) = f(m + n)s = f(m)s + f(n) = (fs)(m) + (fs)(n)$. Furthermore $(fs)(xm) = f(xm)s = xf(m)s = x(fs)(m)$, so indeed $fs \in \operatorname{Hom}_R(M, N)$.

Secondly we show that the action is linear. Indeed for any $m \in M$, $((f + g)s)(m) = (f + g)(m)s = f(m)s + g(m)s = (fs)(m) + (gs)(m) = (fs + gs)(m)$, so $(f + g)s = fs + gs$.

Finally we show that the action is associative. For any $m \in M$, we have $((fr)s)(m) = (fr)(m)s = f(m)rs = (f(rs))(m)$, so $(fr)s = f(sr)$. ☐

The reason we call this the contravariant case is that this shows, for example, that $\operatorname{Hom}_R(\square, {}_RN_S)$ is a contravariant functor ${}_R\mathbf{Mod} \to \mathbf{Mod}_S$. Notice that the sidedness of the S-action is preserved. If we consider the *covariant* case, somewhat unintuitively, the sidedness is reversed.

Proposition 3.20.
1. $\operatorname{Hom}_R({}_RM_S, {}_RN)$ *is a left* S*-module, where* $(sf)(m) = f(ms)$*, and*
2. $\operatorname{Hom}_R({}_SM_R, N_R)$ *is a right* S*-module, where* $(fs)(m) = f(sm)$*.*

This is to say that, in particular, $\operatorname{Hom}_R({}_RM_S, \square)$ is a covariant functor ${}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$, despite M being in $\mathbf{Mod}_S$.

Proof. Again we only prove the first. Let $s, r \in S$, and let $f, g \in \operatorname{Hom}_R(M, N)$.

The action is defined properly, since for any $m, n \in M$, we have $(sf)(m + n) = f(ms + ns) = f(ms) + f(ns) = (sf)(m) + (sf)(n)$, and additionally for any $x \in R$, we have $(sf)(xm) = f(xms) = xf(ms) = x(fs)(m)$. This shows that $sf \in \operatorname{Hom}_R(M, N)$.

The action is linear, since for any $m \in M$, we have $(s(f + g))(m) = f(ms) + g(ms) = (sf + sg)(m)$.

Finally the action is associative, since $(r(sf))(m) = (sf)(mr) = f(mrs) = (f(rs))(m)$. It is worth remarking that this last part is what forces the sidedness of the S-action to be reversed! ☐

Along with previous results about the functoriality of Hom, we may summarise these results as statements about functors.

Corollary 3.21.

(1) $\operatorname{Hom}_R({}_RM_S, \square)\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ *is a covariant functor,*
(2) $\operatorname{Hom}_R({}_SM_R, \square)\colon \mathbf{Mod}_R \to \mathbf{Mod}_S$ *is a covariant functor,*
(3) $\operatorname{Hom}_R(\square, {}_RN_S)\colon {}_R\mathbf{Mod} \to \mathbf{Mod}_S$ *is a contravariant functor, and*
(4) $\operatorname{Hom}_R(\square, {}_SN_R)\colon \mathbf{Mod}_R \to {}_S\mathbf{Mod}$ *is a contravariant functor,*

Remark. Noting that every left R-module is an $\big(R, Z(R)\big)$-bimodule, this corollary can be seen as a strengthening of Proposition 3.3.

Example 3.22. The above results can be put into the context of matrices. If we consider $\operatorname{Hom}_R(R^m, R^n)$, we can identify these maps with matrices $M_{n\times m}(R)$, via:

$$f\colon R^m \to R^n \mapsto \begin{pmatrix} f(e_1)_1 & \cdots & f(e_m)_1 \\ \vdots & \ddots & \vdots \\ f(e_1)_n & \cdots & f(e_m)_n \end{pmatrix},$$

where e_i is the ith basis element of R^m and if $v \in R^n$ then v_j is its jth component.

We know that $n \times m$ matrices are naturally left $M_m(R)$-modules and right $M_n(R)$-modules. This can be seen as a direct result of parts (2) and (4) of Corollary 3.21, since R^n is an $(M_n(R), R)$-bimodule. Showing the fact that $M_{n\times m}(R)$ is an $(M_n(R), M_m(R))$-bimodule would require an extension of the work above.

A comparable property is true for the tensor product.

Proposition 3.23. *The tensor product ${}_SM_R \otimes_R {}_RN$ is a left S-module, and similarly $M_R \otimes_R {}_RN_S$ is a right S-module.*

Proof. We prove this only in the first case, since the second case is the mirror image. Let $s, r \in S$.

We wish to define left S-multiplication on the generators of $M \otimes_R N$ as $s(m\otimes n) = sm\otimes n$. By Proposition 3.12, in order to show that this is well-defined and distributive, we need only show the function $f(m, n) = sm \otimes n$ is biadditive.

Indeed all three parts of Definition 3.9 are satisfied:

(1) $f(m + m', n) = s(m + m') \otimes n = (sm \otimes n) + (sm' \otimes n) = f(m, n) + f(m', n)$,
(2) $f(m, n + n') = sm \otimes (n + n') = (sm \otimes n) + (sm \otimes n') = f(m, n) + f(m, n')$,
(3) for any $x \in R$, we have $f(mx, n) = smx \otimes n = sm \otimes xn = f(m, xn)$.

It remains only to show that multiplication is associative, in proving which it is sufficient to check only the generators of $M \otimes N$. Indeed $r(s(m \otimes n)) = r(sm \otimes n) = rsm \otimes n = rs(m \otimes n)$, and we are done. $\square$

Example 3.24. The above observation allows us to perform 'extension by scalars,' which is a canonical way of producing modules over larger rings from modules over smaller ones. For example, we may convert any $\mathbb{R}$-vector space V into a $\mathbb{C}$-vector space simply by tensoring by $\mathbb{C}$, since $\mathbb{C} \otimes_{\mathbb{R}} V$ is a complex vector space.

Similarly Abelian groups may be shoehorned into being a $\mathbb{Q}$-vector space, although this process may be destructive in the case of torsion. For example, take $T = \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_n$ for any $n \geq 1$. If $q \otimes x \in T$, then $q \otimes x = q/n \otimes nx = q/n \otimes 0 = 0$. So in fact T is the zero module.

Corollary 3.25.

1. ${}_SM_R \otimes_R \square\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ *is a covariant functor, and*
2. $\square \otimes_R {}_RN_S\colon \mathbf{Mod}_R \to \mathbf{Mod}_S$ *is a covariant functor.*

Remark. Similarly to our previous remark, this corollary is a strengthening of Corollary 3.15.

Example 3.26. There is an interesting way to turn R-modules into $R[x]$-modules via the tensor product. Supposing M is a left R-module, we can note that $R[x]$ is an $(R[x], R)$-bimodule, and hence we may define the left $R[x]$-module $M[x] = R[x] \otimes_R M$. An arbitrary element of $M[x]$ is then a sum of polynomials paired with elements of M, so in some sense $M[x]$ consists of polynomials taking coefficients in M.

3.4 The Hom-Tensor Adjunction

The results we have conjured up regarding Hom and tensor seem very similar indeed, and we might wonder why exactly these functors seem to share so many properties. As it turns out, the functors we have outlined above form an *adjoint pair*. Adjunction is a concept in category theory that describes a certain close relationship between a pair of functors.

This connection builds upon the idea of currying that we explored at the beginning of Section 3.2. The adjunction shows that the notion of currying and the notion of biadditive functions coincide in the category of modules.

Proposition 3.27. *There is an isomorphism*

$$\begin{aligned} \tau\colon \operatorname{Hom}_S(A_R \otimes_R {}_R B_S, C_S) &\to \operatorname{Hom}_R(A_R, \operatorname{Hom}_S({}_R B_S, C_S)) \\ f &\mapsto \tau(f), \end{aligned}$$

where $\tau(f)(a)(b) = f(a \otimes b)$.

Note that the well-formedness of this proposition depends on Corollaries 3.21 and 3.25, since it requires $A \otimes_R B$ to be a right S-module, and $\operatorname{Hom}_S(B, C)$ to be a right R-module.

Proof. We first show that τ is a homomorphism. Let $f, g \in \operatorname{Hom}_S(A \otimes_R B, C)$. Then $\tau(f + g)(a)(b) = (f + g)(a \otimes b) = f(a \otimes b) + g(a \otimes b) = \tau(f)(a)(b) + \tau(g)(a)(b) = (\tau(f) + \tau(g))(a)(b)$, so indeed $\tau(f + g) = \tau(f) + \tau(g)$.

We now show that τ is an injection. If $f, g \in \operatorname{Hom}(A \otimes_R B)$ are such that $\tau(f) = \tau(g)$, then certainly $f(a \otimes b) = \tau(f)(a)(b) = \tau(g)(a)(b) = g(a \otimes b)$, so by virtue of agreeing on a generating set, it is necessary that $f = g$.

We finally show that τ is a surjection. Supposing that $p \in \operatorname{Hom}_R(A, \operatorname{Hom}(B, C))$, we define a function $\bar{p}\colon A \times B \to C$ by $\bar{p}(a, b) = p(a)(b)$. By appeal to Proposition 3.12, if this function is R-biadditive, there is a well-defined map $\pi\colon A \otimes_R B \to C$ with $\pi(a \otimes b) = \bar{p}(a, b) = p(a)(b)$, whence $p = \tau(\pi)$.

It therefore remains only to show that $\bar{p}$ is R-biadditive. Indeed, by virtue of $p(a)$ and $p(a)(b)$ being R- and S-maps respectively:

(1) $\bar{p}(a + a', b) = p(a + a')(b) = (p(a) + p(a'))(b) = p(a)(b) + p(a')(b) = \bar{p}(a, b) + \bar{p}(a', b)$,

(2) $\bar{p}(a, b + b') = p(a)(b + b') = p(a)(b) + p(a)(b') = \bar{p}(a, b) = \bar{p}(a, b')$,

(3) for any $x \in R$, we have $\bar{p}(ar, b) = p(ar)(b) = (p(a)r)(b) = p(a)(rb) = \bar{p}(a, rb)$.

So $\bar{p}$ is R-biadditive, and we are done. $\square$

Example 3.28. It is a well-known result in the undergraduate curriculum that bilinear forms $V \times W \to \mathbb{k}$ are in correspondence with maps $V \to W^*$, where $W^* = \operatorname{Hom}_{\mathbb{k}}(W, \mathbb{k})$ is the dual space. This can be seen as a particular case of the Hom-tensor adjunction.

In fact, the statement is slightly stronger, category-theoretically.

Theorem 3.29. *The isomorphism in the previous proposition is natural in A, B, and C.*

Since this statement has a long but uninformative proof, and since our focus will not be on category theory, we will not prove this fact here, but rather use it without lengthy justification.

It may not be obvious why this fact is useful, but it is in fact a powerful tool when reasoning about the somewhat inscrutable tensor product. We will finish this section with a category-theoretic example of this power, after a couple of lemmas.

Lemma 3.30. *Let ${}_R M$ and ${}_R N$ be R-modules. If the covariant functors* $\operatorname{Hom}_R(M, \square)$ *and* $\operatorname{Hom}_R(N, \square)$ *are naturally isomorphic, then $M \cong N$.*

Proof. Let $\tau\colon \operatorname{Hom}(M,\Box) \to \operatorname{Hom}(N,\Box)$ be the posited natural isomorphism. Noting that $\tau_M(1_M)\colon N \to M$, consider the following diagram, which commutes by naturality of τ.

$$\begin{tikzcd}
\operatorname{Hom}(M,M) \arrow[r, "\tau_M"] & \operatorname{Hom}(N,M) \\
\operatorname{Hom}(M,N) \arrow[r, "\tau_N"] \arrow[u, "\tau_M(1_M)^*"] & \operatorname{Hom}(N,N) \arrow[u, "\tau_M(1_M)^*"']
\end{tikzcd}$$

We will use this to show that $\tau_M(1_M)$ is an isomorphism.

The diagram states that for all $\phi \in \operatorname{Hom}(M,N)$, we have

$$\tau_M(\tau_M(1_M) \circ \phi) = \tau_M(1_M) \circ \tau_N(\phi).$$

Note that $\tau_N^{-1}(1_N) \in \operatorname{Hom}(M,N)$, so we will set ϕ to this, and obtain:

$$\tau_M(\tau_M(1_M) \circ \tau_N^{-1}(1_N)) = \tau_M(1_M),$$

whence $\tau_M(1_M) \circ \tau_N^{-1}(1_N) = 1_M$. Showing that the reverse holds may be obtained by replacing the role of $\tau_M(1_M)$ in the above diagram with $\tau_N^{-1}(1_N)$ and going through the same motions. $\Box$

Remark. We proved this in a long-winded way, but this lemma is in fact a special case of the famous Yoneda lemma in category theory.

Lemma 3.31. *The functor* $\operatorname{Hom}_R(R,\Box)\colon {}_R\mathbf{Mod} \to {}_R\mathbf{Mod}$ *is naturally isomorphic to the identity functor. In particular, this means that* $\operatorname{Hom}_R(R,M) \cong M$ *for all* R*-modules* M*.*

Proof. The natural isomorphism $\tau\colon \operatorname{Hom}_R(R,\Box) \to \operatorname{Id}(\Box)$ will be defined by $\tau_M(f) = f(1)$ for some module M. This function is an R-map by virtue of f being an R-map.

We first show that this is indeed an isomorphism. Indeed $\ker \tau_M$ consists of those functions f for which $f(1) = 0$, or in other words $f(r) = f(r1) = rf(1) = 0$, so $\ker \tau_M = 0$, showing injectivity. Furthermore, given some $x \in R$, the function $f_x(r) = rx$ is evidently a map of left R-modules, and $\tau_M(f) = f(1) = x$, so τ_M is surjective too.

We now show naturality. Suppose that we have some map $\phi\colon M \to N$. We must show that the following diagram commutes.

$$\begin{tikzcd}
\operatorname{Hom}(R,M) \arrow[r, "\tau_M"] \arrow[d, "\phi^*"'] & M \arrow[d, "\phi"] \\
\operatorname{Hom}(R,N) \arrow[r, "\tau_N"] & N
\end{tikzcd}$$

Indeed given some $f \in \operatorname{Hom}(R,M)$, we have $\phi(\tau_M(f)) = \phi(f(1))$, and on the other hand. $\tau_N(\phi \circ f) = (\phi \circ f)(1) = \phi(f(1))$. Ergo the diagram commutes, and we are done. $\Box$

Our patience is rewarded with a short and elegant proof.

Proposition 3.32. *For any right* R*-module module* M*, there is an isomorphism* $M \otimes_R R \cong M$*.*

Proof. Note that R is itself an (R,R)-bimodule. Theorem 3.29 and Lemma 3.31 together show that there is a chain of natural isomorphisms of functors:

$$\operatorname{Hom}_R(M \otimes_R R, \Box) \cong \operatorname{Hom}_R(M, \operatorname{Hom}_R(R,\Box)) \cong \operatorname{Hom}_R(M,\Box),$$

after which Lemma 3.30 tells us that $M \otimes_R R \cong M$. $\Box$

Remark. Dually, if N is a left R-module, we of course have $R \otimes_R N \cong N$. Furthermore, the isomorphism is in fact natural in M (dually N), but we would require a stronger version of Lemma 3.30 to show this.

Remark. A less slick but perhaps more informative justification of the above isomorphism can be observed as follows. If we have an element $\tau \in M \otimes_R R$, it is of the form $\tau = m_1 \otimes r_1 + \cdots + m_n \otimes r_n$ for some $m_i \in M$ and $r_i \in R$. Then by bilinearity, $\tau = m_1 r_1 \otimes 1 + \cdots + m_n r_n \otimes 1 = (m_1 r_1 + \cdots + m_n r_n) \otimes 1$, so in fact elements of $M \otimes_R R$ correspond to elements of M.

Another slick proof can be used to show that, just like Hom, the tensor product distributes over direct sums of modules.

Proposition 3.33. *For appropriate modules A, B, and C:*

$$(A \oplus B) \otimes_R C \cong (A \otimes_R C) \oplus (B \otimes_R C).$$

Proof. We will take it for granted that the isomorphisms laid out in Proposition 3.8 are natural. This gives us a chain of natural isomorphisms again:

$$\begin{aligned} & \operatorname{Hom}((A \otimes_R C) \oplus (B \otimes_R C), \square) \\ \cong\ & \operatorname{Hom}(A \otimes_R C, \square) \oplus \operatorname{Hom}(B \otimes_R C, \square) \\ \cong\ & \operatorname{Hom}(A, \operatorname{Hom}(C, \square)) \oplus \operatorname{Hom}(B, \operatorname{Hom}(C, \square)) \\ \cong\ & \operatorname{Hom}(A \oplus B, \operatorname{Hom}(C, \square)) \\ \cong\ & \operatorname{Hom}((A \oplus B) \otimes_R C, \square), \end{aligned}$$

so in fact the claimed isomorphism holds. $\square$

4 Exact Sequences and Functors

Exact sequences are remarkably powerful tools, but it may not be immediately obvious why they are useful. We will use exact sequences a great deal further on, but in this chapter we will merely introduce them with a small amount of motivation, and demonstrate how they interact with the theory of Hom and tensor that we have seen.

As in previous sections, we will assume that R is some ring, with no additional assumptions on it.

4.1 Exact Sequences

Suppose we have a collection of R-modules M_i, indexed by the integers, and connecting maps $\phi_i : M_i \to M_{i-1}$, so that we may draw this diagram[2]:

$$\cdots \xrightarrow{\phi_3} M_2 \xrightarrow{\phi_2} M_1 \xrightarrow{\phi_1} M_0 \xrightarrow{\phi_0} M_{-1} \xrightarrow{\phi_{-1}} M_{-2} \xrightarrow{\phi_{-2}} \cdots$$

We define an exact sequence as a particular such sequence of modules and maps.

Definitions 4.1. A sequence of modules and connecting maps is **exact at** M_i if $\operatorname{im}\phi_{i+1} = \ker\phi_i$. The sequence is called **exact** if it is exact at all M_i.

We will sometimes write only finitely many terms, or seem to omit other indices. Additionally, we will use the same terminology without shoehorning them into the format we laid out above, though it is possible to do so.

Example 4.2. Exact sequences occur outside of algebra, for instance in calculus of several variables. In $\mathbb{R}^3$ for example there is the following exact sequence, modulo some analytic details:

$$\text{Scalar Fields} \xrightarrow{\text{grad}} \text{Vector Fields} \xrightarrow{\text{curl}} \text{Vector Fields} \xrightarrow{\text{div}} \text{Scalar Fields}.$$

This sequence is not always exact in spaces other than $\mathbb{R}^3$, which is a basic observation leading to de Rham cohomology.

Exact sequences seem very abstract at this moment, but we now observe some properties that exact sequences have.

Proposition 4.3. *Let $\phi : M \to N$ be some map. Exactness of the sequences:*

$$0 \longrightarrow M \xrightarrow{\phi} N \qquad \text{and} \qquad M \xrightarrow{\phi} N \longrightarrow 0$$

is equivalent to ϕ being injective and surjective respectively.

Remark. Note that we omitted the labelling of the maps $0 \to M$ and $N \to 0$. There is no need to label them, as each one can only be the zero map $0\colon 0 \to M$ or $0\colon N \to 0$. This notational convention will continue.

Proof. For the first, exactness of the sequence means exactly that $\ker\phi = 0$, or in other words that ϕ is injective. For the second, note that $\ker 0 = N$, so exactness means $N = \operatorname{im}\phi$, that is, ϕ is surjective. ☐

Proposition 4.4. *If the following sequence is exact, then $A \cong \ker\beta$ and $B/\alpha(A) \cong C$:*

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

[2] It might seem strange that the connecting maps ϕ_i are decreasing rather than increasing, but we are introducing this in such a way that chain complexes (which we will meet later) seem more natural.

Proof. We know that α must be injective, so $A \cong \operatorname{im}\alpha$ by the restriction of α to its image. By exactness, we have that $\operatorname{im}\alpha = \ker\beta$, so we have the first part: that $A \cong \ker\beta$. The second part then follows from the first isomorphism theorem – since β is surjective, $C \cong B/\ker\beta = B/\operatorname{im}\alpha = B/\alpha(A)$. □

Example 4.5. Note that the above is necessary, but not sufficient. For example, consider the following non-exact sequence, where we use v_i to denote the ith basis element of the free Abelian group $\mathbb{Z}^{(\mathbb{Z})}$.

$$0 \longrightarrow \mathbb{Z}^{(\mathbb{Z})} \xrightarrow{\alpha} \mathbb{Z}^{(\mathbb{Z})} \xrightarrow{\beta} \mathbb{Z}^{(\mathbb{Z})} \longrightarrow 0$$

In the above sequence, we define:

$$\begin{aligned} \alpha(v_i) &= v_{2i}, \\ \beta(v_i) &= \begin{cases} 0 & \text{if } 2 \nmid i \\ v_i & \text{otherwise.} \end{cases} \end{aligned}$$

This sequence is exact only at the first $\mathbb{Z}^{(\mathbb{Z})}$, despite satisfying the conclusion of the above proposition. In fact, $\operatorname{im}\alpha$ and $\ker\beta$ are completely disjoint!

Definition 4.6. A **short exact sequence** is one of the form:

$$0 \to A \to B \to C \to 0.$$

Note that 'short' does not describe the length of the sequence, as exact sequences with fewer terms are not called short.

Short exact sequences are interesting not only because, as Proposition 4.4 shows, they describe the first isomorphism theorem in some way, but also because we may decompose exact sequences with more elements into a collection of short exact sequences.

Proposition 4.7. *The (finite or infinite) sequence*

$$\cdots \xrightarrow{\phi_2} M_1 \xrightarrow{\phi_1} M_0 \xrightarrow{\phi_0} M_{-1} \xrightarrow{\phi_{-1}} \cdots$$

is exact at M_i if any only if the following is a short exact sequence:

$$0 \longrightarrow \operatorname{im}\phi_{i+1} \hookrightarrow M_i \xrightarrow{\phi_i} \operatorname{im}\phi_i \longrightarrow 0.$$

Proof. The latter sequence is exact when $\operatorname{im}\phi_{i+1} = \ker\phi_i$, or in other words when the former sequence is exact at M_i. □

Let us now use this to prove some small but very useful lemmas about exact sequences, in the case that we are working over a field $R = \Bbbk$ (or when R is a $\Bbbk$-algebra).

Proposition 4.8. *If there is an exact sequence of finite-dimensional vector spaces*

$$0 \longrightarrow V_n \xrightarrow{\phi_n} \cdots \xrightarrow{\phi_1} V_0 \longrightarrow 0,$$

then the following equality holds:

$$\dim V_0 - \dim V_1 + \cdots + (-1)^n \dim V_n = 0.$$

Proof. Proposition 4.7 tells us that we may summarise exactness of the large sequence by exactness of the sequences $0 \to \operatorname{im}\phi_{i+1} \hookrightarrow V_i \to \operatorname{im}\phi_i \to 0$. The rank-nullity theorem applied to $\phi_i \colon V_i \to \operatorname{im}\phi_i$ tells us that $\dim V_i - \dim\operatorname{im}\phi_{i+1} = \dim\operatorname{im}\phi_i$. By a telescoping sum, this shows us that:

$$\sum_{i=0}^{n}(-1)^i \dim V_i + (-1)^{i+1}\dim\operatorname{im}\phi_{n+1} = \dim\operatorname{im}\phi_0,$$

and recognising that ϕ_{n+1} and ϕ_0 are the zero maps, we are done. □

Here is a partial converse to this theorem, which can be very useful.

Proposition 4.9. *Suppose there is sequence of finite dimensional vector spaces:*

$$0 \to V_n \to \cdots \to V_0 \to 0$$

such that, for some $0 \leq m \leq n$,
1. *The sequence is exact at all V_i for $i \neq m$,*
2. *The alternating sum of the dimensions is 0, and*
3. *$\operatorname{im}\phi_{m+i} \subseteq \ker\phi_m$,*

then the sequence is exact everywhere (in particular at V_m).

Proof. We decompose the sequence into two smaller, exact sequences: firstly $0 \to V_n \to \cdots \to V_{m+1} \to \operatorname{im}\phi_{m+1} \to 0$, and also $0 \to \ker\phi_m \hookrightarrow V_m \to \cdots \to V_0 \to 0$. Proposition 4.8 now tells us that:
1. $\dim\operatorname{im}\phi_{m+1} = \sum_{i=m+1}^{n}(-1)^{i-m-1}\dim V_i$, and
2. $\dim\ker\phi_m = (-1)^m\sum_{i=0}^{m}(-1)^i\dim V_i$.

By the second hypothesis, we see that:

$$\begin{aligned} 0 &= \sum_{i=0}^{n}(-1)^i \dim V_i \\ &= \sum_{i=0}^{m}(-1)^i \dim V_i + \sum_{i=m+1}^{n}(-1)^i \dim V_i \\ &= (-1)^m \dim\ker\phi_m + (-1)^{m+1}\dim\operatorname{im}\phi_{m+1}, \end{aligned}$$

so $\dim\ker\phi_m = \dim\operatorname{im}\phi_{m+1}$. Now the third hypothesis and the finite dimension of the spaces involved implies $\ker\phi_m = \operatorname{im}\phi_{m+1}$, and we are done. □

4.2 Exactness of Hom and Tensor

Since exact sequences are, in particular, diagrams, it is a natural question to ask what their images are under some interesting functors. The immediate observation is that exactness may not be preserved under an arbitrary functor.

For example, consider the functor that sends an Abelian group A to the the free Abelian group $\mathbb{Z}^{(A)}$ on its underlying set. The image of the exact sequence of Abelian groups $0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ under this functor, after identifying the groups up to isomorphism, is $\mathbb{Z} \to \mathbb{Z}^2 \to \mathbb{Z}^2 \to \mathbb{Z}$. Inspecting the maps involved, we can see that this is not exact.

More interestingly, consider Hom! Certainly there is an exact sequence of Abelian groups:

$$0 \to 2\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

The image of this under the functor $\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \square)\colon \mathbf{Ab} \to \mathbf{Ab}$ is, after identifying the groups up to isomorphism[3], a sequence $0 \to 0 \to 0 \to \mathbb{Z}/2\mathbb{Z} \to 0$, which simply cannot be exact.

What could be happening here?

Firstly, the free Abelian group functor, defined by sending a set to the free Abelian group on those elements, cannot ever preserve exact sequences since it does not respect the zero map or zero group – we observed this when we defined additive functors (Definition 3.4). The example given reflects this.

The Hom functor is a lot more interesting, as we know it is additive. Whilst we have seen that it does not perfectly preserve exact sequences, note that exactness fails only at the penultimate term. Although trivially so, the sequence is exact everywhere else. This is part of a more important observation: covariant Hom is preserves exact sequences 'on the left'.

Proposition 4.10. *Let M be a module, and let $0 \to A \xrightarrow{i} B \xrightarrow{p} C$ be an exact sequence of modules. Then the sequence $0 \to \mathrm{Hom}(M, A) \to \mathrm{Hom}(M, B) \to \mathrm{Hom}(M, C)$ is exact.*

Proof. Exactness at $\mathrm{Hom}(M, A)$: We need only show that i^* is injective. Indeed since i is injective, if we have $f, g \in \mathrm{Hom}(M, A)$ with $if = ig$, then $if(m) = ig(m)$ implies $f(m) = g(m)$ for all $m \in M$, so indeed $f = g$ ergo i^* is injective too.

$\operatorname{im} i^* \subseteq \ker p^*$: Certainly $p^* i^* = (pi)^* = 0^* = 0$, so we are done.

$\operatorname{im} i^* \supseteq \ker p^*$: Let $f \in \ker p^*$, so $pf = 0$. Then for all $m \in M$, we have $pf(m) = 0$, so there is a unique $b \in B$ with $i(b) = f(m)$. I claim that g defined as sending $m \mapsto b$ is a member of $\mathrm{Hom}(M, B)$, after which $ig = f$ and we are done.

So it remains to show that g is indeed an R-map. Suppose $i(b) = f(m)$ and $i(b') = f(m')$. Then certainly $i(b + b') = f(m) + f(m') = f(m + m')$, so $g(m + m') = g(m) + g(m')$. Similarly $i(rb) = ri(b) = rf(m) = f(rm)$, so $g(rm) = rg(m)$, and we are done. $\square$

As our example showed, the last zero term may not always pull its weight in the image of the sequence, but all the other terms on the left do. We have a name for a functor that behaves like this.

Definition 4.11. A covariant additive functor F is **left exact** if, given a short exact sequence $0 \to A \to B \to C$, the sequence $0 \to F(A) \to F(B) \to F(C)$ is exact.

A contravariant additive functor is **left exact** if it sends the exact sequence $A \to B \to C \to 0$ to an exact sequence $0 \to F(C) \to F(B) \to F(A)$.

Restated in these terms, the previous proposition shows that covariant Hom is left exact. What about contravariant Hom?

Proposition 4.12. *For any module N, the contravariant functor $\mathrm{Hom}(\square, N)$ is left exact.*

Proof. Let $A \xrightarrow{i} B \xrightarrow{p} C \to 0$ be a short exact sequence.

Exactness at $\mathrm{Hom}(C, N)$: We need to show that p_* is injective. Suppose $f \in \mathrm{Hom}(C, N)$ has $fp = 0$. If it were the case that $f \neq 0$, we would have $f(c) \neq 0$ for some $c \in C$, and the surjectivity of p tells us that $c = p(b)$ for some $b \in B$, so in total $fp(b) = f(c) \neq 0$, which cannot be true. So indeed $f = 0$ and p_* is injective.

$\operatorname{im} p_* \subseteq \ker i_*$: Indeed $i_* p_* = (pi)_* = 0_* = 0$, so we are done.

$\operatorname{im} p_* \supseteq \ker i_*$: Suppose $fi = 0$ for some $f \in \mathrm{Hom}(B, N)$. If $c \in C$, then there is some (not necessarily unique) $b \in B$ with $p(b) = c$. I claim that $g(c) = f(b)$ defines a member of $\mathrm{Hom}(C, N)$, after which it is clear that $gp = f$.

Firstly we show that g is well-defined. Suppose b and b' both have $p(b) = p(b') = c$. Then note that $p(b - b') = 0$, so by exactness $b - b' \in \operatorname{im} i$, so $f(b - b') = 0$, ergo $f(b) = f(b')$, and g is well-defined.

[3] We can see that $\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) = 0$ since $f(1)$ must be of finite order, and there is no such element in $\mathbb{Z}$. It is then routine to check that there are only two elements of $\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$.

We now only need to show that g is indeed an R-map. Let $c, c' \in R$ have $p(b) = c$ and $p(b') = c'$. Then $p(b + b') = c + c'$, so $g(c + c') = g(c) + g(c')$. Similarly $p(rb) = rp(b) = rc$, so $g(rc) = f(rb) = rf(b) = rg(c)$. $\square$

Remark. In the previous two propositions, we did not specify what category the functors map into, though of course their inputs come from ${}_R\mathbf{Mod}$ or $\mathbf{Mod}_R$ – in previous propositions (for instance Proposition 3.3 and Corollary 3.21) we showed that it could take values in $\mathbf{Ab}$ or even ${}_S\mathbf{Mod}$ if its second argument is a bimodule.

In fact, it is not terribly important provided that we know it at least maps into $\mathbf{Ab}$, since if a sequence is exact when viewed as a sequence of Abelian groups, then it is exact when viewed as, for example, a sequence in ${}_S\mathbf{Mod}$. For this reason Hom is exact when mapping into any categories of modules that we have previously seen it may.

A similar fact is, as expected, true for the tensor product. But first a useful lemma and another definition.

Lemma 4.13. *Suppose we have maps $i\colon A \to B$ and $p\colon B \to C$, and for any module N, the sequence:*

$$0 \to \mathrm{Hom}(C, N) \xrightarrow{p_*} \mathrm{Hom}(B, N) \xrightarrow{i_*} \mathrm{Hom}(A, N)$$

is exact. Then the following sequence is exact:

$$A \xrightarrow{i} B \xrightarrow{p} C \to 0.$$

Proof. Exactness at C: We must show that p is surjective. Set $N = C/\operatorname{im} p$. Then the natural map $\nu\colon C \to C/\operatorname{im} p$ is certainly an element of $\mathrm{Hom}(C, N)$, meaning that $p_*(\nu) = 0$. But we know that p_* is injective, so $\nu = 0$ and so $\operatorname{im} p = C$.

$\operatorname{im} i \subseteq \ker p$: Set $N = C$. Then certainly $1_C \in \mathrm{Hom}(C, N)$, so recalling that $(pi)_* = 0$, we have $0 = (pi)_a st(1_C) = 1_C pi = pi$.

$\operatorname{im} i \supseteq \ker p$: Set $N = B/\operatorname{im} i$. Once again the map $\nu\colon B \to B/\operatorname{im} i$ is a member of $\mathrm{Hom}(B, N)$, and since $i_*(\nu) = \nu i = 0$, there must be some $f \in \mathrm{Hom}(C, N)$ with $\nu = p_*(f) = fp$. Now assume for contradiction that there is some element $b \in \ker p \setminus \operatorname{im} i$. This would mean that $fp(b) = f(0) = 0$, but conversely $\nu(b)$ nonzero – a contradiction which finishes the proof. $\square$

Definition 4.14. A covariant additive functor F is **right exact** if, given a short exact sequence $A \to B \to C \to 0$, the sequence $F(A) \to F(B) \to F(C) \to 0$ is exact.

A contravariant additive functor is **right exact** if it sends the exact sequence $0 \to A \to B \to C$ to an exact sequence $F(C) \to F(B) \to F(A) \to 0$.

Proposition 4.15. *For any right R-module M, the functor $M \otimes_R \square$ is right exact.*

Proof. We give a very slick proof using Proposition 3.27 combined with the previous lemma.

Let $A \to B \to C \to 0$ be an exact sequence of left R-modules, and let N be any Abelian group. Recall that every left R-module is also a $(R, \mathbb{Z})$-bimodule, and so by the Hom-tensor adjunction, there is a natural isomorphism $\mathrm{Hom}_{\mathbb{Z}}(M \otimes_R \square, C) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(\square, C))$. In particular, the following diagram commutes, where the horizontal maps are taken from the posited exact sequence and the vertical ones are the natural isomorphisms:

$$\begin{array}{ccccccc}
0 \longrightarrow & \mathrm{Hom}(M \otimes_R C, N) & \longrightarrow & \mathrm{Hom}(M \otimes_R B, N) & \longrightarrow & \mathrm{Hom}(M \otimes_R A, N) \\
& \downarrow & & \downarrow & & \downarrow \\
0 \longrightarrow & \mathrm{Hom}(M, \mathrm{Hom}(C, N)) & \longrightarrow & \mathrm{Hom}(M, \mathrm{Hom}(B, N)) & \longrightarrow & \mathrm{Hom}(M, \mathrm{Hom}(A, N))
\end{array}$$

Observe that the top row is exact if and only if the bottom row is too. Observe also that the bottom row is the image of the posited exact sequence under the composed functor $\mathrm{Hom}(M, \Box) \circ \mathrm{Hom}(\Box, N)$. Since both $\mathrm{Hom}(M, \Box)$ and $\mathrm{Hom}(\Box, N)$ are left exact as well as being co- and contravariant respectively, their composition is also left exact. Hence the bottom row is exact, meaning the top row is too, and so we are done. $\Box$

5 Projective, Injective, and Flat Modules

We already know that free modules are an important class of modules, and their universal property makes them very useful. However, somehow they are difficult to use, as in the universal property, we make reference to a completely different category – the category of sets. A question may be posed: can we describe free modules totally in terms of maps and modules, rather than their elements?

Trying to answer this question will lead us to a far more fruitful idea: that of a projective module.

5.1 Projective Modules and Bases

We will waste no time in defining projective modules.

Definition 5.1. A module P is **projective** if, given a surjection $p\colon A \to B$ and a map $f\colon P \to B$, there is a (not necessarily unique) map $g\colon P \to A$ with $pg = f$. This may be summarised with the following diagram with exact rows:

$$\begin{tikzcd} & P \arrow[dl, dashed, "g"'] \arrow[d, "f"] & \\ A \arrow[r, "p"'] & B \arrow[r] & 0. \end{tikzcd}$$

Proposition 5.2. *Free modules are projective.*

Proof. Let $P = R^{(X)}$ be a free module with basis elements from the set X. Let $p\colon A \to B$ be a surjection and let $f\colon R^{(X)} \to B$. By surjectivity, choose an element a_x in A with $p(a_x) = f(v_x)$, where v_x is some basis element of $R^{(X)}$. The function $g(v_x) = a_x$ is a well-defined R-map, and certainly $pg = f$, so we are done. $\square$

This last proposition is instructive. At its core is the idea that free modules have a basis, but at no point did we require that the basis elements uniquely define an element – except perhaps when we defined g. This observation leads to a different definition.

Definition 5.3. A **projective basis** for a left R-module M is a set $V \subset M$ together with R-maps $f_v\colon M \to R$ corresponding to each $v \in V$ such that:

(1) For all $m \in M$, all $f_v(m) = 0$ for all but finitely many V, and

(2) $m = \sum_{v \in V, f_v(m) \neq 0} f_v(m)v$.

Lemma 5.4. *A module M has a projective basis if and only if there is a free module F such that there are maps $p\colon F \to M$ and $f\colon M \to F$ with $pf = 1_M$.*

Proof. If an R-module has a projective basis X with associated maps f_x, we let $F = R^{(X)}$, and define $p(v_x) = x$ and $f(m) = \sum_{x \in X} f_x(m)v_x$, the latter of which is well-defined since $f_x(m) = 0$ for all but finitely many x. The definition of a projective basis then guarantees that $pf = 1_M$.

Conversely, let $F = R^{(X)}$ for some set X. Define the maps $\iota_x\colon R \to R^{(X)}; r \mapsto rv_x$ and $\pi_x\colon R^{(X)} \to R; r_x \mapsto 1$ and $r_y \mapsto 0$ for $y \neq x$. We define the projective basis of M as the elements $u_x = p\iota_x(1)$, and the associated maps as $f_{u_x} = \pi_x f$, which we now prove are suitable.

Certainly $f_{u_x}(m) = 0$ for all but finitely many u_x, since otherwise $f(m) \in R^{(X)}$ cannot be, as it is a finite sum of basis elements of $R^{(X)}$. Now that the sum is well-defined, we can calculate for some $m \in M$:

$$\begin{aligned}
\sum_{x\in X} f_{u_x}(m)u_x &= \sum_{x\in X} \pi_x f(m)\cdot p\iota_x(1) \\
&= \sum_{x\in X} p\iota_x(\pi_x f(m)) \\
&= p\left(\sum_{x\in X} \iota_x\pi_x f(m)\right) \\
&= pf(m) = m.
\end{aligned}$$

So u_x is indeed a projective basis for M. □

Proposition 5.5. *A module is projective if and only if it has a projective basis.*

Proof. Suppose M is a projective module. Certainly there is some surjection $p\colon F \mapsto M$ where F is free – we may take $F = R^{(M)}$. The definition of a projective module then provides a map f making the following diagram commute:

$$\begin{tikzcd}
 & P \arrow[dl, dashed, "f"'] \arrow[d, "1_M"] & \\
F \arrow[r, "p"'] & M \arrow[r] & 0
\end{tikzcd}$$

Ergo, by the previous lemma, there is a projective basis.

Conversely, suppose M has a projective basis, so letting $p\colon F \to M$ and $f\colon M \to F$ be as in the previous lemma, for some appropriate maps $q\colon A \to B$ and $g\colon M \to B$, we have the following diagram, where the existence of the map h is guaranteed by the projectivity of free modules:

$$\begin{tikzcd}
F \arrow[r, "p"] \arrow[d, dashed, "h"'] \arrow[dr, "gp"] & M \arrow[d, "g"] & \\
A \arrow[r, "q"'] & B \arrow[r] & 0
\end{tikzcd}$$

Now $qh = gp$, but this means that $q(hf) = gpf = g$, so hf is the map that shows M to be projective. □

Example 5.6. We can use this to prove that $\mathbb{Q}$ is not a projective $\mathbb{Z}$-module. Suppose for contradiction that there is a projective basis consisting of elements $v_i \in \mathbb{Q}$ and additive maps $f_i\colon \mathbb{Q} \to \mathbb{Z}$. Note that if it were the case that $m = f_i(q) \neq 0$ for some $q \in \mathbb{Q}$, then there is some prime p with $p \nmid m$. However we see that $pf_i(q/p) = m$ by additivity, so in fact $p \mid m$. This means that $f_i = 0$ for all i, and so requirement (2) of a projective basis cannot be satisfied in any case. Hence $\mathbb{Q}$ is not projective.

Remark. The argument in the above example can be modified to show that if R is a unique factorisation domain which is not a field, then the field of fractions of R is not a projective R-module.

This allows us to describe the connection between free and projective modules in a very concrete way.

Proposition 5.7. *A module is M is projective if and only if it is a direct summand of a free module. That is, if and only if there exists a module N such that $M \oplus N$ is isomorphic to a free module.*

Proof. We will make use of Proposition 5.5 and Lemma 5.4 in both directions of this proof.

Suppose M is projective, so let $p\colon F \to M$ and $f\colon M \to F$ be as in the lemma. I claim that $F = \operatorname{im} f \oplus \ker p$. Certainly $\operatorname{im} f \cap \ker p = 0$, since $pf(m) = 0$ implies $m = pf(m) = 0$, so the sum must be direct. Furthermore if $v \in F$, then $p(v - fp(v)) = p(v) - p(v) = 0$, so since $v = (v - fp(v)) + fp(v)$, $F = \operatorname{im} f + \ker p$. Since f is injective (it has a left inverse) $M \cong \operatorname{im} f$, and we are done.

Conversely, suppose $\eta\colon M \oplus N \to F$ is an isomorphism, where F is free. Then $f\colon M \to F$ defined by $f(m) = \eta(m, 0)$ and $p\colon F \to M$ defined by $p = \pi_M \eta^{-1}$ (where $\pi_M(m, n) = m$) satisfies $pf = 1_M$, and so by Lemma 5.4 we are done. ☐

Example 5.8. This leads to a clever observation: a module P is projective if and only if there is a free module F such that $P \oplus F$ is free. The proof of this goes as follows: there is certainly a module Q such that $P \oplus Q$ is free, so then set

$$F = (Q \oplus P) \oplus (Q \oplus P) \oplus \cdots ,$$

which is certainly free. We then have:

$$P \oplus F = P \oplus \big((Q \oplus P) \oplus \cdots\big) = (P \oplus Q) \oplus (P \oplus Q) \oplus \cdots = F \oplus F \oplus \cdots .$$

This trick is delightfully known as the Eilenberg–Mazur swindle.

This proposition is a breath of fresh air – it allows us to start giving some concrete examples of projective modules, and how they differ from free modules, as well as allowing us to prove some convenient facts about them.

Corollary 5.9. *The direct sum of projective modules is also projective.*

Proof. Suppose P, Q are projective. Then there exist P', Q' such that $P \oplus P'$ and $Q \oplus Q'$ are free, so in turn $(P \oplus P') \oplus (Q \oplus Q') \cong (P \oplus Q) \oplus (P' \oplus Q')$ is free, and hence $P \oplus Q$ is projective (being a direct summand of a free module). ☐

Example 5.10. If we take as granted that a subgroup of a free Abelian group is itself free Abelian (this is not at all easy), then we see that every projective $\mathbb{Z}$-module, being a subgroup of a free Abelian group, is itself free. Hence the two notions – free and projective – coincide in the category of $\mathbb{Z}$-modules.

Example 5.11. The same cannot be said for other rings. The simplest examples can be found in quotient rings of $\mathbb{Z}$: working in the ring $R = \mathbb{Z}/6\mathbb{Z}$, the free module on one generator (the ring itself) is isomorphic to $3\mathbb{Z}/6\mathbb{Z} \oplus 2\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Both of these summands are therefore projective when we see them as R-modules, though they are certainly not free, since both of them are smaller than the smallest nonzero free R-module!

For an example of a collection of non-trivial projective modules over a more complicated ring, see Appendix A.1.

5.2 Injective Modules

When we have a definition of an object that is entirely diagrammatic, a natural consequence in the land of categories is to consider what happens when one reverses the arrows, thus considering the same property in the dual category. We have already seen projective modules defined diagrammatically, so by reversing the arrows, we obtain a new and interesting definition.

Definition 5.12. A module E is **injective** if, given an injection $i\colon A \to B$ and a map $f\colon A \to E$, there is a (not necessarily unique) map $g\colon B \to E$ with $gi = f$. This may be summarised with the following diagram with exact rows:

$$\begin{tikzcd} & E & \\ 0 \arrow[r] & A \arrow[u, "f"] \arrow[r, "i"] & B \arrow[ul, dashed, "g"'] \end{tikzcd}$$

Injective modules, unlike projective ones, are much harder to find. It will take considerable work to produce the first examples of injective modules.

We begin with some simple facts about injective modules.

Proposition 5.13. *If E_i is an injective module for all $i \in I$, then the product $\prod_{i\in I} E_i$ is injective also.*

Proof. Let $j\colon A \to B$ be an injection and let $f\colon A \to E = \prod_{i\in I} E_i$ be given. We may then decompose f into its constituent parts $f_i\colon A \to E_i$, which extend to maps $g_i\colon B \to E_i$ with $f_i = g_i j$ by the injectivity of E_i. But then the map $g\colon B \to E$ given by $g(b) = (f_i(b))_{i\in I}$ extends f and we are done. □

Proposition 5.14. *A direct summand of an injective module is also injective.*

Proof. Let $E = E_0 \oplus E_1$ be an injective module. Let $i\colon A \to B$ be an injection, let $f\colon A \to E_0$ be any map, and consider the following diagram, where $j\colon E_0 \to E$ is the inclusion and $p\colon E \to E_0$ is the projection with $pj = 1_{E_0}$.

$$\begin{tikzcd} & E_0 \arrow[r, hook, shift left, "j"] & E \arrow[l, shift left, "p"] \\ 0 \arrow[r] & A \arrow[u, "f"] \arrow[r, "i"] & B \arrow[u, dashed, "g"'] \end{tikzcd}$$

Since E is injective, we know there is a map g with $gi = jf$, and so we see that $(pg)i = pjf = f$, so E_0 is also injective. □

The following theorem is an important result that will allow us to investigate injective modules much more easily, by focusing our attention upon ideals of the ring over which we work.

Theorem 5.15 (Baer's Criterion)**.** *A left R-module E is injective if and only if for every left ideal I of R and map $f\colon I \to E$, there is some $g\colon R \to E$ with $g\big|_I = f$. The same is true for right R-modules. This may be summarised with the following diagram:*

$$\begin{tikzcd} E & \\ I \arrow[u, "f"] \arrow[r, hook] & R \arrow[ul, dashed, "g"'] \end{tikzcd}$$

Proof. The criterion is evidently necessary for E to be injective, so we prove sufficiency. In the definition of an injective module, we may assume that $A \le B$, so that we may omit the injective map. Let $f\colon A \to E$ be given. We wish to find a map $g\colon B \to E$ with $g\big|_B = f$.

Define a poset $\mathcal{A}$ consisting of pairs (A', g') with $A \le A' \le B$ and $g'\colon A' \to E$ such that $g'\big|_A = f$. Define the order as $(A', g') \preceq (A'', g'')$ when $A' \le A''$ and $g''\big|_{A'} = g'$. Now we consider Zorn's lemma. If we have a chain $C \subseteq \mathcal{A}$, we may find an upper bound (A', g') by letting A' be the union of all modules in C, and letting g' be the union of all the maps, where we see functions as sets. This can be seen to be well-defined and an upper bound. We use Zorn's lemma to infer that within $\mathcal{A}$ there is some maximal element (A_0, g_0).

If $A_0 = B$, then we are done, so assume there is some $b \in B \setminus A_0$. Consider the set:

$$I = \{r \in R \mid rb \in A_0\}.$$

We claim that I is a left ideal of R. Certainly it is closed under addition, since if $rb, r'b \in A_0$ then $(r + r')b = rb + r'b \in A_0$, and it is closed under left multiplication since A_0 is a submodule of B. Define the map $\bar{f}: I \to E$ by $\bar{f}(r) = g_0(rb)$. It is clear that this is an R-map, and by assumption there is some map $\bar{g}$ for which the following diagram commutes:

$$\begin{tikzcd}
E & \\
I \arrow[u, "\bar{f}"] \arrow[r, hook] & R \arrow[ul, dashed, "\bar{g}"']
\end{tikzcd}$$

Now we approach the contradiction. Define $A_1 = A_0 + Rb$, and the map $g_1: A_1 \to E$ by

$$g_1(a_0 + rb) = g_0(a_0) + \bar{g}(r), \text{ where } a_0 \text{ is some element of } A_0.$$

We must show that g_1 is well-defined by the above formula. If $a + rb = a' + r'b$, then $a - a' = (r' - r)b \in A_0$, so $r - r' \in I$, and so $g_0(a - a') = g_0((r' - r)b) = \bar{f}(r' - r) = \bar{g}(r' - r)$ Ergo $g_0(a) + \bar{g}(r) = g_0(a') + \bar{g}(r')$, so the map is well-defined.

Note then that $(A_0, g_0) \prec (A_1, g_1)$, contradicting the supposed maximality of the former. Hence we conclude that A_0 was equal to B all along, and we are done. ☐

These facts about injective modules are certainly nice, but we have yet to see a single example of an injective module. We will now introduce some machinery to produce such an example.

Definition 5.16. Let r be an element of a ring R and let a be an element of a left R-module M. We say that a is **divisible by** r if there is some $b \in M$ such that $rb = a$.

We would like to consider modules in which every element is divisible by every nonzero element $r \in R$, but this is flawed, as zero divisors may exist. For instance, if $sr = 0$ despite $r, s \neq 0$, and $a \in M$, then if $sm \neq 0$, certainly m cannot be divisible by r, since if $rn = m$ we have $0 \neq sm = (sr)m = 0m = 0$, which cannot be. Following the example of [Lam99], we use this observation to make a definition.

Definition 5.17. A left R-module M is **divisible** when, given some $m \in M$ and $r \in R$, if we have that $xr = 0$ implies $xm = 0$ for all $x \in R$, we have that m is divisible by r. Written symbolically:

$$\text{If } \forall x \in R,\ xr = 0 \Rightarrow xm = 0, \text{ then } m \text{ is divisible by } r.$$

Remark. If R is a domain, then this definition simply states that every element $m \in M$ is divisible by every nonzero element of r. If we assume that R is commutative, then we see that $\mathrm{Frac}(R)$ is an example of a divisible R-module, since we may simply divide by any nonzero scalar.

Proposition 5.18. *For a commutative domain R, the field of fractions $\mathrm{Frac}(R)$ is an injective R-module.*

Proof. By Baer's criterion (Theorem 5.15) we may restrict our attention to extending maps $f: I \to \mathrm{Frac}(R)$ from left ideals I of R to maps $g: R \to \mathrm{Frac}(R)$, so we assume such a situation.

Suppose $f: I \to \mathrm{Frac}(R)$ is given. If $I = 0$, then $f = 0$ so we may safely set $g = 0$ and be done. We now turn to nonzero ideals. Note that for any nonzero $a, b \in I$, we have $af(b) = f(ab) = bf(a)$, since R is a commutative domain. However this means that $f(a)/a = f(b)/b$. Call this common value c (which must exist, as there is at least one nonzero element of I).

Now we define $g(r) = rc$. This is an R-map that extends f since if $r \in I$, then $c = f(r)/r$ so $g(r) = rf(r)/r = f(r)$, so we are done. ☐

A stronger assumption on the ring produces a stronger result on the characterisation of injective modules.

Proposition 5.19. *Over a principal ideal domain R, every divisible module is injective.*

Proof. We use Baer's criterion (Theorem 5.15) again. Let E be some divisible R-module, let $I = Rx$ where $x \neq 0$ be some ideal (which is principal by assumption) and let $f\colon I \to E$ be given. By the divisibility of E, there is some $e \in E$ with $f(x) = xe$. Letting $g(r) = re$ then extends f, since if $s \in Rx$ then $s = s'x$ for some $s' \in R$, so $g(s) = s'xe = s'f(x) = f(s'x) = f(s)$, and we are done. $\square$

Examples 5.20. We can now give quite a few examples of injective modules.

- Since $\mathbb{Z}$ is a commutative principal ideal domain, we have that $\operatorname{Frac}\mathbb{Z} = \mathbb{Q}$ is an injective $\mathbb{Z}$-module.
- It is not difficult to see that both direct sums and quotients of divisible modules are divisble, hence any $\mathbb{Q}$-vector space is injective over $\mathbb{Z}$, and the quotient $\mathbb{Q}/\mathbb{Z}$ is injective too.
- Let $\Bbbk$ be any field. Recalling that $\Bbbk[x]$ is a commutative principal ideal domain, we see that $\Bbbk(x) = \operatorname{Frac}(\Bbbk[x])$ is an injective $\Bbbk[x]$-module.

Example 5.21. The **character module** of an Abelian group G is defined as $G^* = \operatorname{Hom}_{\mathbb{Z}}(G, \mathbb{R}/\mathbb{Z})$. A natural question to ask is whether or not the character module is trivial for any nonzero group G. We may use injectivity of $\mathbb{R}/\mathbb{Z}$ to show that this is not the case – note indeed that the group above is an injective $\mathbb{Z}$-module since $\mathbb{R}$ is a $\mathbb{Q}$-vector space and we then take a quotient, preserving divisibility.

Let $a \in G$ be some nonzero element. We will show that there is some $g \in G^*$ with $g(a) \neq 0 \in \mathbb{R}/\mathbb{Z}$, by the following diagram:

$$\begin{tikzcd} & \mathbb{R}/\mathbb{Z} & \\ 0 \arrow[r] & \mathbb{Z}a \arrow[u, "f(a)"] \arrow[r, hook] & G \arrow[ul, dashed, "g"'] \end{tikzcd}$$

If a is of infinite order, we set $f(a) = \pi + \mathbb{Z}$ (though any irrational in place of π also works), and if a is of finite order n, we set $f(a) = 1/n + \mathbb{Z}$. The map f is then seen to be a $\mathbb{Z}$-map, and so an extension g exists which necessarily has $g(a) = f(a) \neq 0$.

Note that this proof is very much non-constructive, essentially due to our reliance on Zorn's lemma in the proof of Baer's criterion. It may be very hard in general to describe such a map g.

Our reliance on Zorn's famous result is not incidental. In fact the injectivity of divisible $\mathbb{Z}$-modules is equivalent to the axiom of choice [Bla79, Theorem 2.1], and the very existence of any injective $\mathbb{Z}$-module is not demonstrable in the absence of choice [Bla79, Theorem 3.1].

5.3 Split Exact Sequences

In Section 4, we saw how short exact sequences can be thought of as a quotient of one module by the image of another. In this way, the most generic form of a short exact sequence is $0 \to K \hookrightarrow M \to M/K \to 0$, where the penultimate arrow is the natural map. One might say that, in some way, M is a combination of K and M/K – but can we determine M if we are given the other modules' values?

The answer to this question is a firm 'no', as these two short exact sequences of Abelian groups demonstrate:

$$0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{n \mapsto (n,0)} (\mathbb{Z}/2\mathbb{Z})^2 \xrightarrow{(n,m) \mapsto m} \mathbb{Z}/2\mathbb{Z} \to 0$$

$$0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{n \mapsto 2n} \mathbb{Z}/4\mathbb{Z} \xrightarrow{m \mapsto m} \mathbb{Z}/2\mathbb{Z} \to 0$$

We have terminology for the modules that occur in the middle of these sequences.

Definition 5.22. If there is an exact sequence $0 \to A \to B \to C \to 0$, then B is known as an **extension** of C by A.

We will now characterise when an exact sequence reveals an extension to be nothing more than $A \oplus C$.

Proposition 5.23 (The splitting lemma)**.** *Let there be a short exact sequence of left R-modules:*
$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0.$$
Then the following are equivalent:

(1) There exists a map $q\colon B \to A$ with $qi = 1_A$,

(2) There exists a map $j\colon C \to B$ with $pj = 1_C$, and

(3) There is an isomorphism $\eta\colon B \to A \oplus C$ such that the following diagram commutes:

$$\begin{tikzcd} A \arrow[r, "i"] \arrow[d] & B \arrow[r, "p"] \arrow[d, "\eta"] & C \arrow[d] \\ A \arrow[r] & A \oplus C \arrow[r] & C \end{tikzcd}$$

Proof. We show each implication in order.
(1) $\Rightarrow$ (2): Let $c \in C$, and observe that, since p is a surjection, there is some (not necessarily unique) $b \in B$ with $p(b) = c$. I now claim that $j(c) = b - iq(b)$ is a well-defined function, and in particular the map we're looking for.

Firstly we show that this is independent of choice of b. If b and b' both have $p(b) = p(b') = c$, then observe that $p\left((b - iq(b)) - (b' - iq(b'))\right) = c - c = 0$, so by exactness there is a unique $a \in A$ with $i(a) = (b - iq(b)) - (b' - iq(b')) = (b - b') - iq(b - b')$. Let $x = a + q(b - b')$, and observe that $b - b' = i(x) = i(a + q(b - b')) = i(a + qi(x)) = i(a + x)$, so by injectivity, $x = a + x$, and $a = 0$, so $i(a) = 0$ too, ergo $b - iq(b) = b' - iq(b')$.

The fact that i is an R-map may be seen that if $p(b) = c$, then $p(rb) = rc$, and so $j(rc) = rb - iq(rb) = rj(c)$, and in addition if $p(b') = c'$, then $j(c+c') = (b+b') - iq(b+b') = j(c) + j(c')$.
(2) $\Rightarrow$ (3): Suppose b is some element of B. Then $b = (b - jp(b)) + jp(b)$, so seeing that $b - jp(b) \in \ker p$, we conclude that $b \in \ker p + \operatorname{im} j$ – that is, $B = \ker p + \operatorname{im} j$.

Furthermore, suppose that $b \in \ker p \cap \operatorname{im} j$, which is to say that $p(b) = 0$ and $j(c) = b$ for some appropriate $c \in C$. However, this means that $c = pj(c) = p(b) = 0$, so in fact $b = 0$. In summary, the sum is in fact direct: $B = \ker p \oplus \operatorname{im} j$.

Recalling that i is injective, we see that $\ker p = \operatorname{im} i \cong A$, and similarly j is injective (since it has a left inverse in p) so $\operatorname{im} j \cong C$. So, $B \cong A \oplus C$.
(3) $\Rightarrow$ (1): It is easy to see that the map $j = \eta^{-1}\pi$ is appropriate, where we define $\pi(c)$ as $(0, c)$. $\square$

The splitting lemma above was proved by a technique which is called **diagram chasing**, characterised by references to elements existing due to exactness. This proof method is both highly mechanical, and highly useful in homological algebra as a whole, due to a result we will discuss later called Mitchell's full embedding theorem (Theorem 6.22). We will perform more diagram chases in coming chapters.

If we generalise the notion of a short exact sequence to all groups (since kernels and images work there too) rather than just modules, a short exact sequence being split shows that the middle group is a semidirect product of the other two. For this reason it is notable that the splitting lemma only holds in the context of modules rather than the more general context of arbitrary groups, although the technique of diagram chasing discussed above does often work in the context of groups.

The definitions of projective and injective modules give us an interesting observation.

Proposition 5.24. *Any short exact sequence that begins with an injective module or ends in a projective module splits.*

Proof. In the injective case, the following diagram and the splitting lemma proves the proposition, since we find a map q with $iq = 1_A$:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "i"] \arrow[d, "1_A"'] & B \arrow[r, "p"] \arrow[dl, dashed, "q"] & C \arrow[r] & 0 \\
& A & & &
\end{tikzcd}$$

In the projective case, the following diagram suffices similarly:

$$\begin{tikzcd}
& & & C \arrow[d, "1_C"] \arrow[dl, dashed, "j"'] & \\
0 \arrow[r] & A \arrow[r, "i"'] & B \arrow[r, "p"'] & C \arrow[r] & 0
\end{tikzcd}$$

We have found the maps we needed, so we are done. ☐

Remark. This lemma gives us an alternative proof of one direction Proposition 5.7: that any projective module is a direct summand of a free module. Certainly any module is the quotient of a free module, which gives us a short exact sequence with a projective module at the end and a free module in the middle. Then from Proposition 5.24 the result follows immediately.

An unsurprising converse also holds true.

Proposition 5.25. *A module M is projective if and only if every short exact sequence ending with M splits.*

Proof. Proposition 5.24 shows one direction, so we are left with the other.

Now choose any representation of M as a quotient of a free module, hence finding M to be a direct summand of a free module, after which Proposition 5.7 finishes things. ☐

There is a similar fact that holds for injective modules, namely Proposition 5.31, but we need to develop a bit more before we can show it.

There are further connections between exact sequences and these kinds of modules, namely how Hom interacts with them. In Section 4 we noted that both covariant and contravariant Hom are left exact. We shall show that injective and projective modules somehow repair the exactness of Hom, so that they preserve exact sequences entirely.

Definition 5.26. A functor is **exact** if it preserves exactness of short exact sequences.

Proposition 5.27. *A module M is projective if and only if* $\operatorname{Hom}(M, \square)$ *is exact, and a module N is injective if and only if* $\operatorname{Hom}(\square, N)$ *is exact.*

Proof. Propositions 4.10 and 4.12 show that we can focus our attention on exactness at the last term only, which is what we do.

We need to show that projectivity is equivalent to a surjection $p\colon B \to C$ inducing a surjection $p^*\colon \operatorname{Hom}(M, B) \to \operatorname{Hom}(M, C)$. Indeed the definition of a projective modules requires there to exist a map $h \in \operatorname{Hom}(M, B)$ with $hp = f$ for all $f \in \operatorname{Hom}(M, C)$, which is a restatement of the surjectivity of p^*.

In the injective case, we must show that an injection $i\colon A \to B$ induces a surjection $i_*\colon \operatorname{Hom}(A, N) \to \operatorname{Hom}(B, N)$, and just as before this is precisely what the definition states. ☐

5.4 The Existence of Enough Injectives

We have seen several times that every module is the quotient of a free module. In particular, there is a quotient $R^{(M)} \to M$. This is usually described by saying that the category of R-modules has 'enough projectives,' and we will discuss exceptions to this briefly in Section 6.3.

Since injective modules are dual to projectives in the sense that we define them by reversing the arrows in the diagrammatic definition, we may suspect that there are 'enough injectives' in the sense that every R-module may be *embedded* within an injective module, dually to being a quotient. Indeed this is true, and we work to show that this is the case now.

Proposition 5.28. *Every $\mathbb{Z}$-module may be embedded in an injective $\mathbb{Z}$-module.*

Proof. Recall that Propositions 5.18 and 5.19 show that, as $\mathbb{Z}$-modules, quotients of $\mathbb{Q}$-vector spaces are injective, as $\mathbb{Q}$-vector spaces are divisible and so are their quotients. Since any $\mathbb{Z}$-module M may be presented as a quotient of a free module, we have for some appropriate module K:

$$M \cong \left(\bigoplus_{m \in M} \mathbb{Z} \right) \Big/ K \leq \left(\bigoplus_{m \in M} \mathbb{Q} \right) \Big/ K.$$

The latter module is injective, so we are done. $\square$

This shows that the category of $\mathbb{Z}$-modules has enough injectives, but we want the same result for all rings, so we must press on.

Lemma 5.29. *If E is an injective $\mathbb{Z}$-module, and R is any ring, then $\operatorname{Hom}_{\mathbb{Z}}(R, E)$ is an injective left R-module, where the module structure of Hom is defined as in Proposition 3.20.*

Proof. In order to prove that $M = \operatorname{Hom}_{\mathbb{Z}}(R, E)$ is injective, it suffices by Proposition 5.27 to show that $\operatorname{Hom}_R(\square, M)$ is exact. As functors, we have the following natural isomorphisms:

$$\begin{aligned} \operatorname{Hom}_R(\square, \operatorname{Hom}_{\mathbb{Z}}(R, E)) &\cong \operatorname{Hom}_{\mathbb{Z}}(\square \otimes_R R, E) && \text{by Proposition 3.29,} \\ &\cong \operatorname{Hom}_{\mathbb{Z}}(\square, E) && \text{consequence of Proposition 3.32.} \end{aligned}$$

By Proposition 5.27, we know that the latter functor is exact since E is an injective $\mathbb{Z}$-module. Hence we conclude that $\operatorname{Hom}_{\mathbb{Z}}(R, E)$ is injective as an R-module. $\square$

Naturally, the same holds for right R-modules, as we may take the opposite modules and rings.

Finally we are prepared to show the existence of enough injectives for modules over an arbitrary ring.

Theorem 5.30. *Any R-module can be embedded in an injective R-module.*

Proof. We show this for left R-modules only, as the right-sided case follows thereafter.

Let M be a left R-module. Momentarily, view M as a $\mathbb{Z}$-module ${}_{\mathbb{Z}}M$, and via Proposition 5.28, let E be an injective $\mathbb{Z}$-module containing ${}_{\mathbb{Z}}M$. We have an inclusion $i \colon {}_{\mathbb{Z}}M \to E$.

Consider the map $j \colon M \to \operatorname{Hom}_{\mathbb{Z}}(R, {}_{\mathbb{Z}}M)$ defined by $j(m) = \mu_m$, where $\mu_m(r) = rm$. This can easily be seen to be a map of R-modules, and it is injective since if $\mu_m = \mu_{m'}$ then $m = \mu_m(1) = \mu_{m'}(1) = m'$.

Since the inclusion $i \colon {}_{\mathbb{Z}}M \to E$ is injective and $\operatorname{Hom}_{\mathbb{Z}}(R, \square)$ is left exact (Proposition 4.10), the R-map i_* from $\operatorname{Hom}_{\mathbb{Z}}(R, {}_{\mathbb{Z}}M)$ into $\operatorname{Hom}_{\mathbb{Z}}(R, E)$ is also injective. Hence the following map is injective:

$$i_* j \colon M \to \operatorname{Hom}_{\mathbb{Z}}(R, E).$$

Recalling that Lemma 5.29 tells us that $\mathrm{Hom}_{\mathbb{Z}}(R, E)$ is an injective R-module, we are done. $\square$

This allows us to find an injective sibling for Proposition 5.25, which is proved in an entirely similar way.

Proposition 5.31. *A module M is injective if and only if every short exact sequence beginning with M splits.*

Proof. Proposition 5.24 shows one direction, so we are left with the other.

Now choose any embedding of M within an injective module, hence finding M to be a direct summand of an injective module, after which Proposition 5.14 finishes things. $\square$

5.5 Flat Modules

Projective and injective modules are those modules that make Hom an exact functor, as Proposition 5.27 tells us. Recalling that the tensor product is right exact, we may ask a similar questions: are there modules which always produce an exact tensor product?

This brief section will cover some technical results that will be helpful later.

Definition 5.32. A left R-module M is **flat** if the functor $\square \otimes_R M \colon \mathbf{Mod}_R \to \mathbf{Ab}$ is exact. Similarly, a right R-module N is flat if $N \otimes_R \square$ is exact.

Proposition 5.33. *The module R is a flat R-module.*

Proof. An extension of Proposition 3.32 tells us that the functor $\square \otimes_R R$ is naturally isomorphic to the identity functor, which is of course exact. Hence R is a flat left R-module. The ring R is also a flat right R-module by symmetry. $\square$

Lemma 5.34. *A direct sum of modules is flat if and only if each of its summands is flat.*

Proof. Recall from Proposition 3.17 that the tensor product distributes over direct sums – we will assume without proof that this isomorphism is natural in all its parts.

To show that a module is flat, we only need to show that it preserves injective maps. Suppose $f \colon A \to B$ is an injection. Then for some family of modules, we have the following commutative diagram whose vertical maps are isomorphisms:

$$\begin{tikzcd}
A \otimes_R \bigoplus_{i\in I} N_i \arrow[r, "f\otimes 1"] \arrow[d] & B \otimes_R \bigoplus_{i\in I} N_i \arrow[d] \\
\bigoplus_{i\in I} (A \otimes_R N_i) \arrow[r, "\bigoplus_{i\in I}(f\otimes 1_{N_i})"'] & \bigoplus_{i\in I} (B \otimes_R N_i)
\end{tikzcd}$$

If each N_i is flat, then the bottom map is injective since each of its summands is injective. Hence the top map is injective, and the sum is flat. Conversely, if the sum is flat, then the maps are both injective, and each of the summands of the bottom map must therefore be injective, meaning that each summand N_i is flat. $\square$

Proposition 5.35. *Projective modules are flat.*

Proof. From the lemma above, every free R-module is flat since it is a direct sum of copies of R. Then since every projective module is a direct summand of a free module, again by the lemma we are done. $\square$

The previous result shows that projective modules are flat, but it is important to note that the converse is not necessarily true.

Example 5.36. For instance, the $\mathbb{Z}$-module $\mathbb{Q}$ is flat, but not projective.

To see that it is flat, suppose that $f\colon A \to B$ is an injection – we now aim to prove that $1_{\mathbb{Q}} \otimes f$ is injective too. Let $t = \sum_{i=1}^{n}(p_i/q_i \otimes a_i) \in A \otimes_{\mathbb{Z}} B$ be such that $f(t) = 0$, so:

$$\begin{aligned} t = \sum_i \left(\frac{p_i}{q_i} \otimes a_i\right) &= \sum_i \left(\frac{p_i \prod_{j\neq i} q_j}{\prod_j q_j} \otimes a_i\right) \\ &= \sum_i \left(\frac{1}{\prod_j q_j} \otimes \left(p_i \prod_{j\neq i} q_j\right) a_i\right) \\ &= \frac{1}{\prod_j q_j} \otimes \sum_i \left(p_i \prod_{j\neq i} q_j\right) a_i \end{aligned}$$

So we can calculate that:

$$0 = (1_{\mathbb{Q}} \otimes f)(t) = \frac{1}{\prod_j q_j} \otimes f(\sum_i \left(p_i \prod_{j\neq i} q_j\right) a_i),$$

By the injectivity of f we conclude that the sum on the right is zero, meaning that in fact $t = 0$, and hence $1_{\mathbb{Q}} \otimes f$ is injective, and finally we conclude that $\mathbb{Q}$ is a flat $\mathbb{Z}$-module.

To see that $\mathbb{Q}$ is not projective, observe that it cannot be a submodule of a free $\mathbb{Z}$-module since every element is divisible by any element of $\mathbb{Z}$.

Even so, there are circumstances under which flat modules are projective, namely when they are finitely presented.

Definition 5.37. A module M is **finitely generated** if there is a surjection $F \to M$ where F is a free module of finite rank.

A module M is **finitely presented** if $M \cong F/K$ where F is a free module of finite rank and K is a finitely generated submodule.

Remark. Over a Notherian ring, these notions are equivalent since a free module of finite rank is a Noetherian module, hence any submodule is also finitely generated.

Lemma 5.38. *A sequence is exact if and only if its image under* $\mathrm{Hom}_{\mathbb{Z}}(\square, \mathbb{Q}/\mathbb{Z})$ *is exact.*

Proof. Let A^* denote $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$. One direction of this is clear since $\mathbb{Q}/\mathbb{Z}$ is injective, so we only prove the other. We will lean heavily upon our observation in Example 5.21 that if $a \in A$ is nonzero, there is some $\chi \in A^*$ with $\chi(a) \neq 0$.

Suppose $f\colon A \to B$ and $g\colon B \to C$, and we have an exact sequence:

$$C^* \xrightarrow{g_*} B^* \xrightarrow{f_*} A^*$$

We wish to show that this implies that $\operatorname{im} f = \ker g$.

Firstly, we show that $\operatorname{im} f \subseteq \ker g$. Suppose this were not the case, so there is some $a \in A$ such that $gf(a) \neq 0$. There must exist some $\chi \in C^*$ such that $\chi(gf(a)) \neq 0$, so this means that $g_* f_*(\chi) \neq 0$ also – but this cannot be, as $g_* f_* = 0$.

We now show equality. Let $p\colon B \to B/\operatorname{im} f$ be the natural map. If indeed there is some element $h \in \ker g \setminus \operatorname{im} f$, then let $\chi' \in (B/\operatorname{im} f)^*$ be such that $\chi'(h + \operatorname{im} f) \neq 0$, and note that $\chi = p_*(\chi') \in B^*$ is also nonzero on h. We can see that $f_*(\chi) = 0$ since $pf = 0$, so we see that $\chi \in \ker f_* = \operatorname{im} g_*$, meaning there is some $\zeta \in C^*$ with $g_*(\zeta) = \chi$. But this is contradicted by the presence of h, as $0 \neq \chi(h) = \zeta(g(h)) = \zeta(0) = 0$. So we conclude that $\ker g = \operatorname{im} f$. $\square$

Proposition 5.39. *Finitely presented flat modules are projective.*

Proof. We present a less formal proof here, for the sake of brevity.

Given some finitely presented flat left R-module N, we will argue that there is a natural isomorphism:

$$\Box^* \otimes_R N \cong \mathrm{Hom}_R(N, \Box)^*,$$

where $A^* = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ as before. This will prove the claim as if N is flat, the functor on the left is exact, and the functor on the right is exact only if $\mathrm{Hom}_R(N, \Box)$ is exact due to lemma 5.38, and in turn this implies that N is projective.

The map $\eta_{M,N} \colon M^* \otimes_R N \to \mathrm{Hom}_R(N, M)^*$ is given by:

$$\eta_M(\chi \otimes n) = \chi', \text{ where } \chi'(f) = \chi(f(n)).$$

We assert without proof that this map is natural, and instead focus on showing it is an isomorphism.

In the case that $N = R$, as in Lemma 3.31 and Proposition 3.32, this map τ_M is an isomorphism. Due to a result we will delay until later, Corollary 6.21, these functors preserve finite direct sums, so if $N = R^n$ then again we have an isomorphism.

In the case that N is finitely presented, there is an exact sequence $R^n \to R^m \to N \to 0$, so we have a diagram in which the first two vertical maps are isomorphisms:

$$\begin{tikzcd}
M^* \otimes_R R^n \arrow[r] \arrow[d] & M^* \otimes_R R^m \arrow[r] \arrow[d] & M^* \otimes_R N \arrow[r] \arrow[d] & 0 \\
\mathrm{Hom}_R(R^n, M)^* \arrow[r] & \mathrm{Hom}_R(R^m, M)^* \arrow[r] & \mathrm{Hom}_R(N, M)^* \arrow[r] & 0
\end{tikzcd}$$

It can be shown through diagram chasing (an argument similar to Proposition 5.23) that the final vertical map is also an isomorphism, and so we are done. $\square$

There is also a relationship between flat modules and injective modules.

Proposition 5.40. *A left R-module N is flat if and only if $\mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Q}/\mathbb{Z})$ is an injective R-module.*

Proof. We will write N^* for $\mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Q}/\mathbb{Z})$. By the Hom-tensor adjunction (Theorem 3.29) we have a natural isomorphism:

$$\mathrm{Hom}_{\mathbb{R}}(\Box, N^*) \cong \mathrm{Hom}_{\mathbb{Z}}(\Box \otimes_R N, \mathbb{Q}/\mathbb{Z}).$$

If N is flat, then recalling that $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module, the latter functor is the composition of exact functors, and hence the functor on the left is exact, meaning N^* is an injective R-module. The converse then follows from Lemma 5.38. $\square$

6 Homology

At this point, we need to take what may seem like a detour into something else: homology.

Homology and cohomology are general methods of associating Abelian groups to certain objects – whether those be topological spaces, groups, or as we will use it, modules. These invariants will produce useful ways to reason about these objects.

6.1 Chain Complexes

Definition 6.1. A **chain complex** is a collection C_i of modules and $d_i \colon C_i \to C_{i-1}$ of maps such that $d_i d_{i+1} = 0$ for all $i \in \mathbb{Z}$. We denote a chain complex as the pair $(\mathbf{C}_\bullet, d_\bullet)$ or simply as $\mathbf{C}$, and draw it like so:

$$\mathbf{C} = \qquad \cdots \to C_{i+1} \xrightarrow{d_{i+1}} C_i \xrightarrow{d_i} C_{i-1} \to \cdots$$

Remark. Every exact sequence is a chain complex (if we fill in the gaps with zeros appropriately), but not every chain complex is exact: the requirement that $d_i d_{i+1} = 0$ only requires that $\ker d_i$ contains $\operatorname{im} d_i$, and not that they are equal.

Remark. The image of any chain complex under an additive functor is a chain complex, since if in the covariant case we set $d_i' = F(d_i)$ and $C_i' = F(C_i)$, we have $d_i' d_{i+1}' = F(d_i d_{i+1}) = F(0) = 0$. The covariant case is similar but we must set $C_i' = F(C_{-i})$ and set the maps in a fairly similar way.

Definition 6.2. A **chain map** $f \colon \mathbf{C} \to \mathbf{C}'$ is a collection of maps $f_i \colon C_i \to C_i'$ such that the following diagram commutes for all i:

$$\begin{tikzcd}
C_{i+1} \arrow[r, "d_{i+1}"] \arrow[d, "f_{i+1}"'] & C_i \arrow[d, "f_i"] \\
C_{i+1}' \arrow[r, "d_{i+1}'"] & C_i'
\end{tikzcd}$$

Remark. If we're working with some category $\mathcal{A}$ of modules (i.e., ${}_R\mathbf{Mod}$ or $\mathbf{Mod}_R$) then we can consider the collection of chain complexes and chain maps a category, which we call $\mathrm{Ch}(\mathcal{A})$. Since additive functors $F \colon \mathcal{A} \to \mathbf{Ab}$ preserve chain complexes as we observed above, they also produce functors $\mathrm{Ch}(\mathcal{A}) \to \mathrm{Ch}(\mathbf{Ab})$.

In algebraic topology, the prototypical use of a chain complex is to describe the structure of singular simplices on a particular space. Speaking informally, C_n is a collection of n-dimensional simplices (generalisations of triangles and tetrahedra) and the d_n are 'boundary maps' sending the simplices to their boundary.

This hints at how we should interpret chain complexes: we might think of each C_i as encoding the ith-dimensional data about some object.

Definitions 6.3. Given a chain complex $\mathbf{C}$, we define:
- The n-**chains** as C_n,
- The n-**cycles** as $Z_n(\mathbf{C}) = \ker d_n$, and
- The n-**boundaries** as $B_n(\mathbf{C}) = \operatorname{im} d_{n+1}$.

This terminology is again borrowed from the concept of simplicial homology in algebraic topology. The n-boundaries are indeed boundaries of simplices, and the cycles are collections of simplices that somehow 'close the loop' and hence have no boundary.

Remark. Within the context of a chain complex $\mathbf{C}$ which we omit for brevity, we have $B_i \subseteq Z_i$ and a short exact sequence that holds for all i:

$$0 \to Z_i \hookrightarrow C_i \xrightarrow{d_i} B_{i-1} \to 0.$$

Finally we come to the goal of these definitions. In the context of simplicial homology, topologists had the goal of defining what it meant for a space to have an n-dimensional hole. A hole can be thought of as a loop that cannot be ‘filled in’ within the space – in other words, a cycle that is not a boundary. In this way, by quotienting out the boundaries from the cycles, we achieve an object that describes the holes in a space. This is homology.

Definition 6.4. The nth **homology** of a complex $\mathbf{C}$ is defined as $H_n(\mathbf{C}) = Z_n(\mathbf{C})/B_n(\mathbf{C})$.

We will now show various important facts about homology. From this point forward, $\mathcal{A}$ denotes either ${}_R\mathbf{Mod}$ or $\mathbf{Mod}_R$ for some ring R.

Proposition 6.5. *The nth homology is a functor $H_n\colon \mathrm{Ch}(\mathcal{A}) \to \mathcal{A}$, where*

$$H_n(f)\colon H_n(\mathbf{C}) \to H_n(\mathbf{C}')$$

is defined by $z + B_n(\mathbf{C}) \mapsto f_n(z) + B_n(\mathbf{C}')$, and denoted as f_*.

Proof. We first show that f_* is well-defined. Certainly if $z + B_n(\mathbf{C}) = z' + B_n(\mathbf{C})$, then $z - z' \in B_n(\mathbf{C})$, so $0 = f_{n-1}d_n(z - z') = d'_n f_n(z - z')$, ergo $z - z' \in B_n(\mathbf{C}')$ and $z + B_n(\mathbf{C}') = z' + B_n(\mathbf{C}')$.

Let $g\colon \mathbf{C}' \to \mathbf{C}''$ be another chain map. Then certainly $(gf)_*\colon z + B_n(\mathbf{C}) \mapsto gf(z) + B_n(\mathbf{C}'')$, so it's plain to see that $(gf)_* = g_* f_*$.

Finally, see that $H_n(1_{\mathbf{C}})$ sends $z + B_n(\mathbf{C})$ to itself, so indeed it is the identity map, and we are done. □

It is interesting to observe that $\mathrm{Ch}(\mathcal{A})$ picks up many properties from the category of modules that it is over. For example, we can add two chain maps by defining $(f+g)_n = f_n + g_n$, and due to composition distributing over addition, this remains a chain map. There is also a zero map that is always a chain map, as well as an additive inverse, so in fact $\mathrm{Hom}(\mathbf{C}, \mathbf{C}')$ is an Abelian group. For this reason, we may extend a notion we have seen before to this new category:

Proposition 6.6. *The functor $H_n\colon \mathrm{Ch}(\mathcal{A}) \to \mathcal{A}$ is additive, in the sense that $(f+g)_* = f_* + g_*$.*

Proof. Observe that $(f+g)_*$ sends $z + B_n(\mathbf{C})$ to $f(z) + g(z) + B_n(\mathbf{C}) = \big(f(z) + B_n(\mathbf{C})\big) + \big(g(z) + B_n(\mathbf{C})\big)$, which is exactly what $f_* + g_*$ does. □

This may be thought of as one half of homology. When we want to use homology to study certain objects, say in a category $\mathcal{G}$, we first construct some meaningful chain complex via, say, a functor $\mathcal{G} \to \mathrm{Ch}(\mathbf{Ab})$ as in simplicial homology, then compute the result of the homology functors $H_n\colon \mathrm{Ch}(\mathbf{Ab}) \to \mathbf{Ab}$ to obtain useful invariants.

In algebraic topology, a foundational result is that homotopic maps are the same under singular homology – that is, if maps are the same up to some continuous deformation, then they are the same on the level of homotopy. We have a similar notion for chain complexes.

Definition 6.7. Let $f, g\colon \mathbf{C} \to \mathbf{C}'$ be chain maps. A **chain homotopy** between f and g is a collection of maps $s_i\colon C_i \to C'_{i+1}$ denoted s, such that $f_i - g_i = d'_{i+1}s_i + s_{i-1}d_i$. The maps f and g are called **chain homotopic** if there is such a chain homotopy.

Although the following diagram does not commute, it does describe the setup for the condition upon a chain homotopy s_i:

$$\begin{tikzcd}
\cdots \arrow[r] & C_{n+1} \arrow[r] \arrow[dl] \arrow[d, shift right, "f"'] \arrow[d, shift left, "g"] & C_n \arrow[r] \arrow[dl, "s_n"'] \arrow[d, shift right, "f"'] \arrow[d, shift left, "g"] & C_{n-1} \arrow[r] \arrow[dl, "s_{n-1}"'] \arrow[d, shift right, "f"'] \arrow[d, shift left, "g"] & \cdots \arrow[dl] \\
\cdots \arrow[r] & C'_{n+1} \arrow[r] & C'_n \arrow[r] & C'_{n-1} \arrow[r] & \cdots
\end{tikzcd}$$

Proposition 6.8. *If $f, g\colon \mathbf{C} \to \mathbf{C}'$ are chain homotopic, then $f_* = g_*$ in all degrees of homology.*

Proof. If $z \in Z_n$, then $f_n(z) - g_n(z) = d'_{i+1}s_i(z) + s_{i-1}d_i(z) = d'_{i+1}s_i(z) \in B_{i+1}$, so $f_n(z) + B_{i+1} = g_n(z) + B_{i+1}$ for all i. $\square$

6.2 The Long Exact Sequence

We have seen that we can take the sum of two chain maps, similarly to maps of modules. Continuing the similarities, we may conceptualise the image and kernel of chain maps, and therefore define exactness.

Definition 6.9. If $f : \mathbf{C} \to \mathbf{C}'$ is a chain map, then the image and kernel of f are the chains:

$$\ker f = \qquad \cdots \to \ker f_{i+1} \xrightarrow{d_{i+1}} \ker f_i \xrightarrow{d_i} \ker f_{i-1} \to \cdots$$

$$\operatorname{im} f = \qquad \cdots \to \operatorname{im} f_{i+1} \xrightarrow{d'_{i+1}} \operatorname{im} f_i \xrightarrow{d'_i} \operatorname{im} f_{i-1} \to \cdots$$

Proof that the kernel and image are chain complexes. We need to show that the maps $d_i\colon \ker f_i \to \ker f_{i-1}$ and $d'_i\colon \operatorname{im} f_i \to \operatorname{im} f_{i-1}$ are well-defined, after which the requirement for $d_i d_{i+1}$ to be 0 is inherited from the chains $\mathbf{C}$ and $\mathbf{C}'$.

Suppose that $c \in \ker f_i$, so $0 = d'_i f_i(c) = f_{i-1}d_i(c)$, so $d_i(c) \in \ker f_{i-1}$. Similarly if $f_i(c) \in \operatorname{im} f_i$, then certainly $d'_i f_i(c) = f_{i-1}d'_i(c) \in \operatorname{im} f_{i-1}$. $\square$

This allows us to define exact sequences of chain complexes, which we use now to prove an important theorem of homology.

Theorem 6.10 (The Long Exact Sequence)**.** *Suppose there is an exact sequence of chain complexes:*

$$0 \to \mathbf{C} \xrightarrow{j} \mathbf{C}' \xrightarrow{p} \mathbf{C}'' \to 0.$$

Then there are maps $\partial_i\colon H_i(\mathbf{C}'') \to H_{i-1}(\mathbf{C})$ such that the following sequence is exact:

$$\cdots \to H_i(\mathbf{C}) \xrightarrow{j_*} H_i(\mathbf{C}') \xrightarrow{p_*} H_i(\mathbf{C}'') \xrightarrow{\partial_i} H_{i-1}(\mathbf{C}) \xrightarrow{j_*} H_{i-1}(\mathbf{C}') \to \cdots$$

The proof of this is quite involved and we will break it up into a few different parts.

Proof that the connecting maps exist. The exact sequence of chain complexes is a very succinct way of describing the following commutative diagram whose columns are chain complexes and whose rows are short exact sequences:

$$\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
0 \arrow[r] & C_{i+1} \arrow[r, "j_{i+1}"] \arrow[d, "d_{i+1}"] & C'_{i+1} \arrow[r, "p_{i+1}"] \arrow[d, "d'_{i+1}"] & C''_{i+1} \arrow[r] \arrow[d, "d''_{i+1}"] & 0 \\
0 \arrow[r] & C_i \arrow[r, "j_i"] \arrow[d, "d_i"] & C'_i \arrow[r, "p_i"] \arrow[d, "d'_i"] & C''_i \arrow[r] \arrow[d, "d''_i"] & 0 \\
0 \arrow[r] & C_{i-1} \arrow[r, "j_{i-1}"] \arrow[d] & C'_{i-1} \arrow[r, "p_{i-1}"] \arrow[d] & C''_{i-1} \arrow[r] \arrow[d] & 0 \\
 & \vdots & \vdots & \vdots &
\end{tikzcd}$$

Let $z + B_i(\mathbf{C}'') \in H_i(\mathbf{C}'')$. We know that p_i is surjective, so there is some $c \in C'_i$ such that $p_i(c) = z$. Now note that $p_{i-1}d'_i(c) = d''_i p_i(c) = d''_i(z) = 0$, so $d'_i(c) \in \ker p_{i-1} = \operatorname{im} j_{i-1}$, so there is a unique $b \in C_{i-1}$ with $j_{i-1}(b) = d'_i(c)$. We might draw this diagram, mirroring the path we take along the commutative diagram above:

$$\begin{tikzcd}
 & c \in C'_i \arrow[r, mapsto, "p_i"] \arrow[d, mapsto, "d'_i"] & z \in Z_i(\mathbf{C}'') \\
b \in C_{i-1} \arrow[r, mapsto, "j_{i-1}"] & d'_i(c) \in C'_{i-1} &
\end{tikzcd}$$

We claim that $\partial_i(z + B_i) = b + B_{i-1}$ is the boundary map we're searching for, and we show this is well-defined here.

First we must show that $b \in Z_{i-1}$. Certainly j_{i-2} is injective, so $d_{i-1}(b) = 0$ if and only if $j_{i-2}d_{i-1}(b) = 0$, but then this is equivalent to $0 = d'_{i-1}j_{i-1}(b) = d'_{i-1}d_i(c)$, and this holds due to $\mathbf{C}'$ being a chain complex.

Now we must show that this is independent of choice of c. If c and c' both have $p_i(c) = p_i(c') = z$, then letting b and b' be such that $j_{i-1}(b) = d'_i(c)$ and $j_{i-1}(b') = d'_i(c')$. Certainly there exists some $a \in C_i$ with $j_i(a) = c - c'$, since $p_i(c - c') = z - z = 0$ and the row is exact. This then shows that $j_{i-1}(b - b') = d'_i(c - c') = d'_i j_i(a) = j_{i-1}d_i(a)$, so by injectivity $d_i(a) = b - b'$, so $b - b' \in B_{i-1}(\mathbf{C})$, and indeed this is then independent of choice of c.

Now we show independence of choice of z, which amounts to showing that if $z \in B_i(\mathbf{C}'')$ then the b that is produced is in $B_{i-1}(\mathbf{C})$. If $z \in B_i(\mathbf{C}'')$, then we choose some $c \in C'_i$ with $p_i(c) = z$. Since $z \in B_i(\mathbf{C}'')$ there is some $y \in C''_{i+1}$ with $z = d''_{i+1}(y)$, and by surjectivity some $k \in C'_{i+1}$ with $p_{i+1}(k) = y$. Then $p_i(c) = z = d''_{i+1}p_{i+1}(k) = p_i d'_{i+1}(k)$, and by independence of choice of c, we may freely choose $c = d'_{i+1}(k) \in B_{i+1}(\mathbf{C}')$. But then it's necessarily the case that $b = 0$, since $d'_i d'_{i+1} = 0$.

We finally show that this is indeed a map of modules. We show this for left R-modules, and the right case follows similarly. Suppose $z, z' \in Z_i(\mathbf{C}'')$, where $p_i(c) = z$, $p_i(c') = z'$, $j_{i-1}(b) = d'_i(c)$, and $j_{i-1}(b') = d'_i(c')$. Then certainly $p_i(c + c') = z + z'$ and $j_{i-1}(b + b') = d'_i(c + c')$, so $\partial_i\left((z + B_i) + (z' + B_i)\right) = \partial_i(z + B_i) + \partial_i(z' + B_i)$. Similarly for some $r \in R$, $p_i(rc) = rz$ and $j_{i-1}(rb) = d'_i(rc)$, so $\partial_i(rz + B_i) = r\partial_i(z + B_i)$. ☐

So, the maps $\partial_i \colon H_i(\mathbf{C}'') \to H_{i-1}(\mathbf{C})$ exist – now we need to show that the sequence is exact.

Proof that the sequence is exact. For the sake of brevity, in the following we will write B'_i instead of $B_i(\mathbf{C}')$, and likewise for the similar sets of boundaries and cycles. **Exactness at $H_i(\mathbf{C})$:** Let $z + B''_{i+1} \in H_{i+1}(\mathbf{C}'')$. By the above construction, $\partial_i(z + B_{i+1})$ is $b + B_i \in H_i(\mathbf{C})$ with $j_i(b) = d'_i(c)$ for some $c \in C'_i$ for which $p_{i+1}(c) = z$. We can then calculate that $j_*(b + B_i) = d'_i(c) + B'_i = 0 \in H_i(\mathbf{C}')$.

Conversely, supposing that $j_*(b + B_i) = 0$, we have that $j_i(b) = d'_i(c)$ for some $c \in C'_i$. Setting $z = p_i(c)$, we see that $\partial_{i+1}(z + B''_{i+1}) = b + B_i$ by definition.

Exactness at $H_i(\mathbf{C}')$: We see that $p_*j_*(z + B_i) = pj(z) + B''_i = 0$ since $pj = 0$.

Conversely, if $p_*(z + B'_i) = 0$, then $p_i(z) = d''_{i+1}(c)$ for some $c \in C''_{i+1}$. But p_{i+1} is surjective, so there is some $c' \in C'_{i+1}$ with $p_{i+1}(c') = c$, whence:

$$p_i(z) = d''_{i+1}p_{i+1}(c') = p_i d'_{i+1}(c'),$$

whereafter we see that $z - d'_{i+1}(c') \in \ker p_i = \operatorname{im} j_i$, so there is some $x \in C_i$ with $j_i(x) = z - d'_{i+1}(c')$, which gives us $j_*(x + B_i) = z - d'_{i+1}(c') + B'_i = z + B'_i$.

Exactness at $H_i(\mathbf{C}'')$: Let $z = p_i(x)$ for some $x + B'_i \in H_i(\mathbf{C}')$. Then following the definition of ∂_i, we can choose $c = x$, whereafter $d'_i(c) = 0$ since x is a cycle, and so $b = 0$ is a possible choice, and $\partial_i p_i(x + B'_i) = 0$.

Conversely, suppose that $\partial_i(z + B_i'') = 0$, so setting up the definition of ∂_i, we have $p_i(c) = z$ and $j_{i-1}(b) = d_i'(c)$, as well as the additional fact that $b = d_i(x)$ for some $x \in C_i$. This tells us that:

$$d_i'(c) = j_{i-1}d_i(x) = d_i'j_i(x),$$

so $c - j_i(x) \in Z_i'$, and we can calculate that $p_*(c - j_i(x) + B_i') = p_i(c) + p_i j_i(x) + B_i'' = z + B_i''$. $\square$

What is the use of the long exact sequence? It will allow us to calculate homology groups of complexes in terms of others in a nice way. For example, if, say $\mathbf{C}'$ is exact so that $H_i(\mathbf{C}') = 0$, then a consequence of the long exact sequence is that, given an exact sequence $0 \to \mathbf{C} \to \mathbf{C}' \to \mathbf{C}'' \to 0$, we can conclude that $H_i(\mathbf{C}'') \cong H_{i-1}(\mathbf{C})$ for all i, since those two terms are surrounded by zeros in the long exact sequence.

6.3 A Note on Abelian Categories

We noted while defining the long exact sequence (Theorem 6.10) that we may conceive of exact sequences of chain complexes, due to a seemingly natural definition of kernel and image within $\mathrm{Ch}(\mathcal{A})$. It can also be seen that something approximating a quotient exists too: if we define 'sub-complex' of a chain complex $\mathbf{C}$ as a complex $\mathbf{A}$ such that $A_i \subseteq C_i$, and whose boundary maps are restrictions of $\mathbf{C}$'s, we can define the quotient as having $(C/A)_i = C_i/A_i$, and the obvious boundary maps.

There seem to be some remarkable similarities between chain complexes and ${}_R\mathbf{Mod}$. To name a few:

- We can sum morphisms between objects.
- There are 'zero-like' objects, the maps in and out of which are unique.
- There is a notion of a quotient object for any subobject.
- Kernels and images of maps exist.

These are quite convenient properties, as for instance it is somewhat natural to consider the category $\mathrm{Ch}(\mathrm{Ch}(\mathcal{A}))$, whose definition cannot be given via the construction above, but we might quite naturally consider as 'two-dimensional' complexes. That is, commutative diagrams as below with rows and columns being complexes:

$$\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
\cdots \arrow[r] & C_{i+1,j+1} \arrow[r] \arrow[d] & C_{i,j+1} \arrow[r] \arrow[d] & C_{i-1,j+1} \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r] & C_{i+1,j} \arrow[r] \arrow[d] & C_{i,j} \arrow[r] \arrow[d] & C_{i-1,j} \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r] & C_{i+1,j-1} \arrow[r] \arrow[d] & C_{i,j-1} \arrow[r] \arrow[d] & C_{i-1,j-1} \arrow[r] \arrow[d] & \cdots \\
 & \vdots & \vdots & \vdots &
\end{tikzcd}$$

We introduce a definition which allows us to make some of these similarities considerably more precise, calling upon some of our knowledge from Section 2.

Definition 6.11. An **additive category** $\mathcal{A}$ is a category which satisfies the following:

(a) For any objects $A, B \in \mathcal{A}$, we have an Abelian group in $\mathrm{Hom}(A, B)$.

(b) Composition distributes over addition, meaning that $f \circ (g + h) = (f \circ g) + (f \circ h)$ for appropriate maps f, g, and h, and likewise for the other side.

(c) There is an object within $\mathcal{A}$ which is both initial and terminal, known as the zero object.
(d) The product and coproduct of any two objects exists within $\mathcal{A}$.

Remark. Observe that this definition is 'self-dual', which is to say that $\mathcal{A}^{\mathrm{op}}$ is an additive category exactly when $\mathcal{A}$ is too. This is because, as we noted in Section 2, the initial object in $\mathcal{A}$ is terminal in $\mathcal{A}^{\mathrm{op}}$, and vice versa – similarly for products and coproducts.

This definition is expressive enough to allow us to define some very useful objects in purely category-theoretic terms. For example, since we have a notion of a zero map now (the additive identity of a Hom-group) the definition of a chain complex is immediate. Here is another example of a useful notion we now obtain.

Definition 6.12. Let $f\colon A \to B$ be a morphism of an additive category $\mathcal{A}$. A **kernel** of f is a pair consisting of an object K and a morphism $\iota\colon K \to A$ such that $f\iota = 0$ and for all objects X and maps $g\colon X \to A$ with $fg = 0$, there is a unique map $\gamma\colon X \to K$ such that the following diagram commutes:

$$\begin{tikzcd} X \arrow[d, dashed, "\gamma"] \arrow[dr, "g"] & & \\ K \arrow[r, "\iota"] & A \arrow[r, "f"] & B \end{tikzcd}$$

Proposition 6.13. *If the kernel (K, ι) exists, then it is unique up to isomorphism respecting ι. That is, if there is another kernel (K', ι'), there is an isomorphism $\phi\colon K \to K'$ such that the following diagram commutes:*

$$\begin{tikzcd} K \arrow[dd, "\phi"] \arrow[dr, "\iota"] & \\ & A \\ K' \arrow[ur, "\iota'"] & \end{tikzcd}$$

Intuitively, this means that they are isomorphic in the way that they are embedded in A, rather than merely isomorphic.

Proof. By the universal property there exist maps ϕ and ϕ':

$$\begin{tikzcd} K \arrow[d, "\phi"] \arrow[ddr, "\iota"] & & \\ K' \arrow[d, "\phi'"] \arrow[dr, "\iota'"] & & \\ K \arrow[r, "\iota"] & A \arrow[r, "f"] & B \end{tikzcd}$$

Their composition also respects the diagram, but since 1_K and $1_{K'}$ respect it also and the map is unique, we conclude that they are mutually inverse and we are done. $\square$

Proposition 6.14. *In ${}_R\mathbf{Mod}$, the kernel (K, ι) of a map $f\colon A \to B$ is $K = \ker f$ and the inclusion $\iota\colon \ker f \to A$.*

Proof. Let X be some R-module, and let $g\colon X \to A$ be such that $fg = 0$. Certainly this means that $\operatorname{im} g \subseteq \ker f$, so we may restrict g to $g_0\colon X \to \ker f$ defined by $g_0(x) = g(x)$. This makes the diagram commute since $\iota g_0(x) = g(x)$ by definition.

We now show uniqueness. Suppose $\gamma\colon X \to \ker f$ has $\iota\gamma = g$. Then certainly $\gamma(x) = g(x) = g_0(x)$, so we are done. $\square$

Definition 6.15. The **cokernel** of a morphism $f\colon A \to B$ in an additive category is a kernel of $f^{\mathrm{op}}\colon B \to A$ in the opposite category. Equivalently, it is a pair (C, π) such that $\pi f = 0$ and for all maps $g\colon B \to X$ there is a unique map $\gamma\colon C \to X$ such that the following diagram commutes:

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, "\pi"] \arrow[dr, "g"'] & C \arrow[d, dashed, "\gamma"] \\ & & X \end{tikzcd}$$

We immediately get an analogue of Proposition 6.13 for free since the uniqueness transfers over from the opposite category.

The nature of a cokernel is a little bit less intuitive than that of the kernel, as it is not standard fare to define. However the following proposition explains it in the context of modules.

Proposition 6.16. *In ${}_R\mathbf{Mod}$, the cokernel (C, π) of a map $f\colon A \to B$ is $C = B/\operatorname{im} f$ and the natural map $\pi(b) = b + \operatorname{im} f$.*

Proof. Let X be some R-module and let $g\colon B \to X$ be such that $gf = 0$. We claim that $g_0\colon C \to X$ defined by $g_0(b + \operatorname{im} f) = g(b)$ is well-defined. Indeed it is easily seen to be since $\operatorname{im} f \subseteq \ker g$, and evidently $g_0\pi = g$.

Now we show uniqueness. Since $\gamma\pi = g$, we have $\gamma(b + \operatorname{im} f) = g(b)$ immediately, and we are done. $\square$

In future contexts, we will denote this as $\operatorname{coker} f = B/\operatorname{im} f$.

Now that we have elegant and abstract descriptions of useful concepts that are seemingly common to categories of modules and chain complexes, perhaps we can show more results that share similarities with our intuition regarding modules.

One intuition is that a kernel is a submodule and the cokernel is a quotient. In the context of modules, this can be expressed by saying that the map $\iota\colon K \to A$ is an injection and $\pi\colon B \to C$ is a surjection, but we have no such concepts in an arbitrary category. Instead we will show that they are a monomorphism and an epimorphism respectively.

Proposition 6.17. *Let $f\colon A \to B$ be a morphism in an additive category. If a kernel (K, ι) exists then ι is a monomorphism, and if a cokernel (C, π) exists then π is an epimorphism.*

Proof. Suppose that $p, q\colon X \to K$ are such that $\iota p = \iota q$. Then observe the following diagram:

$$\begin{tikzcd} X \arrow[d, shift right, "p"'] \arrow[d, shift left, "q"] \arrow[dr, "\iota p = \iota q"] & & \\ K \arrow[r, "\iota"] & A \arrow[r, "f"] & B \end{tikzcd}$$

Since $\iota p = \iota q$, this diagram commutes if we ignore either p or q. But the definition of a kernel stipulates that the map is unique, so in fact $p = q$.

For cokernels we could observe that monomorphisms in the opposite category are epimorphisms and apply duality, but we show the argument in full here. Suppose $s, t\colon C \to X$ are such that $s\pi = t\pi$. Then observe the following diagram:

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, "\pi"] \arrow[dr, "s\pi = t\pi"'] & C \arrow[d, shift right, "s"'] \arrow[d, shift left, "t"] \\ & & X \end{tikzcd}$$

By the same argument as above, since the diagram commutes for both s and t, by the uniqueness stipulation, we conclude that $s = t$. $\square$

So kernels and cokernels appear to align with our intuitions, however there are two additional complications. Firstly, there is no guarantee that in some additive category kernels and cokernels exist at all. Secondly, there is a close relationship between subobjects and kernels, and similarly quotient objects and cokernels. By adding two more stipulations, we achieve a definition that generalises much of what we have seen.

Definition 6.18. An **Abelian category** $\mathcal{A}$ is an additive category which satisfies the following additional requirements:
(e) The kernel and cokernel of every morphism exists.
(f) Every monomorphism is the kernel of some morphism, and every epimorphism is the cokernel of some map.

Examples 6.19. The following are examples and non-examples of Abelian categories:
- The categories ${}_R\mathbf{Mod}$ and $\mathbf{Mod}_R$ for any ring R are Abelian.
- Given an Abelian category $\mathcal{A}$, the category of chain complexes $\mathrm{Ch}(\mathcal{A})$ is Abelian.
- If R is a left Noetherian ring, then the category of finitely generated left R-modules is Abelian, since any finitely generated R-module is Noetherian, meaning all quotients and submodules are also finitely generated.
- If R is not left Noetherian, then the category of finitely generated left R-modules is not Abelian, as there will be a kernel which is not finitely generated.
- The category **Grp** of groups is not Abelian, as Hom may not have the structure of an Abelian group in general.

Now we have the full context in which we may define homology, since we may find subobjects like the cycles of a complex, and then quotient by the image of a map, such as the boundaries of a complex. We can also define exactness, projective and injective objects, and as we will soon see, certain other useful homological concepts (in particular, the Ext functor).

Let us prove a useful theorem of Abelian categories, which is based upon the observation in Examples 2.25: in an Abelian category, products and coproducts coincide.

Proposition 6.20. *Let $\mathcal{A}$ be an Abelian category, and let A, A' and M be objects of $\mathcal{A}$. Then $M \cong A \sqcap A'$ if there exist morphisms $i\colon A \to M$, $i'\colon A' \to M$, $p\colon M \to A$, and $p'\colon M \to A'$, such that the following equations hold:*

$$pi = 1_A,\ p'i' = 1_{A'},\ pi' = 0,\ p'i = 0,\ \text{and } ip + i'p' = 1_M.$$

Moreover, this is equivalent to $M \cong A \sqcup A'$.

Proof. We first show that the morphisms are necessary for M to be a product, and then we will show sufficiency.

Supposing $M \cong A \sqcap A'$, we have morphisms $p\colon M \to A$ and $p'\colon M \to A'$ necessarily. The following diagrams give us the maps i and i' and four of the five equations stipulated:

$$\begin{tikzcd} A & M \arrow[l, "p"'] \arrow[r, "p'"] & A' \\ & A \arrow[ul, "1_A"] \arrow[u, dashed, "i"] \arrow[ur, "0"'] & \end{tikzcd} \qquad \begin{tikzcd} A & M \arrow[l, "p"'] \arrow[r, "p'"] & A' \\ & A' \arrow[ul, "0"] \arrow[u, dashed, "i'"] \arrow[ur, "1_{A'}"'] & \end{tikzcd}$$

This leaves us only with proving that $ip + i'p' = 1_M$. Consider the following diagram:

$$\begin{tikzcd} A & M \arrow[l, "p"'] \arrow[r, "p'"] & A' \\ & M \arrow[ul, "p"] \arrow[u, "\eta"] \arrow[ur, "q"'] & \end{tikzcd}$$

Certainly this commutes when $\eta = ip + i'p'$, since $p(ip+i'p') = 1_A p + 0p' = p$, and similarly $p'(ip+i'p') = p'$. However the definition of a product (Definition 2.17) stipulates that this map is unique, and since $\eta = 1_M$ would also make the diagram commute, we must have $ip + i'p' = 1_M$.

Now for sufficiency. Let the stipulated maps be as before, and let X be some object of $\mathcal{A}$, and $f\colon X \to A$ and $f'\colon X \to A'$ be some morphisms. We claim that $\eta = if + i'f'$ is the unique morphism making the following diagram commute, and hence showing that $M \cong A \sqcap A'$:

$$\begin{tikzcd} A & M \arrow[l, "p"'] \arrow[r, "p'"] & A' \\ & X \arrow[ul, "f"] \arrow[u, dashed, "\eta"] \arrow[ur, "f'"'] & \end{tikzcd}$$

The diagram commutes since $p(if + i'f') = 1_A f + 0 = f$ and similarly for the other triangle. Now we must tackle uniqueness. If $f = p\eta$ and $f' = p'\eta$, we can see that $if + i'f' = (ip + i'p')\eta = 1_M \eta = \eta$, so this is unique.

Why should this also characterise coproducts? Recall that coproducts are products in the opposite category. If we reverse the arrows of all the morphisms present in the characterisation we have proved above, we obtain the same conditions but with the roles of i, i' and p, p' swapped. So a product in $\mathcal{A}$ is a product in $\mathcal{A}^{\mathrm{op}}$ too, which is to say that it is a coproduct in $\mathcal{A}$. $\square$

Corollary 6.21. *Let $\mathcal{A}$ and $\mathcal{B}$ be Abelian categories, and let $F\colon \mathcal{A} \to \mathcal{B}$ be a functor such that, for appropriate morphisms f and g in $\mathcal{A}$, $F(f+g) = F(f) + F(g)$ (we might call such a functor additive!). Then for any objects $A, A' \in \mathcal{A}$, we have $F(A \sqcap A') \cong F(A) \sqcap F(A')$.*

Proof. Since the functor distributes over addition of maps, it preserves each of the equations in Proposition 6.20, and so the image of a product remains a product. $\square$

The concept of an Abelian category, it seems, is modelled on the behaviour of categories of modules. But could it be that Abelian categories can be wildly different from those of modules in general? For example, we have seen that every module is the quotient of a projective module and a submodule of an injective one, but there is no clear reason why an arbitrary Abelian category should have the same property. However, in general we can say something quite strong about the nature of an Abelian category, which we state without its arduous proof which can be found in [Mit65].

Theorem 6.22 (Mitchell's Full Embedding Theorem)**.** *For every small*[4] *Abelian category $\mathcal{A}$, there is a ring R and a functor $F\colon \mathcal{A} \to {}_R\mathbf{Mod}$ which has the following properties:*

(i) The map $\mathrm{Hom}(A, B) \to \mathrm{Hom}(F(A), F(B))$ given by $f \mapsto F(f)$ is bijective for all $A, B \in \mathcal{A}$, and

(ii) The functor F is exact.

It is not easy to describe the consequences of this theorem without considerably more precise categorical language. We may intuit this as bounding the differences between an Abelian category and the category of R-modules, and in particular means that diagram chasing proofs (such as that of Theorem 6.10) are true in all Abelian categories thanks to our proof in the category of modules.

Example 6.23. To demonstrate the subtlety involved here, we observe the possible error a reader might make in assuming that every Abelian category has the property that every object is the image of a projective object, or a subobject of an injective object. Take for example, the category of finitely generated Abelian groups, which we stated without proof was Abelian in Examples 6.19.

[4] Recall from Section 2 that a small category is one whose collection of objects and morphisms is a set rather than a proper class.

This category does have enough projectives in the above sense, but it has *no* injective objects except the zero object. To see this, suppose E is a nonzero injective object, and invoke Proposition 5.14 as well as the classification of finitely generated Abelian groups to conclude that $\mathbb{Z}$ is injective or $\mathbb{Z}/n\mathbb{Z}$ is injective for some $n \geq 2$. Consider the following diagrams, which by injectivity must have maps f and g for which they commute:

$$\begin{tikzcd} \mathbb{Z} & \\ 2\mathbb{Z} \arrow[u, "2z\mapsto z"] \arrow[r, hook] & \mathbb{Z} \arrow[ul, dashed, "f"'] \end{tikzcd} \qquad \begin{tikzcd} \mathbb{Z}/n\mathbb{Z} & \\ n\mathbb{Z}/n^2\mathbb{Z} \arrow[u, "nk\mapsto k"] \arrow[r, hook] & \mathbb{Z}/n^2\mathbb{Z} \arrow[ul, dashed, "g"'] \end{tikzcd}$$

Now $f(2) = 1$ but then $2f(1) = 1$, yet $2 \nmid 1$, so we have a contradiction in the first case. In the second case, $g(n) = 1$, so $ng(1) = 1$, but every element of $\mathbb{Z}/n\mathbb{Z}$ is of order n, so $0 = 1 \in \mathbb{Z}/n\mathbb{Z}$ and we have a contradiction for $n \geq 2$.

In light of the new understanding of Abelian categories, we will continue to work in the specific context of modules over a ring rather than the more general domain of Abelian categories that homological algebra presides over.

7 Resolutions and the Ext Functor

In Section 6, we outlined how invariants can be obtained from complexes. In this section, we will find complexes associated with modules that will elucidate some of their structure, and produce strong results on their homological properties.

7.1 Projective and Injective Resolutions

A useful tool in describing certain modules is that of a presentation. We may think of some particular module as being the most general module generated by some number of elements and with some relations between those generators – in other words, as a quotient of a free module. We might describe this as a short exact sequence $0 \to K_1 \hookrightarrow F_0 \to M \to 0$. However, these relations K_1 might themselves have some complicated structure, so we might want to describe it, in turn, as a quotient of a free module F_1 – so on and so forth, ad infinitum. We end up with an exact sequence:

$$\cdots \to F_n \to \cdots \to F_2 \to F_1 \to F_0 \to M \to 0.$$

Such a sequence is called a **free resolution** of M, and in some way is a total description of all the fine detail within a module.

There are some natural questions to ask about these. Firstly, need these always go on forever, or might they eventually reach zero? Secondly, is the sequence uniquely determined in some way by the module it resolves? These questions turn out to be fruitful, and we explore them in the coming sections.

It is more natural, both in terms of generalisations to arbitrary Abelian categories and in terms of the results we will show, to use projective modules instead of free modules when producing resolutions, though of course the latter are instances of the former.

Definition 7.1. A **projective resolution** of a module M is a collection of projective modules P_i and connecting maps $d_{i+1} \colon P_{i+1} \to P_i$ and $\varepsilon \colon P_0 \to M$ such that the following sequence is exact:

$$\cdots \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} \cdots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \longrightarrow 0.$$

We denote such a resolution as $\mathbf{P}$.

It is important to note that in ${}_R\mathbf{Mod}$ and $\mathbf{Mod}_R$, since every module is the quotient of a free module, certainly a projective resolution exists for any module.

Theorem 7.2 (The Comparison Theorem)**.** *Suppose that $\mathbf{P}$ and $\mathbf{P}'$ are projective resolutions of M and M' respectively, and suppose $f \colon M \to M'$ is given. Then there exist functions $f_i \colon P_i \to P_i'$ making the following diagram commute:*

$$\begin{tikzcd}
\cdots \arrow[r, "d_2"] & P_1 \arrow[r, "d_1"] \arrow[d, dashed, "f_1"] & P_0 \arrow[r, "\varepsilon"] \arrow[d, dashed, "f_0"] & M \arrow[r] \arrow[d, "f"] & 0 \\
\cdots \arrow[r, "d_2'"] & P_1' \arrow[r, "d_1'"] & P_0' \arrow[r, "\varepsilon'"] & M' \arrow[r] & 0
\end{tikzcd}$$

Furthermore, the collection of maps f_i as a chain map, then any two choices of chain map are chain homotopic.

Proof. To show that f_n exists, we proceed by induction on n.

For the case that $n = 0$, we know by the surjectivity of ε' and the projectivity of P_0 that there is a map f_0 with $\varepsilon' f_0 = f\varepsilon$. This can be seen diagramatically:

$$\begin{tikzcd}
& P_0 \arrow[dl, dashed, "f_0"'] \arrow[d, "f\varepsilon"] & \\
P_0' \arrow[r, "\varepsilon'"'] & M' \arrow[r] & 0
\end{tikzcd}$$

The inductive step is a bit harder. Supposing f_i exists for $0 \leq i \leq n$, note that $\operatorname{im} f_n d_{n+1} \subseteq \ker d'_n$, since $d'_n f_n d_{n+1} = f_{n-1} d_n d_{n+1} = 0$. Therefore, by exactness, $\operatorname{im} f_n d_{n+1} \subseteq \operatorname{im} d'_{n+1}$.

Now consider the following diagram:

$$\begin{tikzcd} & P_{n+1} \arrow[dl, dashed] \arrow[d, "f_n d_{n+1}"] & \\ P'_{n+1} \arrow[r, "d'_{n+1}"'] & \operatorname{im} d'_{n+1} \arrow[r] & 0 \end{tikzcd}$$

By the defining property of projective modules there is a map marked by the dashed arrow that makes the diagram commute, which we call f_{n+1}.

It remains to show that this choice is unique up to homotopy, so suppose that f'_i is another collection of maps making the diagram commute. Recall that this means we will find maps $s_i \colon P_i \to P'_{i+1}$ such that $f_i - f'_i = d'_{i+1} s_i + s_{i-1} d_i$ as in Definition 6.7. Note that we need to show the existence of these maps for $i \geq -1$, where we define $P_{-1} = M$, $P_{-2} = 0$, and $f_{-1} = f'_{-1} = f$ – and continuing the numbering in the way implied by the diagram – because we can define $s_i = 0$ for lower negative terms. We proceed by induction on $i \geq -1$.

In the case that $i = -1$, we need to find a map $s_{-1} \colon M \to P'_0$ such that $f - f = d'_{i+1} s_{-1}$, so we may safely define $s_{-1} = 0$.

In the inductive case (when $i \geq 0$) note that if we can prove that:

$$\operatorname{im}\left(f_{i+1} - f'_{i+1} - s_i d_{i+1}\right) \subseteq \operatorname{im} d'_{i+2}, \tag{7.3}$$

then the following diagram gives us the map we need in the dashed arrow:

$$\begin{tikzcd} & P_{i+1} \arrow[dl, dashed] \arrow[d, "f_{i+1} - f'_{i+1} - s_i d_{i+1}"] & \\ P'_{i+2} \arrow[r, "d'_{i+1}"'] & \operatorname{im} d'_{i+2} \arrow[r] & 0 \end{tikzcd}$$

Indeed the inclusion in (7.1) holds since $\operatorname{im} d'_{i+2} = \ker d'_{i+1}$ and:

$$\begin{aligned} d'_{i+1}\left(f_{i+1} - f'_{i+1} - s_i d_{i+1}\right) &= d'_{i+1}(f_{i+1} - f'_{i+1}) - d'_{i+1} s_i d_{i+1} \\ &= d'_{i+1}(f_{i+1} - f'_{i+1}) - (f_i - f'_i - s_{i-1} d_i) d_{i+1} \\ &= (d'_{i+1} f_{i+1} - f_i d_i) - (d'_{i+1} f'_{i+1} - f'_i d_i) - 0 \\ &= 0 \end{aligned}$$

Hence we are done. □

There is a natural definition that is dual to that of a projective resolution, which albeit not easy to intuit, will turn out to be very helpful one.

Definition 7.4. An **injective resolution** of a module M is a collection of injective modules Q_i and connecting maps $d_{i+1} \colon Q_i \to Q_{i+1}$ and $\varepsilon \colon M \to Q_0$ such that the following sequence is exact:

$$0 \longrightarrow M \xrightarrow{\varepsilon} Q_0 \xrightarrow{d_0} Q_1 \xrightarrow{d_1} \cdots \xrightarrow{d_{n-1}} Q_n \xrightarrow{d_n} \cdots$$

We denote such a resolution as $\mathbf{Q}$.

In Section 5.4 we went to great lengths to show that there are 'enough injectives,' which is the result in Theorem 5.30. Here we see why: this shows that there is an injective resolution for any R-module, since we may sequentially find injective modules to embed the coimage of the previous inclusion into.

Remark. The statement of Theorem 7.2 carries over to injective resolutions due to the dual nature of injective and projective modules. This could be seen with a proof that is entirely similar to the one given, but we suggest here an unfortunately less rigorous but simpler argument for the same.

In light of Mitchell's full embedding theorem (Theorem 6.22), we may infer that the comparison theorem holds in any Abelian category, and therefore in particular it holds in the opposite category ${}_R\mathbf{Mod}^{\mathrm{op}}$. The statement for injective resolutions is then equivalent to the statement for projective resolutions in the opposite category, where we know it holds.

7.2 The Contravariant Ext Functor

We are now prepared to describe an important homological construction that we will use to ascertain certain properties of rings.

For all modules M, choose a corresponding projective resolution $\mathbf{P}$, which we will consider to be fixed and unchanging from now on. We will write $\mathbf{P}_M$ to denote the **deleted resolution** associated with $\mathbf{P}$, which simply replaces M with 0:

$$\mathbf{P}_M = \cdots \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} \cdots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \longrightarrow 0 \longrightarrow \cdots$$

Now let A and B be R-modules, and let $\mathbf{P}$ be a projective resolution of A. We write $\mathrm{Hom}(\mathbf{P}_A, B)$ to denote the following complex, where we denote the chain maps[5] as $\delta_{-n} = (d_{n+1})^*$:

$$\cdots \to 0 \to \mathrm{Hom}(P_0, B) \xrightarrow{\delta_0} \mathrm{Hom}(P_1, B) \xrightarrow{\delta_{-1}} \cdots \xrightarrow{\delta_{-(n-1)}} \mathrm{Hom}(P_n) \xrightarrow{\delta_{-n}} \cdots$$

Note that the functor $\mathrm{Hom}(\square, B)$ is contravariant, so this complex will be numbered in the negatives.

We now introduce the following definition for left R-modules. While we will work with R-modules in this and future sections, similar results hold for right modules too.

Definition 7.5 (Contravariant Ext)**.** For an R-module B and a natural n, define the contravariant functor $\mathrm{ext}^n_R(\square, B)\colon {}_R\mathbf{Mod} \to \mathbf{Ab}$ by:

$$\mathrm{ext}^n_R(A, B) = H_{-n}(\mathrm{Hom}(\mathbf{P}_A, B)) = \frac{\ker \delta_{-n}}{\mathrm{im}\, \delta_{1-n}} = \frac{\ker((d_{n+1})^*)}{\mathrm{im}((d_n)^*)}.$$

Given a map $f\colon A \to A'$ we define the map $f^{n*}\colon \mathrm{ext}^n_R(A', B) \to \mathrm{ext}^n_R(A, B)$ as follows. By Theorem 7.2 there is a chain map $(f_i)\colon \mathbf{P}_A \to P_{A'}$ which extends f, and moreover any two such maps are homotopic and remain homotopic after applying Hom, so by Proposition 6.8 the map induced on the homology is independent of choice of (f_i). We define f^{n*} to be this map.

Remarkably, this means that ext occurs completely independently of the choice of resolution – the particular case is stripped away by homology. We prove this now.

Proposition 7.6. *The value of* $\mathrm{ext}^n_R(A, B)$ *is independent of choice of projective resolution in its calculation.*

Proof. Let $\mathrm{ext}^n_R(A, B)$ be the value produced from the choice of resolution $\mathbf{P}$, and let $\overline{\mathrm{ext}}^n_R$ be produced from the choice of $\mathbf{P}'$.

The map 1_A extends by Theorem 7.2 to chain maps $(f_i)\colon \mathbf{P} \to \mathbf{P}'$ and $(g_i)\colon \mathbf{P}' \to \mathbf{P}$. Let $f^{n*}\colon \mathrm{ext}^n_R(A, B) \to \overline{\mathrm{ext}}^n_R(A, B)$ be as defined in Definition 7.5, and similarly for g^{n*}.

[5] We give the chain maps specific names so as to emphasise the indices at which they occur, as this affects the numbering of the homology groups.

Now the chain maps $(g_i f_i), (1_{P_i})\colon \mathbf{P} \to \mathbf{P}$ extend the map 1_A, so they are chain homotopic by Theorem 7.2. They remain chain homotopic after applying $\mathrm{Hom}(\square, B)$ since the functor is additive, and by Proposition 6.8 they produce the same map up to homotopy, namely $1 = (f_i g_i)^{n*} = f^{n*} g^{n*}$. A similar argument shows that $1 = g^{n*} f^{n*}$, so $\mathrm{ext}^n_R(A, B) \cong \overline{\mathrm{ext}}^n_R(A, B)$. $\square$

Proposition 7.7. *The functor* $\mathrm{ext}^n_R(\square, B)\colon {}_R\mathbf{Mod} \to \mathbf{Ab}$ *is additive.*

Proof. If we have maps $f, g\colon A \to A'$, then it is easy to check that if f_i and g_i extend the maps f and g to chain maps, then $f_i + g_i$ extends $f + g$ to a chain map. The remaining functors involved in the definition of ext are additive, so since $f_i + g_i$ is unique up to chain homotopy, the functor distributes over addition. $\square$

Corollary 7.8. *If* P *is projective, then* $\mathrm{ext}^n_R(P, B) = 0$ *for all modules* B *and* $n \geq 1$*.*

Proof. If P is projective, then $\mathbf{P} = \cdots \to 0 \to P \to P \to 0$ is a projective resolution. The definition then gives us that $\mathrm{ext}^n_R(P, B) = \ker 0 / \operatorname{im} 0 = 0$ since $Q_n = 0$ for $n \geq 1$. $\square$

Proposition 7.9 (Dimension Shifting)**.** *Let* $\mathbf{P}_A$ *be a projective resolution for a module* A*, with boundary maps* $d_i\colon P_i \to P_{i-1}$*. Define* $K_{i+1} = \ker d_i$*, where we shall say that* $d_{-1} = 0\colon A \to 0$*. Then:*

$$\mathrm{ext}^n_R(A, B) \cong \mathrm{ext}^1_R(K_n, B).$$

Proof. Observe that the following is a projective resolution for K_n:

$$\cdots \to P_{n+1} \xrightarrow{d_{n+1}} P_n \xrightarrow{d_{n+1}} K_n \to 0.$$

We may calculate ext in this case, noting that P_n is now in index 0 from the perspective of K_n:

$$\mathrm{ext}^1_R(K_n, B) = \frac{\ker((d_{n+1})^*)}{\operatorname{im}((d_n)^*)} = \mathrm{ext}^n_R(A, B).$$

This completes the proof. $\square$

Recall the long exact sequence, Theorem 6.10. Since the theorem applies when we have an exact sequence of chain complexes, perhaps we would like to show that, given an exact sequence of modules:

$$0 \to A \to B \to C \to 0,$$

we miraculously have a long exact sequence of deleted resolutions under the image of Hom:

$$0 \to \mathrm{Hom}(\mathbf{P}_A, X) \to \mathrm{Hom}(\mathbf{P}_B, X) \to \mathrm{Hom}(\mathbf{P}_C, X) \to 0.$$

However there is no obvious reason that this powerful result should be true. Why should we obtain an exact sequence in the latter case? A pair of clever lemmas show us the way.

Lemma 7.10 (The Horseshoe Lemma)**.** *Suppose there are modules* A*,* B*,* C*, and projective resolutions* $\mathbf{P}$ *and* $\mathbf{P}''$ *of* A *and* C *respectively, such that the following diagram commutes:*

$$\begin{tikzcd}
 & \vdots \arrow[d] & & \vdots \arrow[d] & \\
 & P_1 \arrow[d] & & P''_1 \arrow[d] & \\
 & P_0 \arrow[d] & & P''_0 \arrow[d] & \\
0 \arrow[r] & A \arrow[r, "f"'] \arrow[d] & B \arrow[r, "g"'] & C \arrow[r] \arrow[d] & 0 \\
 & 0 & & 0 &
\end{tikzcd}$$

Then there also exists a projective resolution $\mathbf{P}'$ of B and chain maps $\mathbf{P} \to \mathbf{P}'$ and $\mathbf{P}' \to \mathbf{P}''$ extending f and g such that the diagram below commutes, and has exact rows and columns:

$$
\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
0 \arrow[r] & P_1 \arrow[r] \arrow[d] & P_1' \arrow[r] \arrow[d] & P_1'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & P_0 \arrow[r] \arrow[d] & P_0' \arrow[r] \arrow[d] & P_0'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A \arrow[r, "f"'] \arrow[d] & B \arrow[r, "g"'] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}
$$

Proof. We will use an observation in Section 4, in particular Proposition 4.7: instead of constructing the entire diagram at once, we will construct short exact sequences and glue them back together.

Consider the following diagram with exact rows and columns, where we choose to define $f_0(x) = (x, 0)$ and $g_0(x, x'') = x''$:

$$
\begin{tikzcd}
 & 0 \arrow[d] & & 0 \arrow[d] & \\
 & \ker d_0 \arrow[d] & & \ker d_0'' \arrow[d] & \\
0 \arrow[r] & P_0 \arrow[r, "f_0"'] \arrow[d] & P_0 \oplus P_0'' \arrow[r, "g_0"'] & P_0'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A \arrow[r, "f"'] \arrow[d] & B \arrow[r, "g"'] & C \arrow[r] \arrow[d] & 0 \\
 & 0 & & 0 &
\end{tikzcd}
$$

Note that, via Corollary 5.9, $P_0 \oplus P_0''$ is projective – call it P_0'. Since P_0'' is projective, we have a map $\sigma \colon P_0'' \to A$ such that $g\sigma = d_0''$. Now define $d_0' \colon P_0' \to B$ by $(x, x'') \mapsto fd_0(x) + \sigma(x'')$.

We wish to show that d_0' is surjective now. Let $b \in B$, and by surjectivity of d_0'' let $y \in P_0''$ be such that $d_0''(y) = g(b)$. Now $g(b - \sigma(y)) = g(b) - d_0''(y) = 0$, so by exactness there is an $a \in A$ and $x \in P_0$ such that $d_0(x) = a$ and $f(a) = b - \sigma(y)$. Then we see that $d_0'(x, y) = fd_0(x) + \sigma(y) = b$, so indeed d_0' is surjective.

So far, we have the following commutative diagram with exact rows and columns – we need to fill out the top row:

$$
\begin{tikzcd}
 & 0 \arrow[d] & & 0 \arrow[d] & \\
0 \arrow[r] & \ker d_0 \arrow[d] & & \ker d_0'' \arrow[d] \arrow[r] & 0 \\
0 \arrow[r] & P_0 \arrow[r, "f_0"'] \arrow[d, "d_0"] & P_0' \arrow[r, "g_0"'] \arrow[d, "d_0'"] & P_0'' \arrow[r] \arrow[d, "d_0''"] & 0 \\
0 \arrow[r] & A \arrow[r, "f"'] \arrow[d] & B \arrow[r, "g"'] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}
$$

We now show that $\ker d_0'$ fits the shoe. If $x \in \ker d_0$, then $d_0' f_0(x) = f d_0(x) = 0$, so f_0 restricted to $\ker d_0$ is a map $\ker d_0 \to \ker d_0'$. A similar argument shows that g_0 restricts to a map $\ker d_0' \to \ker d_0''$. Now we know exactness already from the middle row, so in fact we have filled out the whole three-by-three diagram:

$$
\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \ker d_0 \arrow[r] \arrow[d] & \ker d_0' \arrow[r] \arrow[d] & \ker d_0'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & P_0 \arrow[r, "f_0"'] \arrow[d, "d_0"] & P_0' \arrow[r, "g_0"'] \arrow[d, "d_0'"] & P_0'' \arrow[r] \arrow[d, "d_0''"] & 0 \\
0 \arrow[r] & A \arrow[r, "f"'] \arrow[d] & B \arrow[r, "g"'] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}
$$

The same argument works to complete the following diagram for any $n \geq 1$, provided all previous d_n' exist – that is, by induction:

$$
\begin{tikzcd}
 & \ker d_n \arrow[d] & & \ker d_n'' \arrow[d] & \\
 & P_n \arrow[d] & & P_n'' \arrow[d] & \\
0 \arrow[r] & \ker d_{n-1} \arrow[r] \arrow[d] & \ker d_{n-1}' \arrow[r] & \ker d_{n-1}'' \arrow[r] \arrow[d] & 0 \\
 & 0 & & 0 &
\end{tikzcd}
$$

We then use the aforementioned observation of Proposition 4.7 to glue the diagrams together, obtaining the desired result. □

Corollary 7.11 (The Long Exact Sequence for ext)**.** *Given an exact sequence of R-modules:*

$$0 \to A \to B \to C \to 0,$$

and some other module X, there is an exact sequence:

$$0 \to \mathrm{ext}_R^0(C, X) \to \mathrm{ext}_R^0(B, X) \to \mathrm{ext}_R^0(A, X) \to \mathrm{ext}_R^1(C, X) \to \cdots$$

Proof. By the Horseshoe Lemma, there is an exact sequence:

$$0 \to \mathbf{P}_A \to \mathbf{P}_B \to \mathbf{P}_C \to 0.$$

Every horizontal exact sequence in this splits by Proposition 5.24, and a split exact sequence remains split exact under $\mathrm{Hom}(\square, X)$ – this is a consequence of Proposition 6.20. Ergo we have an exact sequence:

$$0 \to \mathrm{Hom}(\mathbf{P}_C, X) \to \mathrm{Hom}(\mathbf{P}_B, X) \to \mathrm{Hom}(\mathbf{P}_A, X) \to 0,$$

and the long exact sequence (Theorem 6.10) finishes things. $\square$

The functor $\mathrm{ext}^n_R(\square, B)$ is in some way a continuation of $\mathrm{Hom}(\square, B)$, as the following observation shows:

Proposition 7.12. $\mathrm{ext}^0_R(A, B) \cong \mathrm{Hom}_R(A, B)$.

Proof. Given a projective resolution:

$$\mathbf{P} = \cdots \to P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} A \to 0,$$

Applying $\mathrm{Hom}(\square, B)$ and recalling Proposition 4.12, we have an exact sequence:

$$0 \to \mathrm{Hom}(A, B) \xrightarrow{d_0^*} \mathrm{Hom}(P_0, B) \xrightarrow{d_1^*} \mathrm{Hom}(P_1, B).$$

Now recalling the definition of ext:

$$\mathrm{Hom}(A, B) \cong \mathrm{im}\, d_0^* = \ker d_1^* = \frac{\ker d_1^*}{\mathrm{im}\, 0} = \mathrm{ext}^0_R(A, B). \qquad \square$$

Remark. Given the previous proposition and Corollary 7.11, we can see ext as 'repairing' the exactness of $\mathrm{Hom}(\square, X)$. If we have an exact sequence $0 \to A \to B \to C \to 0$, we can only guarantee that the sequence:

$$0 \to \mathrm{Hom}(C, X) \to \mathrm{Hom}(B, X) \to \mathrm{Hom}(A, X)$$

is exact. However in the context of the long exact sequence, we can continue this to obtain an exact sequence:

$$0 \to \mathrm{Hom}(C, X) \to \mathrm{Hom}(B, X) \to \mathrm{Hom}(A, X) \to \mathrm{ext}^1_R(C, X) \to \mathrm{ext}^1_R(B, X) \to \cdots$$

Hence the ext terms 'repair' the partial exactness of contravariant Hom.

7.3 The Covariant Ext Functor

In the previous section, we worked with projective resolutions and applied a left exact, contravariant functor to obtain a chain complex with negative entries. In this brief section, we will apply a *covariant* functor to obtain a chain complex with negative entries, but in doing so, we cannot begin with a projective resolution – we must use injective ones.

As we did previously, choose once and for all an injective resolution $\mathbf{Q}$ for every module B, and denote by $\mathbf{Q}_B$ the deleted resolution:

$$\mathbf{Q}_b = 0 \to Q_0 \xrightarrow{d_0} Q_1 \xrightarrow{d_1} \cdots.$$

Definition 7.13 (Covariant Ext)**.** For an R-module A and a natural n, define the covariant functor $\mathrm{Ext}^n_R(A, \square) \colon {}_R\mathbf{Mod} \to \mathbf{Ab}$ by:

$$\mathrm{Ext}^n_R(A, B) = H_{-n}(\mathrm{Hom}(A, \mathbf{Q}_B)) = \frac{\ker(d_n)_*}{\mathrm{im}(d_{n-1})_*},$$

where we will set $d_{-1} = 0$. Via the dual of Theorem 7.2 and the same argument as in Definition 7.5, we have for every map $f : B \to B'$ a map $f^{n*} \colon \mathrm{Ext}^n_R(A, B) \to \mathrm{Ext}^n_R(A, B')$.

In the light of our comments on Abelian categories (see Section 6.3) we can use the dual statement of much of what we proved about ext to prove the same about Ext.

Corollary 7.14. *The value of* $\operatorname{Ext}^n_R(A, B)$ *is independent of choice of injective resolution for* B.

Proof. We use the dual of Theorem 7.2 and the same argument as in Proposition 7.6 $\square$

Corollary 7.15. *The functor* $\operatorname{Ext}^n_R(A, \square)\colon {}_R\mathbf{Mod} \to \mathbf{Ab}$ *is additive.*

Proof. This is the dual argument to Proposition 7.7. $\square$

Corollary 7.16. *If* Q *is injective, then* $\operatorname{Ext}^n_R(A, Q) = 0$ *for all* $n \geq 1$.

Proof. This is the dual argument to Corollary 7.8. $\square$

Corollary 7.17 (Dimension Shifting)**.** *Let* $\mathbf{Q}_A$ *be an injective resolution for a module* B, *with boundary maps* $d_i\colon Q_i \to Q_{i+1}$. *Define* $C_j = \ker d_j$. *Then:*

$$\operatorname{Ext}^n_R(A, B) \cong \operatorname{Ext}^1_R(A, C_n).$$

Proof. This is the dual argument to Proposition 7.9. $\square$

Corollary 7.18. $\operatorname{Ext}^0_R(A, B) \cong \operatorname{Hom}_R(A, B)$

Proof. This is the dual argument to Proposition 7.12. $\square$

Corollary 7.19 (The Long Exact Sequence for Ext)**.** *Given an exact sequence of* R*-modules:*

$$0 \to A \to B \to C \to 0$$

and some other module X, *there is an exact sequence:*

$$0 \to \operatorname{Ext}^0_R(X, A) \to \operatorname{Ext}^0_R(X, B) \to \operatorname{Ext}^0_R(X, C) \to \operatorname{Ext}^1_R(X, A) \to \operatorname{Ext}^1_R(X, B) \to \cdots.$$

Proof. This uses the dual of Lemma 7.10 and the same argument as Corollary 7.11, but taking care to note that the functor is covariant. $\square$

Example 7.20. Let us characterise all finitely generated $\mathbb{Z}$-modules A such that $\operatorname{Ext}^1_{\mathbb{Z}}(A, \mathbb{Z}) \cong 0$. Firstly, observe the following injective resolution of $\mathbb{Z}$, which we showed to be injective in Examples 5.20.

$$\mathbf{Q} = 0 \to \mathbb{Z} \hookrightarrow \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0.$$

Now it arrives from the definition of covariant Ext that the following is true, where $\eta\colon \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ is the natural map.

$$\operatorname{Ext}^1_{\mathbb{Z}}(A, \mathbb{Z}) \cong \frac{\operatorname{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})}{\{\eta f \mid f \in \operatorname{Hom}_{\mathbb{Z}}(A, \mathbb{Q})\}}$$

The question can then be rephrased as follows: for what Abelian groups A is it true that every map $A \to \mathbb{Q}/\mathbb{Z}$ can be lifted to a map $A \to \mathbb{Q}$? The following diagram illustrates:

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[dr, dashed] & \mathbb{Q}/\mathbb{Z} \\
& \mathbb{Q} \arrow[u, "\eta"']
\end{tikzcd}$$

We claim that this holds exactly when A is free, or in other words when A contains no elements of finite order since A is assumed to be finitely generated.

This is not difficult to see. If A contains an element a of finite order, then firstly $g(a) = 0$ for any $g: A \to \mathbb{Q}$. However, noting that $\mathbb{Z}a$ is a cyclic group, we can define a map $\mathbb{Z}a \to \mathbb{Q}/\mathbb{Z}$ by $a \mapsto 1/n$, where n is the order of a. Then the injectivity of $\mathbb{Q}/\mathbb{Z}$ extends this to a map $f: A \to \mathbb{Q}/\mathbb{Z}$ such that $f(a) = 1/n + \mathbb{Z}$, which now evidently cannot be lifted. That this *can* be done for free $\mathbb{Z}$-modules is a consequence of it being possible for $A = \mathbb{Z}$: if $f(1) = q + \mathbb{Z}$, then we define the map $\bar{f}: A \to \mathbb{Q}$ as $f(1) = q$. The free case then follows from direct sums.

We have therefore calculated that for a finitely generated Abelian group A, we have $\mathrm{Ext}^1(A, \mathbb{Z}) = 0$ exactly when A is free.

7.4 Unifying the Ext Functors

Due to our choice of notation, it has been all but said that the two functors we have just defined in fact produce isomorphic results. We now endeavour to show this to be the case, beginning with some easier results.

Lemma 7.21. *Suppose the following diagram with exact rows commutes:*

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow{p} & C & & \\ & & \alpha\uparrow & & \beta\uparrow & & \gamma\uparrow & & \\ & & A' & \xrightarrow[i']{} & B' & \xrightarrow[p']{} & C' & \longrightarrow & 0 \end{array}$$

There exist maps for which there is an exact sequence:

$$\ker \beta \to \ker \gamma \to \operatorname{coker} \alpha \to \operatorname{coker} \beta.$$

Proof. The reader will be delighted to know that this is another diagram-chasing proof, similar to that of Theorem 6.10 − be prepared!

The map we choose from $\ker \beta \to \ker \gamma$ shall be p', restricted to the smaller domain. To see that this works, suppose $\beta(b) = 0$. Then $0 = p\beta(b) = \gamma p'(b)$, so $p'(b) \in \ker \gamma$.

The map from $\operatorname{coker} \alpha$ to $\operatorname{coker} \beta$ shall also be called i, and defined as $i(a + \operatorname{im} \alpha) = i(a) + \operatorname{im} \beta$. The well-definedness of this reduces to showing that $i(\operatorname{im} \alpha) \subseteq \operatorname{im} \beta$, which is easy to see as $i\alpha(a) = \beta i'(b)$.

The map connecting $\ker \gamma$ and $\operatorname{coker} \alpha$ is more complicated. We shall define this map, called ∂ as follows, using this diagram as guidance:

$$\begin{array}{ccccc} \exists a & \longmapsto & \beta(b) & \longmapsto & 0 \\ & & \uparrow & & \uparrow \\ & & \exists b & \longmapsto & c \end{array}$$

Suppose $c \in \ker \gamma$. Since p' is surjective, there is some $b \in B'$ with $p'(b) = c$. Now $p\beta(b) = \gamma p'(b) = 0$, so $\beta(b) \in \ker p = \operatorname{im} i$, so there is some $a \in A$ such that $i(a) = \beta(b)$.

We claim that $\partial(c) = a + \operatorname{im} \alpha$ is well-defined. Suppose $c \in C$. Then as above, let $b, b' \in B'$ be possibly distinct choices such that $p'(b) = p'(b') = c$. Then let $a, a' \in A$ be such that $i(a) = \beta(b)$ and $i(a') = \beta(b')$. We need only show that $a - a' \in \operatorname{im} \alpha$. Note that $b - b' \in \ker p'$, so there is some $q \in A'$ with $i'(q) = b - b'$. Now $i\alpha(q) = \beta i'(q) = \beta(b) - \beta(b') = i(a - a')$, so by injectivity of i we have $\alpha(q) = a - a'$, and we are done.

We have thoroughly chased the definitions of these maps through the diagram, and we are now prepared to show exactness.

We can see that $\operatorname{im} p' \subseteq \ker \partial$, since if $c = p'(b)$ for some $b \in \ker \beta$, then $\beta(b) = 0$, so $a = 0$ is a possible choice. For the reverse inclusion, suppose a and b are chosen as in the construction of $\partial(c)$. Then supposing $a \in \operatorname{im} \alpha$, let's say $\alpha(q) = a$ for some $q \in A'$.

Then certainly $\beta(b) = i\alpha(q) = \beta i'(q)$ Now note that $\beta(b - i'(q)) = 0$, so $b - i'(q) \in \ker\beta$ Furthermore $p'(b - i'(q)) = c - p'i'(q) = c$, so in fact the reverse inclusion holds.

Finally we show $\operatorname{im}\partial = \ker i$. The inclusion of the former in the latter can be seen by supposing c is given and a, b are as in the construction of $\partial(c)$, and noting that since $i(a) = \beta(b)$, we have $i(a + \operatorname{im}\alpha) = \beta(b) + \operatorname{im}\beta$.

We now show the final inclusion of $\ker i$ in $\operatorname{im}\partial$. Suppose $a \in A$ is such that $i(a) = \beta(b)$ for some $b \in B'$. But then setting $c = p'(b)$, we have followed exactly the construction of $\partial(c)$. By our proof of well-definedness, we conclude that $a + \operatorname{im}\alpha = \partial(c)$. □

This proof should be compared to that of Theorem 6.10. In fact we could have shown a slightly wider sequence to be exact, after which the long exact sequence is a corollary that follows after some short work. In the literature, a slightly stronger version of this would be referred to as the Snake Lemma[6].

Theorem 7.22 (Ext and ext coincide)**.** $\operatorname{Ext}^n_R(A, B) \cong \operatorname{ext}^n_R(A, B)$.

Proof. Suppose that $\mathbf{P}$ and $\mathbf{Q}$ are a projective resolution for A and an injective resolution for B respectively. Let $d_i \colon P_i \to P_{i-1}$ be the boundary maps for $\mathbf{P}$ and let $d'_i \colon Q_i \to Q_{i+1}$ be those for $\mathbf{Q}$. Define $K_{i+1} = \ker d_i$ (where $K_0 = A$) and $C_i = \ker d'_i$, so that we have exact sequences:

$$0 \to K_{i+1} \hookrightarrow P_i \xrightarrow{d_i} K_i \to 0$$
$$0 \to C_i \hookrightarrow Q_i \xrightarrow{d_i} C_{i+1} \to 0$$

Recalling Proposition 5.27, we have the following commutative diagram with exact rows and columns, where we shall temporarily ignore the dashed lines:

$$\begin{tikzcd}
 & W & 0 \arrow[r, dashed] & X & \\
0 \arrow[r] & \operatorname{Hom}(K_{i+1}, C_j) \arrow[r] \arrow[u] & \operatorname{Hom}(K_{i+1}, Q_j) \arrow[r, "f"] \arrow[u] & \operatorname{Hom}(K_{i+1}, C_{j+1}) \arrow[r, "j"] \arrow[u, "i"] & Y \\
0 \arrow[r] & \operatorname{Hom}(P_i, C_j) \arrow[r] \arrow[u, "p"] & \operatorname{Hom}(P_i, Q_j) \arrow[r, "g"] \arrow[u, "q"] & \operatorname{Hom}(P_i, C_{j+1}) \arrow[r] \arrow[u, "r"] & 0 \arrow[u, dashed] \\
0 \arrow[r] & \operatorname{Hom}(K_i, C_j) \arrow[r] \arrow[u] & \operatorname{Hom}(K_i, Q_j) \arrow[r, "h"] \arrow[u] & \operatorname{Hom}(K_i, C_{j+1}) \arrow[r] \arrow[u] & Z \\
 & 0 \arrow[u] & 0 \arrow[u] & 0 \arrow[u] &
\end{tikzcd}$$

We let W, X, Y, and Z be the cokernels of the maps that precede them. By the long exact sequences for Ext and ext (Corollaries 7.11 and 7.19) and noting that $\operatorname{ext}^1_R(P_i, C_j) \cong \operatorname{ext}^1_R(P_i, C_{j+1}) \cong 0$ and $\operatorname{Ext}^1_R(K_{i+1}, Q_j) \cong \operatorname{Ext}^1_R(K_i, Q_j) \cong 0$ by Corollaries 7.8 and 7.16, we see that we may identify these cokernels as follows:

$$W \cong \operatorname{ext}^1_R(K_i, C_j), \qquad Y \cong \operatorname{Ext}^1_R(K_{i+1}, C_j),$$
$$X \cong \operatorname{ext}^1_R(K_i, C_{j+1}), \qquad Z \cong \operatorname{Ext}^1_R(K_i, C_j).$$

Lemma 7.21 gives us the following exact sequence:

$$\ker q \to \ker r \to W \to 0$$

[6] A partial proof of this lemma may be found in the 1980 film *It's My Turn* directed by Claudia Weill.

The diagram gives us explicit values for the kernels listed, and even the map between them So in fact we have the following exact sequences:

$$\mathrm{Hom}(K_i, Q_j) \xrightarrow{h} \mathrm{Hom}(K_i, C_{j+1}) \to W \to 0$$

So in fact $W \cong \operatorname{coker} h \cong Z$. In other words:

$$\mathrm{Ext}^1_R(K_i, C_j) \cong \mathrm{ext}^1_R(K_i, C_j). \tag{7.23}$$

Setting $i = j = 0$, we have the beginnings of a promising conclusion, since $K_0 = A$ and $C_0 \cong B$:

$$\mathrm{Ext}^1_R(A, B) \cong \mathrm{ext}^1_R(A, B).$$

Let us press on so that we may show this for higher Ext and ext.

We now address the dashed lines: indeed they commute with the diagram, which we show now. Our goal is to see that $if = 0$ and $jr = 0$. Observe that $ifq = irg = 0g = 0q$, but q is surjective (or put differently, an epimorphism) so we conclude that $if = 0$. The argument for jr is entirely similar.

The incorporation of these maps into the diagram now tells us that:

$$\begin{aligned} \operatorname{im} f = \ker j \supseteq \operatorname{im} r = \ker i; \\ \operatorname{im} r = \ker i \supseteq \operatorname{im} f = \ker j, \end{aligned}$$

So in fact $\operatorname{im} f = \operatorname{im} r$, so $Y = \operatorname{coker} f = \operatorname{coker} r = X$. By our characterisation of X and Y above, we see that:

$$\mathrm{ext}^1_R(K_i, C_{j+1}) \cong \mathrm{Ext}^1_R(K_{i+1}, C_j). \tag{7.24}$$

Let us reflect upon this for a moment. This isomorphism allows us to step diagonally along the indices of K_{i+1} and C_j. Combining this with dimension shifting (Propositions 7.17 and 7.9) we can argue by a sort of induction – at each application of (7.24) decreasing the index of K_{i+1} and increasing the index of C_j:

$$\begin{aligned} \mathrm{ext}^n_R(A, B) &\cong \mathrm{ext}^1_R(K_n, C_0) && \text{Proposition 7.9} \\ &\cong \mathrm{Ext}^1_R(K_n, C_0) && \text{by. (7.23)} \\ &\cong \mathrm{ext}^1_R(K_{n-1}, C_1) && \text{by (7.24)} \\ &\cong \cdots \\ &\cong \mathrm{Ext}^1_R(K_0, C_n) && \text{by (7.23)} \\ &\cong \mathrm{Ext}^n_R(A, B) && \text{Proposition 7.17} \end{aligned}$$

This finishes the proof. □

From now on, we will leave the distinction between Ext and ext behind, and simply use the notation of the former.

7.5 Ext and Extensions

If we have modules A, B, and C, and an exact sequence:

$$0 \to A \to B \to C \to 0,$$

then we say that B is an **extension** of C by A. A very natural question to ask is, given A and C, what are the possible values of B?

We are already familiar with an extension that occurs in any case: $B = A \oplus C$. However this is far from the only extension in general. For instance, when working with $\mathbb{Z}$-modules, we might consider for example the extensions of $\mathbb{Z}_2$ by itself. There are precisely two:

$\mathbb{Z}_2 \oplus \mathbb{Z}_2$, and $\mathbb{Z}_4$ – this can be found by checking all groups of order 4 – indeed this is all of them.

Remarkably, Ext can measure group extensions in a direct way. We begin with a hint of how it does so.

Proposition 7.25. *If* $\operatorname{Ext}^1_R(C, A) = 0$*, then* $A \oplus C$ *is the only extension of* C *by* A*.*

Proof. Recall the long exact sequence for covariant Ext (Corollary 7.19). If we have a short exact sequence $0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$, we conclude we have an exact sequence after applying $\operatorname{Ext}^i_R(C, \square)$:

$$\operatorname{Hom}(C, B) \xrightarrow{p_*} \operatorname{Hom}(C, C) \to \operatorname{Ext}^1_R(C, A) = 0.$$

This means that p_* is surjective, so in particular there is a map $j \colon C \to B$ with $pj = 1_C$, so by the splitting lemma (Proposition 5.23) the short exact sequence splits. $\square$

Corollary 7.26. *An* R*-module* P *is projective if and only if* $\operatorname{Ext}^1_R(P, B) = 0$ *for all* B*, and* Q *is injective if and only if* $\operatorname{Ext}^1_R(A, Q) = 0$ *for all* A*.*

Proof. The fact that $\operatorname{Ext}^1_R(P, B) = 0$ is necessary is Corollary 7.8. Sufficiency is then Proposition 5.25 combined with the previous proposition. The statement for injective modules is dual, but applying Proposition 5.31 in place of Proposition 5.25. $\square$

Miraculously, the elements of $\operatorname{Ext}^1_R(C, A)$ are in a kind of bijection with the extensions of C by A, meaning that the above result is a small example of a larger pattern.

For a simple illustration of this fact, consider $C = A = \mathbb{Z}_2$. Firstly, we have a free resolution:

$$0 \to \mathbb{Z} \xrightarrow{z \mapsto 2z} \mathbb{Z} \to \mathbb{Z}_2 \to 0,$$

so we may calculate $\operatorname{Ext}^1_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}_2) = \ker d_2^* / \operatorname{im} d_1^*$ by noting that $\operatorname{Hom}(\mathbb{Z}, \mathbb{Z}_2) \cong \mathbb{Z}_2$ via $f \mapsto f(1)$, and hence seeing:

$$\operatorname{Ext}^1_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}_2) \cong \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2.$$

This is a group of order 2, reflecting the fact that there are exactly 2 extensions!

Via a correspondence between the first Ext group and certain equivalence classes of extensions, we obtain an Abelian group structure on the extensions. This structure was first discovered by Baer, hence it is called the Baer sum – although Baer was not privy to the higher Ext groups.

So what do the higher Ext groups represent, if the first corresponds to extensions? We may think of extensions as being merely 1-ary extensions, since there is a single gap to fill in the exact sequence beginning with A and ending with C. In fact, if we look at 2-ary extensions, there is a correspondence between these and Ext^2, and so on. This correspondence is due to the work of Nobuo Yoneda, who is best known for the Yoneda Lemma in category theory. Proving these correspondences is ultimately beyond the scope of this project.

8 Homological Dimensions of Rings

The work we have done in previous sections now culminates to explore certain homological properties of rings. One observation that leads us towards the coming ideas is as follows. If our ring is a vector space, then every module is projective – in particular they are all free. If our ring is the integers, though, the same cannot be said – we have the presence of torsion amongst finitely generated modules, for example. However this deviation from projectivity is only slight! If we look at a presentation for a $\mathbb{Z}$-module M, due to the surprising fact that any submodule of a free $\mathbb{Z}$-module is also free, the module itself is very conveniently described as a quotient.

Put differently, for any $\mathbb{Z}$-module, we have an exact sequence:

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

where F_0 and F_1 are both free. In this way, we might see this as describing how far $\mathbb{Z}$-modules can be from being free. Not far at all, it seems!

We proceed to make these notions precise.

8.1 Projective Dimension, Injective Dimension, and Ext

To describe the distance that a module M is from being projective, we will use the notion of a length of a resolution.

Definition 8.1. A projective resolution $\mathbf{P}$ for a module M is of **length** n if $P_{n+1} = 0$ and $P_n \neq 0$:

$$\mathbf{P} = \cdots \to 0 \to P_n \to P_{n-1} \to \cdots \to P_0 \to M \to 0.$$

It may be that this property is not satisfied for any n as $P_i \neq 0$ for all $i \geq 0$. In this case, we say that the projective resolution has length ∞ – we consider this purely formally.

If we have some projective resolution for an R-module, we can always inflate it to any length we choose due to direct sums. For example if we have a projective resolution $\mathbf{P}$ with boundary maps $d_i \colon P_i \to P_{i-1}$, we can then construct a resolution $\mathbf{P'}$ like so:

$$\mathbf{P'} = \cdots \to P_3 \oplus R^2 \to P_2 \oplus R^2 \to P_1 \oplus R \to P_0 \to M \to 0,$$

where the boundary maps are $d'_1(p, r) = d_1(p)$, $d'_2(p, r, s) = (d_2(p), s)$, and $d'_i(p, r, s) = (d_i(p), s, 0)$. This projective resolution then has length ∞.

Since we may construct such unhelpful examples of resolutions, we must not consider just one projective resolution, but rather those of minimal length when considering how distant a module is from being projective.

Definition 8.2. The **projective dimension** $\mathrm{pd}(M)$ of an R-module M is the minimal length of a projective resolution of M.

It is worth noting that the projective dimension depends on the ring we choose, and we will write $\mathrm{pd}_R(M)$ to elucidate the ring R. Indeed if we look at $\mathbb{Z}$-modules, our comments at the beginning of the chapter show that $\mathrm{pd}_{\mathbb{Z}}(M) \leq 1$ always, but the projective dimension over other rings can be higher – though we have not seen it yet.

The only tool we have acquired so far that is clearly useful in determining the projective dimension of a module is the direct calculation of a projective resolution. This method is useful in determining upper bounds, but woefully unhelpful in finding *lower* bounds on the projective dimension. What tool should we then use to find such a bound? Conveniently, a particularly incisive tool can be found in Ext – but first we must hone its edge for the problem at hand. As always, lemmas will precede the larger result.

Theorem 8.3 (Schanuel's Lemma)**.** *Let M be some module, and let the following sequences be exact, where P and P' are projective:*

$$0 \to K \to P \to M \to 0 \quad \textit{and} \quad 0 \to K' \to P' \to M \to 0.$$

Then $K \oplus P' \cong K' \oplus P$.

Proof. We will consider, without loss of generality, that $K \subseteq P$ and $K' \subseteq P'$. Let $f\colon P \to M$ and $f'\colon P' \to M$ be the surjections. Since P is projective, there exists a map $P \to P'$ with $f'g = f$. Consider the pullback of f and f' – that is, the module $E = \{(p, q) \mid f(p) = f'(q)\}$.

Now define a map from $P \oplus K'$ to E by sending (p, k) to $(p, g(p)+k)$ – indeed this maps to E since $f'(g(p)+k) = f(p)+0 = f(p)$. This is injective since if $p = 0$ then $g(p)+k = k = 0$ also, and it is surjective since if $(p, q) \in E$, then $f'(q - g(p)) = f'(q) - f(p) = 0$, so $(p, q - g(p)) \in P \oplus K'$ maps to (p, q).

So we have an isomorphism $P \oplus K' \cong E$, and symmetrically we also have $P' \oplus K \cong E$ – hence we are done. ☐

Corollary 8.4 (Generalised Schanuel Lemma)**.** *Let $\mathbf{P}$ and $\mathbf{P}'$ be projective resolutions for a module M with boundary maps d_i and d_i' respectively. Then for any $i \geq 0$ there exist projective modules Q and Q' such that:*

$$\ker d_i \oplus Q \cong \ker d_i' \oplus Q'.$$

Proof. We have already shown the $i = 0$ case in the previous theorem. We proceed by induction. Suppose that $\ker d_i \oplus Q \cong \ker d_i' \oplus Q'$ for some projective modules Q and Q'. We have two short exact sequences:

$$0 \to \ker d_{i+1} \to P_{i+1} \to \ker d_i \to 0 \quad \text{and} \quad 0 \to \ker d_{i+1}' \to P_{i+1}' \to \ker d_i' \to 0.$$

We can augment these to the following short exact sequences, both times including the kernel on the left into the first component of the direct sum:

$$0 \to \ker d_{i+1} \to P_{i+1} \oplus Q \xrightarrow{d_{i+1} \oplus 1_Q} \ker d_i \oplus Q \to 0$$
$$0 \to \ker d_{i+1}' \to P_{i+1}' \oplus Q' \xrightarrow{d_{i+1}' \oplus 1_{Q'}} \ker d_i' \oplus Q' \to 0$$

Since the rightmost terms are isomorphic, we apply Theorem 8.3 to obtain that:

$$\ker d_{i+1} \oplus P_{i+1}' \oplus Q' \cong \ker d_{i+1}' \oplus P_{i+1} \oplus Q,$$

and by Corollary 5.9, we are done. ☐

Proposition 8.5. *Suppose that $\mathbf{P}$ and $\mathbf{P}'$ are projective resolutions of a module M with boundary maps d_i and d_i' respectively. Then $\operatorname{Ext}_R^n(\ker d_i, B) \cong \operatorname{Ext}_R^n(\ker d_i', B)$ for any module B and $n, i \geq 0$.*

Proof. From the generalised Schanuel lemma (Corollary 8.4) there are projective modules Q and Q' such that $\ker d_i \oplus Q \cong \ker d_i' \oplus Q'$. Since $\operatorname{Ext}_R^n(\square, B)$ is additive (Proposition 7.7) by Corollary 6.21 and Corollary 7.8, we see that:

$$\begin{aligned}
&\operatorname{Ext}_R^n(\ker d_i, B) \\
\cong\ &\operatorname{Ext}_R^n(\ker d_i, B) \oplus \operatorname{Ext}_R^n(Q, B) \\
\cong\ &\operatorname{Ext}_R^n(\ker d_i \oplus Q, B) \\
\cong\ &\operatorname{Ext}_R^n(\ker d_i' \oplus Q', B) \\
\cong\ &\operatorname{Ext}_R^n(\ker d_i', B) \oplus \operatorname{Ext}_R^n(Q', B) \\
\cong\ &\operatorname{Ext}_R^n(\ker d_i', B).
\end{aligned}$$

This is the desired result. ☐

The use of Ext is in its ability to be independent of choice of resolution, but moreover this allows it to detect projective modules at the same time. The following proposition elucidates this capability further.

Theorem 8.6. *The following are equivalent for all modules A and $n \geq 0$:*
(1) $\mathrm{pd}(A) \leq n$*;*
(2) $\mathrm{Ext}_R^k(A, B) = 0$ *for all modules B and $k \geq n+1$;*
(3) $\mathrm{Ext}_R^{n+1}(A, B) = 0$ *for all modules B;*
(4) There exists a projective resolution of A where $\ker d_{n-1}$ *is projective;*
(5) For every projective resolution of A, we have that $\ker d_{n-1}$ *is projective.*

Proof. We visit each implication in circular fashion, showing them all to be equivalent.

(1) $\Rightarrow$ (2): Since there is a projective resolution $\mathbf{P}$ of length at most n, we have $P_k = 0$ for $k \geq n+1$, and so $\mathrm{Ext}_R^k(A, B) = 0$ too.

(2) $\Rightarrow$ (3): This simply restricts to $k = n+1$.

(3) $\Rightarrow$ (4): We use dimension shifting (Proposition 7.9): for all B, $0 = \mathrm{Ext}_R^{n+1}(A, B) = \mathrm{Ext}_R^1(\ker d_{n-1}, B)$, we know from Corollary 7.26 that $\ker d_{n-1}$ is projective.

(4) $\Rightarrow$ (5): Suppose we have some projective resolution $\mathbf{P}'$ of A in addition to the hypothesised resolution $\mathbf{P}$ wherein $\ker d_{n-1}$ is projective. By the generalised Schanuel lemma (Corollary 8.4) there are projective modules Q and Q' such that $\ker d_{n-1} \oplus Q \cong \ker d'_{n-1} \oplus Q'$. But then $\ker d'_{n-1}$ is a direct summand of a projective module, and hence is a direct summand of a free module, and ergo also projective.

(5) $\Rightarrow$ (1): Take any resolution $\mathbf{P}$ of A. But then we have a resolution of length n, since $\ker d_{n-1}$ is projective:

$$0 \to \ker d_{n-1} \hookrightarrow P_{n-1} \to P_{n-2} \to \cdots .$$

Hence $\mathrm{pd}(A) \leq n$, and we are done. □

This gives us a very powerful way of showing that $\mathrm{pd}(A) > n$ for some n: simply find a single module B for which $\mathrm{Ext}_R^{n+1}(A, B) \neq 0$. This is by no means a foolproof algorithmic method to determine the projective dimension, but it provides a general approach, and a useful characterisation.

Of course, there is a natural dual notion to all of this. Instead of taking a projective resolution, we might take an injective resolution, and consider the *injective* dimension.

Definition 8.7. An injective resolution $\mathbf{Q}$ for a module M is of length n if $Q_{n+1} = 0$ and $Q_n \neq 0$. If $Q_n \neq 0$ for all n, we say that the resolution has length ∞.

Definition 8.8. The **injective dimension** $\mathrm{id}(M)$ of an R-module M is the minimal length of an injective resolution of M.

The theory that we have already seen carries over: there is a result dual to Schanuel's lemma, allowing us to conclude the following:

Corollary 8.9. *The following are equivalent for all modules B, and $n \geq 0$:*
(1) $\mathrm{id}(B) \leq n$*;*
(2) $\mathrm{Ext}_R^k(A, B) = 0$ *for all modules A and $k \geq n+1$;*
(3) $\mathrm{Ext}_R^{n+1}(A, B) = 0$ *for all modules A;*
(4) There exists a injective resolution of B where $\ker d_n$ *is injective;*
(5) For every injective resolution of B, we have that $\ker d_n$ *is injective.*

Proof. This is dual to Theorem 8.6. □

We now prove a few helpful and interesting results on projective dimension of modules.

Proposition 8.10. *Suppose we have an exact sequence of R-modules:*

$$0 \to A \to B \to C \to 0.$$

Then we have the following bound:

$$\mathrm{pd}(C) \leq 1 + \max\{\mathrm{pd}(A), \mathrm{pd}(B)\}.$$

Proof. We use the long exact sequence for Ext (Proposition 7.11) combined with Theorem 8.6.

For some R-module D, the long exact sequence for $\mathrm{Ext}_R^n(\square, D)$ gives us the following exact sequence for any n:

$$\cdots \to \mathrm{Ext}_R^{n+1}(A, D) \to \mathrm{Ext}^{n+2}(C, D) \to \mathrm{Ext}^{n+2}(B, D) \to \cdots$$

This means that if both $\mathrm{Ext}_R^{n+1}(A, D)$ and $\mathrm{Ext}^{n+2}(B, D)$ are zero, then so is $\mathrm{Ext}^{n+2}(C, D)$. If this happens for all modules D, then $\mathrm{pd}(C) \leq 1+\mathrm{pd}(B)$ and $\mathrm{pd}(C) \leq \mathrm{pd}(A) \leq 1+\mathrm{pd}(A)$, so we are done. □

Proposition 8.11. *Let $(M_i)_{i \in I}$ be a collection of R-modules. Then:*

$$\mathrm{pd}\left(\bigoplus_{i \in I} M_i\right) = \sup\{\mathrm{pd}(M_i) \mid i \in I\}.$$

Proof. Since $\mathrm{Ext}_R^n(\square, D)$ is an additive functor for any module D (Proposition 7.7) it preserves finite direct sums (Corollary 6.21). So for any $j \in I$, since:

$$S = \bigoplus_{i \in I} M_i = M_j \oplus \bigoplus_{i \in I \setminus \{j\}} M_i,$$

We have that $\mathrm{Ext}_R^n(S, D)$ is the direct sum of $\mathrm{Ext}_R^n(M_j, D)$ and something else, so in particular Theorem 8.6 part (2) tells us that $\mathrm{pd}(S) \geq \mathrm{pd}(M_j)$ for all j, meaning that $\mathrm{pd}(S) \geq \sup\{\mathrm{pd}(M_i) \mid i \in I\}$.

Now conversely, if M_i has a projective resolution $\mathbf{P}^i$, then we can construct a projective resolution $\mathbf{Q}$ for S of length $\sup\{\mathrm{pd}(M_i) \mid i \in I\}$ by setting:

$$Q_n = \bigoplus_{i \in I} P_n^i.$$

Hence $\mathrm{pd}(S) \leq \sup\{\mathrm{pd}(M_i) \mid i \in I\}$, and we are done. □

8.2 Global Dimension of Rings

We noted earlier that, for $\mathbb{Z}$-modules, we always have a free resolution of length at most 1. This is interesting as it appears to be a property of the ring that gives us an upper bound on all projective dimensions. More evidence for this fact is that, for example, every vector space is free and hence projective. What we observe leads us to the following definition.

Definition 8.12. The **left [right] global dimension** $\ell.\mathrm{gl.dim}(R)$ [$r.\mathrm{gl.dim}(R)$] of a ring R is the supremum of $\mathrm{pd}(M)$ for all left [right] R-modules M. If $\ell.\mathrm{gl.dim}(R) = r.\mathrm{gl.dim}(R)$, we call their common value simply the **global dimension** $\mathrm{gl.dim}(R)$.

Remark. The reason we say the supremum rather than the maximum is due to the potential presence of projective dimension ∞. It is not obvious that we may exclude the possibility that, for some reason, every R-module may have finite but arbitrarily large projective dimension – however it is an immediate corollary of Proposition 8.11, since we may take the direct sum of the modules with arbitrarily large prodjective dimension to obtain one of infinite dimension.

We will proceed to discuss the left global dimension almost exclusively, since:

$$\ell.\text{gl.dim}(R) = r.\text{gl.dim}(R^{\text{op}}).$$

This means that results about the former transfer to the latter, allowing us to avoid smattering our proofs with square brackets. It is notable that, for commutative rings there is no distinction between the left and right global dimension.

Given the discussion of injective dimension previously, we might expect to introduce a notion of global dimension for injective modules as well. However, there is no need to do so – projective dimension describes both, as we see now.

Proposition 8.13. *The supremum of the injective dimensions of left R-modules is equal to $\ell.\text{gl.dim}(R)$.*

Proof. By Theorem 8.6, $\text{Ext}_R^{n+1}(A, B) = 0$ for all modules A, B if and only if $\text{pd}(A) \leq n$ for all left R-modules A, but by Corollary 8.9 the same characterises $\text{id}(B) \leq n$ for all modules B. Hence the supremum of the injective dimensions of R-modules is the same as the supremum of the projective dimensions of R-modules, since they are both the supremum of n where $\text{Ext}_R^n(A, B) \neq 0$ for some modules A and B. □

Given what we have seen – that $\text{gl.dim}(\mathbb{Z}) \leq 1$ – we know now that there is an injective resolution of length at most 1 for any $\mathbb{Z}$-module (c.f. Example 7.20).

Corollary 8.14. *If, for some ring R, every left R-module is projective, then every module is injective too.*

Proof. If every module M is projective, then $0 \to M \to M \to 0$ is a projective resolution of length 0, hence $\ell.\text{gl.dim}(R) = 0$, and by the previous proposition, this means that every module has an injective resolution of length zero: $0 \to M \to Q \to 0$. Hence $M \cong Q$, and so M is injective. □

Why is it that global dimension matters? It characterises and generalises some important properties of rings that are well-studied. Let us give the following as an example.

Definition 8.15. A ring R is **semisimple** if, supposing A is any left R-module and B is any submodule of A, then B is a direct summand of A.

It may seem strange that we specified left modules, but it is a well-known result in algebra that the same definition for right R-modules is in fact equivalent – though we will not prove this here.

Proposition 8.16. *A ring R is semisimple if and only if $\ell.\text{gl.dim}(R) = 0$.*

Proof. Suppose R is semisimple, and let M be some R-module. Then there is a free R-module F with a submodule K such that $F/K \cong M$. But K is a direct summand of F by assumption, so $F = K \oplus K'$ for some $K' \subseteq F$. Hence $M \cong F/K \cong K'$ is a direct summand of a free module and hence projective.

Conversely, suppose $\ell.\text{gl.dim}(R) = 0$, so every left R-module is projective. Then supposing A is a module with a submodule B, so we have an exact sequence:

$$0 \to B \hookrightarrow A \to A/B \to 0.$$

Since A/B is projective, the exact sequence splits and B is a direct summand of A. □

We have only observed so far that $\text{gl.dim}(\mathbb{Z}) \leq 1$, but we can immediately rule out the notion of it being semisimple. An example of a submodule that is not a direct sum is $\mathbb{Z}_2$ within $\mathbb{Z}_4$.

Proposition 8.17. *For a ring R, ℓ.gl.dim$(R) = 1$ if and only if every submodule of a projective left R-module is projective.*

Proof. Suppose ℓ.gl.dim$(R) = 1$, and suppose a projective left R-module P has a submodule M. Now there exists a projective resolution $\cdots \to P' \xrightarrow{d_1} P \to P/M \to 0$ with $\operatorname{im} d_1 = M$, by way of choice of a projective resolution for M. Since ℓ.gl.dim$(R) = 1$, by Theorem 8.6 part (5), we conclude that $\ker d_0 = \operatorname{im} d_1 = M$ is projective. □

This has a name in the literature: such rings are called **hereditary**.

As we ascend to higher global dimensions, the meaning becomes less clear. But nonetheless we can see how these properties might be important even without the context of the many years of research dedicated to these classes of rings – and furthermore, we can now see them as part of a larger homological context.

The global dimension seems to be a property of the ring rather than its modules, and since we have Baer's criterion (Theorem 5.15), we can phrase it as a property of its ideals only.

Lemma 8.18. *A left R-module M is injective if and only if $\operatorname{Ext}^1_R(R/I, M) = 0$ for all left ideals I of R.*

Proof. If M is injective then Corollary 8.9 tells us that $\operatorname{Ext}^1_R(A, M) = 0$ for any module A, so we need only prove the converse.

Suppose $\operatorname{Ext}^1_R(R/I, M) = 0$ for all left ideals I. We have an exact sequence $0 \to I \to R \to R/I \to 0$, so applying the long exact sequence for Ext, we obtain an exact sequence:

$$\operatorname{Hom}_R(R, M) \to \operatorname{Hom}_R(I, M) \to \operatorname{Ext}^1_R(R/I, M) = 0,$$

so the leftmost map is surjective, meaning that every map $I \to M$ extends to a map $R \to M$. This is precisely Baer's criterion, so M is injective. □

Theorem 8.19 (Auslander's Theorem)**.**

$$\ell.\text{gl.dim}(R) = \sup\{\text{pd}(R/I) \mid I \textit{ is a left ideal of } R\}.$$

Proof. The former quantity is no greater than the latter, so we can assume that the supremum is finite, since otherwise both are ∞ and we are done.

So suppose $\text{pd}(R/I) \leq n$ for all left ideals I of R, meaning that $\operatorname{Ext}^{n+1}_R(R/I, M) = 0$ for all modules M. Recall however from Proposition 8.13 that the supremum of the injective dimensions of modules of a ring is equal to the global dimension, so we only need to prove that $\text{id}(M) \leq n$ for all modules M, after which the reverse inequality is clear.

Suppose that we have an injective $\mathbf{Q}$ resolution for M, where $m \geq n$

$$\mathbf{Q} = 0 \to M \to Q_0 \xrightarrow{d_0} Q_1 \xrightarrow{d_1} \cdots \to Q_m \to 0$$

Now via dimension shifting, we have:

$$0 = \operatorname{Ext}^{n+1}_R(R/I) = \operatorname{Ext}^1_R(R/I, \ker d_{n+1}).$$

The previous lemma then tells us that $\ker d_{n+1}$ is injective, so $\text{id}(M) \leq n$ and we are done. □

Auslander's theorem is very helpful in calculating the left and right global dimensions of rings, since it reduces a supremum over a truly enormous collection to a potentially finite calculation.

We close this section with a result that shows our favourite class of rings behave nicely with respect to global dimension.

Theorem 8.20. *If R is a Noetherian ring, then* $\ell.\mathrm{gl.dim}(R) = r.\mathrm{gl.dim}(R)$.

Proof. We will show that $\ell.\mathrm{gl.dim}(R) \leq r.\mathrm{gl.dim}(R)$, whence the result follows by considering the same statement for R^{op}. This inequality holds trivially if $r.\mathrm{gl.dim}(R) = \infty$, so assume that $r.\mathrm{gl.dim}(R) = n$ is finite.

If I is a left ideal of R, then it is finitely generated, meaning that there is a free left R-module F_0 of finite rank for which I is a quotient. Since R is Noetherian, any submodule of F is finitely generated, so continuing this we have part of a free resolution for I, where each F_i is of finite rank, and we wish to show that $\ker d_{n-1}$ is projective:

$$0 \to \ker d_{n-1} \to F_{n-1} \to \cdots \to F_0 \to I \to 0.$$

Set $K = \ker d_{n-1}$. Now since $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module, we have an exact sequence:

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(F_0, \mathbb{Q}/\mathbb{Z}) \to \cdots \to \mathrm{Hom}_{\mathbb{Z}}(K, \mathbb{Q}/\mathbb{Z}) \to 0.$$

By Proposition 5.40, we see that this is an injective resolution for the *right* R-module $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$. We know that $r.\mathrm{gl.dim}(R) \leq n$, so we conclude that $\mathrm{Hom}_{\mathbb{Z}}(K, \mathbb{Q}/\mathbb{Z})$ is injective by Proposition 8.13, and again Proposition 5.40 tells us that K is a flat left R-module. Since K is finitely generated, it must also be a projective module by Proposition 5.39, and we are done. □

There are non-noetherian rings whose left and right global dimensions are mismatched. For an example of such a ring, including a proof of this property, see appendix A.3.

8.3 Hilbert's Syzygy Theorem

We now have an interesting and important notion of a dimension of a ring, namely its (left and right) global dimension. We might ask now if related rings have related global dimensions. One direction that we might look to is geometry, since after all we are thinking of a kind of dimension.

Algebraic geometry leads us to see certain spaces as linked to $\Bbbk$-algebras. For example, we might see n-dimensional affine space as described by $\Bbbk[x_1, \ldots, x_n]$. Now the addition of an extra 'dimension' to a space may be seen as adjoining another 'line' – which we think of as represented by $\Bbbk[x]$. Hence the 'dimension' of a $\Bbbk$-algebra R ought to be one less than $R \otimes_k \Bbbk[x]$ – supposing of course that the tensor product is appropriate here – which, it may be observed, is isomorphic as a $\Bbbk$-algebra to $R[x]$. Perhaps this could be seen as a moral justification, rather than a precise one, for the following theorem.

Theorem 8.21 (Hilbert's Syzygy Theorem)**.** *For any ring R,*

$$\ell.\mathrm{gl.dim}(R[x]) = \ell.\mathrm{gl.dim}(R) + 1,$$

where we agree that $\infty + 1 = \infty$.

We will now endeavour to prove this result by building up theory.

Definition 8.22. If M is a right R-module, define the left $R[x]$-module:

$$M[x] = M \otimes_R R[x].$$

For left R-modules, we would define $M[x] = R[x] \otimes_R M$ instead.

We noted briefly that this was possible in Example 3.26.

Proposition 8.23. *For a right R-module M,* $\mathrm{pd}_R(M) = \mathrm{pd}_{R[x]}(M[x])$.

Proof. First note that $R[x]$ is a free $R[x]$-module (and in fact a free R-module) so in particular it is flat by Proposition 5.35. Moreover, if P is a projective R-module, then since:

$$\mathrm{Hom}_{R[x]}(P \otimes_R R[x], \square) \cong \mathrm{Hom}_R(P, \mathrm{Hom}_{R[x]}(R[x], \square))$$

is the composite of two exact functors (since P and $R[x]$ are projective) we conclude that $P[x]$ is projective.

Suppose we have a projective resolution for M:

$$\mathbf{P} = \cdots \to P_1 \to P_0 \to M \to 0.$$

Tensoring by $R[x]$ preserves exactness since it is flat, and so we have a projective resolution of the same length as $\mathbf{P}$

$$\mathbf{P}[x] = \cdots \to P_1[x] \to P_0[x] \to M[x] \to 0.$$

Hence $\mathrm{pd}_{R[x]}(M[x]) \leq \mathrm{pd}_R(M)$. Now conversely suppose we have a projective resolution for $M[x]$ over the ring $R[x]$:

$$\mathbf{Q} = \cdots \to Q_1 \to Q_0 \to M[x] \to 0.$$

For each Q_i there is a free $R[x]$-module F_i wherein Q_i is a direct summand. However since $R[x]$ is a free R-module, F_i is also a free R-module. Hence Q_i is a direct summand of a free R-module, and hence projective over R too. Hence $\mathbf{Q}$ is a projective resolution in R too, showing us that $\mathrm{pd}_R(M[x]) \leq \mathrm{pd}_{R[x]}(M[x])$. As an R-module however,

$$M[x] \cong \bigoplus_{n \geq 0} M,$$

so by Proposition 8.11 we have $\mathrm{pd}_R(M[x]) = \mathrm{pd}_R(M)$, and we are done. □

Corollary 8.24. $\ell.\mathrm{gl.dim}(R[x]) \geq \ell.\mathrm{gl.dim}(R)$.

Proof. We may exhibit an $R[x]$-module of projective dimension equal to that of any R-module by the above. □

Proposition 8.25. *Suppose M is a left $R[x]$-module. Then there is an exact sequence:*

$$0 \to M[x] \to M[x] \to M \to 0,$$

where we set $M[x] = R[x] \otimes_R M$ as with ordinary R-modules.

Proof. We define the map ϕ from $M[x] \to M$ by $x^i \otimes m \mapsto x^i m$, which works since the action of scalars is bilinear. This is evidently surjective, so all that remains is to show that its kernel is isomorphic to $M[x]$.

We define a map $\psi\colon M[x] \to \ker \phi$ by $\psi(x^i \otimes m) = x^i \otimes xm - x^{i+1} \otimes m$. We need only show now that ψ is a bijection.

Firstly we show it is injective. Suppose that $e = \sum_{i=0}^{k} x^i m_i$ is an arbitrary element of $M[x]$. Then:

$$\begin{aligned} 0 = f(e) &= \sum_{i=0}^{k} x^i \otimes xm_i - x^{i+1} \otimes m_i \\ &= 1 \otimes xm_0 - x^{k+1} \otimes m_k + \sum_{i=0}^{k-1} x^{i+1} \otimes (xm_{i+1} - m_i) \end{aligned}$$

So $xm_0 = 0$, but since $xm_1 = m_0$ too, so $m_1 = 0$. Inductively, we conclude that $m_i = 0$ for all i.

Now we prove surjectivity. If e as above is now an arbitrary element of $\ker\phi$, then we have:

$$0 = m_0 + x\left(m_1 + x\left(m_2 + \cdots\left(m_{k-1} + xm_k\right)\cdots\right)\right).$$

So, there is some n_0 such that $-m_0 = xn_0$, namely $m_1 + x(m_2 + \cdots)$. Similarly, there is some n_1 such that $m_1 = xn_1 - n_0$, namely $m_2 + x(\cdots)$. By repeating this iteratively, we obtain $\sum_{i=0}^{k} x^i \otimes n_i \in M[x]$, whose image under ψ is e. □

Corollary 8.26. $\ell.\text{gl.dim}(R[x]) \leq 1 + \ell.\text{gl.dim}(R)$

Proof. Suppose that M is some left $R[x]$-module, so we can see it as a left R-module as well. We know that $\text{pd}_{R[x]}(M[x]) = \text{pd}_R(M)$ by Proposition 8.23. Now the previous proposition gives us an exact sequence of $R[x]$-modules:

$$0 \to M[x] \to M[x] \to M \to 0,$$

whence Proposition 8.10 tells us that $\text{pd}_R(M) + 1 = \text{pd}_{R[x]}(M[x]) + 1 \geq \text{pd}_{R[x]}(M)$, and we are done. □

We have proved one half of Theorem 8.21. To find the other bound, we need only find a single $R[x]$-module with sufficient projective dimension for any ring R. The following result gives us what we want.

Theorem 8.27. *Let $M \neq 0$ be a left R-module. By setting $xM = 0$, it is automatically a left $R[x]$-module too. If $\text{pd}_R(M)$ is finite, then $\text{pd}_{R[x]}(M) = \text{pd}_R(M) + 1$.*

Proof. We prove the claim via induction on $n = \text{pd}_R(M)$.

In the case that $n = 0$, we mean to say that M is a projective R-module. Now there is an exact sequence:

$$0 \to R[x] \xrightarrow{x\cdot} R[x] \to R[x]_R \to 0,$$

and this is an $R[x]$-projective resolution for $R[x]_R$, so $\text{pd}_{R[x]}(R) \leq 1$. Since M is R-projective, it is the submodule of a free R-module – the direct sum of some number of copies of R, so by Proposition 8.11 we have $\text{pd}_{R[x]}(M) \leq 1$. Finally, M cannot be projective as an $R[x]$-module, since $xM = 0$ despite $M \neq 0$, which means it cannot be a submodule of a free module, let alone a direct summand.

Now suppose that $\text{pd}_R(M) = n$ for some $n \geq 1$. There is an exact sequence, where F is a free R-module:

$$0 \to K \hookrightarrow F \to M \to 0.$$

Certainly $\text{pd}_R(K) = n - 1$ by Theorem 8.6, and the inductive hypothesis means that $\text{pd}_{R[x]}(K) = n$. By Proposition 8.10 and our observation in the $n = 0$ case that $\text{pd}_{R[x]}(F) \leq 1$, we have $\text{pd}_{R[x]}(M) \leq n + 1$.

Now we split into the case that $n = 1$ and that where $n \geq 2$. Let $n = 1$. There is an exact sequence of $R[x]$-modules, where F' is free:

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

Since $xM = 0$, we have $xF' \subseteq K'$. Hence we have another exact sequence:

$$0 \to K'/xF' \hookrightarrow F'/xF' \to M \to 0.$$

Now F'/xF' is a free R-module, so by Theorem 8.6 we have $\text{pd}_R(K'/xF') \leq \text{pd}_R(M) - 1 = 0$ – K'/xF' is projective. Now there is an exact sequence of R-modules which splits:

$$0 \to M \cong F'/K' \cong xF'/xK' \hookrightarrow K'/xK' \to K'/xF' \to 0,$$

So M is a direct summand of K'/xK'. This means that K' cannot be a projective $R[x]$-module, since otherwise K'/xK' is a projective R-module, whence $\mathrm{pd}_R(M) = 0$ too – assumed to be false. Altogether, this means that $\mathrm{pd}_{R[x]}(M) = 1 + \mathrm{pd}_{R[x]}(K') \geq 2$.

Finally, we tackle the case where $n \geq 2$. We know that $\mathrm{pd}_{R[x]}(K) \geq \mathrm{pd}_R(K) = n-1 \geq 1$, so K is not projective. Certainly the sequence

$$0 \to K \hookrightarrow F \to M \to 0$$

remains exact when we see the modules as $R[x]$-modules, and recalling that $\mathrm{pd}_{R[x]}(F) \leq 1$ and the long exact sequence for Ext, we have the following exact sequence for any $R[x]$-module D, and $k \geq 2$:

$$0 = \mathrm{Ext}^k_{R[x]}(F, D) \to \mathrm{Ext}^k_{R[x]}(K, D) \to \mathrm{Ext}^{k+1}_{R[x]}(M, D) \to \mathrm{Ext}^{k+1}_{R[x]}(F, D) = 0.$$

Hence $\mathrm{Ext}^{k+1}_{R[x]}(M, D) \cong \mathrm{Ext}^k_{R[x]}(K, D)$ for all D, and $2 \leq k$, so we conclude that

$$\mathrm{pd}_{R[x]}(M) = \mathrm{pd}_{R[x]}(K) + 1 \geq n,$$

and we are done. $\square$

This finally proves Theorem 8.21, since it gives us a module of sufficient dimension.

By repeatedly applying the syzygy theorem, we arrive at an easy corollary.

Corollary 8.28. $\ell.\mathrm{gl.dim}(R[x_1, \ldots, x_n]) = \ell.\mathrm{gl.dim}(R) + n$.

For an explicit example of a module of a polynomial ring with maximal projective dimension, see appendix A.2.

9 Conclusion

Let us summarise the events of preceding sections. We developed an understanding of modules that lends itself to homological interpretation. Interweaving the derived functor Ext, we produced a framework for homological dimensions of modules, and therefore rings. Finally, we knocked on Hilbert's door to present a more general version of his syzygy theorem.

Needless to say, much of the theory was omitted for the sake of brevity and limiting the scope of this project – we discuss some of these omissions here.

Given that we now know that projective modules are important, a natural question to ask for a given ring is what its projective modules look like. This can be very hard in general, but one result characterises projective modules for polynomial rings over a field: the Quillen–Suslin theorem states that projective $\Bbbk[x_1, \ldots, x_n]$-modules are free. Although the syzygy theorem can be used to show that a free resolution of a certain length exists due to the Eilenberg–Mazur swindle (Example 5.8), this gives a more direct link in the case of polynomial rings.

Free modules were not emphasised in this project, although they have a theory that runs parallel to that of projective modules. In particular, repeating the same process that allowed us to derive Ext and substituting Hom for the tensor product leads us to a derived functor named Tor, which allows us to measure the 'flat dimension' of a module.

We mentioned briefly that Ext 'repairs' the partial exactness of Hom as a consequence Proposition 7.12 and Corollary 7.11. We may remark that this is a very canonical way of doing so. The general notion of a derived function justifies this being canonical, and provides convenient criteria for a functor being a particular derived functor.

Hilbert's other two theorems – his basis theorem and Nullstellensatz – both have undertones of algebraic geometry, although Hilbert likely did not know this at the time. Similarly, the syzygy theorem and related homological results have their uses in algebraic geometry. For instance, the global dimension detects singular points on a variety, which is useful in modern algebraic geometry as global dimension applies to any ring, not just polynomial rings. Flat modules also play an important role in algebraic geometry.

At the time, Hilbert's motivation was the calculation of Hilbert polynomials, which are certain important invariants of graded modules – modules with a natural decomposition into strata of elements of a certain 'degree'. Graded modules and rings lend themselves to homological study particularly nicely, although this is unexplored in this project.

The techniques we exhibited here have been used for more than just rings. Given that much of what we have done works in the context of an arbitrary Abelian category, we can apply similar notions to sheaves – an important kind of object borrowed from topology. Despite them not forming an Abelian category, there is a homology theory of groups that relies upon much of what we have developed here.

The power afforded by spectral sequences and the notion of the derived category are just two places that would lead naturally from the content here – indeed homological algebra has much more to offer than what we presented in this project. The author hopes that any curious reader will, having read this project, leave well-equipped for the homological road ahead.

A Examples and Calculations

In order to avoid interrupting the flow of text elsewhere, we relegate some calculations and examples to the appendix here.

A.1 Examples of Projective Modules via Quiver Algebras

Definition. A **quiver** is a directed multigraph. That is, it consists of a set V of vertices and a set E of edges, alongside a function $s\colon E \to V$ giving an edge a 'source', and another $t\colon E \to V$ giving it a 'target'.

Quivers can be represented entirely graphically, for instance the following defines a quiver Q with a set of vertices $\{A, B, C, D\}$ and edges $\{w, w', x, y, z, i\}$:

$$Q = \begin{tikzcd} & B \arrow[dr, "y"] & \\ A \arrow[ur, bend left, "w"] \arrow[ur, bend right, "w'"'] \arrow[dr, "x"'] & & D \arrow[loop right, "i"] \\ & C \arrow[ur, "z"'] & \end{tikzcd}$$

Definition. A **path** in a quiver starting at a vertex V and ending at V' is a (possibly empty) sequence $e_0, e_1, \cdots, e_n$ of edges such that $s(e_0) = V$, $s(e_{i+1}) = t(e_i)$ for $i < n$, and $t(e_n) = V'$. A path may be empty if $V = V'$, in which case we denote this empty path as ε_V.

Remark. The collection of all paths forms a category alongside the vertices of the quiver in a natural way, where composition of paths is simply concatenation. This may be seen as the 'free category' generated by a quiver, although this requires more formalism to prove properly.

Definition. The **quiver algebra** $\Bbbk Q$ of a quiver Q with finitely many vertices over a field $\Bbbk$ consists of $\Bbbk$-linear combinations of paths of Q, where multiplication is given by:

$$\left(\sum_{i=1}^{n} r_i p_i\right)\left(\sum_{j=1}^{m} s_j q_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} r_i s_j (p_i q_j),$$

where $p_i q_j$ is concatenation where appropriate, and 0 if the target of q_j and the source of p_i do not coincide. The unit of this algebra is then $\sum_{v \in V} 1\varepsilon_v$.

Remark. We could extend this definition to quivers with infinitely many vertices, but this algebra would no longer have a unit, since the sum above would not be finite.

Example. The polynomial ring is a very simple example of a quiver algebra. Specifically, $\Bbbk[x]$ can be seen as this quiver algebra over $\Bbbk$ of the following quiver:

$$\begin{tikzcd} \bullet \arrow[loop right, "x"] \end{tikzcd}$$

Remark. In the case that there are finitely many paths in Q, the path algebra $\Bbbk Q$ is Noetherian since it may be seen as a finitely generated $\Bbbk$-space.

We will now focus on exhibiting some interesting examples of projective modules over $R = \Bbbk Q$.

Observe that the left ideals $R\varepsilon_v$ consist of $\Bbbk$-linear combinations of paths that end at the vertex v, since right multiplication by ε_v preserves paths that end in v but annihilates all others.

Given that every path must terminate somewhere, it is plain to see that as a left R-module,

$$R = \bigoplus_{v \in V} S\varepsilon_v,$$

since paths with differing endpoints cannot be equal. The summands here must be projective, and a similar argument works for right R-modules.

Example. In a quiver algebra $R = \Bbbk Q$ of a quiver Q with finitely many vertices, the left ideals $R\varepsilon_v$ and right ideals $\varepsilon_v R$ are projective for any vertex v.

A.2 Example of Calculating the Projective Dimension

Hilbert's Syzygy Theorem (8.21) states in particular that over a field $\Bbbk$, there is a module of $R = \Bbbk[x_1, \ldots, x_n]$ which has projective dimension n. The theory of Kozsul complexes would allow us to exhibit that $\Bbbk$, seen as the R-module $R/\langle x_1, \ldots, x_n \rangle$, provides an example, however this goes beyond the scope we have set here, and we calculate only one example.

We let $R = \Bbbk[x, y, z]$, and by a minor abuse of notation we will identify $\Bbbk$ with the module $R/\langle x, y, z \rangle$. We now set ourselves to the task of finding a projective resolution for $\Bbbk$:

$$0 \to F_3 \to F_2 \to F_1 \to F_0 \to \Bbbk \to 0.$$

We set $F_0 = R$ Certainly the natural map $d_0 \colon R \to \Bbbk$ suffices as a first step, and the kernel of this map is $K_1 = \langle x, y, z \rangle$.

To generate K_1, we choose $F_1 = R^3$ and the map $d_1 \colon R^3 \to K_1$ given by $(a, b, c) \mapsto xa + yb + zc$. Finding the kernel K_2 of d_1 requires a bit of work. We approach this problem as follows: we find a novel element of the kernel, and then reduce the problem accordingly.

Note that $(y, -x, 0) \in K_2$, so if $xa + yb + zc = 0$ we may assume that b has degree 0 in x by adding an appropriate multiple of $(y, -x, 0)$. Similarly $(z, 0, -x) \in K_2$ so we may assume c has degree 0 in x also, meaning that $a = 0$ in the remaining case, otherwise there would be no multiple of x to cancel with. This means that the solutions $yb + zc = 0$ remain, and these are given by multiples of $(0, z, -y)$. Hence:

$$K_2 = \langle (y, -x, 0), (z, 0, -x), (0, z, -y) \rangle.$$

We now set $F_2 = R^3$ and let $d_2 \colon R^3 \to K_2$ have $d_2(1, 0, 0) = (y, -x, 0)$, $d_2(0, 1, 0) = (z, 0, -x)$, and $d_2(0, 0, 1) = (0, z, -y)$. If $d_2(a, b, c) = 0$, then we have:

$$ya + zb = 0, \quad -xa + zc = 0, \quad \text{and} \quad xb + yc = 0.$$

This means that $a = zp$, $b = -yp$, and $c = xp$ for some $p \in R$, meaning that $K_3 = \langle (z, -y, x) \rangle$.

Finally we set $F_3 = R$, and $d_3(r) = r(z, -y, x)$. This map is injective and so we have no more work to do.

We can now write out a resolution in totality. Note that we denote the maps d_i via matrices – we see each R^i as a collection of column vectors.

$$0 \to R \xrightarrow{\left[\begin{smallmatrix} z \\ -y \\ x \end{smallmatrix}\right]} R^3 \xrightarrow{\left[\begin{smallmatrix} y & z & 0 \\ -x & 0 & z \\ 0 & -x & -y \end{smallmatrix}\right]} R^3 \xrightarrow{[\,x\ y\ z\,]} R \to \Bbbk \to 0.$$

This is a free resolution of length 3, so we know that $\mathrm{pd}_R(\Bbbk) \leq 3$. To show that $\mathrm{pd}_R(\Bbbk) \geq 3$, we will calculate $\mathrm{Ext}^3_R(\Bbbk, R)$ to be nonzero, and invoke Theorem 8.6. But first we prove a lemma that is useful when calculating Ext.

Lemma. *Suppose a map* $f\colon R^m \to R^n$ *of left* R*-modules is given by a matrix* $M \in R^{n\times m}$ *so that* $f(v) = Mv$*. Then noting* $\operatorname{Hom}_R(R^i, R) \cong R^i$ *by additivity, the dual map* $f^*\colon R^n \to R^m$ *of right* R*-modules is given by* $f^*(w) = wM^\top$*, where we now see elements of* R^n *as row vectors.*

Proof. The isomorphism $\operatorname{Hom}_R(R^i, R) \to R^i$ is as follows. If R^i has a basis $e_1, \dots, e_i$, we let e_j^* take the jth component of a member of R^i. Call the isomorphism $\eta_i(e_j) = e_j^*$.

Suppose $f\colon R^m \to R^n$ is given by $f = Mv$, and let R^m have a basis $v_1, \dots, v_m$ and R^n have basis $w_1, \dots, w_n$. This means in particular that $Mv_j = \sum_{i=1}^n M_{i,j} w_i$.

Now looking at the basis w_i^* of R^n, the map f^* sends w_i^* to $w_i^* \circ f$, which is characterised by sending v_j to $M_{i,j}$. Hence $f^*(w_i^*) = \sum_{j=1}^n M_{j,i}^\top v_j$, so it is indeed given by the transpose of M. $\square$

Using the isomorphism outlined in the above lemma, we can obtain a commutative diagram which will help us calculate $\operatorname{Ext}^3_R(\Bbbk, R)$, whose vertical maps are isomorphisms, and whose labels M_i are the matrices in the resolution above.

$$\begin{tikzcd}
\operatorname{Hom}(F_2, R) \arrow[r, "d_3^*"] \arrow[d] & \operatorname{Hom}(F_3, R) \arrow[r, "d_4^*"] \arrow[d] & \operatorname{Hom}(0, R) \arrow[d] \\
R^3 \arrow[r, "M_3^\top"'] & R \arrow[r, "0"'] & 0
\end{tikzcd}$$

To see that $0 \neq \operatorname{Ext}^3_R(\Bbbk, R) = \ker d_4^* / \operatorname{im} d_3^*$, we need only find a single element of R which is not in the image of $M_3^\top$. We can note that $v = [x \;\; 0 \;\; 0]$ is not in the image of $M_3^\top$, since the first component of every vector in image of $M_3^\top$ must be of the form $yf + zg$ for some $f, g \in R$:

$$[f \;\; g \;\; h]M_3^\top = [f \;\; g \;\; h]\begin{bmatrix} y & -x & 0 \\ z & 0 & -x \\ 0 & z & -y \end{bmatrix} = [yf + zg \quad -xf + zh \quad -xg - yh].$$

This shows that $\operatorname{Ext}^3_R(\Bbbk, R) \neq 0$, hence we conclude that $\operatorname{pd}_R \Bbbk = 3$.

A.3 Example of a Ring with Mismatched Global Dimension

In the following, we will show that the following ring has $r.\mathrm{gl.dim}(s) \leq 1$ yet $\ell.\mathrm{gl.dim}(R) \geq 1$:

$$R = \begin{bmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{bmatrix} = \left\{ \begin{bmatrix} z & p \\ 0 & q \end{bmatrix} \,\middle|\, z \in \mathbb{Z},\; p, q \in \mathbb{Q}. \right\}$$

While it is not hard to extend this calculation to show that $r.\mathrm{gl.dim}(R) = 1$ (we only need to find a nonzero Ext^2 group for it) it may be more challenging to determine $\ell.\mathrm{gl.dim}(R)$ precisely.

A.3.1 Bounding the Right Global Dimension

Recall via Auslander's Theorem (Theorem 8.19) that in order to calculate the right global dimension of R, we need only inspect cyclic modules – that is, quotients of R by its right ideals. Furthermore if we can show that every ideal of R is projective, then certainly we have a projective resolution $0 \to I \to R \to R/I \to 0$, meaning that $r.\mathrm{gl.dim}(R) \leq 1$.

We first classify all right ideals of R. Suppose I is a nonzero right ideal of R. Now let $n \in \mathbb{Z}$ be the lowest non-negative integer for which:

$$\begin{bmatrix} n & p \\ 0 & q \end{bmatrix} \quad \text{for some } p, q \in \mathbb{Q}.$$

We now consider two cases. If $n \neq 0$, then note that for any $x \in \mathbb{Q}$ and $z \in \mathbb{Z}$:

$$\begin{bmatrix} n & p \\ 0 & q \end{bmatrix} \begin{bmatrix} z & x/n \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} zn & x \\ 0 & 0 \end{bmatrix} \in I.$$

If q is always 0 then this gives us our first example of an ideal:

$$I_1 = \begin{bmatrix} n\mathbb{Z} & \mathbb{Q} \\ 0 & 0 \end{bmatrix} \quad \text{for some } n \neq 0.$$

If $q \neq 0$, then note that for any $y \in \mathbb{Q}$:

$$\begin{bmatrix} 0 & 0 \\ 0 & q \end{bmatrix} \in I \quad \text{so} \quad \begin{bmatrix} 0 & 0 \\ 0 & q \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & y/q \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & y \end{bmatrix} \in I,$$

So we have a second example of an ideal:

$$I_2 = \begin{bmatrix} n\mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{bmatrix} \quad \text{for some } n \neq 0.$$

Now we go back to our assumption that $n \neq 0$, and inspect the case when in fact n is always 0. We assumed that I is a nonzero ideal, so we must have that one of p and q is nonzero. Let us assume that q is nonzero first. Note that:

$$\begin{bmatrix} 0 & p \\ 0 & q \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1/q \end{bmatrix} = \begin{bmatrix} 0 & p/q \\ 0 & 1 \end{bmatrix} \in I.$$

If q is always nonzero (except in the case of the zero matrix) and p/q is constant for every element of I, we obtain a principal ideal:

$$I_3 = \begin{bmatrix} 0 & x \\ 0 & 1 \end{bmatrix} R \quad \text{for some } x \in \mathbb{Q}.$$

However if the lower right entry of any element is zero while the top right entry is nonzero, then we have for some $0 \neq x \in \mathbb{Q}$:

$$\begin{bmatrix} 0 & p/q \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & p/qx \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \in I,$$

Overall this gives us a fairly large ideal, since any rational number can now be placed in the entries on the right:

$$I_4 = \begin{bmatrix} 0 & \mathbb{Q} \\ 0 & \mathbb{Q} \end{bmatrix}.$$

The final case to consider is when the lower right entry is always zero, after which we must conclude by our assumption that I is nonzero that $p \neq 0$. Hence we see that, for any $x \in \mathbb{Q}$:

$$\begin{bmatrix} 0 & p \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & x/p \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in I,$$

So our final ideal is as follows:

$$I_5 = \begin{bmatrix} 0 & \mathbb{Q} \\ 0 & 0 \end{bmatrix}.$$

Now that we have the full suite of ideals, we may observe that they are all finitely generated, hence the ring R is right Noetherian. One could interpret our forthcoming proof that $\ell.\text{gl.dim}(R) \neq r.\text{gl.dim}(R)$ as a particlarly long-winded proof that R is not left Noetherian, due to Theorem 8.20!

We focus our attention on demonstrating each ideal to be projective. First note the following direct sum of ideals:

$$R = \begin{bmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & 0 \end{bmatrix} \oplus \begin{bmatrix} 0 & 0 \\ 0 & \mathbb{Q} \end{bmatrix}.$$

This shows that I_1 is projective when $n = 1$ due to Proposition 5.7. In other cases, there is an isomorphism of right R-modules given by:

$$\begin{bmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & 0 \end{bmatrix} \to \begin{bmatrix} n\mathbb{Z} & \mathbb{Q} \\ 0 & 0 \end{bmatrix}; \quad M \mapsto \begin{bmatrix} n & 0 \\ 0 & 0 \end{bmatrix} M.$$

Hence I_1 is projective for all $n \neq 0$. Furthermore, since it is a direct sum of projective modules, I_2 is also projective – the latter ideal being projective due to the composition above.

$$I_2 = I_1 \oplus \begin{bmatrix} 0 & 0 \\ 0 & \mathbb{Q} \end{bmatrix}.$$

To show that I_3 is projective for some $x \in \mathbb{Q}$, we observe the following isomorphism of right R-modules:

$$\begin{bmatrix} 0 & 0 \\ 0 & \mathbb{Q} \end{bmatrix} \to \begin{bmatrix} 0 & x \\ 0 & 1 \end{bmatrix} R; \quad M \mapsto \begin{bmatrix} 0 & x \\ 0 & 1 \end{bmatrix} M.$$

A similar isomorphism shows us that I_5 is projective:

$$\begin{bmatrix} 0 & 0 \\ 0 & \mathbb{Q} \end{bmatrix} \to \begin{bmatrix} 0 & \mathbb{Q} \\ 0 & 0 \end{bmatrix}; \quad M \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} M.$$

Finally, since $I_4 = I_3 \oplus I_5$ when $x = 0$, we have shown that all the ideals of R are projective, and Theorem 8.19 tells us that $r.\mathrm{gl.dim}(R) \leq 1$.

A.3.2 Bounding the Left Global Dimension

Compared with the work of bounding the right global dimension from above, the work in bounding the left global dimension from below is more straightforward. To show that $\ell.\mathrm{gl.dim}(R) > 1$ we need only find a single left R-module A with $\mathrm{pd}(A) > 1$, and we do just that.

Observe that if G is any subgroup of $\mathbb{Q}$, then the following is a left ideal of R:

$$I = \begin{bmatrix} 0 & G \\ 0 & 0 \end{bmatrix},$$

since it is evidently an additive subgroup of R and if $g \in G$, given any $z \in \mathbb{Z}$ and $p, q \in \mathbb{Q}$.

$$\begin{bmatrix} z & p \\ 0 & q \end{bmatrix} \begin{bmatrix} 0 & g \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & zg \\ 0 & 0 \end{bmatrix} \in I.$$

We define G as the following subgroup of $\mathbb{Q}$:

$$G = \left\{ \frac{a}{2^n} \,\middle|\, a \in \mathbb{Z},\ n \geq 0. \right\}.$$

In particular, this means that every element of G is $a/2^n$ for some $a \in \mathbb{Z}$ and $n \geq 0$.

We will now aim to show that $\mathrm{pd}(R/I) > 1$. To do so, it suffices to show that I is not projective. Why is this? There are two cases we want to exclude: firstly when $\mathrm{pd}(R/I) = 0$, R/I is projective, so by Proposition 5.24 we have $R \cong I \oplus (R/I)$, so in turn I is projective. If $\mathrm{pd}(R/I) = 1$, then by Theorem 8.6 we would have that $\ker d_0$ is projective for any projective resolution of R/I. Certainly we may begin a resolution for R/I with

$\cdots \to R \to R/I \to 0$, so in this case $I = \ker d_0$ is projective. Excluding the possibility that I is projective hence shows that $\mathrm{pd}(R/I) > 1$.

To show that I is not projective, we will show that it has no projective basis, after which Proposition 5.5 does the work.

Suppose we have a projective basis $(f_v \colon I \to R)_{v \in V}$. Note that for any $p, q \in \mathbb{Q}$ and any $g \in G$:

$$\begin{bmatrix} 1 & p \\ 0 & q \end{bmatrix} \begin{bmatrix} 0 & g \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & g \\ 0 & 0 \end{bmatrix},$$

we see that elements of I are fixed by matrices of the above form. Hence:

$$f_v\left(\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\right) = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix},$$

for some $a \in \mathbb{Z}$ and $b \in \mathbb{Q}$. Note that this means that, by additivity:

$$f_v\left(\begin{bmatrix} 0 & 1/2^n \\ 0 & 0 \end{bmatrix}\right) = \begin{bmatrix} a/2^n & b/2^n \\ 0 & 0 \end{bmatrix},$$

so in fact $a = 0$ since $a/2^n$ is required to always be an integer.

By linearity, we have shown that for every $v \in V$ there is a rational number b_v such that:

$$f_v\left(\begin{bmatrix} 0 & g \\ 0 & 0 \end{bmatrix}\right) = \begin{bmatrix} 0 & b_v g \\ 0 & 0 \end{bmatrix}.$$

However supposing the top-right entry of v is $h \in G$, we see that:

$$f_v\left(\begin{bmatrix} 0 & g \\ 0 & 0 \end{bmatrix}\right) v = \begin{bmatrix} 0 & b_v g \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & h \\ 0 & 0 \end{bmatrix} = 0,$$

So this projective basis cannot satisfy property (2) of Definition 5.3, and we are done.

We have shown that $\mathrm{pd}(R/I) > 1$, hence $\ell.\mathrm{gl.dim}(R) > 1$.

References

[Bla79] Andreas Blass. Injectivity, projectivity, and the axiom of choice. *Trans. Amer. Math. Soc.*, 255:31–59, 1979.

[CE56] Henri Cartan and Samuel Eilenberg. *Homological algebra*. Princeton University Press, Princeton, N. J., 1956.

[Hil90] David Hilbert. Über die Theorie der algebraischen Formen. *Math. Ann.*, 36(4):473–534, 1890.

[Kap72] Irving Kaplansky. *Fields and rings*. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, Ill.-London, second edition, 1972.

[Lam99] Tsit Yuen Lam. *Lectures on modules and rings*, volume 189 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999.

[Mit65] Barry Mitchell. *Theory of categories*. Pure and Applied Mathematics, Vol. XVII. Academic Press, New York-London, 1965.

[NvO87] Constantin Năstăsescu and Freddy van Oystaeyen. *Dimensions of ring theory*, volume 36 of *Mathematics and its Applications*. D. Reidel Publishing Co., Dordrecht, 1987.

[Rot09] Joseph Rotman. *An introduction to homological algebra*. Universitext. Springer, New York, second edition, 2009.