Ext and Tor

Jihan Lee

July 16, 2023

Abstract

The functors Ext and Tor provide valuable information pertaining to sequences of modules and their interactions with the functors Hom and ⊗ respectively; this exposition provides an elementary (non-category theoretic) definition of Ext and Tor, as well as the basic sequence extending properties of each functor.

Contents

1 Introduction

The functors Hom and $\otimes$ fail to be exact; Ext and Tor measures the failure of these functors to be exact and in fact characterizes the cases in which they succeed to be exact, related to the notions of projective and flat modules–both of which are of great importance in fields such as algebraic geometry. The exposition begins with a brief overview of the preliminaries, then moves into the discussion of elementary homological algebra, afterwards defining Ext and Tor. We discuss the independece of these functors from choice of projective resolution in their construction, as well as their sequence extending properties and their classification of projective and flat modules.

2 Preliminaries

2.1 Groups

Definition 2.1 (Group)**.** A group is a set G equipped with a binary operation $*\colon G \times G \to G$ (where $a*b$ denotes $*(a,b)$) that satisfies the following properties:

$$\text{There exists an } e_G \in G \text{ such that } g * e_G = e_G * g = g \text{ for all } g \in G.$$

$$a * (b * c) = (a * b) * c \text{ for all } a, b, c \in G.$$

$$\text{For all } g \in G, \text{ there is a } g^{-1} \text{ such that } g * g^{-1} = g^{-1} * g = e_G.$$

A group is said to be *abelian* if $*$ is commutative.

e_G is said to be an *identity element* of G, and g^{-1} is said to be an *inverse element* of g.

Remark. *When there is no risk of confusion, e_G will be abbreviated to e.*

Examples.

- The integers under addition form a group, as addition is associative, 0 acts as an identity, and inverses exist. In particular, the integers are an abelian group.
- The set of all $n \times n$ matrices of nonzero determinant with coefficients in a field $\mathbb{F}$ form a group under multiplication, as matrix multiplication is associative, matrices of nonzero determinant are invertible (given the coefficients are from a field), and the identity matrix acts as an identity. This group is denoted $\mathrm{GL}_n(\mathbb{F})$.
- The set of permutations of n points forms a group, denoted S_n. Consider the elements of S_n to be bijections from the set of n points to itself, and the satisfication of the group axioms follow.

Remark. *The group operation is often ommitted when writing down expressions, such that $a * b$ is reduced to ab. Repeated operation of an element to* *itself is also abbreviated to exponential notation, such that* $\underbrace{aa\dots a}_{n \text{ times}} = a^n$*. This is well-defined because of the assumed associativity of* $*$*.*

Theorem 2.2. *Inverses and identities are unique.*

Proof. Suppose e and e' are two identity elements in a group G. Then, $ee' = e$, but $ee' = e'$, so $e = e'$. Now suppose b and c are two inverses of a. Then $cab = ce = e$, but $cab = eb = b$, so $c = b$. □

We will henceforth refer to e as *the* identity element of G, and g^{-1} as *the* inverse of g.

Definition 2.3 (Subgroup)**.** A *subgroup* of a group G is a subset H of G containing the identity such that $hh' \in H$ for all $h, h' \in H$. A subgroup is denoted $H \leq G$.

Proposition 2.4 (The subgroup criterion)**.** *Let* G *be a group, and let* H *be a nonempty subset of* G*.* H *is a subgroup of* G *iff* $xy^{-1} \in H$ *for all* $x, y \in H$*.*

Proof. Working in the forward direction, the identity is in H, as for any $h \in H$, set $x = y = h$ and $xy^{-1} = hh^{-1} = e$ is contained in H. Observe that H contains inverses, for if $x = e$ and $y = h \in H$, then $xy^{-1} = ey^{-1} = y^{-1}$ is contained in H. Finally, H is also closed under $*$, for if $a, b \in H$, set $x = a$, $y = b^{-1}$, such that $xy^{-1} = ab \in H$ (note that $(x^{-1})^{-1} = x$ for all $x \in G$).

The converse is clear. □

Definition 2.5 (Group Homomporhism)**.** Let G and H be groups, and $\varphi : G \to H$ a set map. The map φ is a *homomorphism* if $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$.

G is said to be the domain of φ, H is said to be the codomain. If φ is bijective, φ is said to be an *isomorphism.* Essentially, this means G and H have the same structure, i.e., any group-theoretic fact about G carries over to H. In this case, we write $G \cong H$. Any isomorphism has an inverse that is also an isomorphism, and if a homomorphism has an inverse, it is an isomorphism. Compositions of homomorphisms are homomorphisms, and compositions of isomorphisms are isomorphisms.

Remark. *When there is no danger of confusion, group homomorphism will be abbreviated to homomorphism.*

Definition 2.6 (Image, Kernel)**.** Let G, H be groups and $\varphi : G \to H$ a homomorphism. The *kernel* of φ (denoted $\ker \varphi$) is the set

$$\{x \in G \mid \varphi(x) = e_H\}$$

i.e., the set of all $x \in G$ such that $\varphi(x)$ is the identity in H.

The *image* of φ (denoted $\operatorname{im}\varphi$) is the set

$$\{h \in H \mid \text{there exists } g \in G \text{ such that } h = \varphi(g)\}.$$

Proposition 2.7. *Let G, H be groups and $\varphi : G \to H$ a homomorphism.*

$$\ker\varphi \leq G. \ \operatorname{im}\varphi \leq H.$$

Proof. Suppose $x, y \in \ker\varphi$. Then, $\varphi(xy) = \varphi(x)\varphi(y) = e_H e_H = e_H$, so $xy \in \ker\varphi$. We have $\varphi(xx^{-1}) = \varphi(e_G) = e_H = \varphi(x)\varphi(x^{-1}) = e_H\varphi(x^{-1})$, so $x^{-1} \in \ker\varphi$.

The second statement follows from the fact that $\operatorname{im}\varphi$ must be a group, but φ is not guaranteed to be surjective. □

Definition 2.8 (Coset)**.** Fix a group G, and a subgroup H. A *left coset* of H is the set of all elements of H "shifted on the left" by an element g of G, denoted gH.

$$H = \{h_1, h_2, \dots\}$$

$$gH = \{gh_1, gh_2, \dots\}$$

Right cosets are defined analagously.

We denote the set of all cosets of H in G by G/H.

Theorem 2.9. *Elements of G/H partition G.*

Proof. We first observe that all elements of G must be contained in some element of G/H, as H contains the identity.

Next, suppose $gH, g'H \in G/H$ have nontrivial intersection, say $gh_1 = g'h_2$. Then, $gh_1h_2^{-1} = g'$. Multiplying by $h' \in H$, $g(h_1h_2^{-1}h') = g'h'$, such that every element of $g'H$ is an element of gH. A symmetric argument shows $gH \subseteq g'H$, so $gH = g'H$.

Since $G = \bigcup_{g \in G} gH$ and $gH = g'H$ if $gH \cap g'H \neq \emptyset$, it follows that elements of G/H partition G. □

We wish to define a group structure on G/H by $xHyH = xyH$. This operation is well defined iff $xH = Hx$ for all $x \in G$, equivalent to the condition $xHx^{-1} = H$, i.e. $xhx^{-1} \in H$ for all $h \in H$.

Definition 2.10 (Normal Subgroup)**.** Let $N \leq G$. N is said to be *normal* if $gNg^{-1} = N$ for all $g \in G$, denoted $N \trianglelefteq G$.

Definition 2.11. Let G be a group. If N is a normal subgroup of G, then G/N (with group operation $gNg'N = gg'N$) is said to be the quotient group of G by N.

Proposition 2.12. *Let* $\varphi\colon G \to H$ *be a homomorphism. Then,* $\ker\varphi \trianglelefteq G$.

Proof. We have already proved **Proposition 2.7**.

We now show the normality of $\ker\varphi$. Let $x \in \ker\varphi$, $g \in G$, and consider $\varphi(gxg^{-1})$. This expression reduces to $\varphi(g)\varphi(g^{-1}) = \varphi(g)\varphi(g)^{-1} = e_H$, such that $gxg^{-1} \in \ker\varphi$. □

Theorem 2.13 (First Isomorphism Theorem)**.** *Let* G*,* H *be groups and* $\varphi\colon G \to H$ *a homomorhpism. Then,* $\operatorname{im}\varphi \cong G/\ker\varphi$*. In particular, if* φ *is surjective,* $H \cong G/\ker\varphi$*.*

Proof. Let $f\colon G \to H$ be a surjective homomorphism, and $K = \ker f$. We show that the map $f'\colon G/K \to H$ defined by $f'(gK) \mapsto f(g)$ is a well-defined isomorphism, which proves the theorem–for an arbitrary homomorphism g, the statement $G/\ker g \cong \operatorname{im} g$ follows by defining $g'\colon G \to \operatorname{im} g$, observing g' is surjective.

If $g'K = gK$, then $g^{-1}g'K = K$ and $g^{-1}g' \in K$. Thus, we have $e_H = f(g^{-1}g')$. Rewriting, $e_H = f(g)^{-1}f(g')$, and we achieve $f(g) = f(g')$, showing the well-definedness of f'. The surjectivity of f' follows from the surjectivity of f, so we now seek to show the injectivity of f'. Suppose $f'(gK) = f'(g'K)$. Then, $f(g) = f(g')$, and $e_H = f(g)^{-1}f(g') = f(g^{-1})f(g') = f(g^{-1}g')$, thus $g^{-1}g' \in gK$, and $g'K = gK$. □

Example.

The group $5\mathbb{Z}$ is an additive subgroup of $\mathbb{Z}$, with cosets $0+5\mathbb{Z}, 1+5\mathbb{Z}, \dots, 4+5\mathbb{Z}$. Because $n + 5\mathbb{Z} - n = 5\mathbb{Z}$ for all $n \in \mathbb{Z}$, $5\mathbb{Z}$ is a normal subgroup in $\mathbb{Z}$, and we can construct the quotient group $\mathbb{Z}/5\mathbb{Z}$, the integers modulo 5.

2.2 Rings and Modules

2.2.1 Basics

Definition 2.14 (Ring)**.** A ring is a set R equipped with an abelian group structure $+$ (ring addition) and an operation $*\colon R\times R \to R$ (ring multiplication) such that for all $a, b, c \in R$,

$$a * (b + c) = ab + ac,$$

$$a * (b * c) = (a * b) * c.$$

When $*$ is commutative, R is said to be a commutative ring. When there exists an identity for $*$ (some $1 \in R$ such that $1 * r = r * 1 = r$ for all $r \in R$), R is said to be unital. It is not required in general for the $*$ operation to be commutative, or have an identity. In this paper, we will consider all rings to be commutative and unital.

The identity element of the operation + is denoted 0.

Definition 2.15 (Module)**.** A left R-module is a set M that is an abelian group under + (module addition) together with an operation $*\colon R \times M \to M$ (scalar multiplication) such that for all $m, m' \in M$ and $r, r' \in R$,

$$r * (r' * m) = (rr') * m,$$

$$(r + r') * m = r * m + r' * m$$

$$r * (m + m') = r * m + r * m',$$

$$1_R * m = m,$$

$$0_R * m = 0_M.$$

It is said that M is a module *over* R.

Remark. *The $*$ symbol will often be ommitted, so it is important that the reader keep in mind the distinction between ring multiplication and scalar multiplication on module elements. When the ring R is clear from context, R-modules may be referred to simply as modules.*

Examples.

Rings.

- Consider the set $\mathbb{Z}$ equipped with integer addition and multiplication. This set is a ring. Note that multiplicative inverses do not exist for all elements.
- Consider the set of all $n \times n$ matrices with entries in some ring R, denoted $M_n(R)$. Notably, this ring is not commutative.

Modules.

- Every ring is a module over itself, as ring multiplication satisfies the axioms of scalar multiplication, and all rings are groups under addition.
- Vector spaces are modules over fields.
- The zero module, 0, is a module over every ring–its underlying group is the trivial group, consisting only of the identity.

Theorem 2.16 ($\mathbb{Z}$-modules)**.** *Every abelian group is a $\mathbb{Z}$-module and vice-versa.*

Proof. Let M be a $\mathbb{Z}$ module. By definition, M is an abelian group, so the backwards direction is shown. By the module axioms, $(a + b)m = am + bm$ for all $a, b \in \mathbb{Z}$, $m \in M$. Define $a * m$ as $\underbrace{m + \cdots + m}_{a \text{ times}}$. In particular, take $a = b = 1 \in \mathbb{Z}$. Note that elements of $\mathbb{Z}$ can be written uniquely as a sum of 1's, and the statement follows. □

Definition 2.17 (Submodule)**.** A subset N of M is said to be a submodule of M if $N \leq M$ and $rn \in N$ for all $n \in N$, $r \in R$.

Definition 2.18 (Module Homomorphism)**.** A set map $\varphi\colon M \to N$ between two left(or right) R-modules is said to be a *module homomorphism* if for all $m, m' \in M$ and $r \in R$,

$$\varphi(rm + m') = r\varphi(m) + \varphi(m').$$

Such maps may also be called R-linear maps, or just as linear maps when the ring R is understood. If φ is bijective, φ is said to be an *isomorphism*, and we write $M \cong N$. Note that all module homomorphisms must be group homomorhpisms.

The kernel and image of a module homomorphism are as the definitions for a group homomorphism.

Proposition 2.19. *Let $\varphi\colon M \to N$ be a module homomorphism. Then, $\ker\varphi$ is a submodule of M, and $\operatorname{im}\varphi$ is a submodule of N.*

Proof. This follows almost directly from Proposition 2.7; all that remains to be shown is the closure of $\ker\varphi$ under scalar multiplication.

Take $x \in \ker\varphi$, $r \in R$. Then, $\varphi(rx) = r0_N = 0_N$, so $rx \in \ker\varphi$.

The second statement follows from the fact that $\operatorname{im}\varphi$ is a module, but φ is not necessarily surjective. $\square$

Observe that modules are groups, thus we can take their quotients. We wish to define a module structure on these quotient groups.

Definition 2.20 (Quotient Module)**.** Let M be a module, N be a submodule of M. Construct the quotient *group* M/N, which is possible due to the assumed commutativity of M under $+$. Define $r * (m + N)$ (for some $m + N \in M/N$, $r \in R$) as $r * m + N$. This is well-defined because N is closed under scalar multiplication. This is the **quotient module** M/N.

Theorem 2.21 (First Isomorphism Theorem for Modules.)**.** *Given a module homomorphism $\varphi\colon M \to N$, $\operatorname{im}\varphi \cong M/\ker\varphi$. In particular, if φ is surjective, $N \cong M/\ker\varphi$.*

Proof. Let $f\colon M \to N$ be a surjective homomorphism, and $K = \ker f$. Like before, we show that the map $f'\colon M/K \to N$ defined by $f'(m + K) \mapsto f(m)$ is a well-defined isomorphism, and the statement $M/\ker g \cong \operatorname{im} g$ for an arbitrary lienar map g follows similarly to the proof of **Theorem 2.13**.

If $m'+K = m+K$, then $m'-m \in K$, and $0_N = f(m'-m) = f(m')-f(m)$, so f' is well-defined. The surjectivity of f' follows from the surjectivity of f. Suppose $f'(m+K) = f'(m'+K)$ so $f(m) = f(m')$, and $0_N = f(m')-f(m) = f(m'-m)$, thus $m' - m' \in K$, and $m + K = m' + K$. $\square$

2.2.2 Sums, Hom, and Free Modules

Definition 2.22 (Direct Sum)**.** Let A, B be R-modules. The direct sum of A and B, denoted $A \oplus B$, is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$. For an arbitrary direct sum $\bigoplus_{i \in I} M_i$, we require that only finitely many elements are nonzero.

Intuitively, we consider A, B to be submodules of a larger module $A \oplus B$ such that every element can be written uniquely as $a + b$ for $a \in A$, $b \in B$, which justifies the condition on infinite direct sums.

Note that $A \oplus B \cong B \oplus A$.

Definition 2.23 (Hom)**.** We denote the set of all homomorphisms from two R-modules A to B by $\mathrm{Hom}_R(A, B)$. When the ring R is clear, we write $\mathrm{Hom}(A, B)$ instead. We can define an abelian group structure on $\mathrm{Hom}(A, B)$ by $(f+g)(a) = f(a) + g(a)$ for $f, g \in \mathrm{Hom}(A, B)$, $a \in A$.

Proposition 2.24. *Let A, B, C be R-modules.*

1. $\mathrm{Hom}(A, B \oplus C) \cong \mathrm{Hom}(A, C) \oplus \mathrm{Hom}(B, C)$
2. $\mathrm{Hom}(A \oplus B, C) \cong \mathrm{Hom}(A, C) \oplus \mathrm{Hom}(B, C)$.

Proof. (1) Let π_1 be the natural projection from $B \oplus C \to B$, π_2 be the natural projection from $B \oplus C \to C$. If $f \in \mathrm{Hom}(A, B \oplus C)$, then $\pi_1 \circ f$ and $\pi_2 \circ f$ give elements of $\mathrm{Hom}(A, B)$ and $\mathrm{Hom}(A, C)$. The map $f \mapsto (\pi_1 \circ f, \pi_2 \circ f)$ is a homomorphism, as $f + g \mapsto (\pi_1 \circ (f + g), \pi_2 \circ (f + g)) = (\pi_1 \circ f + \pi_1 \circ g, \pi_2 \circ f + \pi_2 \circ g)$ $= (\pi_1 \circ f, \pi_2 \circ f) + (\pi_1 \circ g, \pi_2 \circ g)$. We wish to show this map is in fact an isomorphism, so we now construct an inverse mapping. Given (f_1, f_2) with $f_1 \in \mathrm{Hom}(A, B)$ and $f_2 \in \mathrm{Hom}(A, C)$, define $f \in \mathrm{Hom}(A, B \oplus C)$ by $f(a) = (f_1(a), f_2(a))$ for $a \in A$. This defines a homomorphism from $\mathrm{Hom}(A, B) \oplus \mathrm{Hom}(A, C)$ to $(\mathrm{Hom}(A, B \oplus C))$, which is an inverse to the map constructed before.

(2) Let $f \in \mathrm{Hom}(A \oplus B, C)$. Then, define a map $f \mapsto (f \circ \pi_1, f \circ \pi_2)$, where π_1, π_2 are natural projections from $A \oplus B$ to A and B respectively. This map is a homomorphism, and its inverse is the map $(f_1, f_2) \mapsto f := f(a) = (f_1(a), f_2(a))$, thus, the isomorphism is shown. □

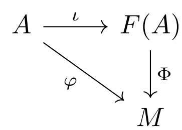
Definition 2.25 (Free Module)**.** Let F be an R-module. F is said to be *free*, or be a *free module*, if there exists a basis for F. That is, there exists a set $E \subseteq F$ such that every $f \in F$ can be written as an R-linear combination of elements of E, and if $r_1 e_1 + \cdots + r_n e_n = 0$ for $r_i \in R$, $e_i \in E$, then $r_i = 0$ for all i. Consequently, every f can be written uniquely as an R-linear combination of elements of F. It is said that F is free *on* E.

Examples.

1. Modules over fields are called vector spaces, and are all free.

2. For any ring R, R is a free module over itself.

Theorem 2.26. *Given a basis A, there is a free R-module on the elements of A $F(A)$ with the property that given an R-module M and a set map $\varphi\colon A \to M$, there is a unique $\Phi\colon F(A) \to M$ such that the following diagram commutes.*



Proof. For nonempty A, define $F(A)$ to be the set of all set maps $A \to R$ with finite support. We define for $f, g \in F(A)$, $a \in A$, $r \in R$, $(f+g)(a) = f(a) + g(a)$ and $(rf)(a) = r(f(a))$. Then, $F(A)$ is a module, and ι sends a to the function that is 0 at all inputs but a. We can consider elements of $F(A)$ to be linear combinations of the $\iota(a)$, abbreviated a for simplicity. the Define Φ by $\Phi(\sum ra) = \sum r\varphi(a)$. We observe Φ is well defined by the uniqueness of the linear combination representation of $F(A)$, and by definition Φ restricted to A is φ. Given that $F(A)$ is generated by A, a homomorphism on $F(A)$ is determined by its values on A, proving uniqueness. □

2.2.3 Bilinear Maps and Tensor Products

Definition 2.27 (Bilinear Map)**.** An R-bilinear map is a map of the form $\varphi\colon A \times B \to C$ (where A, B, C are R-modules) such that the maps $a \mapsto \varphi(a, b')$ and $b \mapsto \varphi(a', b)$ are module homomorphisms for all $a' \in A$, $b' \in B$. When the ring R is clear from context, φ may be referred to as a bilinear map.

Proposition 2.28. *Let A, B be R-modules. Then, there exists an R-module T and a bilinear map $t\colon A \times B \to T$ such that for any R-module C and bilinear map $f\colon A \times B \to C$, there is a unique module homomorhpism $f'\colon T \to P$ such that $f = f' \circ t$. This module T is unique up to unique isomorphism.*

Proof. We first show the uniqueness of the module T. Using notation from the proposition, Let T' be another module with the same property, and t' be the corresponding bilinear map. Then, there is a unique $j\colon T \to T'$ such that $t' = j \circ g$, as well as a $j'\colon T' \to T$ such that $t = j' \circ t'$. Each of $j \circ j'$ and $j' \circ j$ must be the identity, thus j is an isomorphism and uniqueness is proved.

We now show the existence of such a module. Let F be the free R-module on elements of $A \times B$. Let D be the submodule of F of all elements of the forms:

$$(x + x', y) - (x, y) - (x', y)$$

$$(x, y + y') - (x, y) - (x, y')$$

$$(rx, y) - r(x, y)$$

$$(x, ry) = r(x, y)$$

for $x, x' \in A$, $y, y' \in B$, $r \in R$. Let $T = F/D$, and let $x \otimes y$ denote the image of $(x, y) \in C$ in T. Then, T is generated by elements of the form $x \otimes y$, and from the definitions this quotient map is bilinear (all elements of D are killed in T; e.g. $(x + x') \otimes y = x \otimes y + x' \otimes y$).

Any linear map f from $A \times B$ into another module P extends linearly to another linear map $\bar{f}\colon F \to P$. Suppose f is bilinear. Then, $\bar{f}$ vanishes on the generators of D, and thus on D, and induces a well-defined linear map f' of T into P such that $f'(x \otimes y) = f(x, y)$. The map f' is uniquely determined, thus, T together with the map $g\colon A \times B \to T$ where $g(x, y) \mapsto x \otimes y$ satisfies the conditions specified in the proposition. □

Definition 2.29 (Tensor Product)**.** In the notation of the above propotision, the module T is said to be the *tensor product* of A and B, denoted $A \otimes_R B$, or $A \otimes B$ when the ring R is understood.

Let $f\colon A \to A'$ and $g\colon B \to B'$ be linear maps. Then, there is a unique map $f \otimes g\colon A \otimes B \to A' \otimes B'$ such that $(f \otimes g)(a \otimes b) = f(a) \otimes g(b)$ for all $a \in A$, $b \in B$.

Remark. *The remainder of this paper concerns modules over a fixed ring R.*

3 Basic Homological Algebra

3.1 Definitions

Definition 3.1 (Cochain Complex)**.** Let $\{C^\bullet, d^\bullet\}$ be a sequence of modules module homomorphisms:

$$\cdots \xrightarrow{d^{n-2}} C^{n-1} \xrightarrow{d^{n-1}} C^n \xrightarrow{d^n} C^{n+1} \xrightarrow{d^{n-1}} \cdots.$$

This sequence is called a cochain complex if $d_{n+1} \circ d_n = 0$ for all n, that is, $d_{n+1}(d_n(x)) = 0$ for all $x \in C_n$. Equivalently, $\operatorname{im} d_n \subseteq \ker d_{n+1}$.

This concept can be dualized by reversing all of the arrows in the diagram, leading to the notion of a chain complex. In this case, the indices are denoted by a subscript ($\{C_\bullet, d_\bullet\}$).

Definition 3.2 (Exact Sequence)**.** A sequence is said to be exact at C^n if $\operatorname{im} d^{n-1} = \ker d^n$. A sequence is exact, or is an *exact sequence*, if it is exact at every term.

In particular, if

$$0 \longrightarrow M \xrightarrow{f} M'$$

is exact, f is injective, and if

$$N \xrightarrow{f'} N' \longrightarrow 0$$

is exact, f' is surjective.

A *short exact sequence* is an exact sequence of the form

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0.$$

If $B \cong A \oplus C$, the above sequence is said to split, or be a split exact sequence.

Definition 3.3 (Homology, Cohomology)**.** The cohomology module of a cochain sequence $\{C^\bullet, d^\bullet\}$ at n (denoted $H^n(C)$, $H_n(C)$ for homology) is defined to be $\ker d^n / \operatorname{im} d^{n-1}$ ($\ker d_n / \operatorname{im} d_{n+1}$ for homology).

Definition 3.4 (Homomorphism of Cochain Complexes)**.** A homomorphism between cochain complexes $\{C^\bullet, d^{C,\bullet}\}, \{D^\bullet, d^{D,\bullet}\}$ is a family of module homomorphisms $f_i \colon C^i \to D^i$ such that the following diagram commutes.

$$\begin{array}{ccccccc} \cdots & \xrightarrow{d^{C,n-1}} & C^n & \xrightarrow{d^{C,n}} & C^{n+1} & \xrightarrow{d^{C,n+1}} & \cdots \\ & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n+1}} & & \\ \cdots & \xrightarrow[d^{D,n-1}]{} & D^n & \xrightarrow[d^{D,n}]{} & D^{n+1} & \xrightarrow[d^{D,n+1}]{} & \cdots \end{array}$$

Symbolically, $f_{n+1} d^{C,n} = d^{D,n} f_n$ Homomorphisms are defined analagously for cochain complexes.

Proposition 3.5. *A homomorphism between (co-)chain complexes induces homomorphisms between their respective (co-)homology groups.*

Proof. We first show f maps $\ker d^{C,n}$ to $\ker d^{D,n}$. Let $x \in \ker d^{C,n}$. Then, $f_{n+1} d^{C,n}(x) = 0$ because f_{n+1} maps 0 to 0, and $f_{n+1} d^{C,n}(x) = d^{D,n} f_n(x) = 0$, so $f_n(\ker d^{C,n}) \subseteq \ker d^{D,n}$.

We now show f maps $\operatorname{im} d^{C,n-1}$ to $\operatorname{im} d^{D,n-1}$. Note that $d^{C,n-1}(C^{n-1}) = \operatorname{im} d^{C,n-1}$, and $d^{D,n-1}(D^{n-1}) = \operatorname{im} d^{D,n-1}$. Because $f_{n-1}(C^{n-1}) \subseteq D^{n-1}$, we observe $d^{D,n-1} f_{n-1}(C^{n-1}) \subseteq \operatorname{im} d^{D,n-1}$. Then, $d^{D,n-1} f_{n-1}(C^{n-1}) = f_n d^{C,n-1}(C^{n-1}) = f_n(\operatorname{im} d^{C,n-1}) \subseteq \operatorname{im} d^{D,n-1}$, so f maps $\operatorname{im} d^{C,n-1}$ to $\operatorname{im} d^{D,n-1}$.

Thus, f induces a map from $H^n(C)$ to $H^n(D)$.

This proof is analagous for chains. □

Definition 3.6 (Short Exact Sequence of Cochains.)**.** A sequence of cochains

$$0 \to \{A^\bullet\} \to \{B^\bullet\} \to \{C^\bullet\} \to 0$$

is a short exact sequence if each

$$0 \to A^n \to B^n \to C^n \to 0$$

is exact.

3.2 The Snake Lemma and the Long Exact Sequence of Cohomology

The following theorems play a major role in the importance of Ext and Tor, namely in the extension of sequences that fail to be exact under Hom and $\otimes$.

Theorem 3.7 (The Snake Lemma)**.** *Consider a commutative diagram*

$$\begin{array}{ccccccccc} & & A' & \xrightarrow{f} & A & \xrightarrow{g} & A'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d'} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d''} & & \\ 0 & \longrightarrow & B' & \xrightarrow[f']{} & B & \xrightarrow[g']{} & B'' & & \end{array}$$

with exact rows. Then, there exists an exact sequence

$$\ker d' \longrightarrow \ker d \longrightarrow \ker d'' \xrightarrow{\delta} \operatorname{coker} d' \longrightarrow \operatorname{coker} d \longrightarrow \operatorname{coker} d''$$

Proof. The individual sequences $\ker d' \to \ker d \to \ker d''$ and $\operatorname{coker} d' \to \operatorname{coker} d \to \operatorname{coker} d''$ are easy to understand, and exactness follows from the hypothesized exactness of the diagram.

We construct δ as follows: consider an element $x \in \ker d''$ and select $y \in A$ such that $g(y) = x$. We observe $d \circ g'(y) = d'' \circ g(y) = d''(x) = 0$, so $d(y) \in \ker g'$. By exactness, we find $z \in B'$ such that $f'(z) = d(y)$. The element z is unique by exactness, and we can define $\delta(x) = z + \operatorname{im} d' \in \operatorname{coker} d'$.

We first show δ is well-defined. Suppose instead of y, we chose y' with $g(y') = x$. Then, $g(y - y') = 0$, $y - y' \in \ker g = \operatorname{im} f$, so we can choose $a \in A'$ with $(y - y') = f(a)$. By exactness, there are unique b, b' with $d(y) = f'(b)$ and $d(y') = f'(b')$, and we observe $f'(d'(a)) = d(f(a)) = d(y - y') = f'(b - b')$. Since f' is injective, $b - b' = d'(a) \in \operatorname{im} d$, so $b + \operatorname{im} d' - \delta(x) = b + \operatorname{im} d'$. ☐

Theorem 3.8 (Long Exact Sequence in Cohomology)**.** *Let*

$$0 \to \{A^\bullet\} \to \{B^\bullet\} \to \{C^\bullet\} \to 0$$

be a short exact sequence of cochains. Then, there exists an exact sequence

$$\begin{array}{cccccccccc} 0 & \longrightarrow & H^0(A) & \longrightarrow & H^0(B) & \longrightarrow & H^0(C) & & & \\ & & & & & & {\scriptstyle \delta_0}\downarrow & & & \\ & & & & & & H^1(A) & \longrightarrow & H^1(B) & \longrightarrow & H^1(C) \\ & & & & & & & & & & {\scriptstyle \delta_1}\downarrow \\ & & & & & & & & & & \cdots \end{array}$$

Where the maps between H^n are the induced maps on cohomology modules. The δ_n are called connecting homomorphisms.

Proof. Consider the diagram

$$\begin{array}{ccccccc} & & A^n/\operatorname{im} d^{A,n-1} & \longrightarrow & B^n/\operatorname{im} d^{B,n-1} & \longrightarrow & C^n/\operatorname{im} d^{C,n-1} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \ker d^{A,n} & \longrightarrow & \ker d^{B,n} & \longrightarrow & \ker d^{C,n} & & \end{array}$$

We observe that (in the notation of the snake lemma) the kernels are the nth cohomology groups of the respective sequence, and the cokernels are the $n-1$th groups. Then, the sequence exists and is exact by the snake lemma. □

4 Ext$(-, D)$

4.1 Definitions

Proposition 4.1. *Suppose we have an exact sequence*

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

and a module D. Then, there exists an exact sequence

$$0 \longrightarrow \operatorname{Hom}(C, D) \xrightarrow{g'} \operatorname{Hom}(B, D) \xrightarrow{f'} \operatorname{Hom}(A, D)$$

with $g' := \varphi \mapsto \varphi \circ g$, $f' := \psi \mapsto \psi \circ f$ for $\varphi \in \operatorname{Hom}(C, D)$, $\psi \in \operatorname{Hom}(B, D)$

Proof. g' is injective because g is surjective, meaning $k \circ g = k' \circ g$ implies $k = k'$, so the induced map is injective.

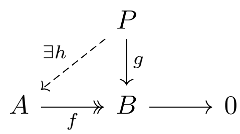
We wish to show $\ker f' \subseteq \operatorname{im} g'$. Let $t \in \ker f'$, so $t \circ f = 0$. If $a \in A$, $t(f(a)) = 0$, so $f(a) \in \ker t$ (because a is an arbitrary element of A, this means $f(A) \subseteq \ker t$, and in fact, $\ker g \subseteq \ker t$). Note that $C \cong B/f(A)$. Let $t' \colon B/f(A) \to D$ such that $t'(b+f(A)) \mapsto t(b)$. This map is well defined because if $b+f(A) = b'+f(A)$, i.e. $b - b' \in f(A)$, then $t(b - b') = 0 = t(b) - t(b')$ and $t(b) = t(b')$. Let φ denote the canonical isomorphism from $B/f(A)$ to C. Observe $t = t' \circ \varphi^{-1} \circ g$, and we have shown that if $t \in \ker f'$, there exists a map $t' \circ \varphi$ such that $g'(t' \circ \varphi) = t$, showing $\ker f' \subseteq \operatorname{im} g'$.

Reverse contaiment follows from the fact that $f' \circ g' = 0$, which in turn follows from the observation that $g \circ f = 0$.

□

Note that neither the map $A \mapsto \operatorname{Hom}(D, A)$ nor $A \mapsto \operatorname{Hom}(A, D)$ completely preserve exact sequences.

Definition 4.2 (Projective module)**.** Let P be a module. P is said to be projective if for every surjective linear map $f\colon A \to B$ and every linear map $g\colon P \to B$, there exists a (not necessarily unique) linear map $h\colon P \to A$ such that $f \circ h = g$. Pictorially, this can be represented by the commutative diagram

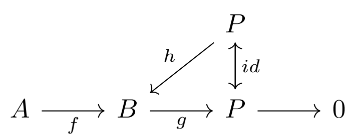


where the row is exact.

Proposition 4.3. *The following are equivalent:*

1. *P is projective.*
2. *Every exact sequence $0 \to A \to B \to P \to 0$ splits.*
3. *There exists an M such that $P \oplus M$ is free.*

Proof. (1)→(2) Consider the diagram



where the row is exact. Let $b \in B$. Then, $b - h(g(b)) \in \ker g$, so $M = \ker g + \operatorname{im} f$; that is, every element of B can be written as a sum of an element of $\ker g$ and an element of $\operatorname{im} f$. This is a direct sum, because if $b = k + i$ with $k \in \ker g$ and $i = f(a) \in \operatorname{im} f$ for some $a \in A$, $g(b) = a$. Then, a is uniquely determined by b, and so is i, and so is k. Then, $B \cong \ker g \oplus \operatorname{im} h$, and the sequence splits.

(2)→(3) Let F be the free module on elements of P, and let $f\colon F \to P$ be the "evaluation" homomorphism (rp as an element of F is mapped to rp as an element of P, with $r \in R$). Then, the sequence

$$0 \longrightarrow \ker f \longrightarrow F \xrightarrow[f]{} P \longrightarrow 0$$

is exact, and we can apply (2) to split F into a direct sum with P.

(3)→(1) Suppose $P \oplus Q \cong F$ where F is free with basis S. Let π denote the natural projection $F \to P$. In the notation of (2), $g \circ \pi$ is a map $F \to B$. Define $b_s = f(\pi(s))$ for $s \in S$ and a_s as any element of A such that $f(a_s) = b_s$. There is a unique $\varphi\colon F \to A$ with $\varphi(s) = a_s$, and by definition $f \circ \varphi(s) = f(a_s) = b_s = f \circ \pi(s)$. Define $\varphi'\colon P \to A$ by $\varphi'(p) = \varphi((p, 0))$. Then, $f \circ \varphi' = g$.

□

Definition 4.4 (Projective Resolution)**.** A projective resolution of a module A is an exact sequence

$$0 \longleftarrow A \longleftarrow P_0 \longleftarrow P_1 \longleftarrow \cdots$$

such that all P_i are projective.

We now ivnestigate the failure of $\mathrm{Hom}(-, D)$ to preserve exact sequences. To do so, we will define Ext.

Definition 4.5 (Ext)**.** Let A be a module, fix a module D, and let

$$0 \longleftarrow A \xleftarrow{\epsilon'} P_0 \xleftarrow{d_1'} P_1 \xleftarrow{d_2'} \cdots$$

be a projective resolution of A. Form the sequence $\{P_A^\bullet\} =$

$$0 \longrightarrow \mathrm{Hom}(A, D) \xrightarrow{\epsilon} \mathrm{Hom}(P_0, D) \xrightarrow{d_1} \mathrm{Hom}(P_1, D) \xrightarrow{d_2} \cdots$$

and note that while not necessarily exact, this sequence is still a cochain complex. We define

$$\mathrm{Ext}_R^n(A, D) = H^n(P_A^\bullet)$$

for $n \geq 1$, and

$$\mathrm{Ext}_R^0(A, D) = \ker d_1.$$

Equivalently, $\mathrm{Ext}_R^n(A, D)$ are the cohomology groups of $\mathrm{Hom}(P_A^\bullet, D)$ with the $\mathrm{Hom}(A, D)$ term removed.

Proposition 4.6.

$$\mathrm{Ext}^0(A, D) \cong \mathrm{Hom}(A, D).$$

Proof. By **Proposition 4.1**, the term $\mathrm{Hom}(A, D)$ in the diagram of the definition of Ext is exact, so $\ker d_1 = \mathrm{im}\,\epsilon \cong \mathrm{Hom}(A, D)$. □

4.2 Independence

We now wish to show that this construction is independent of the particular choice of projective resolution $\{P_A^\bullet\}$. We first observe a "lifting" property for homomorphisms of projective resolutions.

Proposition 4.7. *Given projective resolutions of A and A' and a map $f \colon A \to A'$,*

$$\begin{array}{ccccccccc} 0 & \longleftarrow & A & \xleftarrow{\epsilon} & P_0 & \xleftarrow{d_0} & P_1 & \xleftarrow{d_1} & \cdots \\ & & \downarrow{\scriptstyle f} & & & & & & \\ 0 & \longleftarrow & A' & \xleftarrow[\epsilon]{} & P_0' & \xleftarrow[d_0']{} & P_1' & \xleftarrow[d_1']{} & \cdots \end{array}$$

There are lifts $f_n\colon P_n \to P'_n$ of f such that the following diagram commutes.

$$\begin{array}{ccccccccc}
0 & \longleftarrow & A & \xleftarrow{\epsilon} & P_0 & \xleftarrow{d_1} & P_1 & \xleftarrow{d_2} & \cdots \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f_1} & & \\
0 & \longleftarrow & A' & \xleftarrow[\epsilon]{} & P'_0 & \xleftarrow[d'_1]{} & P'_1 & \xleftarrow[d'_2]{} & \cdots
\end{array}$$

Proof. [DF03]. Since P_0 is projective, we can lift $f \circ \epsilon$ to $f_0\colon P_0 \to P'_0$ such that the square commutes, and we may inductively continue this process to achieve the remaining f_n. □

Proposition 4.8. *We refer to the second diagram of* ***Proposition 4.7****. For every n, there is a homomorphism φ_n between the* Ext *groups of each resolution, and these maps depend only on f, not on the lifts f_n.*

Proof. [DF03]. The induced maps are clear. The second statement of the proposition is seen to be equivalent to the statement that the zero map between A and A' induces the zero maps as φ_n. Suppose $f = 0$. We define $s_n\colon P_n \to P'_{n+1}$ such that

$$f_n = d'_{n+1} \circ s_n + s_{n-1} \circ d_n.$$

Applying $\mathrm{Hom}(-, D)$ preserves the properties of the s_n (with the induced maps, arrows reversed as always).

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}(A,D) & \longrightarrow & \mathrm{Hom}(P_0,D) & \longrightarrow & \mathrm{Hom}(P_1,D) & \longrightarrow & \cdots \\
 & \nwarrow{\scriptstyle s_{-1}} & \uparrow{\scriptstyle f} & \nwarrow{\scriptstyle s_0} & \uparrow{\scriptstyle f_0} & \nwarrow{\scriptstyle s_1} & \uparrow{\scriptstyle f_1} & \nwarrow{\scriptstyle s_2} & \\
0 & \longrightarrow & \mathrm{Hom}(A',D) & \longrightarrow & \mathrm{Hom}(P'_0,D) & \longrightarrow & \mathrm{Hom}(P'_1,D) & \longrightarrow & \cdots
\end{array}$$

Note that this diagram is not necessarily commutative.

Given the maps and the relations with s_n, we can see that the induced maps are 0, proving the propostition. □

Theorem 4.9. *The groups $\mathrm{Ext}^n(A, D)$ are independent of particular projective resolution.*

Proof. [DF03]. Consider the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}(A,D) & \longrightarrow & \mathrm{Hom}(P_0,D) & \longrightarrow & \mathrm{Hom}(P_1,D) & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f_1} & & \\
0 & \longrightarrow & \mathrm{Hom}(A',D) & \longrightarrow & \mathrm{Hom}(P'_0,D) & \longrightarrow & \mathrm{Hom}(P'_1,D) & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g_0} & & \downarrow{\scriptstyle g_1} & & \\
0 & \longrightarrow & \mathrm{Hom}(A,D) & \longrightarrow & \mathrm{Hom}(P_0,D) & \longrightarrow & \mathrm{Hom}(P_1,D) & \longrightarrow & \cdots
\end{array}$$

With $A = A'$, $f = \mathrm{id}_{A\to A'}$, $g = \mathrm{id}_{A'\to A}$. These maps induce maps $\varphi_n\colon \operatorname{Ext}^n(A, D) \to \operatorname{Ext}^n(A', D)$ and $\psi_n\colon \operatorname{Ext}^n(A', D) \to \operatorname{Ext}^n(A, D)$. The maps $g_n \circ f_n$ are seen to be lifts of id_A, which is seen to induce maps $\psi_n \circ \varphi_n$, which is the identity, and reversing the roles of A and A' as well as f and g allows us to deduce that ψ and φ are two-sided inverses of each other, and thus are isomorphisms. □

4.3 Projectivity and Extending Exact Sequences Under Hom

We have shown Ext to be independent of choice of projective resolution. Now we seek to show the extending property of Ext.

Lemma 4.10. *A direct sum of two projective modules is projective.*

Proof. Let P, P' be projective modules. Since there are modules Q, Q' such that $P \oplus Q$ and $P' \oplus Q'$ are free, direct sums commute, and the sum of a free module with a free module is free, we observe $P \oplus P' \oplus Q \oplus Q' \cong P \oplus Q \oplus P' \oplus Q'$ is a free module. □

Lemma 4.11. *Let*

$$0 \longrightarrow \{A^\bullet\} \longrightarrow \{B^\bullet\} \longrightarrow \{C^\bullet\} \longrightarrow 0$$

be a short exact sequence of cochains. If $\{A^\bullet\}, \{C^\bullet\}$ are exact, then so is $\{B^\bullet\}$.

Proof. Using **Theorem 3.8**, we observe an exact sequence

$$\cdots \longrightarrow 0 \longrightarrow H^n(B) \longrightarrow 0 \longrightarrow \cdots$$

The only way for this sequence to be exact is for $H^n(B)$ to be zero, thus $\{B^\bullet\}$ is exact. □

Proposition 4.12. *Let*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

be a short exact sequence of modules, and let A and C have projective resolutions P_n and P'_n respectively. Then, B has a resolution given by $P_n \oplus P'_n$, and the *following diagram is commutative with exact columns, and split exact rows.*

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P_1 & \longrightarrow & P_1 \oplus P_1' & \longrightarrow & P_1' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P_0 & \longrightarrow & P_0 \oplus P_0' & \longrightarrow & P_0' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Proof. [DF03]. The middle column is projective via **Lemma 4.10**. The maps to make each row exact are the appropriate inclusion and projection maps.

We define $\mu\colon P_0' \to B$ as a projective lift of the map $P_0' \to C$, which by definition commutes with the appropriate arrows. Define λ as the composition of maps $P_0 \to A \to M$ (it may be helpful to recall the informal characterization of the direct sum to see why this map commutes with the relevant arrows), and $\pi\colon P_0 \oplus P_0' \to M$ such that $\pi(p, p') \mapsto \lambda(p) + \mu(p')$. This process can be extended inductively to produce the relevant (commutative!) grid. The exactness of the middle column follows from **Lemma 4.11**. ☐

Theorem 4.13. *Let*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

be a short exact sequence of modules. Then,

$$\begin{array}{cccccccccc}
0 & \longrightarrow & \mathrm{Hom}(C,D) & \longrightarrow & \mathrm{Hom}(B,D) & \longrightarrow & \mathrm{Hom}(A,D) & & & \\
 & & & & & & \downarrow{\scriptstyle \delta_0} & & & \\
 & & & & & & \mathrm{Ext}^1(C,D) & \longrightarrow & \mathrm{Ext}^1(B,D) & \longrightarrow \ \mathrm{Ext}^1(A,D) \\
 & & & & & & & & & \downarrow{\scriptstyle \delta_1} \\
 & & & & & & & & & \cdots
\end{array}$$

is a long exact sequence.

Proof. [DF03]. Removing the row A, B, C and taking homomorphisms into D, we observe a diagram

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \mathrm{Hom}(P_1, D) & \longrightarrow & \mathrm{Hom}(P_1 \oplus P_1', D) & \longrightarrow & \mathrm{Hom}(P_1', D) & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \mathrm{Hom}(P_0, D) & \longrightarrow & \mathrm{Hom}(P_0 \oplus P_0', D) & \longrightarrow & \mathrm{Hom}(P_0', D) & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

with split rows by **Proposition 2.24**. Then, by **Thorem 3.8**, we observe the desired exact sequence. □

Theorem 4.14. *Let P be a module. Then, P is projective iff* $\mathrm{Ext}^n(P, A) = 0$ *for all modules A and $n \geq 1$.*

Proof. It is clear by **Proposition 4.3** and **Theorem 4.13** that P is projective if the higher Ext groups vanish. To show the converse, we note that P has a projective resolution

$$0 \longleftarrow P \xleftarrow[\mathrm{id}]{} P \longleftarrow 0$$

from which we derive

$$0 \longrightarrow \mathrm{Hom}(P, A) \xrightarrow{\mathrm{id}} \mathrm{Hom}(P, A) \longrightarrow 0 \longrightarrow 0 \longrightarrow \cdots$$

and we deduce the vanishing of Ext^n. □

In this sense, $\mathrm{Ext}(-, D)$ measures how “close” D is to being projective.

5 Tor($D \otimes -$)

5.1 Definitions

Proposition 5.1. *Given an exact sequence of modules*

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

we have an exact sequence

$$D \otimes A \xrightarrow{1 \otimes f} D \otimes B \xrightarrow{1 \otimes g} D \otimes C \longrightarrow 0.$$

Proof. [DF03]. Given that g is surjective, we note that $D \otimes C$ is generated by simple tensors of the form $d \otimes c$ for $d \in D$, $c \in C$. Thus, $c = g(b)$ for some $b \in B$, and $1 \otimes g(d \otimes b) = d \otimes g(b) = d \otimes b$ shows $1 \otimes g$ is surjective.

We have $\operatorname{im} 1 \otimes f \subseteq \operatorname{im} 1 \otimes g$ because $(1 \otimes g)(\sum d \otimes f(a)) = \sum d \otimes g \circ f(a) = 1 \otimes 0 = 0$. There is a projection $\pi \colon D \otimes B / \operatorname{im}(1 \otimes f) \to D \otimes B / \ker(1 \otimes g) = D \otimes C$. The composite projection with the natural projection $(D \otimes B \to D \otimes B / \operatorname{im}(1 \otimes f))$, $D \otimes B \to D \otimes B / \operatorname{im}(1 \otimes f) \to D \otimes C$ is just the map $1 \otimes g$. We seek to show that π is an isomorphism.

Define $\pi' \colon D \times C \to D \otimes B / \operatorname{im}(1 \otimes f)$ so that $\pi'(d, c) \mapsto d \times b$ for any $b \in B$ where $g(b) = c$. This is well defined because any other element b' mapping to c differs from b by an element of $\ker g = \operatorname{im} f$, so $b' = b + f(a)$ for some $a \in A$, and $d \otimes f(a) \in \operatorname{im} 1 \otimes f$. We observe $\pi'(rd, c) = \pi'(d, rc)$, which induces a map $\overline{\pi} \colon D \times C \to D \otimes M / \operatorname{im}(1 \otimes f)$ where $\overline{\pi}(d \otimes c) = d \otimes b$. Thus, $\overline{\pi} \circ \pi = 1$ because $\overline{\pi} \circ \pi(d \otimes b) = \overline{\pi}(d \otimes g(b)) = d \otimes b$. Likewise, $\pi \circ \overline{\pi} = 1$, so π is an isomorphism and exactness is proved. □

We note $\otimes$ does not necessarily preserve exact sequences, but there are some cases in which it does–in this case, the module D is said to be flat.

Definition 5.2 (Tor)**.** Let D, B be modules. Form a projective resolution $\{B_\bullet\}$ of B

$$0 \longleftarrow B \xleftarrow[\epsilon]{} P_0 \xleftarrow[d_1]{} P_1 \xleftarrow[d_2]{} \cdots$$

and apply $D \otimes -$ to achieve $\{D \otimes B_\bullet\}$.

$$0 \longleftarrow D \otimes B \xleftarrow[1 \otimes \epsilon]{} D \otimes P_0 \xleftarrow[1 \otimes d_1]{} D \otimes P_1 \xleftarrow[1 \otimes d_2]{} \cdots$$

This is still a chain complex by an argument in the proof of **Proposition 5.1**, and we define

$$\operatorname{Tor}_n(D, B) = H_n(D \otimes B_\bullet)$$

for $n \geq 1$, and

$$\operatorname{Tor}_0(D, B) = H_n(D \otimes P_0 / \operatorname{im} 1 \otimes d_1).$$

Proposition 5.3.

$$Tor_0(D, B) \cong D \otimes B$$

Proof. See **Proposition 5.1**. □

Proposition 5.4. Tor *is independent of choice of projective resolution.*

Proof. The same argument used in the proof of **Theorem 4.9** applies to Tor. □

5.2 Flatness and Extending Exact Sequences under $\otimes$

We now seek to prove an analagous property of "extending sequences" for Tor and $\otimes$.

Proposition 5.5 (Long Exact Sequence in Homology)**.** *Given a short exact sequence of chains*

$$0 \longrightarrow \{A_\bullet\} \longrightarrow \{B_\bullet\} \longrightarrow \{C_\bullet\} \longrightarrow 0$$

there is a long exact sequence

$$\begin{array}{ccccccc} 0 \longrightarrow H_0(A) & \longrightarrow & H_0(B) & \longrightarrow & H_0(C) & & \\ & & & & \downarrow \delta & & \\ & & & & H_1(A) & \longrightarrow & \cdots \end{array}$$

Proof. Apply **Theorem 3.7** to

$$\begin{array}{ccccccc} & A_n/\operatorname{im} d_{n+1} & \longrightarrow & B_n/\operatorname{im} d_{n+1} & \longrightarrow & C_n/\operatorname{im} d_{n+1} & \longrightarrow 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 \longrightarrow & \ker d_{n+1} & \longrightarrow & \ker d_{n+1} & \longrightarrow & \ker d_{n+1} & \end{array}$$

□

Lemma 5.6.

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

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

Proof. Consider the map $(A \oplus B) \times C \to A \otimes C \oplus B \otimes C$ where $((a, b), c) \mapsto (a \otimes b, a \otimes c)$. This map is bilinear, so by the definition of the tensor product there is a unique homomorphism $t\colon (A \oplus B) \otimes C \to A \otimes C \oplus B \otimes C$ so $t((a, b) \otimes c) = (a \otimes c, b \otimes c)$.

Now consider the maps $A \times C \to (A \oplus B) \otimes C$ where $(a, c) \to (a, 0) \otimes n$ and $B \times C \to (A \oplus B) \otimes C$ where $(b, c) \to (0, b) \otimes n$. These maps are bilinear, so there are maps $f_1\colon A \otimes C \to (A \oplus B) \otimes C$ s.t. $f_1(a \otimes c) = (a, 0)$ and $f_2\colon B \otimes C \to (A \oplus B) \otimes C$ s.t $f_2(b \otimes c) = (0, b)$. Then, we define $F\colon A \otimes C \oplus B \otimes C \to (A \oplus B) \otimes C$ s.t. $F(a \otimes c, b \otimes c') = f_1(a \otimes c) + f_2(b \otimes c')$ is an inverse to t. □

Theorem 5.7. *Given an exact sequence*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

there is an exact sequence

$$\begin{array}{ccccccccc}
\cdots & & & & & & & & \\
\downarrow \delta_1 & & & & & & & & \\
\mathrm{Tor}_1(D,A) & \longrightarrow & \mathrm{Tor}_1(D,B) & \longrightarrow & \mathrm{Tor}_1(D,C) & & & & \\
& & & & \downarrow \delta_0 & & & & \\
& & & & D \otimes A & \longrightarrow & D \otimes B & \longrightarrow & D \otimes C \longrightarrow 0
\end{array}$$

Proof. Form projective resolutions of A, B, and C as in **Proposition 4.12** and apply $D \otimes -$. By **Lemma 5.6** we have a short exact sequence of chain complexes, and we can apply **Proposition 5.5** to observe the desired exact sequence. □

Theorem 5.8. *Let D be a module. Then, D is flat iff $\mathrm{Tor}_n(D,B) = 0$ for all modules B and $n \geq 1$.*

Proof. See **Theorem 4.14**. □

Acknowledgements

I would like to thank Simon Rubinstein-Salzedo for running the Euler Circle program and for his guidance on my topic. I would also like to thank Ryan Catullo for his invaluable feedback and insightful discussions, as well as Jinfei Huang for his feedback regarding the exposition of the preliminaries section.

References

[DF03] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2003.