

Defining Group Homology and Cohomology

HUANG Qinpei (with the assistance of AI)

October 9, 2026

Abstract

These notes develop group homology and cohomology as derived functors of coinvariants and invariants for a group acting on an abelian group. A companion volume supplies prerequisites on categories, modules, and complexes. Here projective and injective resolutions lead to Tor and Ext. Group actions, the augmentation ideal, and the two degree-zero constructions make the definitions concrete; bar resolutions then give equivalent chain and cochain formulas.

Contents

1	Free Modules, Projective Modules, and Resolutions	2
1.1	Free modules, generators, relations, and free resolutions	2
1.2	Projective modules: definition and characterizations	6
1.3	Projective resolutions and their augmentations	13
1.4	Comparison and uniqueness up to chain homotopy	16
2	Injective Modules and Injective Resolutions	21
2.1	Injective modules: definition and characterizations	21
2.2	Injective resolutions, their augmentations, and existence	24
2.3	Comparison and uniqueness up to cochain homotopy	27
3	Derived Functors	30
3.1	Definitions, vanishing, and long exact sequences	30
3.2	Exactness of Hom and tensor	35
3.3	Tor, Ext, and equivalent computations	40
4	Group Homology and Cohomology via Derived Functors	49
4.1	Group actions, invariants, and coinvariants	49
4.2	The invariant and coinvariant functors and their exactness	52
4.3	Derived definitions, equivalent computations, and long exact sequences	54
5	Group Homology and Cohomology via Explicit Complexes	58
5.1	The bar resolution: one construction for every group	58
5.2	The right bar resolution and the coefficient chain complex	62
5.3	Cochains as functions and the equivalent definitions	63

1 Free Modules, Projective Modules, and Resolutions

A presentation describes a module by generators and relations. Resolving successive relation modules extends that description to a complex. Free modules make the construction possible; projectivity isolates the lifting property needed to compare all such descriptions. The exactness and homotopy language will be used from the preparatory notes.

1.1 Free modules, generators, relations, and free resolutions

Let $U : R\text{-Mod} \rightarrow \mathbf{Set}$ be the functor that remembers only the underlying set.

Definition 1.1 (Free module on a set). A *free R -module on a set S* is a module $F(S)$ together with a function $\iota : S \rightarrow U(F(S))$ such that, for every R -module M and every function $a : S \rightarrow U(M)$, there is a unique R -linear map $\tilde{a} : F(S) \rightarrow M$ satisfying $U(\tilde{a})\iota = a$.

Thus each element of S may be assigned an arbitrary image in M , and that assignment extends uniquely to a module homomorphism. No linearity is required of a : its domain is only a set. The resulting bijection is

$$\mathrm{Hom}_R(F(S), M) \cong \mathrm{Map}(S, U(M)).$$

It is compatible with functions between generating sets and linear maps between target modules. This is the free-module universal property written as a natural bijection of sets.

Existence by finite formal sums

Define

$$R^{(S)} = \{(r_s)_{s \in S} : r_s \in R, r_s = 0 \text{ for all but finitely many } s\},$$

with coordinatewise operations. Let e_s have coefficient 1 at s and zero elsewhere, and put $\iota(s) = e_s$. We write its elements as finite formal sums $\sum_s r_s e_s$, with uniquely specified coefficients.

Given $a : S \rightarrow M$, define

$$\tilde{a} \left(\sum_s r_s e_s \right) = \sum_s r_s a(s).$$

The sum is finite, so the expression is defined, and the module axioms show that it is R -linear. It sends e_s to $a(s)$. Any linear map with those values must have this formula, proving uniqueness. Thus $R^{(S)}$ is free on S .

The family (e_s) is called its *basis*: every element is a unique finite linear combination of these elements. Conversely, a module supplied with such a family has the universal property. For a finite set with t elements, the construction is R^t . For $R \neq 0$, ι is injective; the universal-property definition also makes sense for the zero ring.

Uniqueness: the standard universal-property argument

Suppose (F, ι) and (F', ι') are free on the same set S . The universal property gives unique linear maps

$$u : F \rightarrow F', \quad u\iota = \iota', \quad v : F' \rightarrow F, \quad v\iota' = \iota.$$

Now $(vu)\iota = \iota$, and $\mathrm{id}_F \iota = \iota$ as well. Uniqueness in the universal property of F gives $vu = \mathrm{id}_F$. Similarly, $uv = \mathrm{id}_{F'}$. Therefore u is an isomorphism, with inverse v .

The isomorphism is unique *subject to preserving the specified generators*. The module F by itself can have many automorphisms. The same proof pattern establishes uniqueness for products, coproducts, kernels, and quotients with their structural maps.

Generators, relations, and free resolutions

Let M be any R -module and choose a generating family $(m_s)_{s \in S}$. The free-module property gives a surjection

$$\varepsilon : F_0 = R^{(S)} \twoheadrightarrow M, \quad e_s \mapsto m_s.$$

This is always possible: one may take $S = U(M)$ and send the basis symbol e_m to the corresponding element m . The symbols in F_0 are formal; an equation among their images in M need not be an equation in F_0 .

Set $K_0 = \ker \varepsilon$. Its elements are precisely the relations among the chosen generators. Choose a generating family $(k_t)_{t \in T}$ of K_0 and a free module $F_1 = R^{(T)}$. The map $F_1 \rightarrow K_0$ followed by the inclusion in F_0 gives

$$F_1 \xrightarrow{d_1} F_0 \xrightarrow{\varepsilon} M \longrightarrow 0, \quad d_1(e_t) = k_t.$$

Then $\text{im } d_1 = \ker \varepsilon$, so $M \cong F_0 / \text{im } d_1$. This is a *free presentation*.

The kernel $K_1 = \ker d_1$ records the relations among the chosen relations. Choose a free surjection $F_2 \twoheadrightarrow K_1$ and compose with $K_1 \hookrightarrow F_1$ to get d_2 . Continue inductively, always mapping a free module onto the preceding kernel. This gives an exact sequence

$$\cdots \longrightarrow F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{\varepsilon} M \longrightarrow 0.$$

Exactness is built into the construction: the image of each new map is the kernel that the preceding step produced.

Definition 1.2 (Resolution and free resolution). An *augmented resolution* of M is an exact sequence

$$\cdots \longrightarrow C_2 \longrightarrow C_1 \longrightarrow C_0 \xrightarrow{\varepsilon} M \longrightarrow 0.$$

It is a *free resolution* if every C_i is free. The map ε is its *augmentation*. A finite resolution has length d if $C_d \neq 0$ and $C_i = 0$ for $i > d$; the target M is not counted as a resolution term.

If a kernel becomes zero, all further terms may be zero. Otherwise the construction can continue indefinitely. There is no problem with the existence of generating sets, but the resulting sets may be large. Moreover, the kernels need not themselves be free over a general ring.

Key point. The construction records generators in degree 0, relations in degree 1, relations among relations in degree 2, and so on. The exact sequence, rather than this informal description, is what makes it a resolution.

Three resolutions and what their differences mean

All three examples are over $\mathbb{Z}$. Thus their free terms have a well-defined *rank*; this is the appropriate word here in place of vector-space dimension.

Example 1: one generator and one relation

For $n \geq 2$, multiplication by n is injective and has image $n\mathbb{Z}$. Consequently

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \xrightarrow{\text{mod } n} \mathbb{Z}/n\mathbb{Z} \longrightarrow 0 \tag{A}$$

is a free resolution of length 1. Its degree-0 and degree-1 terms both have rank 1.

Example 2: a larger presentation of the same object

Consider

$$M = \mathbb{Z}^2 / \langle (2, 0), (1, 3) \rangle_{\mathbb{Z}}.$$

The map

$$\varepsilon : \mathbb{Z}^2 \rightarrow \mathbb{Z}/6\mathbb{Z}, \quad (x, y) \mapsto \overline{y - 3x},$$

is surjective and kills both relation vectors. If $y - 3x = 6k$, then

$$(x, y) = -k(2, 0) + (x + 2k)(1, 3),$$

so its kernel is exactly the given relation subgroup. The first isomorphism theorem gives $M \cong \mathbb{Z}/6\mathbb{Z}$.

Use a new copy of $\mathbb{Z}^2$ to label the two relations. Its map to the generator module is

$$d_1(a, b) = (2a + b, 3b), \quad [d_1] = \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}.$$

If $d_1(a, b) = 0$, then $3b = 0$ and $2a + b = 0$, which imply $a = b = 0$. Hence

$$0 \longrightarrow \mathbb{Z}^2 \xrightarrow{\begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}} \mathbb{Z}^2 \xrightarrow{\varepsilon} \mathbb{Z}/6\mathbb{Z} \longrightarrow 0 \quad (\text{B})$$

is a free resolution of length 1.

Compare (B) with (A) at $n = 6$. They resolve the same object and have the same length, but the ranks of their terms are $(2, 2)$ and $(1, 1)$. They cannot be isomorphic term by term. The relation $(1, 3) = 0$ allows one generator to be eliminated in the quotient, but the two displayed relation vectors are linearly independent in the free module. Thus this example has no nonzero degree-2 term.

Example 3: a redundant relation adds a degree

Now present the same cyclic module as

$$\mathbb{Z}/\langle n, 2n \rangle_{\mathbb{Z}} = \mathbb{Z}/n\mathbb{Z} \quad (n \geq 2).$$

There is one generator, but two chosen relations. Thus $F_0 = \mathbb{Z}$, $F_1 = \mathbb{Z}^2$, and

$$d_1(a, b) = na + 2nb = n(a + 2b).$$

The relation vectors are dependent: $-2n + (2n) = 0$. More precisely,

$$\ker d_1 = \mathbb{Z}(-2, 1).$$

The map $d_2 : \mathbb{Z} \rightarrow \mathbb{Z}^2$, $t \mapsto (-2t, t)$, is injective and has exactly that image. We obtain

$$0 \longrightarrow \mathbb{Z} \xrightarrow{t \mapsto (-2t, t)} \mathbb{Z}^2 \xrightarrow{(a, b) \mapsto n(a + 2b)} \mathbb{Z} \xrightarrow{\text{mod } n} \mathbb{Z}/n\mathbb{Z} \longrightarrow 0. \quad (\text{C})$$

This resolution has length 2, while (A) has length 1. The extra degree records a relation among our chosen relations, rather than a new feature of the target module.

These examples ask for a way of comparing resolutions that does not require their terms to be isomorphic or their displayed lengths to agree. The tools developed in the preparatory notes are *chain maps* and *chain homotopies*. We will prove that any two projective resolutions of the same module are chain homotopy equivalent. That result will later make derived-functor calculations independent of the chosen resolution.

A useful consequence: Hom from generators and relations

Evaluation at 1 gives a natural isomorphism of abelian groups

$$\mathrm{Hom}_R(R, N) \cong U_{\mathbf{Ab}}(N), \quad f \mapsto f(1), \quad n \mapsto (r \mapsto rn).$$

Linearity forces $f(r) = rf(1)$, and the displayed inverse is linear. For $u : N \rightarrow N'$, evaluation of $u \circ f$ is $u(f(1))$, which proves naturality. There is no need to put a pointwise R -action on the Hom group when R is noncommutative.

More generally, the universal property of a free module gives

$$\mathrm{Hom}_R(R^{(S)}, N) \cong \prod_{s \in S} U_{\mathbf{Ab}}(N), \quad f \mapsto (f(e_s))_{s \in S}.$$

The right side is a product, not a direct sum: infinitely many generator images may be nonzero, since each input uses only finitely many generators. For instance $(1, 1, \dots)$ determines the map $\bigoplus_{i \geq 1} \mathbb{Z} \rightarrow \mathbb{Z}$, $(a_i) \mapsto \sum_i a_i$.

Proposition 1.3 (The presentation formula). *Suppose M has a free presentation $F_1 \xrightarrow{d} F_0 \xrightarrow{\varepsilon} M \rightarrow 0$. Then, naturally in the target N ,*

$$\mathrm{Hom}_R(M, N) \cong \ker(\mathrm{Hom}_R(F_0, N) \xrightarrow{d^*} \mathrm{Hom}_R(F_1, N)), \quad d^*(h) = h \circ d.$$

If $F_0 = R^{(S)}$ and the chosen relation generators are $d(e_t) = \sum_s r_{ts} e_s$, this is the group of families (n_s) with $\sum_s r_{ts} n_s = 0$ for every t .

Proof. Precomposition with the surjection ε is injective. Its image consists precisely of maps $h : F_0 \rightarrow N$ that kill $\ker \varepsilon = \mathrm{im} d$, by the quotient universal property. Killing the chosen relation generators kills their span, which proves the formula in coordinates. Postcomposition by a map $N \rightarrow N'$ preserves these equations and the factorization, proving naturality. $\square$

Example 1.4 (A cyclic relation selects torsion elements). Apply the formula to $\mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow 0$. Both Hom groups of free terms are A , and precomposition by $\times n$ becomes multiplication by n , since $(f \circ (\times n))(1) = nf(1)$. Consequently

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A[n] = \{a \in A : na = 0\}, \quad f \mapsto f(\bar{1}).$$

Its inverse is $a \mapsto (\bar{t} \mapsto ta)$; the condition $na = 0$ proves well-definedness. The associated exact sequence is $0 \rightarrow A[n] \rightarrow A \xrightarrow{\times n} A$, without a final zero unless multiplication by n is surjective. For $u : A \rightarrow B$, the isomorphisms fit into the commuting square

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) & \xrightarrow{u_*} & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, B) \\ \mathrm{ev}_{\bar{1}} \downarrow \cong & & \cong \downarrow \mathrm{ev}_{\bar{1}} \\ A[n] & \xrightarrow{u[n]} & B[n]. \end{array}$$

Both paths send f to $u(f(\bar{1}))$. For example, a map $\mathbb{Z}/4\mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z}$ sends $\bar{1}$ to either $\bar{0}$ or $\bar{3}$, giving exactly the maps $\bar{a} \mapsto \bar{0}$ and $\bar{a} \mapsto \bar{3a}$. Their Hom group is $\mathbb{Z}/2\mathbb{Z}$.

Example 1.5 (Polynomial and two-generator relations). For $R = k[x]$, evaluation at $1 + (x^2)$ identifies

$$\mathrm{Hom}_R(R/(x^2), N) \cong \{n \in N : x^2 n = 0\}.$$

The inverse sends n to $p + (x^2) \mapsto pn$. Equivalently, precomposing with $R \xrightarrow{\times x^2} R$ becomes multiplication by x^2 on N . For the integer presentation (B), the generator images $u, v \in A$ must satisfy $2u = 0$ and $u + 3v = 0$. These are equivalent to $u = -3v$ and $6v = 0$, so the same method recovers $\mathrm{Hom}_{\mathbb{Z}}(M, A) \cong A[6]$.

Remark (Relations also reveal an extension problem). For $n \geq 2$, the map $n\mathbb{Z} \rightarrow \mathbb{Z}$, $nk \mapsto k$, does not extend to $\mathbb{Z} \rightarrow \mathbb{Z}$: such an extension would require $nf(1) = 1$. Under evaluation at 1, precomposition with $\times n$ is therefore a nonsurjective map $\mathbb{Z} \xrightarrow{\times n} \mathbb{Z}$ on Hom groups. This elementary failure will reappear in the exactness of Hom and in the calculation of Ext.

Key point. A map from a presented module is a choice of generator images satisfying all the relations. Free resolutions extend this description to successive relations among relations.

1.2 Projective modules: definition and characterizations

Projectivity as a lifting property

Suppose that $q : E \twoheadrightarrow B$ is surjective and that $f : P \rightarrow B$ is a module homomorphism. For every $x \in P$, there is an element of E mapping to $f(x)$. Choosing such elements independently, however, need not produce a linear map: their choices must respect all the additive and scalar relations in P .

Definition 1.6 (Projective object and projective module). An object P of a category is *projective* if every morphism $f : P \rightarrow B$ and every epimorphism $q : E \twoheadrightarrow B$ admit a morphism $\tilde{f} : P \rightarrow E$ with $q\tilde{f} = f$. In a module category, epimorphisms are exactly the surjective module homomorphisms. Thus an R -module is projective precisely when every diagram of the following form has a dashed arrow making it commute:

$$\begin{array}{ccc} & P & \\ & \swarrow \tilde{f} & \downarrow f \\ E & \xrightarrow{q} & B. \end{array}$$

The map $\tilde{f}$ is called a *lift* of f through q .

This is an existence condition, not a uniqueness condition. All three arrows must be module homomorphisms. A choice of preimages as a function of sets does not suffice.

Proposition 1.7 (Free modules are projective). *Every free R -module is projective.*

Proof. Let $F = \bigoplus_{s \in S} Re_s$ have basis $(e_s)_{s \in S}$. Given $q : E \twoheadrightarrow B$ and $f : F \rightarrow B$, choose, for each $s \in S$, an element $y_s \in E$ satisfying $q(y_s) = f(e_s)$. For an arbitrary basis set this choice uses the usual axiom of choice.

The universal property of the free module gives a unique linear map $\tilde{f} : F \rightarrow E$ with $\tilde{f}(e_s) = y_s$ for every s . Explicitly,

$$\tilde{f}\left(\sum_{s \in S} r_s e_s\right) = \sum_{s \in S} r_s y_s.$$

Every input involves finitely many nonzero coefficients, so the formula contains only a finite sum. It is additive and R -linear by the module axioms. Furthermore,

$$q\tilde{f}\left(\sum_s r_s e_s\right) = \sum_s r_s q(y_s) = \sum_s r_s f(e_s) = f\left(\sum_s r_s e_s\right).$$

This proves the required commutativity:

$$\begin{array}{ccc}
 & F = \bigoplus_{s \in S} Re_s & \\
 \tilde{f} \swarrow & \downarrow f & \\
 E & \xrightarrow{q} & B.
 \end{array}$$

The universal property gives uniqueness after all the y_s have been specified. It does not make those preimages unique. $\square$

Example 1.8 (Many lifts of the same map). Over $\mathbb{Z}$, let $q : \mathbb{Z}^2 \rightarrow \mathbb{Z}$ be $q(a, b) = a$ and let $f = \text{id}_{\mathbb{Z}}$. For every integer k , the map

$$\tilde{f}_k : \mathbb{Z} \rightarrow \mathbb{Z}^2, \quad \tilde{f}_k(n) = (n, kn)$$

is a lift, since $q\tilde{f}_k(n) = n$. Distinct values of k give distinct lifts. The source $\mathbb{Z}$ is free, but its projectivity does not single out one of them.

Example 1.9 ($\mathbb{Z}/2\mathbb{Z}$ is not projective over $\mathbb{Z}$). Consider the surjection $q : \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$. If $\mathbb{Z}/2\mathbb{Z}$ were projective, the identity map of $\mathbb{Z}/2\mathbb{Z}$ would have a lift s :

$$\begin{array}{ccc}
 & \mathbb{Z}/2\mathbb{Z} & \\
 s \swarrow & \downarrow \text{id} & \\
 \mathbb{Z} & \xrightarrow{q} & \mathbb{Z}/2\mathbb{Z}.
 \end{array}$$

But $2s(\bar{1}) = s(2\bar{1}) = 0$, and the only integer killed by 2 is zero. Hence $s(\bar{1}) = 0$, so $s = 0$ and $qs \neq \text{id}$. The contradiction proves nonprojectivity. Choosing the representatives $0, 1$ gives a set-theoretic section, but it is not additive: the relation $\bar{1} + \bar{1} = \bar{0}$ would be sent to $1 + 1 = 0$.

Over a field k , every vector space, including an infinite-dimensional one, has a basis under the axiom of choice. Therefore every vector space is a free k -module and hence projective. A vector in an infinite-dimensional space is still a *finite* linear combination of basis vectors. These statements do not extend to arbitrary rings.

The ring and its action matter

The abelian group $\mathbb{Z}$ is free, and therefore projective, as a $\mathbb{Z}$ -module. Now consider

$$R = \mathbb{Z}[t]/(t^2 - 1),$$

and make $\mathbb{Z}$ an R -module by letting t act as the identity. Every element of R has a unique expression $a + bt$, $a, b \in \mathbb{Z}$, and its action on an integer m is $(a + bt)m = (a + b)m$. Evaluation at $t = 1$ defines a surjective R -linear map

$$\varepsilon : R \rightarrow \mathbb{Z}, \quad \varepsilon(a + bt) = a + b.$$

Indeed, $\varepsilon(rs) = \varepsilon(r)\varepsilon(s) = r \cdot \varepsilon(s)$ for $r, s \in R$.

If this R -module $\mathbb{Z}$ were projective, ε would have an R -linear section $s : \mathbb{Z} \rightarrow R$. Write $s(1) = a + bt$. Since $t \cdot 1 = 1$ in the source, linearity would imply

$$ts(1) = s(t \cdot 1) = s(1).$$

But $t(a + bt) = b + at$, so uniqueness of the expression in the basis $1, t$ gives $a = b$. It follows that $\varepsilon s(1) = 2a$, which cannot equal 1. Thus $\mathbb{Z}$ is not projective for this R -action.

The same surjection has the additive section $m \mapsto m \cdot 1_R$. That section is $\mathbb{Z}$ -linear but not R -linear. Thus projectivity is a property of a module over its specified ring, not merely of its underlying abelian group.

Projective modules are direct summands of free modules

Theorem 1.10. *An R -module P is projective if and only if it is a direct summand of some free R -module.*

Proof. **Projective implies a direct summand of a free module.** Choose a free surjection $q : F \twoheadrightarrow P$ using a generating set of P . Apply projectivity to id_P :

$$\begin{array}{ccc} & P & \\ & \downarrow \text{id}_P & \\ F & \xrightarrow{q} & P. \end{array}$$

(Note: In the original image, a dashed arrow labeled 's' points from P to F, completing the triangle.)

Then $qs = \text{id}_P$. Lemma P3.3 of the *Preparatory Notes* gives $F = s(P) \oplus \ker q$, with the explicit isomorphism

$$P \oplus \ker q \longrightarrow F, \quad (a, k) \longmapsto s(a) + k.$$

Its inverse is $x \mapsto (q(x), x - s(q(x)))$. Therefore P is a direct summand of this free module.

A direct summand of a free module is projective. Suppose F is free and there are maps $i : P \rightarrow F$, $p : F \rightarrow P$ with $pi = \text{id}_P$. Let $q : E \rightarrow B$ and $f : P \rightarrow B$ be arbitrary. We cannot assume that f already lifts: that is what we must prove. Instead, compose with p to obtain $fp : F \rightarrow B$. Since F is free and hence projective, this new map has a lift $h : F \rightarrow E$ satisfying $qh = fp$:

$$\begin{array}{ccccc} P & \xrightarrow{i} & F & & \\ & \searrow f & \downarrow fp & \swarrow h & \\ & & B & \xleftarrow{q} & E. \end{array}$$

The left triangle commutes because $fpi = f$, and the right triangle commutes by the construction of h . Restrict along i by setting $\tilde{f} = hi : P \rightarrow E$. Then

$$q\tilde{f} = qhi = fpi = f.$$

This is a lift of the original arbitrary map, proving that P is projective. □

The last argument works whenever F is projective, whether or not it is free. Thus every direct summand of a projective module is projective. The forward direction, however, uses a free surjection to supply a specific free module containing P as a summand.

Corollary 1.11 (A projective quotient splits a short exact sequence). *If $0 \rightarrow A \xrightarrow{i} B \xrightarrow{q} P \rightarrow 0$ is exact and P is projective, then the specified sequence splits.*

Proof. Lift id_P along q to get $s : P \rightarrow B$ with $qs = \text{id}_P$. The splitting lemma gives the compatible isomorphism

$$A \oplus P \xrightarrow{\cong} B, \quad (a, p) \longmapsto i(a) + s(p).$$

For completeness, it is surjective because $b - s(q(b)) \in \ker q = i(A)$. If $i(a) + s(p) = 0$, applying q gives $p = 0$, and then injectivity of i gives $a = 0$. □

In fact, a module P is projective exactly when every short exact sequence ending in P splits. One implication is the corollary. Conversely, apply the assumed splitting to $0 \rightarrow \ker q \rightarrow F \xrightarrow{q} P \rightarrow 0$ with F free; the theorem then makes P projective. In Section 3.2, we will give the further characterization in terms of exactness of the functor $\text{Hom}_R(P, -)$.

Example 1.12 (A projective submodule whose specified embedding does not split). The map $\mathbb{Z} \rightarrow 2\mathbb{Z}$, $n \mapsto 2n$, is an isomorphism of $\mathbb{Z}$ -modules. Thus $2\mathbb{Z}$ is free on the generator 2 and is projective. Its usual inclusion $i : 2\mathbb{Z} \hookrightarrow \mathbb{Z}$, however, has no retraction.

Indeed, a homomorphism $r : \mathbb{Z} \rightarrow 2\mathbb{Z}$ has $r(1) = 2k$ for some integer k . It follows that $r(2) = 4k$, whereas $ri = \text{id}_{2\mathbb{Z}}$ would require $r(2) = 2$. Equivalently, the sequence

$$0 \longrightarrow 2\mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

does not split.

There is no contradiction with the direct-summand theorem: $2\mathbb{Z}$ is a summand of *some* free module, for instance itself, but need not be a summand through every specified embedding. Nor does the corollary apply: the projective term here is the *submodule*, while the quotient $\mathbb{Z}/2\mathbb{Z}$ is not projective.

Idempotents, projective modules without bases, and evaluation

An element $e \in R$ is *idempotent* if $e^2 = e$. For an arbitrary, possibly noncommutative ring, the left ideals Re and $R(1 - e)$ give

$${}_R R = Re \oplus R(1 - e).$$

Every r is $re + r(1 - e)$. If x lies in both summands, then $xe = x$ from $x \in Re$, but $xe = 0$ from $x \in R(1 - e)$. Thus the intersection is zero.

The associated projection of the *left* regular module is right multiplication, $\rho_e : R \rightarrow R$, $\rho_e(r) = re$. It is left linear because $\rho_e(ar) = a\rho_e(r)$, and $\rho_e^2 = \rho_e$. Hence Re is projective. For right modules the corresponding statement is $R_R = eR \oplus (1 - e)R$, with projection $r \mapsto er$. Over a noncommutative ring, the side cannot be interchanged silently.

More generally, an *idempotent endomorphism* $T : M \rightarrow M$, meaning an R -linear map with $T^2 = T$, gives a decomposition

$$M = \text{im } T \oplus \ker T.$$

Indeed, $m = T(m) + (m - T(m))$, and the second term lies in $\ker T$. If $x = T(y)$ also belongs to $\ker T$, then $x = T^2(y) = T(x) = 0$. Conversely, projection onto either factor of an internal direct sum is an idempotent endomorphism. This is the module form of an idempotent decomposition.

If e is a *central* idempotent of R , the map $m \mapsto em$ is R -linear on every left module, and the same argument yields

$$M = eM \oplus (1 - e)M.$$

Centrality ensures that these are R -submodules. For the regular module decomposition $R = Re \oplus R(1 - e)$ above, no centrality was needed, because its projection was right multiplication.

Example 1.13 (Projective need not mean free). Let $R = \mathbb{Z}/6\mathbb{Z}$ and put $e = \bar{4}$, $f = \bar{3}$. Computations in this ring give

$$e^2 = e, \quad f^2 = f, \quad e + f = 1, \quad ef = fe = 0.$$

Therefore

$$R = eR \oplus fR, \quad eR = \{\bar{0}, \bar{2}, \bar{4}\}, \quad fR = \{\bar{0}, \bar{3}\}.$$

The projections are $r \mapsto er$ and $r \mapsto fr$; for instance, the addition map $eR \oplus fR \rightarrow R$ has inverse $r \mapsto (er, fr)$. The ring is commutative, so these are decompositions of both left and right regular modules.

Both summands are projective by Theorem 1.10, but neither is free over R . A nonzero finite-rank free module R^m has 6^m elements, whereas these summands have 3 and 2. A free module on an infinite basis has infinitely many distinct basis elements, so it cannot equal either finite module.

These ideals are also submodules of the free module R . Consequently a submodule of a free module need not itself be free. This is one reason that a resolution is constructed by mapping a new free module onto a kernel, rather than assuming that kernel is free.

Proposition 1.14 (Evaluation at an idempotent). *Let $e^2 = e$ in an arbitrary unital ring and let M be a left module. There is a natural isomorphism of abelian groups*

$$\mathrm{Hom}_R(Re, M) \xrightarrow{\cong} eM, \quad \varphi \mapsto \varphi(e),$$

where $eM = \{em : m \in M\} = \{m \in M : em = m\}$.

Proof. For a linear map φ , the identity $e^2 = e$ gives $\varphi(e) = \varphi(e^2) = e\varphi(e)$, so its value lies in eM . The map is determined by this value because $\varphi(re) = r\varphi(e)$.

Conversely, given $m \in eM$, define

$$\varphi_m : Re \rightarrow M, \quad \varphi_m(re) = rm.$$

An element of Re can have several expressions as re , so well-definedness must be checked. If $re = r'e$, then

$$(r - r')m = (r - r')em = 0,$$

using $em = m$. Hence the formula is independent of the expression. It is additive and left linear: $\varphi_m(a(re)) = (ar)m = a\varphi_m(re)$. Moreover, $\varphi_m(e) = em = m$, while $\varphi_{\varphi(e)}(re) = r\varphi(e) = \varphi(re)$. The two constructions are inverse and preserve addition.

If $u : M \rightarrow N$ is linear, then $u(em) = eu(m)$, so u carries eM into eN . The equation $(u\varphi)(e) = u(\varphi(e))$ proves naturality. $\square$

For general R , the subgroup eM need not be an R -submodule: although $em = m$, it need not follow that $e(rm) = rm$. This is why the proposition asserts an isomorphism of abelian groups. In the commutative example $R = \mathbb{Z}/6\mathbb{Z}$, one has $Re = eR$ and eM is an R -submodule. The proposition then reads $\mathrm{Hom}_R(eR, M) \cong eM$, and is also R -linear for the usual pointwise action on Hom . This is the idempotent version of evaluating $\mathrm{Hom}_R(R, M)$ at 1.

When are submodules and projective modules free?

The preceding examples separate three conditions: being free, being projective, and being a submodule of a free module. Additional hypotheses on the ring can bring these conditions closer together. For the first results below, assume that R is a *commutative integral domain*: $1 \neq 0$, and a product of two nonzero elements is nonzero. A *principal ideal domain*, or *PID*, is such a ring in which every ideal is generated by one element. The examples $\mathbb{Z}$ and $k[x]$, for a field k , will be particularly useful.

Theorem 1.15 (Submodules of free modules over a PID). *If R is a PID, every submodule of a free R -module is free. In particular, a submodule of R^n has a basis of at most n elements. The assertion also holds for arbitrary infinite bases, under the usual axiom of choice.*

Proof for a finite basis. We induct on n . For $n = 0$ the only submodule is zero, with its empty basis. Let $N \subseteq R^n$, and let $\pi : R^n \rightarrow R$ be projection onto the last coordinate. The image $J = \pi(N)$ is an ideal, so $J = aR$ for some $a \in R$. The kernel of $\pi|_N$ is

$$K = N \cap (R^{n-1} \oplus 0).$$

By induction K is free on at most $n - 1$ generators. If $a = 0$, then $N = K$, and we are done.

If $a \neq 0$, choose $v \in N$ with $\pi(v) = a$. Since R is a domain, aR is free on a . The map $aR \rightarrow N$, $ra \mapsto rv$, is well defined and is a section of $\pi|_N$. Equivalently, every $w \in N$ has $\pi(w) = ra$ for a unique r , and $w - rv \in K$. Also $rv \in K$ implies $ra = 0$, hence $r = 0$. Therefore

$$N = K \oplus Rv.$$

Appending v to a basis of K gives a basis of N with at most n elements, completing the induction. $\square$

Why the infinite case also holds. Well-order a basis $(e_\alpha)_{\alpha < \kappa}$ of the ambient free module F , and put

$$F_\alpha = \bigoplus_{\beta < \alpha} Re_\beta, \quad N_\alpha = N \cap F_\alpha.$$

The coefficient of e_α identifies $N_{\alpha+1}/N_\alpha$ with an ideal $J_\alpha \subseteq R$. If this ideal is zero, no basis element is added. Otherwise choose a generator $a_\alpha \neq 0$ of it and lift that generator to $v_\alpha \in N_{\alpha+1}$. The same argument as above gives

$$N_{\alpha+1} = N_\alpha \oplus Rv_\alpha.$$

At a limit ordinal λ , finite support gives $N_\lambda = \bigcup_{\alpha < \lambda} N_\alpha$; taking the union of the previously chosen bases gives a basis there. Transfinite induction therefore produces a basis of N . Every linear combination used in this argument is finite. The axiom of choice supplies the well-order and the choices of lifts.

Corollary 1.16. *Every projective module over a PID is free, including projective modules that are not finitely generated.*

Proof. A projective module is isomorphic to a direct summand, hence a submodule, of a free module. Apply Theorem 1.15. $\square$

Among commutative domains the submodule theorem actually *characterizes* PIDs. Suppose every submodule of every free R -module is free. Each ideal $J \subseteq R$ is then free. A nonzero ideal cannot have two distinct basis elements u, v : commutativity would give the nontrivial relation

$$vu - uv = 0,$$

whose coefficients $v, -u \in R$ are nonzero. Thus a nonzero ideal has a one-element basis and is principal; the zero ideal is principal as well. Consequently

R a commutative domain: every submodule of a free R -module is free $\iff R$ is a PID.

The commutative-domain hypothesis belongs to this statement; it is not a characterization of arbitrary unital rings.

Torsion-free does not by itself mean free

Over a commutative domain, a module M is *torsion-free* if $rm = 0$ with $r \neq 0$ forces $m = 0$. Every free module, and every submodule of a free module, is torsion-free. Over a PID there is a useful converse with a finiteness hypothesis: every *finitely generated* torsion-free module is free. This follows, for example, from the structure theorem for finitely generated modules over a PID: the cyclic torsion summands must all vanish.¹

The finite-generation qualification cannot simply be removed. The $\mathbb{Z}$ -module $\mathbb{Q}$ is torsion-free, and every rational number is twice another rational number. In contrast, in a nonzero free $\mathbb{Z}$ -module a basis element cannot be twice another element: comparison of its coordinate would require $1 = 2a$ with $a \in \mathbb{Z}$. Thus $\mathbb{Q}$ is not free over $\mathbb{Z}$, despite $\mathbb{Z}$ being a PID.

The PID qualification matters too. Over the domain $R = k[x, y]$, the ideal $J = (x, y)$ is a submodule of the free module R and is torsion-free, but it is not free. If it were free, the argument for ideals above would force it to have one generator, say $J = (f)$. Then f would divide both x and y . Since x is irreducible and does not divide y , their common divisors are units. This would give $J = R$, contrary to the fact that every element of J vanishes at $(0, 0)$.

Finitely generated projectives over a local ring

A nonzero commutative ring R is *local* if it has a unique maximal ideal $\mathfrak{m}$. Elements outside $\mathfrak{m}$ are units, and $\kappa = R/\mathfrak{m}$ is its *residue field*. Locality gives another important freeness criterion, even when the ring has zero divisors.

We use the following finite-module form of *Nakayama's lemma*: if a finitely generated module L over a local ring satisfies $L = \mathfrak{m}L$, then $L = 0$. Here is a short proof. If $L \neq 0$, choose a generating set $x_1, \dots, x_t$ of minimal positive size. The equation $L = \mathfrak{m}L$ expresses $x_t = \sum_i a_i x_i$ with $a_i \in \mathfrak{m}$. Since $1 - a_t$ is a unit, this expresses x_t in terms of the first $t - 1$ generators, a contradiction. It also follows that lifts of generators of $L/\mathfrak{m}L$ generate L : apply the lemma to the quotient by their span.²

Proposition 1.17. *Every finitely generated projective module over a commutative local ring is free of finite rank.*

Proof. Let P be such a module. Choose $p_1, \dots, p_r \in P$ whose classes form a basis of the finite-dimensional vector space $P/\mathfrak{m}P$. Nakayama's lemma makes the map $q : R^r \rightarrow P$, $e_i \mapsto p_i$, surjective. Projectivity splits it, giving $R^r \cong P \oplus K$, where $K = \ker q$ is finitely generated: project the finitely many standard generators of R^r onto this summand. Taking quotients by $\mathfrak{m}$ yields

$$\kappa^r \cong (P/\mathfrak{m}P) \oplus (K/\mathfrak{m}K).$$

The first summand already has dimension r , so $K/\mathfrak{m}K = 0$. Nakayama's lemma gives $K = 0$, and therefore q is an isomorphism. $\square$

The finite-generation assumption is used in this proof when applying Nakayama's lemma.³

Locality alone does not make every submodule of a free module free. For $R = k[\epsilon]/(\epsilon^2)$, the ideal (ϵ) is the unique maximal ideal: $a + b\epsilon$ is a unit exactly when $a \neq 0$, with inverse $a^{-1} - ba^{-2}\epsilon$. The nonzero submodule $(\epsilon) \subset R$ is not free. Indeed, ϵ annihilates all of (ϵ) , whereas it does

¹For the finite-basis submodule theorem and the structure theorem, see K. Conrad, *Modules over a PID*.

²See the [Stacks Project](#), Nakayama's lemma, Tag 00DV.

³For finite projective modules, see the [Stacks Project](#), Section 10.78. The stronger theorem that arbitrary projective modules over a local ring are free is recorded in Tag 058Z; its proof is beyond the argument given here.

not annihilate a basis vector in any nonzero free R -module. This finitely generated ideal is consequently not projective either, by Proposition 1.17.

1.3 Projective resolutions and their augmentations

Projective resolutions: existence, augmentation, and purpose

Definition 1.18 (Projective resolution). A *projective resolution* of an R -module M consists of a sequence $P_\bullet$ of projective modules P_n , $n \geq 0$, with differentials $d_n : P_n \rightarrow P_{n-1}$ for $n \geq 1$, together with an *augmentation* $\varepsilon : P_0 \rightarrow M$, such that

$$\cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \longrightarrow 0$$

is exact. We may write this data as $(P_\bullet, \varepsilon)$ or $P_\bullet \xrightarrow{\varepsilon} M$. The target M is not required to be projective. If every P_n is free, this is a *free resolution*.

Concretely, the required exactness says

$$\varepsilon \text{ is surjective,} \quad \text{im } d_1 = \ker \varepsilon, \quad \text{im } d_{n+1} = \ker d_n \quad (n \geq 1).$$

In particular, $\varepsilon d_1 = 0$ and $d_n d_{n+1} = 0$. The latter equations are the chain-complex conditions defined in Section P3.2 of the *Preparatory Notes*.

The augmented sequence and its underlying complex

There are two useful objects here, with different degree conventions. If we include M in degree -1 and let the differential out of P_0 be ε , the resulting *augmented complex* $\tilde{P}_\bullet$ is exact in every degree:

$$\cdots \longrightarrow \underbrace{P_1}_{\text{degree } 1} \xrightarrow{d_1} \underbrace{P_0}_{\text{degree } 0} \xrightarrow{\varepsilon} \underbrace{M}_{\text{degree } -1} \longrightarrow 0.$$

The term in degree -1 need not be projective; projectivity is required of the P_n in nonnegative degrees.

The notation $P_\bullet$ by itself will instead mean the *unaugmented*, nonnegative complex obtained by removing M :

$$\cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \longrightarrow 0.$$

Here we set $P_{-1} = 0$ and $d_0 = 0$. The homology is the quotient of the kernel of a differential by the image of the preceding one. Consequently

$$H_0(P_\bullet) = P_0 / \text{im } d_1 \xrightarrow{\cong} M, \quad [p] \longmapsto \varepsilon(p),$$

and $H_n(P_\bullet) = 0$ for $n > 0$. The displayed map is well defined because $\varepsilon d_1 = 0$, injective because $\ker \varepsilon = \text{im } d_1$, and surjective because ε is. Thus the target survives as the zeroth homology, and the augmentation specifies its identification with that homology. It is only the *augmented* complex that is exact in every degree; the *unaugmented* complex has nonzero H_0 whenever $M \neq 0$.

The word *resolution* suggests unpacking the module into successive layers. In a free resolution, degree zero supplies formal generators, degree one supplies labels for relations, and degree two supplies relations among those relations. Further degrees continue the process. The maps keep track of how these layers fit together, and passing to zeroth homology reassembles the original module. A projective resolution retains this exactness and lifting structure without requiring a chosen basis for each layer.

Example 1.19 (Projective terms do not alone make a resolution). Place $C_1 = C_0 = \mathbb{Z}$ in degrees 1, 0, with $d_1 = 0$ and all other terms zero. Every term is free and successive differentials compose to zero, but $H_1(C_\bullet) = \mathbb{Z}$. No augmentation from C_0 can correct this failure of exactness at C_1 . Therefore this complex is not a projective resolution of a module concentrated in degree zero.

Existence and the extra flexibility of projective terms

Every module has a projective resolution: the free-resolution construction of Section 1.1 already provides one, since every free module is projective. In particular, module categories have *enough projectives*: every module is a quotient of a projective module.

The converse implication between types of resolutions fails: a projective resolution need not be a free resolution. Take $R = \mathbb{Z}/6\mathbb{Z}$, $e = \bar{4}$, and $P = eR$ as above. The exact sequence

$$0 \longrightarrow \underbrace{P}_{P_0} \xrightarrow{\text{id}_P} \underbrace{P}_{\text{target}} \longrightarrow 0$$

is a projective resolution, with $P_i = 0$ for $i > 0$. Its term P_0 is projective but not free over R , so this particular resolution is not free. Its unaugmented complex has the single nonzero term P in degree zero and hence has $H_0 = P$.

We can therefore choose projective terms without choosing bases for them. The lifting property will be the essential ingredient for comparing resolutions. The augmentation need not split, and the kernels of the differentials need not be projective. The examples that follow make these distinctions visible.

Checking resolutions and their augmentations in examples

Example 1.20 (The short resolution of $\mathbb{Z}/n\mathbb{Z}$). For $n \geq 2$, the sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \xrightarrow{\text{mod } n} \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

is exact at every term: multiplication by n is injective because $na = 0$ in $\mathbb{Z}$ implies $a = 0$; its image is $n\mathbb{Z}$, which is the kernel of the quotient map; and the quotient map is surjective. Both resolution terms are free, with $P_1 = P_0 = \mathbb{Z}$ and $P_i = 0$ for $i \geq 2$.

For the unaugmented complex $0 \rightarrow \mathbb{Z} \xrightarrow{n} \mathbb{Z} \rightarrow 0$,

$$H_1 = \ker(\times n) = 0, \quad H_0 = \mathbb{Z}/n\mathbb{Z}.$$

In particular, at $n = 6$ these values are 0 and $\mathbb{Z}/6\mathbb{Z}$. Adding the quotient map fills the zeroth-degree gap and gives the exact augmented sequence. Removing its target restores precisely that quotient as H_0 .

The augmentation is nonetheless not split. If $s : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}$ were a section, then $ns(\bar{1}) = s(n\bar{1}) = 0$ would force $s(\bar{1}) = 0$. Hence the composite of s with reduction modulo n could not be the identity. Exactness asserts that the quotient is recovered; it does not supply a linear choice of representatives for its elements.

Example 1.21 (A periodic resolution over the dual numbers). Let k be a field, $R = k[\epsilon]/(\epsilon^2)$, and $M = k = R/(\epsilon)$. Write $q : R \rightarrow k$, $q(a + b\epsilon) = a$, for the quotient map. Every element has a unique expression $a + b\epsilon$, and

$$\epsilon(a + b\epsilon) = a\epsilon.$$

It follows that

$$\ker(\epsilon \cdot) = (\epsilon) = \text{im}(\epsilon \cdot), \quad \ker q = (\epsilon).$$

Thus

$$\cdots \xrightarrow{\epsilon} R \xrightarrow{\epsilon} R \xrightarrow{\epsilon} R \xrightarrow{q} k \longrightarrow 0$$

is a free resolution, with $P_n = R$ in every nonnegative degree and d_n multiplication by ϵ for $n \geq 1$. The equation $d_n d_{n+1} = 0$ follows from $\epsilon^2 = 0$; the stronger equality of image and kernel follows from the explicit calculation above. Exactness at P_0 uses $\ker q = (\epsilon)$, and exactness at k uses surjectivity of q . Consequently the unaugmented complex has $H_0 \cong k$ and $H_n = 0$ for $n > 0$.

None of the positive-degree differentials is injective: each has the nonzero kernel (ϵ) . Exactness holds because the preceding differential maps onto precisely that kernel. We have exhibited an infinite periodic resolution. This calculation alone does not prove that no finite resolution can exist; such a minimal-length claim requires an additional argument.

Over the different ring $S = k[x]$, the same field k , now regarded as $S/(x)$, has the short free resolution

$$0 \longrightarrow S \xrightarrow{x} S \xrightarrow{q_0} k \longrightarrow 0, \quad q_0(f) = f(0).$$

Indeed, $xf = 0$ implies $f = 0$ because S is a domain; the image of multiplication by x is (x) ; and a polynomial vanishes at 0 exactly when it belongs to (x) . Finally q_0 is surjective because every scalar is a constant polynomial. Hence $H_1 = 0$ and $H_0 = S/(x) \cong k$ after removing the augmentation target. In the dual-number example multiplication by ϵ has a nonzero kernel that the next term must cover; multiplication by x has zero kernel, so this construction terminates. The coefficient ring and its action control this difference.

Example 1.22 (A cubic nilpotent requires alternating differentials). Let $R = k[\epsilon]/(\epsilon^3)$ and $M = k = R/(\epsilon)$. If we use multiplication by ϵ at every step, two adjacent differentials compose to multiplication by ϵ^2 . This map is nonzero, since it sends 1 to $\epsilon^2 \neq 0$. Therefore the proposed sequence is not even a chain complex.

Instead, set $P_n = R$ for $n \geq 0$ and

$$d_n = \begin{cases} \epsilon \cdot, & n \text{ odd,} \\ \epsilon^2 \cdot, & n \text{ even,} \end{cases} \quad (n \geq 1),$$

with augmentation $q(a + b\epsilon + c\epsilon^2) = a$. The proposed resolution is

$$\cdots \xrightarrow{\epsilon} R \xrightarrow{\epsilon^2} R \xrightarrow{\epsilon} R \xrightarrow{\epsilon^2} R \xrightarrow{\epsilon} R \xrightarrow{q} k \longrightarrow 0.$$

Successive differentials compose to multiplication by $\epsilon^3 = 0$. To check exactness, compute

$$\epsilon(a + b\epsilon + c\epsilon^2) = a\epsilon + b\epsilon^2, \quad \epsilon^2(a + b\epsilon + c\epsilon^2) = a\epsilon^2.$$

Uniqueness of the coefficients yields

$$\begin{aligned} \ker(\epsilon \cdot) &= (\epsilon^2) = \text{im}(\epsilon^2 \cdot), \\ \ker(\epsilon^2 \cdot) &= (\epsilon) = \text{im}(\epsilon \cdot). \end{aligned}$$

For odd n , the first equality gives $\ker d_n = \text{im } d_{n+1}$; for even $n > 0$, the second does. At degree zero, $\ker q = (\epsilon) = \text{im } d_1$, and q is surjective. We have therefore checked every position in the augmented sequence. It is a free resolution with period two in its differentials, and its unaugmented homology is k in degree zero and zero in every positive degree. As in the preceding example, its being displayed as infinite does not establish minimal length.

Key point. Free modules provide existence. Projective modules retain the lifting property needed for comparison. Resolutions combine those lifts with exactness to control the choices made in presenting a module.

Using the chain maps and homotopies established in the preparatory notes, we now compare different resolutions of the same target while keeping track of their augmentations.

1.4 Comparison and uniqueness up to chain homotopy

The resolutions above are visibly not unique. The correct uniqueness statement concerns their homotopy type and the maps they induce, rather than their chosen generators or termwise ranks.

Maps compatible with augmentations

For the resolutions already defined, the unaugmented complex $P_\bullet$ has $H_0(P_\bullet) \cong A$ and zero positive homology. Its differential d_0 is zero; the augmentation $\varepsilon_P : P_0 \rightarrow A$ remains separate. A chain map $f : P_\bullet \rightarrow Q_\bullet$ between resolutions of A and B lifts a map $u : A \rightarrow B$ if, in addition, $\varepsilon_Q f_0 = u\varepsilon_P$. Thus the entire augmented diagram must commute:

$$\begin{array}{ccccccc} \cdots & \rightarrow & P_2 & \xrightarrow{d_2^P} & P_1 & \xrightarrow{d_1^P} & P_0 \xrightarrow{\varepsilon_P} A \rightarrow 0 \\ & & \downarrow f_2 & & \downarrow f_1 & & \downarrow f_0 & \downarrow u \\ \cdots & \rightarrow & Q_2 & \xrightarrow{d_2^Q} & Q_1 & \xrightarrow{d_1^Q} & Q_0 \xrightarrow{\varepsilon_Q} B \rightarrow 0. \end{array}$$

Under the identifications of degree-zero homology with A and B , the induced map $H_0(f)$ is precisely u .

The comparison theorem

Resolutions have a second, different reason that degree-zero homology can control their maps: projectivity and exactness together solve the required lifting problems.

Theorem 1.23 (Comparison theorem). *Let $P_\bullet \rightarrow A$ and $Q_\bullet \rightarrow B$ be projective resolutions. Every module homomorphism $u : A \rightarrow B$ lifts to an augmentation-compatible chain map $f : P_\bullet \rightarrow Q_\bullet$. Any two lifts of the same u are chain homotopic.*

Proof. **Existence in degree zero.** Projectivity of P_0 supplies f_0 in

$$\begin{array}{ccc} & P_0 & \\ f_0 \swarrow & \downarrow u\varepsilon_P & \\ Q_0 & \xrightarrow{\varepsilon_Q} & B. \end{array}$$

Thus $\varepsilon_Q f_0 = u\varepsilon_P$, as required.

Degree one. The map $a_1 = f_0 d_1^P : P_1 \rightarrow Q_0$ satisfies $\varepsilon_Q a_1 = u\varepsilon_P d_1^P = 0$. Hence it factors through $K_0^Q = \ker \varepsilon_Q$. Exactness provides a surjection $\bar{d}_1^Q : Q_1 \twoheadrightarrow K_0^Q$. Projectivity of P_1 lifts this factorization to f_1 , and composing with $K_0^Q \hookrightarrow Q_0$ gives $d_1^Q f_1 = f_0 d_1^P$.

The inductive step. Suppose $f_0, \dots, f_{n-1}$ are constructed with the required equations, where $n \geq 2$. For $a_n = f_{n-1} d_n^P$, one has

$$d_{n-1}^Q a_n = d_{n-1}^Q f_{n-1} d_n^P = f_{n-2} d_{n-1}^P d_n^P = 0.$$

Thus a_n factors through $K_{n-1}^Q = \ker d_{n-1}^Q$. As in degree one, exactness and projectivity give the lift:

$$\begin{array}{ccccc} & P_n & & & \\ f_n \swarrow & \downarrow \bar{a}_n & & & \\ Q_n & \xrightarrow{\bar{d}_n^Q} & K_{n-1}^Q & \xrightarrow{j_{n-1}} & Q_{n-1}. \end{array}$$

Here $j_{n-1}\bar{a}_n = a_n$ and $j_{n-1}\bar{d}_n^Q = d_n^Q$. Therefore $d_n^Q f_n = f_{n-1}d_n^P$, completing the construction.

Homotopy in degree zero. Let f, g both lift u . Then $\varepsilon_Q(f_0 - g_0) = 0$, so $f_0 - g_0$ takes values in $\ker \varepsilon_Q$. Lift it through $Q_1 \twoheadrightarrow \ker \varepsilon_Q$ using projectivity of P_0 . This gives $h_0 : P_0 \rightarrow Q_1$ satisfying $f_0 - g_0 = d_1^Q h_0$, with $h_{-1} = 0$.

The first residual difference. Put $r_1 = f_1 - g_1 - h_0 d_1^P$. Then

$$d_1^Q r_1 = (f_0 - g_0)d_1^P - d_1^Q h_0 d_1^P = 0.$$

Thus r_1 takes values in $\ker d_1^Q$ and lifts through $Q_2 \twoheadrightarrow \ker d_1^Q$ to h_1 . This establishes $f_1 - g_1 = d_2^Q h_1 + h_0 d_1^P$.

The general homotopy step. For $n \geq 2$, suppose $h_0, \dots, h_{n-1}$ have established the equations through degree $n-1$. Put $r_n = f_n - g_n - h_{n-1}d_n^P$. Then

$$\begin{aligned} d_n^Q r_n &= (f_{n-1} - g_{n-1})d_n^P - d_n^Q h_{n-1}d_n^P \\ &= h_{n-2}d_{n-1}^P d_n^P = 0. \end{aligned}$$

The same kernel-lifting step now supplies h_n :

$$\begin{array}{ccc} & P_n & \\ & \downarrow \bar{r}_n & \\ Q_{n+1} & \xrightarrow[\bar{d}_{n+1}^Q]{} & \ker d_n^Q. \end{array}$$

(Note: A dashed arrow labeled h_n points from P_n to Q_{n+1} in the original diagram.)

Composing with the kernel inclusion gives $d_{n+1}^Q h_n = r_n$, exactly the required equation in degree n . $\square$

Key point. Exactness of the target supplies surjections onto kernels. Projectivity of the source lifts maps through those surjections. The same mechanism first constructs a comparison map and then absorbs the difference between two choices into a homotopy.

The proof does not need the terms of the target resolution to be projective. Both resolutions are assumed projective so that the theorem may also be applied in the other direction.

Corollary 1.24 (Homology detects maps between projective resolutions). *For projective resolutions $P \rightarrow A$ and $Q \rightarrow B$, augmentation induces a bijection*

$$\mathrm{Hom}_{K_{\geq 0}(R\text{-Mod})}(P, Q) \cong \mathrm{Hom}_R(A, B).$$

In particular, chain maps $f, g : P \rightarrow Q$ are homotopic if and only if their induced maps $H_0(P) \rightarrow H_0(Q)$ agree.

Proof. For any chain map f , the composite $\varepsilon_Q f_0$ kills $\mathrm{im} d_1^P$, because $\varepsilon_Q f_0 d_1^P = \varepsilon_Q d_1^Q f_1 = 0$. It therefore factors uniquely through $\varepsilon_P : P_0 \rightarrow A$, giving a map $u : A \rightarrow B$. This is $H_0(f)$ under the augmentation identifications. Existence in the comparison theorem gives every u , and homotopy uniqueness identifies precisely the maps producing that u . The converse direction also follows from homotopy invariance. $\square$

This is a statement about resolutions, not merely about projective terms. In Example P3.16 of the *Preparatory Notes*, the target has nonzero homology in degree one, so it is not a resolution of a module in degree zero and the corollary does not apply.

Independence of the resolution and explicit comparisons

Let $P_\bullet \rightarrow A$ and $Q_\bullet \rightarrow A$ be projective resolutions. Lift id_A in both directions: $f : P_\bullet \rightarrow Q_\bullet$ and $g : Q_\bullet \rightarrow P_\bullet$. Their degree-zero maps fit into

$$\begin{array}{ccccc} P_0 & \xrightarrow{f_0} & Q_0 & \xrightarrow{g_0} & P_0 \\ \varepsilon_P \downarrow & & \varepsilon_Q \downarrow & & \downarrow \varepsilon_P \\ A & \xrightarrow{\text{id}_A} & A & \xrightarrow{\text{id}_A} & A \end{array}$$

In particular,

$$\varepsilon_P(gf)_0 = \varepsilon_P g_0 f_0 = \varepsilon_Q f_0 = \varepsilon_P.$$

Thus gf really is a lift of id_A , as is id_P . Similarly, $\varepsilon_Q(fg)_0 = \varepsilon_P g_0 = \varepsilon_Q$. Applying homotopy uniqueness gives

$$gf \simeq \text{id}_P, \quad fg \simeq \text{id}_Q.$$

Projective resolutions of the same module are therefore chain homotopy equivalent, even when their terms have different ranks or their lengths are different. For a calculation, any resolution whose projectivity and augmented exactness have been checked may be used; one can choose whichever is most convenient for the problem. This conclusion neither selects a canonical resolution nor asserts the existence of a preferred minimal or shortest one.

A complete comparison of two length-one resolutions

Let $P_1 = P_0 = \mathbb{Z}$, $d_1^P = 6$, and $\varepsilon_P(z) = \bar{z} \in \mathbb{Z}/6\mathbb{Z}$. For a second resolution put $Q_1 = Q_0 = \mathbb{Z}^2$ and

$$d_1^Q(u, v) = (u, -u + 6v), \quad \varepsilon_Q(a, b) = \overline{a + b}.$$

All other terms are zero. The map ε_Q is surjective, since $\varepsilon_Q(a, 0) = \bar{a}$. If $d_1^Q(u, v) = 0$, then $u = 0$ and $6v = 0$, so $v = 0$; thus d_1^Q is injective. Its image equals $\ker \varepsilon_Q$: its outputs have sum $6v$; conversely, if $a + b = 6v$, then $(a, b) = d_1^Q(a, v)$. This proves exactness of the augmented sequence.

Define maps in each degree by

	degree 0	degree 1
$f : P \rightarrow Q$	$f_0(z) = (z, 0)$	$f_1(z) = (6z, z)$
$g : Q \rightarrow P$	$g_0(a, b) = a + b$	$g_1(u, v) = v$.

They commute with the differentials because

$$d_1^Q f_1(z) = (6z, 0) = f_0(6z), \quad g_0 d_1^Q(u, v) = 6v = 6g_1(u, v).$$

They also lift $\text{id}_{\mathbb{Z}/6\mathbb{Z}}$: $\varepsilon_Q f_0(z) = \bar{z} = \varepsilon_P(z)$ and $\varepsilon_P g_0(a, b) = \overline{a + b} = \varepsilon_Q(a, b)$. For example, all squares in the augmented diagram for f commute:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\times 6} & \mathbb{Z} & \xrightarrow{\varepsilon_P} & \mathbb{Z}/6\mathbb{Z} \longrightarrow 0 \\ & & \downarrow f_1 & & \downarrow f_0 & & \parallel \\ 0 & \longrightarrow & \mathbb{Z}^2 & \xrightarrow{d_1^Q} & \mathbb{Z}^2 & \xrightarrow{\varepsilon_Q} & \mathbb{Z}/6\mathbb{Z} \longrightarrow 0. \end{array}$$

The composite gf is exactly the identity in both degrees: $g_0f_0(z) = z$ and $g_1f_1(z) = z$. The other composite is

$$(fg)_0(a, b) = (a + b, 0), \quad (fg)_1(u, v) = (6v, v).$$

Define $h_0 : Q_0 \rightarrow Q_1$ by $h_0(a, b) = (-b, 0)$ and set all other h_j equal to zero. Direct calculation gives

$$\begin{aligned} d_1^Q h_0(a, b) &= (-b, b) = (\text{id}_Q - fg)_0(a, b), \\ h_0 d_1^Q(u, v) &= (u - 6v, 0) = (\text{id}_Q - fg)_1(u, v). \end{aligned}$$

These are the complete degree-zero and degree-one homotopy equations. Consequently $fg \simeq \text{id}_Q$, as the comparison theorem predicted. This computation exhibits every comparison map and homotopy without requiring termwise isomorphisms.

A redundant relation produces a contractible summand

For the redundant-relation resolution in Section 1.1, write $T_2 = \mathbb{Z}$, $T_1 = \mathbb{Z}^2$, $T_0 = \mathbb{Z}$ and

$$d_1^T(x, y) = nx + 2ny, \quad d_2^T(z) = (-2z, z) \quad (n \geq 2).$$

The vectors $a = (1, 0)$ and $b = (-2, 1)$ form a basis of T_1 , since $(x, y) = (x + 2y)a + yb$. Moreover $d_1^T(a) = n$, $d_1^T(b) = 0$, and $d_2^T(1) = b$. Thus this complex is the direct sum of the short resolution $S_1 = \mathbb{Z}a \xrightarrow{n} S_0 = \mathbb{Z}$ and a disk $\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}b$ in degrees 2, 1.

Explicit comparison maps are $i : S \rightarrow T$ and $p : T \rightarrow S$, with $i_1(z) = (z, 0)$, $p_1(x, y) = x + 2y$, and $i_0 = p_0 = \text{id}_{\mathbb{Z}}$; the degree-two maps are zero. The equations

$$d_1^T i_1(z) = nz, \quad p_0 d_1^T(x, y) = n(x + 2y) = d_1^S p_1(x, y), \quad p_1 d_2^T(z) = 0$$

verify the chain map conditions; all remaining equations have zero source or target. Both preserve the quotient augmentation to $\mathbb{Z}/n\mathbb{Z}$, and $pi = \text{id}_S$. Taking $h_1(x, y) = y : T_1 \rightarrow T_2$ and $h_j = 0$ otherwise gives

$$(\text{id}_T - ip)_0 = 0, \quad d_2^T h_1(x, y) = (-2y, y), \quad h_1 d_2^T(z) = z.$$

These are exactly the homotopy equations in degrees 0, 1, 2. The additional relation and its relation among relations form an explicitly removable contractible summand.

Why equal homology groups alone would not be enough

Knowing only that $H_0(P) \cong A \cong H_0(Q)$ and that all their higher homology groups vanish provides a list of isomorphism classes. It does not provide maps between the complexes or equations comparing their composites. The comparison theorem supplies both: actual chain maps lifting id_A and actual homotopies to the identities. For a map between different resolved modules, homotopy uniqueness also controls the ambiguity in its lift.

The distinction matters when an operation fails to preserve exactness. For example, applying $\text{Hom}_{\mathbb{Z}}(-, \mathbb{Z})$ degree by degree to the acyclic complex in Example P3.19 of the *Preparatory Notes* reverses its arrows and gives groups $0, \mathbb{Z}, \mathbb{Z}$ in cochain degrees 0, 1, 2, with the last differential multiplication by 2. Its degree-two cohomology is $\mathbb{Z}/2\mathbb{Z}$, whereas the zero complex still gives zero. Thus an additive operation need not preserve an isomorphism on homology coming from an arbitrary quasi-isomorphism.

Homotopy equivalence provides stronger comparison data: its equations use sums, differences, compositions, and identities. An additive functor preserves those equations even when it destroys exactness. Section P3.3 of the *Preparatory Notes* established the precise functorial statement,

including the reversal to cochain complexes for contravariant functors. It is this stronger comparison, rather than the bare equality of the original homology groups, that will make the later constructions independent of resolutions.

2 Injective Modules and Injective Resolutions

Projective modules solve lifting problems through surjections. We now reverse the direction of the mapping problem: a map is already defined on a submodule, and we want to extend it to the whole module. This leads to injective modules and to resolutions formed by successive embeddings. Their existence requires a different construction from that of free modules; their comparison uses the cochain maps and homotopies introduced earlier. Throughout this chapter, R is an associative unital ring and all modules are unital left R -modules unless another ring is specified.

2.1 Injective modules: definition and characterizations

Definition 2.1 (Injective module). A module I is *injective* if, for every pair of modules X, Y , every injective R -linear map $u : X \hookrightarrow Y$, and every R -linear map $f : X \rightarrow I$, there exists an R -linear map $\tilde{f} : Y \rightarrow I$ with $\tilde{f}u = f$:

$$\begin{array}{ccc} X & \xhookrightarrow{u} & Y \\ f \downarrow & \swarrow \tilde{f} & \\ I & & \end{array}$$

The solid arrows are given, and the dashed arrow is the required extension. Identifying X with $u(X)$ gives the equivalent statement that every map from a submodule into I extends to the whole module.

The quantifiers range over *all* injections and *all* maps into I . An injective *map* is a monomorphism; an injective *module* has this extension property as an object of the module category. Having an identity injection does not make every module injective.

The distinguished module is the common target in this diagram. For a projective module it is the common source in a lifting diagram. Reversing arrows interchanges the two definitions, and both ask for existence rather than uniqueness.

Example 2.2 (Extensions need not be unique). Let k be a field, $X = k(1, 0) \subseteq k^2 = Y$, and $f(x, 0) = x$. For every $c \in k$ the formula

$$\tilde{f}_c(x, y) = x + cy$$

defines a linear extension to Y . In particular, $c = 0$ and $c = 1$ give distinct extensions. Injectivity allows an extension without specifying how it acts on a complementary subspace.

Example 2.3 (Free modules need not be injective). Fix $n \geq 2$. The homomorphism

$$f : n\mathbb{Z} \longrightarrow \mathbb{Z}, \quad f(na) = a,$$

cannot extend to $\mathbb{Z}$: an extension would satisfy $n\tilde{f}(1) = \tilde{f}(n) = 1$, which has no integer solution. Thus the free $\mathbb{Z}$ -module $\mathbb{Z}$ is not injective. The map $n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ sending na to $\bar{a}$ also cannot extend. Such an extension would give

$$\bar{1} = \tilde{f}(n) = n\tilde{f}(1) = \bar{0} \quad \text{in } \mathbb{Z}/n\mathbb{Z}.$$

This proves directly from the definition that $\mathbb{Z}/n\mathbb{Z}$ is not injective over $\mathbb{Z}$ either. The last equality concerns the target group, not the nonzero integer n in the source.

Proposition 2.4 (Vector spaces are injective). *Every vector space over a field k , including an infinite-dimensional one, is injective as a k -module.*

Proof. For a linear map $f : X \rightarrow V$ from a subspace $X \subseteq Y$, extend a basis of X to a basis of Y . The additional basis vectors span a complement C , so $Y = X \oplus C$. The formula $\tilde{f}(x + c) = f(x)$ defines an extension. An arbitrary injection reduces to a subspace inclusion by identifying its domain with its image. $\square$

This argument uses the usual axiom of choice to obtain and extend bases. There is no finite-dimensional restriction: under that assumption every subspace has a complement, and every vector space is both projective and injective.

Example 2.5 (The ring and the action matter). Make k a module over $R = k[x]$ by evaluation at $x = 0$. Although it is injective over k , it is not injective over R . Indeed,

$$f : xR \longrightarrow k, \quad f(xp(x)) = p(0)$$

is well defined and R -linear: for $r \in R$, $f(rxp) = r(0)p(0) = rf(xp)$. An extension to R would give $1 = f(x) = \tilde{f}(x) = x\tilde{f}(1) = 0$. The final equality uses the specified action on the target.

The same obstruction also occurs over a ring with nilpotents. For $R = k[\epsilon]/(\epsilon^2)$, let ϵ act as zero on k . The map $\epsilon R \rightarrow k$, $a\epsilon \mapsto a$, is R -linear, since $b + c\epsilon$ acts as multiplication by b on both modules. An extension would again have to send ϵ to $\epsilon\tilde{f}(1) = 0$ instead of 1. Thus neither the underlying abelian group nor injectivity over a smaller ring settles the question over R .

Proposition 2.6 (Splittings and retracts). *If I is injective, every short exact sequence*

$$0 \longrightarrow I \xrightarrow{u} E \longrightarrow C \longrightarrow 0$$

splits. Every retract of an injective module is injective, and hence so is every direct summand of an injective module.

Proof. Extend $\text{id}_I : I \rightarrow I$ across u to obtain $r : E \rightarrow I$ with $ru = \text{id}_I$. Then

$$e = u(r(e)) + (e - u(r(e))) \quad (e \in E)$$

decomposes E as $u(I) \oplus \ker r$. Equivalently, the retraction gives a splitting by Lemma P3.4 of the *Preparatory Notes*.

Now suppose E is injective and $i : I \rightarrow E$, $p : E \rightarrow I$ satisfy $pi = \text{id}_I$. Given $u : X \hookrightarrow Y$ and $f : X \rightarrow I$, extend $if : X \rightarrow E$ to $h : Y \rightarrow E$. Then $ph : Y \rightarrow I$ extends f , because $phu = pif = f$. $\square$

Proposition 2.7 (A splitting characterization). *A module I is injective if and only if every short exact sequence with first nonzero term I splits.*

Proof. The forward implication was just proved. For the converse, use Theorem 2.13, proved independently in the next subsection, to embed I into an injective module E . By hypothesis $0 \rightarrow I \rightarrow E \rightarrow E/I \rightarrow 0$ splits. Thus I is a retract of E and is injective by the preceding proposition. $\square$

This is dual to the splitting criterion with a projective module as the last nonzero term. There is also an equivalent Hom criterion:

$$I \text{ is injective} \iff \text{Hom}_R(-, I) \text{ is an exact contravariant functor.}$$

The restriction map $\text{Hom}_R(Y, I) \rightarrow \text{Hom}_R(X, I)$ sends an extension to its restriction; injectivity asks that this map be surjective whenever $X \hookrightarrow Y$ is injective. Section 3.2 proves the full characterization and distinguishes it from the covariant functor $\text{Hom}_R(I, -)$.

Definition 2.8 (Divisible abelian group). An abelian group D is *divisible* if for every integer $n \geq 1$ and $a \in D$ there exists $b \in D$ with $nb = a$. Equivalently, multiplication by each positive integer is surjective. This condition does not require a unique solution.

Theorem 2.9 (Injectivity over the integers). *An abelian group is injective as a $\mathbb{Z}$ -module if and only if it is divisible.*

Proof. Suppose D is injective. Given $a \in D$ and $n \geq 1$, define $f : n\mathbb{Z} \rightarrow D$ by $f(nk) = ka$. Extend it to $\tilde{f} : \mathbb{Z} \rightarrow D$. Then $b = \tilde{f}(1)$ satisfies $nb = \tilde{f}(n) = f(n) = a$.

Conversely, suppose D is divisible. Let $A \subseteq B$ be abelian groups and $f : A \rightarrow D$ a homomorphism. Consider all pairs (H, u) where $A \subseteq H \subseteq B$ and $u : H \rightarrow D$ extends f . Order these pairs by extension: $(H, u) \leq (H', u')$ means $H \subseteq H'$ and $u'|_H = u$. The set is nonempty because it contains (A, f) . For a totally ordered collection of such pairs, the union of the subgroups is a subgroup. The maps agree wherever both are defined, so they define a homomorphism on that union extending every map in the collection. Thus every such chain has an upper bound. Zorn's lemma gives a maximal pair (H, u) .

If $H \neq B$, choose $b \in B \setminus H$. We seek an extension to $H + \mathbb{Z}b$ by assigning an image $y \in D$ to b and setting

$$u'(h + nb) = u(h) + ny \quad (h \in H, n \in \mathbb{Z}).$$

The possible relations with H are recorded by the subgroup

$$J = \{n \in \mathbb{Z} : nb \in H\} = d\mathbb{Z} \quad \text{for a unique integer } d \geq 0.$$

If $d = 0$, equality $h + nb = h' + n'b$ implies $(n - n')b \in H$, hence $n = n'$ and $h = h'$. The expression is unique, and we may take $y = 0$.

If $d > 0$, divisibility gives $y \in D$ with $dy = u(db)$. Suppose $h + nb = h' + n'b$. There is an integer ℓ with $n - n' = \ell d$ and $h - h' = -\ell db$. Therefore

$$u(h) - u(h') + (n - n')y = -\ell u(db) + \ell dy = 0.$$

In both cases the formula is well defined. It is additive, agrees with u on H , and is defined on a strictly larger subgroup. This contradicts maximality. Hence $H = B$, giving the required extension to all of B . $\square$

The integer d in the proof is the order of $b + H$ in B/H when that order is finite; $d = 0$ records infinite order. The element db need not be zero in H , so the required equation is $dy = u(db)$, not $dy = 0$. Divisibility supplies the solution for one additional element, while Zorn's lemma assembles the extensions for a group that need not be countable. This is the divisibility criterion of Weibel, Corollary 2.3.2.

Example 2.10 (The groups $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$). Both are divisible and therefore injective over $\mathbb{Z}$. For $q \in \mathbb{Q}$, the unique solution of $nb = q$ is q/n . For a coset $q + \mathbb{Z}$, the coset $q/n + \mathbb{Z}$ is a solution; this establishes existence without defining division independently of the chosen representative. In fact

$$(\mathbb{Q}/\mathbb{Z})[n] = \frac{1}{n}\mathbb{Z}/\mathbb{Z} = \{0, \frac{1}{n} + \mathbb{Z}, \dots, \frac{n-1}{n} + \mathbb{Z}\} \cong \mathbb{Z}/n\mathbb{Z}.$$

If b_0 is one solution of $nb = a$, all solutions are exactly $b_0 + (\mathbb{Q}/\mathbb{Z})[n]$. Thus there are exactly n solutions in $\mathbb{Q}/\mathbb{Z}$. For instance, both $\frac{1}{6} + \mathbb{Z}$ and $\frac{2}{3} + \mathbb{Z}$ double to $\frac{1}{3} + \mathbb{Z}$. Every element of $\mathbb{Q}/\mathbb{Z}$ has finite order, so divisibility is compatible with torsion and does not supply a rational vector space structure.

There is also a second example of nonunique extension: the zero map $\mathbb{Z} \rightarrow \mathbb{Q}/\mathbb{Z}$ extends along $\mathbb{Z} \subseteq \mathbb{Q}$ both to the zero map and to the quotient map. Finally, $\mathbb{Q}/\mathbb{Z}$ is not projective over $\mathbb{Z}$: a projective abelian group is a direct summand of a free abelian group and is therefore torsion-free, whereas $\mathbb{Q}/\mathbb{Z}$ has nonzero torsion.

Example 2.11 (An injective quotient does not force a splitting). The sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

does not split, even though its last term is injective. Any homomorphism $\mathbb{Q}/\mathbb{Z} \rightarrow \mathbb{Q}$ is zero: it sends torsion elements to torsion elements, and $\mathbb{Q}$ has no nonzero torsion. Hence the quotient map cannot have a section. The splitting criterion requires the injective term at the *left*, where the extension property gives a retraction.

Example 2.12 (Divisibility does not settle injectivity over a group ring). Let $R = \mathbb{Q}[t, t^{-1}]$ act on $\mathbb{Q}$ by evaluation ε at $t = 1$. Define

$$f : (t - 1)R \longrightarrow \mathbb{Q}, \quad f((t - 1)r) = \varepsilon(r).$$

The ring is a domain, so $(t - 1)r$ uniquely determines r and the formula is well defined. Moreover

$$f(s(t - 1)r) = \varepsilon(sr) = \varepsilon(s)\varepsilon(r) = sf((t - 1)r),$$

so it is R -linear. An extension would satisfy $1 = f(t - 1) = (t - 1)\tilde{f}(1) = 0$. Thus $\mathbb{Q}$ is injective over $\mathbb{Z}$ and over $\mathbb{Q}$, but not for this action of R . Divisibility controls integer multiplication; an extension over a larger ring must also respect the additional action.

2.2 Injective resolutions, their augmentations, and existence

For projectives, the free module on the elements of a module provided a surjection. The corresponding assertion for injectives is that every module admits an embedding into an injective module. There is no basis construction obtained just by reversing arrows, and the noninjectivity of $\mathbb{Z}$ shows why free modules cannot play this role in general.

Theorem 2.13 (Enough injectives). *Every left module over a unital ring embeds into an injective left module.*

Proof. We first show that $\mathbb{Q}/\mathbb{Z}$ detects nonzero elements of abelian groups. Let A be an abelian group and $0 \neq a \in A$. If a has finite order $t \geq 2$, define a homomorphism on $\langle a \rangle$ by $a \mapsto \frac{1}{t} + \mathbb{Z}$. If it has infinite order, use $a \mapsto \frac{1}{2} + \mathbb{Z}$ instead. In both cases the image of a is nonzero. Injectivity of $\mathbb{Q}/\mathbb{Z}$ extends this map to a character $\chi : A \rightarrow \mathbb{Q}/\mathbb{Z}$.

Set

$$S = \text{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}), \quad D = (\mathbb{Q}/\mathbb{Z})^S, \quad j(a) = (\chi(a))_{\chi \in S}.$$

Here D is a *product*, with no finite-support restriction. The evaluation map $j : A \rightarrow D$ is additive and injective, since every nonzero a is detected by at least one coordinate. Each individual character can have a kernel; separation requires the whole family. The group D is divisible: for a fixed positive integer n , choose an n th root in each coordinate. Thus D is an injective abelian group. Choosing these roots uses the usual axiom of choice for an arbitrary index set.

Now let A be a left R -module. Apply the preceding construction to its underlying abelian group to obtain $j : A \hookrightarrow D$. At this point D has no chosen R -action, and j is only an additive map. Define

$$J = \text{Hom}_{\mathbb{Z}}(R, D), \quad (r\phi)(s) = \phi(sr).$$

This gives a left R -module structure: explicitly,

$$(r_1(r_2\phi))(s) = \phi((sr_1)r_2) = ((r_1r_2)\phi)(s), \quad (1\phi)(s) = \phi(s),$$

and the distributive axioms follow from additivity. The order sr in the definition is essential when R is noncommutative. Define

$$\eta : A \longrightarrow J, \quad \eta(a)(s) = j(sa).$$

The map $\eta(a)$ is additive in s , and $\eta(ra)(s) = j(sra) = (r\eta(a))(s)$ proves R -linearity of η . If $\eta(a) = 0$, evaluation at $s = 1$ gives $j(a) = 0$, so $a = 0$.

It remains to prove that J is injective. For an inclusion $X \subseteq Y$ of left R -modules and an R -linear map $f : X \rightarrow J$, evaluation at 1 gives the additive map

$$u : X \longrightarrow D, \quad u(x) = f(x)(1).$$

Extend it additively to $v : Y \rightarrow D$, using injectivity of D as an abelian group. Put

$$\tilde{f}(y)(s) = v(sy).$$

Each $\tilde{f}(y)$ is additive in s , and $\tilde{f}(ry)(s) = v(sry) = (r\tilde{f}(y))(s)$. Thus $\tilde{f} : Y \rightarrow J$ is R -linear. For $x \in X$,

$$\tilde{f}(x)(s) = u(sx) = f(sx)(1) = (sf(x))(1) = f(x)(s).$$

It therefore extends f , proving injectivity of J and completing the embedding construction. $\square$

Proposition 2.14 (A direct-summand description of injectives). *Put $E = \text{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$ with the action just defined. A left R -module is injective if and only if it is a direct summand of a product of copies of E .*

Proof. The preceding proof with $D = \mathbb{Q}/\mathbb{Z}$ shows that E is injective. A product of injectives is injective: extend each coordinate map across a given injection and assemble the resulting maps into one map to the product. For any module A , taking $S = \text{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ gives the injection

$$A \longrightarrow E^S, \quad a \longmapsto (s \mapsto \chi(sa))_{\chi \in S}.$$

This is the earlier construction written using $\text{Hom}_{\mathbb{Z}}(R, (\mathbb{Q}/\mathbb{Z})^S) \cong E^S$. If A is injective, the embedding splits and makes A a direct summand. Conversely, a summand of the injective module E^S is injective by the retract argument. $\square$

This construction explains the role of the divisible target. Using ordinary integer duals instead would lose information: $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = 0$ for $n \geq 2$. The maps into $\mathbb{Q}/\mathbb{Z}$ both extend and separate elements. There is no assertion of a basis for injectives. The products in the construction can be very large; their purpose is to establish existence, while calculations often use smaller injective modules.

Definition 2.15 (Injective resolution). An *injective resolution*, also called an *injective coresolution*, of A is an augmented exact sequence

$$0 \longrightarrow A \xrightarrow{\iota_0} I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \longrightarrow \dots$$

whose terms I^n are injective. We denote it by $(I^\bullet, \iota_0)$, retaining both the unaugmented cochain complex and its map from A .

Here is the construction and the exactness check in every degree. Put $A_0 = A$ and choose an embedding $\iota_0 : A_0 \hookrightarrow I^0$. Inductively, after choosing $\iota_n : A_n \hookrightarrow I^n$, form the quotient and embed it in another injective:

$$A_{n+1} = I^n / \iota_n(A_n), \quad q_n : I^n \twoheadrightarrow A_{n+1}, \quad \iota_{n+1} : A_{n+1} \hookrightarrow I^{n+1}.$$

Define $d^n = \iota_{n+1}q_n$. Since $q_{n+1}\iota_{n+1} = 0$, we have

$$d^{n+1}d^n = \iota_{n+2}q_{n+1}\iota_{n+1}q_n = 0.$$

More strongly, injectivity of ι_{n+1} gives

$$\ker d^n = \ker q_n = \operatorname{im} \iota_n,$$

and for $n \geq 1$, surjectivity of q_{n-1} gives

$$\operatorname{im} d^{n-1} = \operatorname{im}(\iota_n q_{n-1}) = \operatorname{im} \iota_n = \ker d^n.$$

At degree zero this says $\ker d^0 = \iota_0(A)$, and ι_0 itself is injective. Thus the augmented sequence is exact at every term.

The differential d^n is generally *not* an injection: it first takes a quotient and then embeds that quotient. The injection is ι_{n+1} , whose domain is A_{n+1} , not I^n . Projective resolutions successively cover kernels; injective resolutions successively embed cokernels. If one of the quotients A_{n+1} is already injective, we may take $I^{n+1} = A_{n+1}$ and $\iota_{n+1} = \operatorname{id}$, and then put all subsequent terms equal to zero.

When taking cohomology of $I^\bullet$, remove the augmentation object A and set the negative-degree terms equal to zero. The cohomology already defined for cochain complexes then satisfies

$$H^0(I^\bullet) = \ker d^0 \cong A, \quad H^n(I^\bullet) = 0 \quad (n > 0),$$

where the degree-zero isomorphism is precisely ι_0 with codomain restricted to $\ker d^0$. If instead A is included in degree -1 , the augmented complex is exact everywhere and has zero cohomology. These are different complexes. The unaugmented complex records A in degree-zero cohomology; the augmentation specifies that identification. Having injective terms alone does not make a complex an injective resolution: the exactness and the augmentation conditions remain necessary.

Example 2.16 (Two explicit resolutions over $\mathbb{Z}$). First consider

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\text{inclusion}} \mathbb{Q} \xrightarrow{q \mapsto q + \mathbb{Z}} \mathbb{Q}/\mathbb{Z} \longrightarrow 0. \quad (1)$$

The inclusion is injective, the quotient map is surjective, and its kernel is $\mathbb{Z}$. Both $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are divisible, hence injective. Thus this is an injective resolution with $I^0 = \mathbb{Q}$, $I^1 = \mathbb{Q}/\mathbb{Z}$, and higher terms zero. Removing $\mathbb{Z}$ leaves $H^0 \cong \mathbb{Z}$ and $H^1 = 0$.

For $m \geq 2$, there is also the resolution

$$0 \longrightarrow \mathbb{Z}/m\mathbb{Z} \xrightarrow{j} \mathbb{Q}/\mathbb{Z} \xrightarrow{\times m} \mathbb{Q}/\mathbb{Z} \longrightarrow 0, \quad j(\bar{a}) = a/m + \mathbb{Z}. \quad (2)$$

If $a' = a + mk$, their images differ by $k \in \mathbb{Z}$, proving that j is well defined. If $j(\bar{a}) = 0$, then m divides a , proving injectivity. Its image is $\frac{1}{m}\mathbb{Z}/\mathbb{Z}$, exactly the kernel of multiplication by m , and multiplication by m is surjective by divisibility. The two terms following $\mathbb{Z}/m\mathbb{Z}$ are injective. The differential is multiplication by m , not the zero map; this distinction will matter when applying a functor to the resolution. The resolved module itself need not be injective.

Proposition 2.17 (Every abelian group has a short injective resolution). *Every abelian group admits an injective resolution of length at most one.*

Proof. Embed A in an injective abelian group D . The group D is divisible, and its quotient D/A is divisible too: for a coset $d + A$ and $n \geq 1$, choose $x \in D$ with $nx = d$; then $n(x + A) = d + A$. Hence both terms following A in

$$0 \longrightarrow A \longrightarrow D \longrightarrow D/A \longrightarrow 0$$

are injective over $\mathbb{Z}$. □

This short construction uses the special equivalence between divisibility and injectivity over $\mathbb{Z}$. For a $\mathbb{Z}[G]$ -module, injectivity requires extensions to respect the G -action. Divisibility of an underlying abelian group does not ensure that property, nor does it prove that a quotient is injective over $\mathbb{Z}[G]$. Thus this argument cannot be transferred to arbitrary group rings by forgetting the action. Although the general existence construction is cumbersome, it establishes that injective resolutions are always available. The later balanced computation of Ext will often permit a projective resolution of the other variable instead.

2.3 Comparison and uniqueness up to cochain homotopy

We now compare resolutions using the cochain-map and homotopy conventions already established. The argument below is the dual of projective comparison, but we give each extension step because its domain is an image submodule rather than an entire resolution term.

Theorem 2.18 (Injective comparison). *Let $(I^\bullet, \iota_A)$ and $(J^\bullet, \iota_B)$ be injective resolutions of A and B . Every module homomorphism $f : A \rightarrow B$ extends to a cochain map $\varphi : I^\bullet \rightarrow J^\bullet$ satisfying*

$$\varphi^0 \iota_A = \iota_B f, \quad \varphi^{n+1} d_I^n = d_J^n \varphi^n \quad (n \geq 0).$$

Equivalently, the following augmented diagram commutes:

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & A & \xrightarrow{\iota_A} & I^0 & \xrightarrow{d_I^0} & I^1 & \xrightarrow{d_I^1} & I^2 & \longrightarrow & \cdots \\ & & \downarrow f & & \downarrow \varphi^0 & & \downarrow \varphi^1 & & \downarrow \varphi^2 & & \\ 0 & \longrightarrow & B & \xrightarrow{\iota_B} & J^0 & \xrightarrow{d_J^0} & J^1 & \xrightarrow{d_J^1} & J^2 & \longrightarrow & \cdots \end{array}$$

Any two such extensions φ, ψ are cochain homotopic.

Proof. Existence of the comparison map. The rule $\iota_A(a) \mapsto \iota_B(f(a))$ defines a map from the submodule $\iota_A(A) \subseteq I^0$ to J^0 . Injectivity of J^0 extends it to $\varphi^0 : I^0 \rightarrow J^0$, making the augmentation square commute.

Suppose $\varphi^0, \dots, \varphi^n$ have been constructed and the earlier squares commute. On $\text{im } d_I^n \subseteq I^{n+1}$ propose the map

$$t(d_I^n x) = d_J^n \varphi^n(x).$$

To check well-definedness, it suffices to show that the right side is zero whenever $x \in \ker d_I^n$. For $n = 0$, such an x has the form $\iota_A(a)$, so

$$d_J^0 \varphi^0(x) = d_J^0 \iota_B(f(a)) = 0.$$

For $n \geq 1$, exactness gives $x = d_I^{n-1} y$, and

$$d_J^n \varphi^n(x) = d_J^n d_J^{n-1} \varphi^{n-1}(y) = 0.$$

Thus t is a well-defined R -linear map. Injectivity of its target J^{n+1} extends it to $\varphi^{n+1} : I^{n+1} \rightarrow J^{n+1}$. The extension step is the commuting triangle

$$\begin{array}{ccc} \text{im } d_I^n & \hookrightarrow & I^{n+1} \\ \downarrow t & \searrow \varphi^{n+1} & \\ J^{n+1} & & \end{array}$$

The formula on the image gives $\varphi^{n+1}d_I^n = d_J^n\varphi^n$, completing the induction.

Uniqueness up to homotopy. Suppose φ and ψ extend the same f . We construct maps $h^n : I^n \rightarrow J^{n-1}$ for $n \geq 1$, with $h^0 = 0$, satisfying the established homotopy formula

$$\varphi^n - \psi^n = d_J^{n-1}h^n + h^{n+1}d_I^n \quad (n \geq 0). \quad (3)$$

Terms in negative degrees are zero, so the first summand is zero when $n = 0$. Because $\varphi^0 - \psi^0$ vanishes on $\iota_A(A) = \ker d_I^0$, the rule

$$h^1(d_I^0x) = (\varphi^0 - \psi^0)(x)$$

is well defined on $\text{im } d_I^0$. Extend it to $h^1 : I^1 \rightarrow J^0$ by injectivity of J^0 . This gives the degree-zero equation.

For $n \geq 1$, assume that $h^1, \dots, h^n$ have been chosen and the homotopy formula holds in degrees below n . Put

$$u^n = \varphi^n - \psi^n - d_J^{n-1}h^n.$$

The cochain-map equations give

$$\begin{aligned} u^n d_I^{n-1} &= d_J^{n-1}(\varphi^{n-1} - \psi^{n-1} - h^n d_I^{n-1}) \\ &= 0. \end{aligned}$$

For $n = 1$, the bracket is zero by the degree-zero homotopy equation. For $n \geq 2$, it equals $d_J^{n-2}h^{n-1}$ by the preceding homotopy equation, and two consecutive differentials compose to zero. Since $\ker d_I^n = \text{im } d_I^{n-1}$, the map u^n vanishes on $\ker d_I^n$. Consequently

$$\bar{u}^n : \text{im } d_I^n \longrightarrow J^n, \quad \bar{u}^n(d_I^n x) = u^n(x)$$

defines a map on $\text{im } d_I^n$ into J^n . Extend it to all of I^{n+1} using injectivity of J^n . This time the extension triangle is

$$\begin{array}{ccc} \text{im } d_I^n & \xhookrightarrow{\quad} & I^{n+1} \\ \bar{u}^n \downarrow & \swarrow h^{n+1} & \\ J^n & & \end{array}$$

The target degree is n , one less than the domain degree of h^{n+1} . This is the degree shift required for a cochain homotopy. The defining equation is precisely (3) in degree n . This completes the homotopy construction. $\square$

Both inductions use the same pattern: show that a proposed map kills $\ker d_I^n$, define it on $\text{im } d_I^n$, and then extend its domain to I^{n+1} . The source resolution's exactness makes the partial map well defined, and the target term's injectivity supplies its extension. Injectivity does not make the choices unique term by term; the homotopy accounts for their difference.

Corollary 2.19 (Uniqueness of an injective resolution). *Any two injective resolutions of a module A are cochain homotopy equivalent by maps extending id_A .*

Proof. Choose comparison maps $\varphi : I^\bullet \rightarrow J^\bullet$ and $\psi : J^\bullet \rightarrow I^\bullet$, both extending id_A . Write the two augmentations as $\iota_I : A \rightarrow I^0$ and $\iota_J : A \rightarrow J^0$. Their compatibility gives explicitly

$$(\psi\varphi)^0 \iota_I = \psi^0 \varphi^0 \iota_I = \psi^0 \iota_J = \iota_I, \quad (\varphi\psi)^0 \iota_J = \varphi^0 \psi^0 \iota_J = \varphi^0 \iota_I = \iota_J.$$

The composite $\psi\varphi$ and the identity of $I^\bullet$ are two extensions of id_A , so comparison uniqueness gives $\psi\varphi \simeq \text{id}_{I^\bullet}$. Likewise $\varphi\psi \simeq \text{id}_{J^\bullet}$. Thus these maps are homotopy inverses. The homotopy class of either comparison map is itself independent of its construction. $\square$

More generally, comparison maps for $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$ compose to a comparison map for gf . Any other chosen comparison map for gf is homotopic to that composite, and a comparison map for id_A is homotopic to the identity. Hence the comparison construction respects composition and identities at the level of homotopy classes. Section P3.3 of the *Preparatory Notes* explains why an additive functor preserves these homotopies; that is the next step needed to define right derived functors independently of the resolutions and comparison maps chosen.

Key point. An injective resolution exists because every module can be embedded in an injective one. Exactness preserves the original module, while comparison and homotopy make different choices compatible. These are separate parts of the construction.

3 Derived Functors

Projective and injective resolutions replace a module by an exact complex whose terms have useful lifting or extension properties. An additive functor can be applied to that complex, but it may destroy exactness. Derived functors record the resulting homology or cohomology. The comparison theorems make this construction independent of choices. Throughout, the target category $\mathcal{D}$ is abelian; taking $\mathcal{D} = \mathbf{Ab}$ gives all of the concrete calculations below.

3.1 Definitions, vanishing, and long exact sequences

The notions of additive, left exact, right exact, and exact functor are those of Sections P2.3 and P3.1 of the *Preparatory Notes*. The extension of an additive functor to complexes, including its preservation of homotopies, was proved in Section P3.3 of the *Preparatory Notes*.

Definitions and well-definedness

Definition 3.1 (Left derived functors). Let $F : R\text{-}\mathbf{Mod} \rightarrow \mathcal{D}$ be covariant, additive, and right exact. Choose a projective resolution $P_\bullet \xrightarrow{\varepsilon} M$, omit its augmentation, and apply F :

$$\cdots \longrightarrow F(P_2) \xrightarrow{F(d_2)} F(P_1) \xrightarrow{F(d_1)} F(P_0) \longrightarrow 0.$$

The term $F(P_0)$ has degree zero. Define

$$L_j F(M) = H_j(F(P_\bullet)) \quad (j \geq 0).$$

Thus $L_0 F(M) = \text{coker } F(d_1)$; for $j > 0$, in a module target this is the explicit quotient $\ker F(d_j) / \text{im } F(d_{j+1})$. For a module homomorphism $a : M \rightarrow N$, choose a chain map $\tilde{a} : P_\bullet(M) \rightarrow P_\bullet(N)$ lifting a and set

$$L_j F(a) = H_j(F(\tilde{a})) : L_j F(M) \longrightarrow L_j F(N).$$

The comparison theorem provides the lift. Its independence of choices, and hence the well-definedness of the functor, are proved below.

Definition 3.2 (Right derived functors). Let $G : R\text{-}\mathbf{Mod} \rightarrow \mathcal{D}$ be covariant, additive, and left exact. Choose an injective resolution $0 \rightarrow M \xrightarrow{\iota} I^0 \xrightarrow{d^0} I^1 \rightarrow \cdots$, omit M , and form

$$0 \longrightarrow G(I^0) \xrightarrow{G(d^0)} G(I^1) \xrightarrow{G(d^1)} G(I^2) \longrightarrow \cdots.$$

Here $G(I^0)$ has degree zero. Define

$$R^j G(M) = H^j(G(I^\bullet)) \quad (j \geq 0).$$

In particular $R^0 G(M) = \ker G(d^0)$, and for $j > 0$ the quotient is $\ker G(d^j) / \text{im } G(d^{j-1})$. For a module homomorphism $a : M \rightarrow N$, choose a cochain map $\tilde{a} : I^\bullet(M) \rightarrow I^\bullet(N)$ extending a and set

$$R^j G(a) = H^j(G(\tilde{a})) : R^j G(M) \longrightarrow R^j G(N).$$

The injective comparison theorem provides this extension; the same well-definedness argument applies.

The transformed sequences are complexes because functoriality and additivity give $G(d^{j+1})G(d^j) = G(d^{j+1}d^j) = G(0) = 0$, and similarly for F . This proves only that images lie in kernels. Their equality is the additional condition that may fail. The words *left* and *right* describe these classical derivation conventions; they do not describe the side of a module action. The letter R in $R^j G$ denotes right derivation, not a power of the coefficient ring.

Proposition 3.3 (Canonical comparison after applying a functor). *For an additive $F : R\text{-Mod} \rightarrow \mathcal{D}$, applying F to projective resolutions and taking homology gives additive functors of the module, independent of the resolutions up to canonical natural isomorphism. The analogous statement holds for injective resolutions and cohomology. This assertion requires no exactness of F .*

Proof. We give the cochain argument explicitly. Let $I^\bullet$ and $J^\bullet$ be injective resolutions of M . By Section 2.3, a map $u : I^\bullet \rightarrow J^\bullet$ extending id_M exists, and any two such maps are cochain homotopic. Define

$$\theta_{I,J} = H^j(F(u)) : H^j(F(I^\bullet)) \longrightarrow H^j(F(J^\bullet)).$$

To see exactly why a different lift gives the same map, let $u - v = dh + hd$. Additivity preserves this equality. For an actual cocycle $z \in F(I^j)$ when $\mathcal{D} = \mathbf{Ab}$, it gives

$$(F(u^j) - F(v^j))z = F(d_J^{j-1})F(h^j)z,$$

because $F(d_I^j)z = 0$. The right-hand side is a coboundary. In any abelian target the same argument uses the kernel and image factorizations, as in the homotopy-invariance theorem. Thus $\theta_{I,J}$ is independent of the lift; no left exactness was used.

A comparison in the reverse direction has both composites homotopic to the respective identity maps. Hence $\theta_{J,I}$ is the inverse of $\theta_{I,J}$. For three resolutions of M , composition of comparisons still extends id_M , so

$$\theta_{J,K}\theta_{I,J} = \theta_{I,K}, \quad \theta_{I,I} = \text{id}.$$

These equalities explain the word *canonical*: the isomorphisms are compatible with one another, rather than being arbitrarily chosen.

For fixed choices of resolutions, the same argument applies to extensions of any module map $a : M \rightarrow N$. Homotopy uniqueness therefore makes the map on cohomology independent of the extension, as required in the definition of right derived functors above. An identity cochain map extends the identity module map, and a composite of extensions extends the composite module map. Consequently identity maps and composition are preserved. The sum of two extensions extends the sum of the module maps, which proves additivity. If a second family of resolutions is chosen, both paths around the comparison square extend the same module map. They are therefore homotopic, proving naturality of the comparison isomorphisms.

For projective resolutions use chain comparison maps lifting module maps. Their homotopies are preserved by F ; the identical argument with H_j gives every assertion for left derived functors. $\square$

Only additivity was needed to define these homology objects and their maps independently of resolutions. Right exactness for left derived functors, or left exactness for right derived functors, is what makes degree zero equal the original functor. Knowing merely that two resolutions have isomorphic homology would be insufficient: an arbitrary additive functor need not preserve quasi-isomorphisms. The stronger comparison by actual homotopy equivalences supplies exactly what is needed.

Proposition 3.4 (Degree zero recovers the original functor). *There are natural isomorphisms*

$$L_0F(M) \cong F(M), \quad R^0G(M) \cong G(M).$$

They are induced by the augmentation maps.

Proof. For the first statement, put $K = \ker \varepsilon$ and factor $d_1 = j\pi$, where $\pi : P_1 \twoheadrightarrow K$ and $j : K \hookrightarrow P_0$. Right exactness applied to $0 \rightarrow K \rightarrow P_0 \rightarrow M \rightarrow 0$ identifies $F(M)$ with $\text{coker } F(j)$. It also makes $F(\pi)$ epic, by applying right exactness to the short exact sequence of π and its kernel. Hence $\text{im } F(d_1) = \text{im } F(j)$, proving $\text{coker } F(d_1) \cong F(M)$.

For the second statement write the beginning of the injective resolution as

$$0 \longrightarrow M \xrightarrow{\iota} I^0 \xrightarrow{q_0} M_1 \longrightarrow 0, \quad d^0 = \iota_1 q_0,$$

where $\iota_1 : M_1 \hookrightarrow I^1$. Left exactness gives $\ker G(q_0) = \operatorname{im} G(\iota)$ and makes $G(\iota)$ monic. Applying it to $0 \rightarrow M_1 \rightarrow I^1 \rightarrow I^1/M_1 \rightarrow 0$ also makes $G(\iota_1)$ monic. Consequently

$$\begin{aligned} \ker G(d^0) &= \ker(G(\iota_1)G(q_0)) \\ &= \ker G(q_0) = \operatorname{im} G(\iota) \cong G(M). \end{aligned}$$

This argument does not require $G(q_0)$ to be onto: it uses only its kernel and the injectivity of the following map. The comparison maps commute with augmentations, so these identifications are natural and compatible with the canonical identifications between choices of resolutions proved above. $\square$

Vanishing and the meaning of acyclicity

Proposition 3.5 (Two different reasons for higher vanishing). *For $j > 0$,*

$$L_j F(P) = 0 \quad \text{if } P \text{ is projective,} \quad R^j G(I) = 0 \quad \text{if } I \text{ is injective.}$$

If F is exact, then $L_j F(M) = 0$ for every M and $j > 0$. If G is exact, then $R^j G(M) = 0$ for every M and $j > 0$.

Proof. For a projective input use the length-zero resolution $0 \rightarrow P \xrightarrow{\operatorname{id}} P \rightarrow 0$; for an injective input use $0 \rightarrow I \xrightarrow{\operatorname{id}} I \rightarrow 0$. After removing the input and applying the functor, the sole nonzero term is in degree zero. Canonical independence permits this choice even if another resolution is much longer.

For an exact functor, Section P3.1 of the *Preparatory Notes* proves that preserving short exact sequences implies preserving every exact position of a sequence, including an infinite resolution. Thus the transformed augmented resolution is exact. In every positive degree its kernel equals its image, and the homology quotient is zero. For example,

$$L_j F(M) = \ker F(d_j) / \operatorname{im} F(d_{j+1}) = 0 \quad (j > 0).$$

The cochain calculation is the same with degree raised by the differential. These expressions denote subobject quotients in $\mathcal{D}$. $\square$

The restriction to positive degrees is essential. The input is omitted from the complex used for derivation. At the remaining degree-zero term, its outward differential is zero in the chain case, and there is no incoming coboundary in the cochain case. Thus $L_0 F(M) \cong F(M)$ and $R^0 G(M) \cong G(M)$ need not vanish. For the identity functor, for example, degree zero is M and every positive derived functor is zero.

Definition 3.6 (Acyclic for a specified functor). A module A is G -acyclic for a left exact G if $R^j G(A) = 0$ for all $j > 0$. For a right exact F , it is F -acyclic for left derivation if $L_j F(A) = 0$ for all $j > 0$. The functor and the direction of derivation are part of this statement.

Example 3.7 (The quantifiers cannot be reversed). Every injective module is G -acyclic for every left exact G , but acyclicity for one fixed G does not imply injectivity. Take $G = \operatorname{id}_{\mathbf{Ab}}$ and $A = \mathbb{Z}$: the functor is exact, so all positive $R^j G(\mathbb{Z})$ vanish, although $\mathbb{Z}$ is not injective. Conversely, a functor can fail to be exact and still have no higher derived functors on a particular input. For $n \geq 2$, take $G = \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, -)$ and $I = \mathbb{Q}$. This functor is not right exact, as verified in Example 3.19, but $\mathbb{Q}$ is injective over $\mathbb{Z}$, so all $R^j G(\mathbb{Q})$ vanish for $j > 0$. In fact its degree-zero value is also zero, because $\mathbb{Q}$ has no nonzero elements annihilated by n .

The ring must also be specified: injectivity of an underlying abelian group is not sufficient for injectivity as an R -module. For group cohomology the relevant ring will be $\mathbb{Z}[G]$, and any vanishing claim from injectivity must be checked over that ring.

The first right derived functor as a concrete quotient

Write the successive short exact sequences of an injective resolution as

$$0 \longrightarrow A_k \xrightarrow{\iota_k} I^k \xrightarrow{q_k} A_{k+1} \longrightarrow 0, \quad A_0 = A, \quad d^k = \iota_{k+1} q_k.$$

Left exactness gives $\ker G(d^1) = \ker G(q_1) = \operatorname{im} G(\iota_1)$, since $G(\iota_2)$ is monic. The monomorphism $G(\iota_1)$ identifies this kernel with $G(A_1)$. Under that identification, $\operatorname{im} G(d^0)$ corresponds precisely to $\operatorname{im} G(q_0)$, because $G(d^0) = G(\iota_1)G(q_0)$. Therefore

$$R^1 G(A) \cong \operatorname{coker}(G(I^0) \xrightarrow{G(q_0)} G(A_1)).$$

For an abelian-group target this is $G(A_1)/\operatorname{im} G(q_0)$. It measures exactly the failure of the originally surjective q_0 to remain surjective after applying G . This direct proof does not presuppose the derived long exact sequence, which we establish next.

Long exact sequences of derived functors

The connecting map is an obstruction to lifting a *homology class* to the middle complex: exactness says that $\partial_n[z] = 0$ precisely when $[z]$ is the image of a class in $H_n(C)$. The cochain statement is identical, with degree raised by one. To apply this principle to derived functors we need compatible resolutions, rather than three unrelated choices.

Lemma 3.8 (Horseshoe lemma). *Given $0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$ and projective resolutions $P'_\bullet \rightarrow A'$ and $P''_\bullet \rightarrow A''$, there is a projective resolution $P_\bullet \rightarrow A$ and a compatible short exact sequence of augmented resolutions whose sequence in every nonnegative degree is the split sequence*

$$0 \longrightarrow P'_n \longrightarrow P'_n \oplus P''_n \longrightarrow P''_n \longrightarrow 0.$$

The injection and projection are the usual summand maps. The differential of the middle resolution need not be diagonal.

Proof. We give the inductive construction, including its exactness step. Suppose first that $0 \rightarrow X' \xrightarrow{i} X \xrightarrow{p} X'' \rightarrow 0$ is exact and we have projective surjections $e' : Q' \twoheadrightarrow X'$ and $e'' : Q'' \twoheadrightarrow X''$. Lift e'' to $t : Q'' \rightarrow X$ using projectivity of Q'' , and put

$$e : Q' \oplus Q'' \longrightarrow X, \quad e(q', q'') = i(e'(q')) + t(q'').$$

This map is surjective: first lift the image of x in X'' using Q'' , then correct the remaining element of $i(X')$ using Q' .

The kernel of e fits into an exact sequence

$$0 \longrightarrow \ker e' \longrightarrow \ker e \longrightarrow \ker e'' \longrightarrow 0.$$

The maps are induced by summand inclusion and projection. A kernel element $(q', 0)$ satisfies $e'(q') = 0$, giving exactness at the first two positions. For surjectivity onto $\ker e''$, take q'' with $e''(q'') = 0$. Then $t(q'') \in \ker p = i(X')$, so choose q' with $i(e'(q')) = -t(q'')$. The pair (q', q'') belongs to $\ker e$ and projects to the prescribed q'' .

Apply this construction first with $(X', X, X'') = (A', A, A'')$ and $(Q', Q'') = (P'_0, P''_0)$. It gives the middle augmentation and a short exact sequence of its kernels. Apply it next to this kernel sequence with the prescribed projective surjections from P'_1, P''_1 . Repeat. At every step the chosen map onto the middle kernel, followed by the kernel inclusion in the preceding term, is the new middle differential. Hence its image is exactly that kernel, its composite with the preceding differential is zero, and the summand maps commute with the differentials. Induction gives the required exact augmented complex and compatible maps. Each middle term is a finite direct sum of projectives, hence projective: lift the maps from the two summands separately and add the resulting lifts. $\square$

The dual statement uses injective resolutions: compatible resolutions may be chosen in a degreewise split short exact sequence, with middle term $I^n \oplus I'^n$. This is the horseshoe lemma in the opposite abelian category, where injectives are projectives. Its existence hypothesis is justified by the earlier theorem on enough injectives; it is not an assumption that free modules are injective.

Theorem 3.9 (Long exact sequences of derived functors). *Let $F : R\text{-Mod} \rightarrow \mathcal{D}$ be covariant, additive, and right exact, and let $G : R\text{-Mod} \rightarrow \mathcal{D}$ be covariant, additive, and left exact, where $\mathcal{D}$ is abelian. A short exact sequence $0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$ induces natural long exact sequences*

$$\begin{aligned} \cdots \rightarrow L_j F(A') \rightarrow L_j F(A) \rightarrow L_j F(A'') \xrightarrow{\partial} L_{j-1} F(A') \rightarrow \cdots, \\ \cdots \rightarrow R^j G(A') \rightarrow R^j G(A) \rightarrow R^j G(A'') \xrightarrow{\delta} R^{j+1} G(A') \rightarrow \cdots. \end{aligned}$$

The first ends in $F(A') \rightarrow F(A) \rightarrow F(A'') \rightarrow 0$; the second begins in $0 \rightarrow G(A') \rightarrow G(A) \rightarrow G(A'')$.

Proof. Choose compatible projective resolutions using Lemma 3.8, and remove the augmented modules before applying F . In each degree the sequence is split exact, so it is preserved by an additive functor: a decomposition into a finite biproduct is preserved together with its inclusions and projections. Thus

$$0 \longrightarrow F(P'_\bullet) \longrightarrow F(P_\bullet) \longrightarrow F(P''_\bullet) \longrightarrow 0$$

is a short exact sequence of complexes in $\mathcal{D}$. Theorem P3.24 of the *Preparatory Notes* supplies its long exact sequence, and $L_0 F \cong F$ identifies the tail. The dual horseshoe lemma and Theorem P3.25 of the *Preparatory Notes* prove the statement for G , using $R^0 G \cong G$.

These constructions are independent of the compatible resolutions and natural in the original short exact sequence. To see why the comparison maps can be made compatible, lift a map on the left endpoint to its projective resolutions. At each degree lift a map from the projective right summand to the target right resolution; choose a middle lift and correct its differential error in the left summand. Exactness and projectivity give this correction by the same kernel-lifting induction as the comparison theorem. Equivalently, repeat the horseshoe construction for the map between the successive kernel short exact sequences. This gives a morphism of the compatible resolution sequences. Each of its three component maps induces the canonical derived map of Proposition 3.3, because any two lifts of the same module map are homotopic. Naturality of the connecting map for complexes therefore proves both the asserted naturality and the independence of the connecting maps from the resolutions. Reverse arrows for injective resolutions. $\square$

Applying F directly to an arbitrary short exact sequence would not justify this argument: a right exact functor can destroy its initial injection. The horseshoe lemma supplies the stronger, degreewise *split* exact sequence that additivity preserves.

Proposition 3.10 (Acyclic resolutions can also compute derived functors). *Let G be additive and left exact. If $0 \rightarrow A \rightarrow J^0 \rightarrow J^1 \rightarrow \cdots$ is exact and every J^k is G -acyclic, then $R^j G(A) \cong H^j(G(J^\bullet))$. Dually, a resolution by F -acyclic modules computes $L_j F$ for an additive right exact F .*

Proof. Put $A_0 = A$ and express the first resolution as short exact sequences $0 \rightarrow A_k \xrightarrow{\iota_k} J^k \xrightarrow{q_k} A_{k+1} \rightarrow 0$, with differential $d^k = \iota_{k+1} q_k$. The long exact sequence and $R^r G(J^k) = 0$ for $r > 0$ give

$$\begin{aligned} 0 \rightarrow G(A_k) \rightarrow G(J^k) \rightarrow G(A_{k+1}) \rightarrow R^1 G(A_k) \rightarrow 0, \\ R^r G(A_{k+1}) \cong R^{r+1} G(A_k) \quad (r \geq 1). \end{aligned}$$

As in the direct first-obstruction calculation, $\ker G(d^k)$ is identified by $G(\iota_k)$ with $G(A_k)$. For $k > 0$, its subobject of coboundaries corresponds to $\operatorname{im} G(q_{k-1})$. Therefore

$$H^k(G(J^\bullet)) \cong R^1 G(A_{k-1}) \cong R^k G(A).$$

The last isomorphism follows by repeatedly using the preceding dimension shifts. In degree zero, the earlier left-exactness argument identifies the kernel with $G(A)$. All maps here come from the short exact sequences and their connecting maps, so they are compatible with morphisms of such resolutions. The chain argument reverses the arrows and uses kernels of successive surjections instead of cokernels. $\square$

This theorem requires both an exact augmented resolution and acyclicity of its terms for the specified functor. An arbitrary resolution by arbitrary modules cannot be used merely because it is exact before the functor is applied. Injective terms are a sufficient uniform condition for all right derived functors, while G -acyclicity is the weaker condition adapted to one particular G .

3.2 Exactness of Hom and tensor

We now establish the one-sided exactness that makes Hom and tensor product fit the preceding definitions. Their actions on morphisms and additivity were established in the preparatory notes; here each missing half of exactness will be tied to a property of the fixed module.

Proposition 3.11 (Covariant Hom is always left exact). *For every module M , the functor $\operatorname{Hom}_R(M, -)$ is left exact. Thus every short exact sequence*

$$0 \longrightarrow A' \xrightarrow{i} A \xrightarrow{p} A'' \longrightarrow 0$$

induces an exact sequence of abelian groups

$$0 \longrightarrow \operatorname{Hom}_R(M, A') \xrightarrow{i_*} \operatorname{Hom}_R(M, A) \xrightarrow{p_*} \operatorname{Hom}_R(M, A''),$$

where $i_(g) = i \circ g$ and $p_*(f) = p \circ f$.*

Proof. First, i_* is injective: if $i \circ g = 0$, then injectivity of i gives $g(m) = 0$ for every $m \in M$, hence $g = 0$.

Next, $p_* i_*(g) = p \circ i \circ g = 0$, so $\operatorname{im} i_* \subseteq \ker p_*$. Conversely, suppose $f : M \rightarrow A$ satisfies $p \circ f = 0$. For each $m \in M$, exactness gives $f(m) \in \ker p = \operatorname{im} i$. Since i is injective, there is a unique $g(m) \in A'$ such that $i(g(m)) = f(m)$. This defines a function $g : M \rightarrow A'$.

It is a module homomorphism. Indeed,

$$\begin{aligned} i(g(m + m')) &= f(m + m') = f(m) + f(m') = i(g(m) + g(m')), \\ i(g(rm)) &= f(rm) = rf(m) = i(rg(m)). \end{aligned}$$

Injectivity of i gives additivity and R -linearity of g . Therefore $f = i \circ g$ lies in $\text{im } i_*$. Moreover, g is the unique such factorization, because $i \circ g = i \circ h$ implies $g = h$. This proves $\ker p_* = \text{im } i_*$ and hence left exactness. $\square$

Proposition 3.12 (Projectivity is exactness of covariant Hom). *For a module M , the following conditions are equivalent:*

1. M is projective;
2. $\text{Hom}_R(M, -)$ is right exact;
3. $\text{Hom}_R(M, -)$ is exact.

Proof. By Proposition 3.11, this functor is already left exact, so conditions (2) and (3) are equivalent. The only additional requirement is that $q_* : \text{Hom}_R(M, B) \rightarrow \text{Hom}_R(M, C)$ be surjective for each short exact sequence ending in $B \xrightarrow{q} C$.

If M is projective, every $f : M \rightarrow C$ lifts to $\tilde{f} : M \rightarrow B$ with $q\tilde{f} = f$. Thus q_* is surjective and (1) implies (3). Conversely, assume (2), let $q : B \twoheadrightarrow C$ be any surjection, and let $f : M \rightarrow C$ be any homomorphism. Every such q belongs to the short exact sequence in the lower row of

$$\begin{array}{ccccccc}
 & & & & M & & \\
 & & & & \downarrow f & & \\
 0 & \longrightarrow & \ker q & \hookrightarrow & B & \xrightarrow{q} & C \longrightarrow 0 \\
 & & & & \nwarrow \tilde{f} & & \\
 & & & & & &
 \end{array}$$

Right exactness says that q_* is onto, so it provides the dashed map. This is exactly the lifting property defining projectivity, proving (1). The lift need not be unique; this differs from the unique factorization through a kernel in the preceding proof. $\square$

We next fix a target module I ; the letter I here does *not* yet assume injectivity. The functor $\text{Hom}_R(-, I)$ reverses each arrow, so its left exact sequence starts with maps out of the quotient.

Proposition 3.13 (Contravariant Hom is always left exact). *For every module I and every short exact sequence $0 \rightarrow A' \xrightarrow{i} A \xrightarrow{p} A'' \rightarrow 0$, the sequence*

$$0 \longrightarrow \text{Hom}_R(A'', I) \xrightarrow{p^*} \text{Hom}_R(A, I) \xrightarrow{i^*} \text{Hom}_R(A', I)$$

is exact, where $p^(g) = g \circ p$ and $i^*(f) = f \circ i$.*

Proof. First, p^* is injective. If $g \circ p = 0$, then for any $a'' \in A''$ we can choose $a \in A$ with $p(a) = a''$ and obtain $g(a'') = g(p(a)) = 0$. Hence $g = 0$.

Since $p \circ i = 0$, we have $i^*p^* = 0$, giving $\text{im } p^* \subseteq \ker i^*$. Conversely, let $f : A \rightarrow I$ satisfy $f \circ i = 0$. Define $g : A'' \rightarrow I$ by $g(a'') = f(a)$ for any lift a of a'' . If a and b are two lifts, then $a - b \in \ker p = \text{im } i$, so $f(a) - f(b) = 0$; the definition is independent of the lift. Lifts of $a'' + b''$ and ra'' can be chosen as $a + b$ and ra . Linearity of f then gives $g(a'' + b'') = g(a'') + g(b'')$ and $g(ra'') = rg(a'')$. Thus g is R -linear and satisfies $g \circ p = f$. It is unique because p is surjective. Hence $\ker i^* = \text{im } p^*$, proving left exactness after reversing the arrows. $\square$

Proposition 3.14 (Injectivity is exactness of contravariant Hom). *A module I is injective if and only if $\text{Hom}_R(-, I)$ is exact. Equivalently, since this functor is already left exact, it is enough that it be right exact with the order of each sequence reversed.*

Proof. By Proposition 3.13, the only missing condition is surjectivity of $i^* : \text{Hom}_R(A, I) \rightarrow \text{Hom}_R(A', I)$. If I is injective, every map $A' \rightarrow I$ extends along the injection $i : A' \hookrightarrow A$, giving this surjectivity. Therefore Hom is exact.

Conversely, suppose Hom is exact. For any injection $u : A \hookrightarrow B$ and any map $f : A \rightarrow I$, form the short exact sequence $0 \rightarrow A \xrightarrow{u} B \rightarrow B/u(A) \rightarrow 0$. Exactness of the reversed Hom sequence says that restriction $u^* : \text{Hom}_R(B, I) \rightarrow \text{Hom}_R(A, I)$ is onto. Thus the following diagram has a dashed arrow making its triangle commute:

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \xrightarrow{u} & B & \longrightarrow & B/u(A) \longrightarrow 0 \\ & & \downarrow f & & \swarrow \tilde{f} & & \\ & & I & & & & \end{array}$$

This means $\tilde{f} \circ u = f$, which is precisely the extension property defining injectivity. Extensions, like projective lifts, are not required to be unique. $\square$

Right exactness in both tensor variables

Proposition 3.15 (Tensor product is right exact in each variable). *For a short exact sequence of left modules $0 \rightarrow A' \xrightarrow{i} A \xrightarrow{p} A'' \rightarrow 0$ and a right module N ,*

$$N \otimes_R A' \xrightarrow{1 \otimes i} N \otimes_R A \xrightarrow{1 \otimes p} N \otimes_R A'' \longrightarrow 0$$

is exact. For a short exact sequence of right modules $0 \rightarrow N' \xrightarrow{j} N \xrightarrow{q} N'' \rightarrow 0$ and a left module M ,

$$N' \otimes_R M \xrightarrow{j \otimes 1} N \otimes_R M \xrightarrow{q \otimes 1} N'' \otimes_R M \longrightarrow 0$$

is exact as well.

Proof. The left-module variable. Every pure tensor $n \otimes a''$ lifts by choosing a with $p(a) = a''$. Finite sums of pure tensors generate the target, so $1 \otimes p$ is surjective. Since $pi = 0$, its composite with $1 \otimes i$ is zero. Thus $J = \text{im}(1 \otimes i) \subseteq \ker(1 \otimes p)$. Let $T = (N \otimes_R A)/J$. The actual induced map is

$$\phi : T \longrightarrow N \otimes_R A'', \quad \phi([n \otimes a]) = n \otimes p(a).$$

Define $\beta(n, a'') = [n \otimes a]$ using any lift a of a'' . Two lifts differ by $i(a')$, and $n \otimes i(a')$ belongs to J , so the value is independent of the lift. Choosing sums of lifts proves biadditivity. If a lifts a'' , then ra lifts ra'' , and balancing in $N \otimes_R A$ gives $\beta(nr, a'') = \beta(n, ra'')$. The tensor universal property supplies $\psi : N \otimes_R A'' \rightarrow T$.

On a generator $[n \otimes a]$ we have $\psi\phi([n \otimes a]) = [n \otimes a]$, and on $n \otimes a''$ we have $\phi\psi(n \otimes a'') = n \otimes a''$. In particular, $\ker \phi = 0$. If $z \in N \otimes_R A$ is killed by $1 \otimes p$, then $\phi([z]) = 0$, hence $[z] = 0$ and $z \in J$. Together with the earlier inclusion, this proves equality of the kernel and image for the original maps, not merely an abstract isomorphism between two quotient groups.

The right-module variable. Each $n'' \otimes m$ has a lift $n \otimes m$, so $q \otimes 1$ is surjective. Its composite with $j \otimes 1$ is zero. Set $K = \text{im}(j \otimes 1)$ and $T' = (N \otimes_R M)/K$. The induced map is

$$\phi' : T' \longrightarrow N'' \otimes_R M, \quad \phi'([n \otimes m]) = q(n) \otimes m.$$

The rule $(n'', m) \mapsto [n \otimes m]$, using any lift n of n'' , is independent of the lift because changing n by $j(n')$ changes the tensor by an element of K . It is biadditive, and it is balanced: if n lifts n'' , then nr lifts $n''r$, while $[nr \otimes m] = [n \otimes rm]$. It gives an inverse $\psi' : N'' \otimes_R M \rightarrow T'$ to ϕ' , as checked on generators. Consequently $\ker \phi' = 0$. For z in the kernel of $q \otimes 1$, $\phi'([z]) = 0$ forces $[z] = 0$, so $z \in K$. This proves the second equality of image and kernel. $\square$

Definition 3.16 (Flat modules). A right module N is *flat* if $N \otimes_R -$ is exact; a left module M is *flat* if $- \otimes_R M$ is exact. Since these functors are always right exact, flatness is equivalent to their left exactness, or to their preserving all injections in the variable module.

Every projective module is flat. To see this for a free right module, the natural isomorphism $R^{(S)} \otimes_R A \cong A^{(S)}$ identifies tensoring with taking a direct sum of copies. Direct sums preserve exactness: kernel membership and preimages are checked coordinatewise, and only finitely many coordinates of any given element are nonzero. A projective module is a direct summand of a free module, so the corresponding tensor sequence is a direct summand of an exact sequence. Kernels and images of a direct sum of maps are the direct sums of their kernels and images; each summand sequence is therefore exact. The proof for free and projective left modules is identical with the sides reversed.

Key point. The fixed module determines when the missing half of exactness holds: a source of Hom must be projective, a target of Hom must be injective, and a factor of tensor product must be flat.

Example 3.17 (An injective first argument does not make covariant Hom exact). Put $I = \mathbb{Q}/\mathbb{Z}$. Since I is injective, every short exact sequence $0 \rightarrow U \rightarrow V \rightarrow W \rightarrow 0$ gives the reversed short exact sequence

$$0 \rightarrow \text{Hom}_{\mathbb{Z}}(W, I) \rightarrow \text{Hom}_{\mathbb{Z}}(V, I) \rightarrow \text{Hom}_{\mathbb{Z}}(U, I) \rightarrow 0.$$

Here the fixed injective module is the target. In contrast, applying $\text{Hom}_{\mathbb{Z}}(I, -)$ to $0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$ gives

$$0 \rightarrow 0 \rightarrow 0 \rightarrow \text{Hom}_{\mathbb{Z}}(I, I) \rightarrow 0.$$

Both $\text{Hom}(I, \mathbb{Z})$ and $\text{Hom}(I, \mathbb{Q})$ are zero: every element of I has finite order, whereas $\mathbb{Z}$ and $\mathbb{Q}$ are torsion-free. The last Hom group contains the nonzero identity map, so exactness fails there. Thus the same injective module placed in the first variable supplies no covariant exactness guarantee.

One short exact sequence under eight choices of functor

Fix $n \geq 2$, put $C = \mathbb{Z}/n\mathbb{Z}$, and write

$$0 \rightarrow \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \xrightarrow{q} C \rightarrow 0. \quad (*)$$

We use evaluation at 1 or $\bar{1}$ to identify Hom groups, and the natural tensor identifications from Section P1.3 of the *Preparatory Notes*. In each displayed image below we retain both endpoint zeros so that any failure of exactness is visible. An arrow between zero groups is the zero map.

Example 3.18 (1. The functor $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}, -)$). The image of $(*)$ is

$$0 \rightarrow \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \xrightarrow{q} C \rightarrow 0.$$

Postcomposition sends $f(1) = a$ to na and then to $\bar{a}$. Multiplication by n is injective, its image $n\mathbb{Z}$ is the kernel of q , and q is surjective. The entire sequence is exact; the fixed source $\mathbb{Z}$ is free and hence projective.

Example 3.19 (2. The functor $\text{Hom}_{\mathbb{Z}}(C, -)$). A map $C \rightarrow \mathbb{Z}$ is zero, since the image of $\bar{1}$ must be annihilated by n . Evaluation identifies $\text{Hom}_{\mathbb{Z}}(C, C)$ with C . Thus the image sequence is

$$0 \rightarrow 0 \xrightarrow{0} 0 \xrightarrow{0} C \rightarrow 0.$$

It is exact at both zero Hom groups, but not at the final C : the incoming image is zero and the outgoing kernel is all of C . Removing the terminal zero leaves precisely the valid left exact sequence. The identity of C cannot lift along q , because every map $C \rightarrow \mathbb{Z}$ is zero. This exhibits the nonprojectivity of C over $\mathbb{Z}$ and the associated failure of right exactness.

Example 3.20 (3. The functor $\text{Hom}_{\mathbb{Z}}(-, \mathbb{Z})$). Reversing the arrows gives

$$0 \longrightarrow 0 \xrightarrow{0} \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \longrightarrow 0.$$

Indeed, $\text{Hom}_{\mathbb{Z}}(C, \mathbb{Z}) = 0$, and precomposition sends a map f with $f(1) = a$ to the map with value $f(n) = na$ at 1. The first map is injective, and its zero image equals the kernel of multiplication by n . Exactness fails only at the final $\mathbb{Z}$, since the incoming image is $n\mathbb{Z}$. Equivalently, the map $n\mathbb{Z} \rightarrow \mathbb{Z}$, $nk \mapsto k$, cannot extend to $\mathbb{Z}$: an extension would require $n\hat{f}(1) = 1$. Thus $\mathbb{Z}$ is not injective, despite being projective.

Example 3.21 (4. The functor $\text{Hom}_{\mathbb{Z}}(-, C)$). The image sequence is

$$0 \longrightarrow C \xrightarrow{\text{id}} C \xrightarrow{0} C \longrightarrow 0.$$

For $f : C \rightarrow C$, precomposition with q retains its value at the generator, so q^* is the identity in these coordinates. Precomposition with multiplication by n is zero because $nC = 0$. The first map is injective and its image is the kernel of the zero map. The last C is not exact: its incoming image is zero. The nonextendable map $n\mathbb{Z} \rightarrow C$, $nk \mapsto \bar{k}$, witnesses the failure of injectivity of C . Any extension would send n to n times an element of C , which is zero instead of $\bar{1}$.

Example 3.22 (5. The functor $\mathbb{Z} \otimes_{\mathbb{Z}} -$). The image is

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \xrightarrow{q} C \longrightarrow 0.$$

The identification $\mathbb{Z} \otimes A \rightarrow A$, $a \otimes b \mapsto ab$, takes $1 \otimes (\times n)$ to multiplication by n and $1 \otimes q$ to q . Thus the first map is injective, the middle kernel is $n\mathbb{Z}$, and the final map is surjective. All terms are exact; the fixed right module $\mathbb{Z}$ is free and flat.

Example 3.23 (6. The functor $C \otimes_{\mathbb{Z}} -$). The image is

$$0 \longrightarrow C \xrightarrow{0} C \xrightarrow{\text{id}} C \longrightarrow 0.$$

Under $C \otimes A \cong A/nA$, the two induced maps are multiplication by n , hence zero on C , and reduction modulo n , hence the identity on C . Exactness fails at the first C , whose outgoing kernel is all of C while its incoming image is zero. At the middle C , both image and kernel are zero, and the last map is surjective. Thus tensoring is right exact but loses the original injection; the fixed right module C is not flat.

Example 3.24 (7. The functor $- \otimes_{\mathbb{Z}} \mathbb{Z}$). The image is again

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \xrightarrow{q} C \longrightarrow 0.$$

This time the identifications are $A \otimes \mathbb{Z} \rightarrow A$, $a \otimes b \mapsto ba$, and the maps are $(\times n) \otimes 1$ and $q \otimes 1$. Their formulas are $a \mapsto na$ and $a \mapsto \bar{a}$, respectively. The sequence is exact at each position, as in case 5; the fixed left module $\mathbb{Z}$ is flat.

Example 3.25 (8. The functor $- \otimes_{\mathbb{Z}} C$). The image is

$$0 \longrightarrow C \xrightarrow{0} C \xrightarrow{\text{id}} C \longrightarrow 0.$$

Under $A \otimes C \cong A/nA$, $(\times n) \otimes 1$ is zero, and $q \otimes 1$ is the identity on C . Exactness fails at the first C and holds at the other two positions. The fixed left module C is not flat. Cases 6 and 8 agree over $\mathbb{Z}$, but over a general noncommutative ring the two fixed modules have different sides.

Example 3.26 (Different moduli in the source and coefficients). Apply $\text{Hom}_{\mathbb{Z}}(-, \mathbb{Z}/6\mathbb{Z})$ to $0 \rightarrow \mathbb{Z} \xrightarrow{4} \mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z} \rightarrow 0$. Using the Hom calculation from Section 1.1, the valid left exact sequence is

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\bar{a} \mapsto \overline{3a}} \mathbb{Z}/6\mathbb{Z} \xrightarrow{\times 4} \mathbb{Z}/6\mathbb{Z}.$$

The first image is $\{\bar{0}, \bar{3}\}$, exactly the kernel of multiplication by 4. The final image is $\{\bar{0}, \bar{2}, \bar{4}\}$, so a terminal zero cannot be added. Tensoring the same original sequence with $\mathbb{Z}/6\mathbb{Z}$ instead gives the right exact sequence

$$\mathbb{Z}/6\mathbb{Z} \xrightarrow{\times 4} \mathbb{Z}/6\mathbb{Z} \xrightarrow{\text{mod } 2} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0.$$

The middle kernel equals the preceding image $\{\bar{0}, \bar{2}, \bar{4}\}$ and the final map is onto. Here an initial zero cannot be added because multiplication by 4 has the nonzero kernel $\{\bar{0}, \bar{3}\}$. Hom detects the kernel of the relation map; tensor product forms its cokernel. Their abstract answers happen to be isomorphic in this example.

These computations locate the missing information precisely: Hom can lose surjectivity at the right end of its induced sequence, and tensor product can lose injectivity at the left end. Nevertheless all eight functors preserve every isomorphism. The derived functors defined above retain the new homology created by these failures of exactness.

3.3 Tor, Ext, and equivalent computations

Definition 3.27 (Tor). For a right R -module N and a left R -module M , set

$$\text{Tor}_j^R(N, M) = L_j(N \otimes_R -)(M) = H_j(N \otimes_R P_\bullet),$$

where $P_\bullet \rightarrow M$ is a projective resolution of left modules. Thus $\text{Tor}_0^R(N, M) \cong N \otimes_R M$.

Example 3.28 (Tensoring with the regular module has no higher terms). The left regular module ${}_R R$ is free, hence projective. Its length-zero resolution has $P_0 = R$, augmentation id_R , and $P_j = 0$ for $j > 0$. After removing the augmentation and tensoring with a right module N , only $N \otimes_R R$ in degree zero remains. Consequently

$$\text{Tor}_0^R(N, R) \cong N, \quad \text{Tor}_j^R(N, R) = 0 \quad (j > 0).$$

The degree-zero isomorphism is $n \otimes r \mapsto nr$, with inverse $n \mapsto n \otimes 1$. Balancing gives $nr \otimes 1 = n \otimes r$, so the formulas are inverse. This is the earlier length-zero vanishing argument applied to the tensor functor, over an arbitrary unital ring and with the module sides specified.

The following double-complex lemma is the additional tool used in the two balancing arguments below. In our convention, a *double chain complex* is a grid $D_{p,q}$ with commuting maps $d_h : D_{p,q} \rightarrow D_{p-1,q}$ and $d_v : D_{p,q} \rightarrow D_{p,q-1}$, each squaring to zero. Its *total complex* has $\text{Tot}_j D = \bigoplus_{p+q=j} D_{p,q}$ and differential $d_h + (-1)^p d_v$ on $D_{p,q}$. The sign cancels the two mixed terms in its square. For a double cochain complex both maps raise their respective degrees, and the same sign convention applies.

Lemma 3.29 (First-quadrant collapse). *Let D be a double chain complex of abelian groups concentrated in bidegrees (p, q) with $p, q \geq 0$, and form its total complex using the signed sum of the two differentials. Suppose that homology in one direction vanishes outside degree zero. The surviving degree-zero groups, with differential induced by the other direction, form a complex E . There is then a natural isomorphism $H_j(\text{Tot } D) \cong H_j(E)$. The analogous statement holds for double cochain complexes and cohomology.*

Proof. Suppose first that vertical cohomology of a double cochain complex is concentrated in degree zero. Put $E^p = \ker(d_v : D^{p,0} \rightarrow D^{p,1})$. These kernels form a horizontal cochain complex, embedded in $\text{Tot } D$ along $q = 0$. The quotient double complex K has $K^{p,0} = D^{p,0}/E^p$ and $K^{p,q} = D^{p,q}$ for $q > 0$. Every vertical column of K is exact, including its degree-zero term. There is a short exact sequence of total complexes

$$0 \longrightarrow E \longrightarrow \text{Tot } D \longrightarrow \text{Tot } K \longrightarrow 0.$$

We prove that the last complex is acyclic by a finite elimination. For a degree- n cocycle z , its component in $(0, n)$ is vertically closed. If $n > 0$, vertical exactness writes it as $d_v w$ for an element in $(0, n-1)$. Subtracting the total coboundary of w removes that component, and changes only the next component in $(1, n-1)$. The cocycle equation now makes that next component vertically closed. Repeat with $(p, n-p)$, inserting the factor $(-1)^p$ when taking a vertical preimage to match the total sign. At the final component $(n, 0)$, vertical closedness forces it to be zero because the column is exact at its initial term. When $n = 0$ this last argument applies immediately. Thus every cocycle is a coboundary. The long exact sequence then makes $E \rightarrow \text{Tot } D$ an isomorphism on cohomology.

For a double chain complex, instead put $E_p = D_{p,0}/\text{im}(d_v : D_{p,1} \rightarrow D_{p,0})$. There is a surjection $\text{Tot } D \rightarrow E$ whose kernel double complex has exact vertical columns: at $q = 0$ its term is $\text{im } d_v$, and in positive vertical degrees its terms are those of D . For a cycle of total degree n in this kernel, start at $(n, 0)$ and subtract a total boundary from $(n, 1)$ to remove it. This changes only $(n-1, 1)$. The cycle equation makes the latter vertically closed; remove it by a vertical preimage, with the total sign, and continue down to column zero. After finitely many steps no component remains. The kernel total complex is therefore acyclic, and the long exact sequence gives $H_j(\text{Tot } D) \cong H_j(E)$.

If horizontal rather than vertical homology is concentrated in zero, interchange the two coordinates; the sign correction $(-1)^{pq}$ identifies the two total-differential conventions. All edge maps used above are induced by kernels or quotients and commute with maps of double complexes, so the isomorphisms are natural. The first-quadrant condition is what makes each elimination finite. $\square$

Theorem 3.30 (Balanced computation of Tor). *If $Q_\bullet \rightarrow N$ is a projective resolution of right modules, then*

$$H_j(N \otimes_R P_\bullet) \cong H_j(Q_\bullet \otimes_R M)$$

naturally in N and M . Tor is covariant in both variables.

Proof. Projective modules are flat by the proof in Section 3.2. Consider the first-quadrant double complex $Q_p \otimes_R P_q$. Its total complex has degree- j term $\bigoplus_{p+q=j} Q_p \otimes_R P_q$ and differential $d_Q \otimes 1 + (-1)^p 1 \otimes d_P$ on bidegree (p, q) . For each fixed q , tensoring the augmented resolution $Q_\bullet \rightarrow N$ with the flat left module P_q is exact. Hence its unaugmented horizontal homology is zero for $p > 0$ and is $N \otimes_R P_q$ for $p = 0$. The induced remaining differential is $1 \otimes d_P$. The augmentation of Q defines an actual map

$$\text{Tot}(Q_\bullet \otimes_R P_\bullet) \longrightarrow N \otimes_R P_\bullet :$$

use $\varepsilon_Q \otimes 1$ on the summands with $p = 0$, and zero on those with $p > 0$. The augmentation equation makes this a chain map, and Lemma 3.29 says that it induces an isomorphism on homology.

Similarly, for fixed p , flatness of the right module Q_p makes the vertical homology vanish for $q > 0$ and identifies the degree-zero vertical homology with $Q_p \otimes_R M$. The map from the total complex to $Q_\bullet \otimes_R M$, given by $1 \otimes \varepsilon_P$ on $q = 0$ and zero elsewhere, likewise induces an isomorphism. Comparing through total homology gives the stated isomorphism.

For maps in either module variable, lift to their projective resolutions. Tensoring the lifts gives a map of double complexes commuting with both augmentations. The two homology isomorphisms are therefore natural. Different lifts are homotopic and give the same maps, by the canonical comparison already proved. $\square$

Balancing permits resolving either variable, while the first argument remains a right module and the second a left module.

Definition 3.31 (Ext). For left R -modules M, N , set

$$\mathrm{Ext}_R^j(M, N) = R^j \mathrm{Hom}_R(M, -)(N) = H^j(\mathrm{Hom}_R(M, I^\bullet)),$$

using an injective resolution $N \rightarrow I^\bullet$ of the second variable. The degree- j differential sends $f : M \rightarrow I^j$ to $d_I^j \circ f$. In degree zero the preceding recovery theorem gives $\mathrm{Ext}_R^0(M, N) \cong \mathrm{Hom}_R(M, N)$.

This is a right derived functor in the second variable, where Hom is covariant and left exact. Its computation from a projective resolution of the first variable is an additional theorem, not permission to interchange the two arguments.

Theorem 3.32 (The two computations of Ext). *For a projective resolution $P_\bullet \rightarrow M$ and an injective resolution $N \rightarrow I^\bullet$, there are natural isomorphisms*

$$\begin{aligned} \mathrm{Ext}_R^j(M, N) &= H^j(\mathrm{Hom}_R(M, I^\bullet)) \\ &\cong H^j(\mathrm{Hom}_R(P_\bullet, N)). \end{aligned}$$

In the last cochain complex, degree j is $\mathrm{Hom}_R(P_j, N)$ and the differential is $f \mapsto f \circ d_{j+1}$. Ext is contravariant in M and covariant in N .

Proof. Use the first-quadrant double cochain complex $D^{p,q} = \mathrm{Hom}_R(P_p, I^q)$. Its horizontal differential is composition with d_{p+1} , and its vertical differential is composition with the differential of $I^\bullet$. They commute; inserting $(-1)^p$ before the vertical differential makes their sum square to zero. Since P_p is projective, $\mathrm{Hom}_R(P_p, -)$ is exact. Applying it to the entire augmented injective resolution is legitimate by Section P3.1 of the *Preparatory Notes*. Thus vertical cohomology is zero for $q > 0$; at $q = 0$ its kernel consists precisely of maps factoring through $N \hookrightarrow I^0$, and is $\mathrm{Hom}_R(P_p, N)$. The horizontal differential on these kernels is precomposition with d_P , exactly the differential of $\mathrm{Hom}_R(P_\bullet, N)$.

In the other direction, injectivity of I^q makes the contravariant functor $\mathrm{Hom}_R(-, I^q)$ exact. Applied to the augmented projective resolution, it gives an exact sequence

$$0 \rightarrow \mathrm{Hom}_R(M, I^q) \rightarrow \mathrm{Hom}_R(P_0, I^q) \rightarrow \mathrm{Hom}_R(P_1, I^q) \rightarrow \cdots$$

Hence horizontal cohomology vanishes for $p > 0$, while its degree-zero kernel is $\mathrm{Hom}_R(M, I^q)$. The vertical differential on these kernels is postcomposition with d_I .

More concretely, the augmentation and coaugmentation define maps

$$\begin{aligned} \mathrm{Hom}_R(P_\bullet, N) &\longrightarrow \mathrm{Tot } D, \\ \mathrm{Hom}_R(M, I^\bullet) &\longrightarrow \mathrm{Tot } D. \end{aligned}$$

The first places $P_p \rightarrow N \rightarrow I^0$ in bidegree $(p, 0)$; the second places $P_0 \rightarrow M \rightarrow I^q$ in bidegree $(0, q)$. Each is a cochain map: its differential in the other direction is zero by the augmentation equations. By Lemma 3.29, both maps induce isomorphisms on cohomology. Composing one with the inverse of the other proves the displayed equivalence of computations.

A map $M' \rightarrow M$ is lifted to a map of projective resolutions and then used by precomposition; a map $N \rightarrow N'$ is extended to injective resolutions and used by postcomposition. These operations give maps of double complexes commuting with the two displayed maps. They prove naturality in both variables, with exactly the stated variance. Homotopy uniqueness makes the resulting maps independent of every comparison choice. $\square$

This theorem identifies the projective computation with the right derived functor in the second variable. One resolves the *first* variable projectively or the *second* variable injectively. In particular,

$$\mathrm{Ext}_R^j(P, N) = 0 = \mathrm{Ext}_R^j(M, I) \quad (j > 0)$$

when P is projective and I injective. Projectivity of the *second* variable alone gives no such conclusion.

One resolution, four calculations

For $n \geq 2$ and an abelian group A , reuse the resolution $0 \rightarrow \mathbb{Z} \xrightarrow{n} \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow 0$. By the balancing theorem, tensoring its unaugmented complex with A computes $\mathrm{Tor}_*^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$:

$$0 \longrightarrow \underset{\text{degree } 1}{A} \xrightarrow{n} \underset{\text{degree } 0}{A} \longrightarrow 0.$$

Applying $\mathrm{Hom}_{\mathbb{Z}}(-, A)$ gives instead

$$0 \longrightarrow \underset{\text{degree } 0}{A} \xrightarrow{n} \underset{\text{degree } 1}{A} \longrightarrow 0.$$

Taking kernels and cokernels in the indicated degrees gives

	degree 0	degree 1
$\mathrm{Tor}_*^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$	A/nA	$A[n]$
$\mathrm{Ext}_*^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$	$A[n]$	A/nA

and both groups vanish in every degree $j \geq 2$. All these identifications are natural in A . In particular, $\mathrm{Ext}_{\mathbb{Z}}^1(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$, although its second argument is free. The identical multiplication map produces different answers in degree one because chain and cochain degrees run in opposite directions.

Remark (The position of a projective module in Ext matters). For $n \geq 2$, the two orders give

$$\mathrm{Ext}_{\mathbb{Z}}^1(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}, \quad \mathrm{Ext}_{\mathbb{Z}}^1(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = 0.$$

The first group was just computed; the second uses the length-zero projective resolution of the first argument $\mathbb{Z}$. Thus projectivity of the first argument forces higher Ext to vanish. Projectivity of the second argument does not, as the first displayed group shows. The sufficient condition on the second argument is injectivity.

Example 3.33 (Finite cyclic inputs: a kernel and a quotient). Let $m, n \geq 2$ and put $d = \mathrm{gcd}(m, n)$. The preceding two-term calculation, using the resolution of $\mathbb{Z}/m\mathbb{Z}$, gives

$$\begin{aligned} \mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) &\cong \ker(\times m : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}), \\ \mathrm{Ext}_{\mathbb{Z}}^1(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) &\cong (\mathbb{Z}/n\mathbb{Z})/m(\mathbb{Z}/n\mathbb{Z}). \end{aligned}$$

Write $m = dm'$ and $n = dn'$ with $\mathrm{gcd}(m', n') = 1$. The condition $m\bar{a} = 0$ is equivalent to $n \mid ma$, hence to $n' \mid a$. The kernel is therefore generated by $\overline{n/d}$, of order d ; explicitly,

$$\mathbb{Z}/d\mathbb{Z} \xrightarrow{\cong} \ker(\times m), \quad \bar{k} \mapsto \overline{k(n/d)}.$$

Bézout's identity gives $m(\mathbb{Z}/n\mathbb{Z}) = d(\mathbb{Z}/n\mathbb{Z})$: one inclusion follows from $d \mid m$, and integers u, v with $d = um + vn$ give the reverse inclusion modulo n . Reduction modulo d consequently identifies the quotient with $\mathbb{Z}/d\mathbb{Z}$. Thus both groups are abstractly cyclic of order d , but Tor is obtained as a subgroup and Ext as a quotient. For example, when $m = 4, n = 6$, the kernel is $\{\bar{0}, \bar{3}\}$, while the subgroup divided out is $\{\bar{0}, \bar{2}, \bar{4}\}$. Their isomorphism types agree; their places in the calculation differ.

Example 3.34 (Injective coefficients can have nonzero Hom and Tor). Fix $n \geq 2$. Apply the same formulas to the injective abelian groups $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$:

A	$\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$	$\text{Ext}_{\mathbb{Z}}^1(\mathbb{Z}/n\mathbb{Z}, A)$	$\text{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$
$\mathbb{Q}$	0	0	0
$\mathbb{Q}/\mathbb{Z}$	$\mathbb{Z}/n\mathbb{Z}$	0	$\mathbb{Z}/n\mathbb{Z}$

Entries indicate the groups up to the displayed natural cyclic identifications. Indeed, $\mathbb{Q}[n] = 0$ and $n\mathbb{Q} = \mathbb{Q}$. On the other hand,

$$(\mathbb{Q}/\mathbb{Z})[n] = \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}, \quad n(\mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}.$$

The cyclic isomorphism sends $\bar{k}$ to $k/n + \mathbb{Z}$. The two Ext entries vanish because the quotients A/nA are zero; equivalently, both second arguments are injective over $\mathbb{Z}$. Injectivity in this position forces all positive Ext groups to vanish, but it imposes no such vanishing on degree-zero Hom or on Tor . The second row exhibits both distinctions explicitly.

Two complete calculations from injective resolutions

Fix $n \geq 2$ and let $G(B) = \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, B)$. Evaluation at $\bar{1}$ identifies $G(B)$ naturally with $B[n] = \{b \in B : nb = 0\}$. Indeed, such an image determines the map $\bar{a} \mapsto ab$, and every $b \in B[n]$ gives a well-defined map. A homomorphism $B \rightarrow C$ takes this torsion subgroup to $C[n]$, so its action under G is the restriction of the original map. We are deriving the operation of taking n -torsion.

For $B = \mathbb{Z}$, use the injective resolution already constructed in (1):

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

After removing $\mathbb{Z}$ and applying G , the cochain complex is

$$\underbrace{0}_{\text{degree } 0} \longrightarrow \underbrace{\mathbb{Z}/n\mathbb{Z}}_{\text{degree } 1} \longrightarrow 0.$$

Here $\mathbb{Q}[n] = 0$, whereas $(\mathbb{Q}/\mathbb{Z})[n]$ is generated by $1/n + \mathbb{Z}$ and has order n . Thus

$$\text{Ext}_{\mathbb{Z}}^j(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \cong \begin{cases} 0, & j = 0, \\ \mathbb{Z}/n\mathbb{Z}, & j = 1, \\ 0, & j \geq 2. \end{cases}$$

The nonzero degree-one group records a lost surjection: the map $\mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z}$ is onto, but its restriction to n -torsion is the zero map from zero to a nonzero group.

For $B = \mathbb{Z}/m\mathbb{Z}$, use (2), where the initial map sends $\bar{a}$ to $a/m + \mathbb{Z}$:

$$0 \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Q}/\mathbb{Z} \xrightarrow{\times m} \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

Both injective terms have n -torsion identified with $\mathbb{Z}/n\mathbb{Z}$ by $\bar{a} \mapsto a/n + \mathbb{Z}$. Postcomposition with multiplication by m sends this element to $ma/n + \mathbb{Z}$. The induced complex is therefore exactly

$$\underbrace{\mathbb{Z}/n\mathbb{Z}}_{\text{degree 0}} \xrightarrow{\times m} \underbrace{\mathbb{Z}/n\mathbb{Z}}_{\text{degree 1}} \longrightarrow 0.$$

Put $d = \gcd(n, m)$. The kernel of multiplication by m is generated by $\overline{n/d}$ and has order d , since $n \mid ma$ is equivalent to $(n/d) \mid a$. Its image is $d(\mathbb{Z}/n\mathbb{Z})$, by Bézout's identity, so the cokernel is also cyclic of order d . Consequently

$$\text{Ext}_{\mathbb{Z}}^j(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \begin{cases} \mathbb{Z}/d\mathbb{Z}, & j = 0, 1, \\ 0, & j \geq 2. \end{cases}$$

These are two abstractly isomorphic groups arising in different positions: degree zero is a kernel, and degree one is a cokernel. The fact that their final isomorphism types agree does not allow the two steps of the calculation to be exchanged.

Example 3.35 (Checking both orders of the moduli 4 and 6). For $n = 4, m = 6$, the injective computation is $\mathbb{Z}/4\mathbb{Z} \xrightarrow{\times 6} \mathbb{Z}/4\mathbb{Z}$, which is multiplication by 2. Its kernel and image are both $\{\bar{0}, \bar{2}\}$, so its kernel and cokernel are each $\mathbb{Z}/2\mathbb{Z}$. The projective computation of the same Ext groups uses $\mathbb{Z}/6\mathbb{Z} \xrightarrow{\times 4} \mathbb{Z}/6\mathbb{Z}$: its kernel is $\{\bar{0}, \bar{3}\}$ and its image is $\{\bar{0}, \bar{2}, \bar{4}\}$, again yielding $\mathbb{Z}/2\mathbb{Z}$ in degrees zero and one. For $n = 6, m = 4$, the injective computation itself is this latter map on $\mathbb{Z}/6\mathbb{Z}$. These calculations display the actual differentials behind both methods and both choices of input.

A first interpretation of an Ext class

For $0 \rightarrow K \xrightarrow{j} P_0 \rightarrow M \rightarrow 0$ with P_0 projective, the projective Hom complex gives

$$\text{Ext}_R^1(M, N) \cong \frac{\text{Hom}_R(K, N)}{\{h \circ j : h \in \text{Hom}_R(P_0, N)\}}.$$

Indeed, extend $P_0 \rightarrow M$ to a projective resolution, writing $d_1 = j\pi$ with $\pi : P_1 \twoheadrightarrow K$. A degree-one cocycle $f : P_1 \rightarrow N$ satisfies $fd_2 = 0$; since $\ker \pi = \text{im } d_2$, it factors uniquely as $f = \bar{f}\pi$ for $\bar{f} : K \rightarrow N$. A degree-one coboundary is $hd_1 = (hj)\pi$. Taking the quotient gives the displayed formula without using a long exact sequence. Thus degree one records maps on relations that cannot be extended to the chosen projective generators.

It also classifies module extensions $0 \rightarrow N \rightarrow E \rightarrow M \rightarrow 0$, where equivalence means an isomorphism of the short exact sequences acting identically on the specified endpoints. To see the link, lift $P_0 \rightarrow M$ to $P_0 \rightarrow E$ and restrict to K . The resulting map $K \rightarrow N$ is determined modulo restrictions of maps $P_0 \rightarrow N$. Conversely, $f : K \rightarrow N$ gives the extension with middle module

$$E_f = (N \oplus P_0) / \{(-f(k), j(k)) : k \in K\}.$$

The map $n \mapsto [(n, 0)]$ is injective, and $[(n, p)] \mapsto \bar{p}$ has kernel exactly its image. These constructions are inverse on equivalence classes; the zero class corresponds to the split extension with middle module $N \oplus M$.

For an extension $0 \rightarrow A \xrightarrow{i} E \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow 0$, choosing a lift e of $\bar{1}$ gives $ne = i(a)$ for some $a \in A$. Replacing e by $e + i(b)$ changes a to $a + nb$. The invariant is therefore $[a] \in A/nA$, exactly the Ext group above. For example, the nonzero class in $\text{Ext}_{\mathbb{Z}}^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$ is represented by $0 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$.

Example 3.36 (The two extensions with integral kernel and quotient of order two). Consider extensions of abelian groups $0 \rightarrow \mathbb{Z} \xrightarrow{i} E \xrightarrow{q} \mathbb{Z}/2\mathbb{Z} \rightarrow 0$, with equivalences required to act identically on both endpoints. Choose $e \in E$ with $q(e) = \bar{1}$. There is a unique integer b such that $2e = i(b)$. Replacing e by $e + i(c)$ replaces b by $b + 2c$. The preceding classification therefore gives exactly two extension classes, indexed by $\mathbb{Z}/2\mathbb{Z}$.

For a representative b , their concrete models are

$$E_b = (\mathbb{Z} \oplus \mathbb{Z}) / \langle (-b, 2) \rangle, \quad i_b(a) = [(a, 0)], \quad q_b([(a, k)]) = \bar{k}.$$

The relation is exactly $2[(0, 1)] = [(b, 0)]$. Every extension above is equivalent to its model through the map $[(a, k)] \mapsto i(a) + ke$. It is well defined by $2e = i(b)$, and surjective since subtracting a suitable multiple of e puts any element in $i(\mathbb{Z})$. If $i(a) + ke = 0$, applying q gives $k = 2t$, and injectivity of i then gives $a = -bt$. Thus $(a, k) = t(-b, 2)$, proving injectivity of the model map.

For $b = 0$, the model is $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and the extension is

$$0 \rightarrow \mathbb{Z} \xrightarrow{i_0} \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \xrightarrow{q_0} \mathbb{Z}/2\mathbb{Z} \rightarrow 0.$$

Here $i_0(a) = (a, \bar{0})$ and $q_0(a, \bar{k}) = \bar{k}$. It splits by $\bar{k} \mapsto (0, \bar{k})$. For $b = 1$, the map

$$E_1 \rightarrow \mathbb{Z}, \quad [(a, k)] \mapsto 2a + k$$

is an isomorphism: it kills $(-1, 2)$, is surjective, and its kernel before passage to the quotient consists precisely of multiples of $(-1, 2)$. Under this isomorphism the extension becomes

$$0 \rightarrow \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \xrightarrow{\text{mod } 2} \mathbb{Z}/2\mathbb{Z} \rightarrow 0.$$

It cannot split, since any homomorphism $\mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}$ is zero. In particular, the nonzero class has middle group $\mathbb{Z}$ with inclusion $a \mapsto 2a$, whereas the zero class has middle group $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ with inclusion $a \mapsto (a, \bar{0})$. The specified maps are part of the extension being classified.

Long exact sequences in the two variables

For a fixed right R -module N , the Tor sequence in the left module variable ends in

$$\begin{aligned} \text{Tor}_1^R(N, A) &\rightarrow \text{Tor}_1^R(N, A'') \xrightarrow{\partial} N \otimes_R A' \\ &\rightarrow N \otimes_R A \rightarrow N \otimes_R A'' \rightarrow 0. \end{aligned}$$

For a fixed left module M , the Ext sequence in the second variable begins

$$\begin{aligned} 0 &\rightarrow \text{Hom}_R(M, A') \rightarrow \text{Hom}_R(M, A) \rightarrow \text{Hom}_R(M, A'') \\ &\xrightarrow{\delta} \text{Ext}_R^1(M, A') \rightarrow \dots \end{aligned}$$

The balancing results for Tor and Ext allow the same argument in the other variable. Tor is covariant in both variables. For Ext, the first variable is contravariant, so its sequence reverses the original order:

$$\begin{aligned} \dots &\rightarrow \text{Ext}_R^j(A'', N) \rightarrow \text{Ext}_R^j(A, N) \rightarrow \text{Ext}_R^j(A', N) \\ &\rightarrow \text{Ext}_R^{j+1}(A'', N) \rightarrow \dots \end{aligned}$$

For this displayed Ext sequence, N, A', A, A'' are left modules; the symbol N is no longer the fixed right module of the preceding Tor sequence. One may prove the sequence by fixing an injective resolution of N and applying $\text{Hom}_R(-, I^n)$, which is exact, to the short exact sequence in each degree.

Dimension shifting

If $0 \rightarrow K \rightarrow P \rightarrow M \rightarrow 0$ is exact with P projective, the higher Tor and Ext groups contributed by P vanish. The adjacent portions of the long exact sequences consequently give

$$\begin{aligned}\mathrm{Tor}_j^R(N, M) &\cong \mathrm{Tor}_{j-1}^R(N, K) & (j \geq 2), \\ \mathrm{Ext}_R^{j+1}(M, B) &\cong \mathrm{Ext}_R^j(K, B) & (j \geq 1).\end{aligned}$$

Here N is a right module and B is a left module. Successive kernels in a projective resolution therefore turn a higher-degree problem into a lower-degree one. The stated ranges matter: degree-zero tensor products and Hom groups need not vanish on projective modules.

Dually, from $0 \rightarrow B \rightarrow I \rightarrow Q \rightarrow 0$ with I injective we obtain

$$\mathrm{Ext}_R^{j+1}(M, B) \cong \mathrm{Ext}_R^j(M, Q) \quad (j \geq 1).$$

These are connecting-map isomorphisms, so they are compatible with maps of the short exact sequences from which they were obtained.

An Ext connecting map is a lifting obstruction

Take $0 \rightarrow A' \xrightarrow{i} A \xrightarrow{p} A'' \rightarrow 0$ and a map $f : M \rightarrow A''$. Form the pullback module

$$E_f = \{(m, a) \in M \oplus A : f(m) = p(a)\}.$$

It lies in the short exact sequence

$$0 \longrightarrow A' \xrightarrow{a' \mapsto (0, i(a'))} E_f \xrightarrow{(m, a) \mapsto m} M \longrightarrow 0.$$

Projection is surjective because p is surjective, and its kernel is precisely the displayed copy of A' . Under the extension interpretation of $\mathrm{Ext}_R^1(M, A')$, its class is

$$\delta(f) \in \mathrm{Ext}_R^1(M, A').$$

This also follows directly from the connecting construction. Take a projective resolution $P_\bullet \xrightarrow{\varepsilon} M$. The degree-zero cocycle representing f is $f\varepsilon$. Lift it to $t : P_0 \rightarrow A$ using projectivity of P_0 ; then td_1 has image in $i(A')$ and defines the degree-one cocycle representing $\delta(f)$. The lift

$$P_0 \longrightarrow E_f, \quad x \longmapsto (\varepsilon(x), t(x))$$

restricts on $\ker \varepsilon$ to exactly this map into A' . The presentation description of extension classes therefore identifies the two classes, with the positive connecting-map convention used above.

A section of $E_f \rightarrow M$ has the form $m \mapsto (m, \tilde{f}(m))$, where $\tilde{f} : M \rightarrow A$ is linear and $p\tilde{f} = f$. Hence the extension splits, or equivalently $\delta(f) = 0$, precisely when f lifts to A . This makes the exactness statement at $\mathrm{Hom}_R(M, A'')$ concrete.

Example 3.37 (A torsion element that cannot be lifted). Specialize to the first quotient of an injective resolution, $0 \rightarrow A \xrightarrow{i_0} I^0 \xrightarrow{q_0} A_1 \rightarrow 0$, and take $G = \mathrm{Hom}_R(M, -)$. The direct quotient formula from the first subsection says that the obstruction to lifting $\beta : M \rightarrow A_1$ is its class in

$$\mathrm{Ext}_R^1(M, A) \cong \mathrm{Hom}_R(M, A_1) / \{q_0 h : h \in \mathrm{Hom}_R(M, I^0)\}.$$

The pullback, with its two coordinates in the opposite order from the preceding general construction, is

$$E_\beta = \{(i, m) \in I^0 \oplus M : q_0(i) = \beta(m)\}.$$

Its injection is $a \mapsto (\iota_0(a), 0)$ and its projection is $(i, m) \mapsto m$. A section is exactly a map $m \mapsto (h(m), m)$ with $q_0 h = \beta$. Thus this is a lifting problem through a surjection, even though injective modules were used to set up its computation; it is distinct from extending a map from a submodule into a fixed injective target.

Now put $A = \mathbb{Z}$, $I^0 = \mathbb{Q}$, $A_1 = \mathbb{Q}/\mathbb{Z}$, and $M = \mathbb{Z}/n\mathbb{Z}$. Define $\beta(\bar{a}) = a/n + \mathbb{Z}$. It cannot lift to a homomorphism $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Q}$, since the latter must vanish whereas β is nonzero. Its pullback has an explicit identification

$$\begin{aligned} E_\beta &\xrightarrow{\cong} \frac{1}{n}\mathbb{Z}, & (q, \bar{a}) &\mapsto q, \\ \frac{1}{n}\mathbb{Z} &\longrightarrow E_\beta, & b/n &\mapsto (b/n, \bar{b}). \end{aligned}$$

The defining equality $q + \mathbb{Z} = a/n + \mathbb{Z}$ proves that these maps are well defined and inverse. Multiplication by n then identifies $\frac{1}{n}\mathbb{Z}$ with $\mathbb{Z}$; under this identification the injection of A becomes multiplication by n . We recover

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0.$$

This is the nonzero generator found by the injective Ext calculation. It cannot split because every homomorphism $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}$ is zero.

Tor restores a kernel lost by tensor product

Apply the Tor sequence to $0 \rightarrow \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow 0$, for $n \geq 2$, with fixed first argument $N = \mathbb{Z}/n\mathbb{Z}$. Its relevant part is

$$\begin{aligned} 0 = \mathrm{Tor}_1^{\mathbb{Z}}(N, \mathbb{Z}) &\longrightarrow \mathrm{Tor}_1^{\mathbb{Z}}(N, \mathbb{Z}/n\mathbb{Z}) \xrightarrow{\partial} N \otimes_{\mathbb{Z}} \mathbb{Z} \\ &\xrightarrow{\times n} N \otimes_{\mathbb{Z}} \mathbb{Z}. \end{aligned}$$

The last map is zero, while the first Tor group is zero because $\mathbb{Z}$ is projective in its second argument. Exactness thus makes the connecting map an isomorphism

$$\mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}.$$

It supplies exactly the kernel that appears when tensoring turns the injective map $\mathbb{Z} \xrightarrow{n} \mathbb{Z}$ into the zero map on $\mathbb{Z}/n\mathbb{Z}$. A left or right derived functor does not arbitrarily repair an isolated arrow: its terms and connecting maps occur together in a natural long exact sequence.

Returning to group cohomology

For a group G , a left $\mathbb{Z}[G]$ -module is an abelian group with a compatible G -action. Its invariants satisfy the natural identification

$$A^G \cong \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A),$$

where $\mathbb{Z}$ has the trivial action: evaluate a homomorphism at 1, and recover it from an invariant element a by $k \mapsto ka$. The group-cohomology construction will therefore read

$$H^j(G, A) = R^j((-)^G)(A) = \mathrm{Ext}_{\mathbb{Z}[G]}^j(\mathbb{Z}, A).$$

By this definition the injective resolution is one of A over $\mathbb{Z}[G]$. A resolution that is injective only as a sequence of abelian groups cannot be substituted without checking the additional module structure and injectivity. The equivalent computation theorem allows us instead to resolve the trivial module $\mathbb{Z}$ projectively over $\mathbb{Z}[G]$, which is often the more accessible calculation.

Key point. Choose the relevant ring and variable, take a resolution, remove the augmentation, apply the functor, and compute kernels modulo images. Comparison homotopies make the result canonical; one-sided exactness recovers degree zero; higher classes measure the remaining failures, and the connecting maps identify concrete lifting obstructions.

4 Group Homology and Cohomology via Derived Functors

Fix a group G . A group acting on an abelian group gives us two natural constructions: select the elements fixed by the action, or impose relations that make the action trivial. We first describe these constructions and their exactness. Their derived functors will then define group cohomology and group homology.⁴

4.1 Group actions, invariants, and coinvariants

Group actions and the group ring

Definition 4.1. A *left G -module* is an abelian group M together with a homomorphism $G \rightarrow \text{Aut}_{\mathbf{Ab}}(M)$. Writing the action as gm , the conditions are

$$1m = m, \quad (gh)m = g(hm), \quad g(m + m') = gm + gm'.$$

A *G -module homomorphism* $f : M \rightarrow N$ is an additive map such that $f(gm) = gf(m)$ for every $g \in G$ and $m \in M$. We write $\mathbf{GMod}$ for the category of left G -modules and these homomorphisms.

In particular, a G -module is more than an arbitrary set with a G -action: its underlying set has an abelian-group structure, and every group element acts by an additive automorphism. The inverse of the action of g is the action of g^{-1} .

The *integral group ring* is

$$R = \mathbb{Z}[G] = \left\{ \sum_{g \in G} a_g g : a_g \in \mathbb{Z}, \quad a_g = 0 \text{ for all but finitely many } g \right\}.$$

Addition is coefficientwise, and multiplication extends the group law by distributivity:

$$\left(\sum_g a_g g \right) \left(\sum_h b_h h \right) = \sum_{g,h} a_g b_h (gh).$$

Its identity is $1e_G$, usually written 1, and each $g \in G$ is a unit of R . Finite support is part of the definition even when G is infinite. If G is noncommutative, R is noncommutative as well.

A G -module structure on M extends uniquely to a unital left R -module structure by the formula

$$\left(\sum_g a_g g \right) m = \sum_g a_g (gm).$$

Conversely, restricting a left R -module structure to the elements $g \in G$ gives a G -module structure. These operations undo one another: restriction recovers each gm , and additivity recovers the action of every finite sum in R . Moreover, an additive map is G -equivariant if and only if it is R -linear, since

$$f \left(\sum_g a_g (gm) \right) = \sum_g a_g f(gm).$$

Thus we may use *left G -module* and *left $\mathbb{Z}[G]$ -module* as two descriptions of the same data, including the maps between them. We will use module theory over R in this sense.

⁴The definitions and the identifications with Tor and Ext follow C. A. Weibel, *An Introduction to Homological Algebra*, Section 6.1, especially Exercise 6.1.1, Lemma 6.1.1, and Definition 6.1.2.

Trivial modules and the augmentation ideal

The *augmentation map* is

$$\varepsilon : R \longrightarrow \mathbb{Z}, \quad \varepsilon \left(\sum_g a_g g \right) = \sum_g a_g.$$

It is a surjective unital ring homomorphism: multiplication of two group-ring elements multiplies their sums of coefficients, and $\varepsilon(ne_G) = n$. Its kernel

$$I = \ker \varepsilon$$

is the *augmentation ideal*, a two-sided ideal of R . It is generated by the differences $g - 1$. Indeed, these differences belong to the kernel, and if $\sum_g a_g = 0$, then

$$\sum_g a_g g = \sum_g a_g (g - 1).$$

This also shows that they generate I as an abelian group. The augmentation induces an isomorphism of rings

$$R/I \xrightarrow{\sim} \mathbb{Z}, \quad r + I \longmapsto \varepsilon(r).$$

For an abelian group A , write $T(A)$ for A with the *trivial G -action*, $ga = a$. Its corresponding R -action is

$$ra = \varepsilon(r)a.$$

In particular, the trivial action does not say that every element of the group ring acts as the identity: an integer multiple of 1 still acts by the corresponding integer multiplication. A left R -module M has trivial G -action if and only if $IM = 0$, since this is equivalent to $(g - 1)m = 0$ for every g and m .

The module $\mathbb{Z}$ in the homology and cohomology formulas will always have this trivial action. The augmentation description gives

$$\mathbb{Z} \cong R/I$$

as a left R -module and also as a right R -module, with right action $kr = k\varepsilon(r)$. These side conventions will matter for tensor products. The trivial module $\mathbb{Z}$ and the regular module R with left multiplication are generally very different G -modules.

The two constructions and their universal properties

Definition 4.2. For a left G -module M , its *invariants* and *coinvariants* are

$$\begin{aligned} M^G &= \{m \in M : gm = m \text{ for every } g \in G\}, \\ M_G &= M / \langle gm - m : g \in G, m \in M \rangle. \end{aligned}$$

Here the brackets in the denominator mean the additive subgroup generated by all the indicated differences.

The augmentation ideal describes both constructions:

$$M^G = \{m \in M : Im = 0\}, \quad M_G = M/IM.$$

For the first formula, $Im = 0$ implies $(g - 1)m = 0$ for every g , and the converse follows because these elements generate I . For the second, every $gm - m$ belongs to IM , while the expression

$r = \sum_g a_g(g - 1)$ for $r \in I$ gives $rm = \sum_g a_g(gm - m)$. Thus the subgroup being divided out is exactly IM ; in particular, it is an R -submodule.

The action on M^G is trivial, and the quotient action on M_G is trivial. These constructions have the following universal properties.

Proposition 4.3. *The inclusion $j : T(M^G) \hookrightarrow M$ is universal for maps from trivial G -modules: every G -module map $T(A) \rightarrow M$ factors uniquely through j . The quotient $q : M \twoheadrightarrow T(M_G)$ is universal for maps to trivial G -modules: every G -module map $M \rightarrow T(A)$ factors uniquely through q .*

Proof. If $f : T(A) \rightarrow M$ is equivariant, then $gf(a) = f(ga) = f(a)$, so its image is in M^G . The only possible factorization is the same function with codomain restricted to M^G , and it is additive. Conversely, any additive map $A \rightarrow M^G$ is equivariant because both actions are trivial.

If $f : M \rightarrow T(A)$ is equivariant, then $f(gm - m) = gf(m) - f(m) = 0$. Thus $IM \subseteq \ker f$ and there is a unique additive map $\bar{f} : M_G \rightarrow A$ with $\bar{f}([m]) = f(m)$. This map is equivariant between the trivial modules. Conversely, composing any such map with q gives a G -module map from M . $\square$

In particular, $T(M^G)$ is the largest trivial submodule of M , and $T(M_G)$ is its universal trivial quotient. The factorizations give isomorphisms of abelian groups

$$\mathrm{Hom}_R(T(A), M) \cong \mathrm{Hom}_{\mathbf{Ab}}(A, M^G), \quad \mathrm{Hom}_R(M, T(A)) \cong \mathrm{Hom}_{\mathbf{Ab}}(M_G, A).$$

They commute with composition of maps in either variable. This is their naturality; no additional categorical machinery is required to use these universal properties.

Proposition 4.4 (Invariants are Hom; coinvariants are tensor). *There are natural isomorphisms*

$$\mathrm{Hom}_R(\mathbb{Z}, M) \cong M^G, \quad \mathbb{Z} \otimes_R M \cong M_G.$$

The first $\mathbb{Z}$ is a trivial left R -module; the second is a trivial right R -module.

Proof. Evaluation at 1 sends $f : \mathbb{Z} \rightarrow M$ to $f(1)$. Since $g1 = 1$, $gf(1) = f(g1) = f(1)$, so this element is invariant. Conversely, an invariant element m determines $f_m(k) = km$. This map is R -linear because $rm = \varepsilon(r)m$. The two constructions are inverse.

For coinvariants, define

$$\Phi : \mathbb{Z} \otimes_R M \longrightarrow M_G, \quad k \otimes m \longmapsto k[m].$$

This respects the balancing relation because $kr = k\varepsilon(r)$ and $[rm] = \varepsilon(r)[m]$. Its inverse is $[m] \mapsto 1 \otimes m$, which is well defined since

$$1 \otimes (gm - m) = (1g) \otimes m - 1 \otimes m = 0.$$

The identity $k \otimes m = 1 \otimes km$ verifies that the maps are inverse. Postcomposition in the Hom formula and the map $1 \otimes f$ in the tensor formula show that both identifications commute with every coefficient map $f : M \rightarrow N$. $\square$

Example 4.5 (Swapping two coordinates). Let $G = C_2 = \{1, s\}$ act on $M = \mathbb{Z}^2$ by $s(a, b) = (b, a)$. An invariant element satisfies $a = b$, so

$$M^G = \{(n, n) : n \in \mathbb{Z}\} \cong \mathbb{Z}, \quad (n, n) \longmapsto n.$$

Furthermore, $s(a, b) - (a, b) = (b - a, a - b)$, and every multiple of $(1, -1)$ occurs this way. Hence

$$M_G = \mathbb{Z}^2 / \mathbb{Z}(1, -1) \cong \mathbb{Z}, \quad [(a, b)] \mapsto a + b.$$

The sum map is surjective and has kernel $\mathbb{Z}(1, -1)$, which proves the second isomorphism. Although both groups are isomorphic to $\mathbb{Z}$, the canonical composite

$$M^G \hookrightarrow M \twoheadrightarrow M_G$$

becomes $\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}$ under these identifications. Thus the two constructions have different maps even in this simple case.

The quotient $M_G \cong \mathbb{Z}$ can be embedded equivariantly into M by $n \mapsto (n, n)$. Nevertheless, the prescribed quotient map $q : M \rightarrow M_G$ has no G -linear section: the image of any such section would consist of invariant elements, whose coordinate sums are all even, whereas q must send the section of 1 to 1. An abstract embedding of a quotient into a module is weaker than a section of its quotient map.

Remark (A quotient need not be realizable as a submodule). There need not even be an abstract embedding. For $G = C_2$, let $\mathbb{Z}_-$ be $\mathbb{Z}$ with $sm = -m$. Then

$$(\mathbb{Z}_-)^G = 0, \quad (\mathbb{Z}_-)_G = \mathbb{Z}/2\mathbb{Z}.$$

The latter cannot embed into $\mathbb{Z}_-$ even as an abelian group: $\mathbb{Z}$ has no nonzero element annihilated by 2. More generally, for a quotient $q : M \rightarrow M/N$, a module section s would give the specific direct-sum decomposition $M = N \oplus s(M/N)$. The existence of such a section is an additional splitting condition, not a property of quotients in general.

Example 4.6 (The regular module). Give $R = \mathbb{Z}[G]$ its left regular action. Since $IR = I$,

$$R_G = R/I \cong \mathbb{Z}.$$

To compute R^G , write $x = \sum_h a_h h$ with finite support. The coefficient of k in gx is $a_{g^{-1}k}$. Thus $gx = x$ for all g if and only if all coefficients a_h are equal, since left translation is transitive on G .

If G is finite, put $N_G = \sum_{g \in G} g \in R$. The invariant elements are exactly the integer multiples of this element:

$$R^G = \mathbb{Z}N_G \cong \mathbb{Z}.$$

If G is infinite, a constant family of coefficients has finite support only when every coefficient is zero, so $R^G = 0$. The expression $\sum_{g \in G} g$ is not a group-ring element in that case. For finite G , the canonical map $R^G \rightarrow R_G$ sends aN_G to $a|G|$, again distinguishing the two constructions.

4.2 The invariant and coinvariant functors and their exactness

The preceding constructions act on maps as well as on objects. For a G -module map $f : M \rightarrow N$, set

$$f^G : M^G \longrightarrow N^G, \quad m \mapsto f(m),$$

and

$$f_G : M_G \longrightarrow N_G, \quad [m] \mapsto [f(m)].$$

The first is well defined because $gf(m) = f(gm) = f(m)$ when m is invariant. The second is well defined because $f(gm - m) = gf(m) - f(m) \in IN$. Restrictions and induced quotient maps preserve identities and composition:

$$(h \circ f)^G = h^G \circ f^G, \quad (h \circ f)_G = h_G \circ f_G.$$

They also preserve addition of module homomorphisms. We therefore obtain two additive covariant functors

$$(-)^G, (-)_G : \mathbf{GMod} = R\text{-}\mathbf{Mod} \longrightarrow \mathbf{Ab},$$

where the equality indicates the two descriptions of modules already explained. The Hom and tensor identifications above are natural isomorphisms of these functors.

Proposition 4.7. *The invariant functor is left exact, and the coinvariant functor is right exact. More explicitly:*

- (i) *If $0 \rightarrow A \xrightarrow{u} B \xrightarrow{v} C$ is exact, then $0 \rightarrow A^G \xrightarrow{u^G} B^G \xrightarrow{v^G} C^G$ is exact.*
- (ii) *If $A \xrightarrow{u} B \xrightarrow{v} C \rightarrow 0$ is exact, then $A_G \xrightarrow{u_G} B_G \xrightarrow{v_G} C_G \rightarrow 0$ is exact.*

The first assertion does not require v to be surjective; the second does not require u to be injective.

Proof. These statements follow from left exactness of $\text{Hom}_R(\mathbb{Z}, -)$ and right exactness of $\mathbb{Z} \otimes_R -$. The direct proofs also explain what each construction does.

For invariants, u^G is injective because u is. If $b \in B^G$ and $v(b) = 0$, exactness gives a unique $a \in A$ with $u(a) = b$. For every $g \in G$,

$$u(ga - a) = gu(a) - u(a) = gb - b = 0.$$

Injectivity implies $ga = a$, so $a \in A^G$. This proves $\ker v^G = \text{im } u^G$.

For coinvariants, v_G is surjective because v is, and $v_G u_G = 0$. Suppose $[b] \in B_G$ maps to zero. Then $v(b) \in IC$, so for some finite collection $g_j \in G$ and $c_j \in C$,

$$v(b) = \sum_j (g_j c_j - c_j).$$

Choose $b_j \in B$ with $v(b_j) = c_j$. The element $b - \sum_j (g_j b_j - b_j)$ lies in $\ker v = \text{im } u$; write it as $u(a)$. Passing to coinvariants gives $[b] = [u(a)] = u_G([a])$. Thus $\ker v_G = \text{im } u_G$. $\square$

In particular, a short exact sequence of G -modules gives

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \quad \text{and} \quad A_G \longrightarrow B_G \longrightarrow C_G \longrightarrow 0.$$

Neither missing endpoint can be supplied in general.

Example 4.8 (One action exhibits both failures). Let $G = C_2 = \{1, s\}$ and let $\mathbb{Z}_-$ be the sign module. Reduction modulo 2 gives a short exact sequence of G -modules

$$0 \longrightarrow \mathbb{Z}_- \xrightarrow{\times 2} \mathbb{Z}_- \longrightarrow \mathbb{F}_2 \longrightarrow 0,$$

where the last action is trivial, since $-1 = 1$ modulo 2. Taking invariants gives

$$0 \longrightarrow 0 \longrightarrow 0 \longrightarrow \mathbb{F}_2.$$

The final map is not surjective: the invariant residue class of 1 has no invariant integer lift. Thus invariants do not preserve all surjections and are not right exact in general.

Taking coinvariants instead gives

$$\mathbb{F}_2 \xrightarrow{0} \mathbb{F}_2 \xrightarrow{\text{id}} \mathbb{F}_2 \longrightarrow 0.$$

The first map sends $[m]$ to $[2m] = 0$ and the second sends $[m]$ to the same residue class. The first map is not injective, although the original multiplication-by-2 map was. Thus coinvariants do not preserve all injections and are not left exact in general.

Key point. Selecting fixed elements and forcing the action to be trivial preserve opposite halves of exactness. Their failures provide the starting point for group cohomology and group homology.

4.3 Derived definitions, equivalent computations, and long exact sequences

The definitions derive in the coefficient variable

Definition 4.9 (Group homology and group cohomology). For a fixed group G , a left G -module M , and $n \geq 0$, define

$$\begin{aligned} H_n(G, M) &= L_n((-)_G)(M), \\ H^n(G, M) &= R^n((-)^G)(M). \end{aligned}$$

These are abelian groups, natural in the coefficient module M .

The functors being derived have source **GMod** and target **Ab**. We fix G and derive in the *coefficient variable*. The superscript in R^n denotes a right derived functor; this R is unrelated to the abbreviation $R = \mathbb{Z}[G]$.

For homology, choose a projective resolution of M by left R -modules,

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

Apply coinvariants to the *unaugmented* complex $P_\bullet$. The natural tensor description gives

$$H_n(G, M) = H_n((P_\bullet)_G) \cong H_n(\mathbb{Z} \otimes_R P_\bullet) = \mathrm{Tor}_n^R(\mathbb{Z}, M).$$

Here $\mathbb{Z}$ is a trivial right module. The differential in positive degree is $1 \otimes d_n$, and the differential out of degree zero is zero; the complex does not include M_G as an additional term.

For cohomology, choose an injective resolution by left R -modules,

$$0 \longrightarrow M \longrightarrow J^0 \longrightarrow J^1 \longrightarrow J^2 \longrightarrow \cdots.$$

Apply invariants to $J^\bullet$, omitting its augmentation term M . The natural Hom description gives

$$H^n(G, M) = H^n((J^\bullet)^G) \cong H^n(\mathrm{Hom}_R(\mathbb{Z}, J^\bullet)) = \mathrm{Ext}_R^n(\mathbb{Z}, M),$$

where $\mathbb{Z}$ is now a trivial left module. Resolution comparison ensures independence of the choices and gives the induced maps for every coefficient homomorphism $M \rightarrow N$. Consequently,

$$\begin{aligned} H_n(G, M) &\cong \mathrm{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, M), \\ H^n(G, M) &\cong \mathrm{Ext}_{\mathbb{Z}[G]}^n(\mathbb{Z}, M). \end{aligned}$$

The degree-zero identifications are

$$H_0(G, M) \cong M_G, \quad H^0(G, M) \cong M^G.$$

For instance, the regular-module calculations above already say $H_0(G, \mathbb{Z}[G]) \cong \mathbb{Z}$, while $H^0(G, \mathbb{Z}[G])$ is $\mathbb{Z}N_G$ for finite G and zero for infinite G .

Resolving the trivial module instead

The definitions resolve M , but the balance theorem for Tor and the projective–injective computation theorem for Ext allow a more convenient choice. We may resolve the trivial module $\mathbb{Z}$ once and use the same resolution for every coefficient module.

For homology, choose a projective resolution $Q_\bullet \rightarrow \mathbb{Z}$ in **Mod- R** . Then

$$H_n(G, M) \cong H_n(Q_\bullet \otimes_R M), \quad \partial_n = d_n \otimes \mathrm{id}_M.$$

The natural chain map associated with $f : M \rightarrow N$ is $\text{id}_{Q_n} \otimes f$ in degree n . For cohomology, choose a projective resolution $E_\bullet \rightarrow \mathbb{Z}$ in $R\text{-Mod}$. Then

$$H^n(G, M) \cong H^n(\text{Hom}_R(E_\bullet, M)), \quad \delta^n(\varphi) = \varphi \circ d_{n+1}.$$

Here $\text{Hom}_R(E_n, M)$ lies in cohomological degree n , and $\delta^{n+1}\delta^n = 0$ follows from $d_{n+1}d_{n+2} = 0$. The cochain map associated with $f : M \rightarrow N$ is postcomposition $\varphi \mapsto f \circ \varphi$. In both computations the complex contains resolution terms in nonnegative degrees, without the augmentation target $\mathbb{Z}$.

There is a special way to switch sides over a group ring. The map

$$\iota : R \longrightarrow R, \quad \sum_g a_g g \longmapsto \sum_g a_g g^{-1}$$

satisfies $\iota(rs) = \iota(s)\iota(r)$ and $\iota^2 = \text{id}$; equivalently, it is a ring isomorphism $R \cong R^{\text{op}}$. A left module becomes a right module by $m \cdot r = \iota(r)m$, in particular $m \cdot g = g^{-1}m$. The same operation in reverse recovers the left module, and the underlying additive maps and exact sequences are unchanged. It also takes free modules to free modules: for the regular module, $x \mapsto \iota(x)$ identifies its converted action with the regular right action, and the construction commutes with direct sums. It therefore takes direct summands of free modules to direct summands of free modules, preserving projectivity. The trivial module $\mathbb{Z}$ remains trivial. Thus a left projective resolution of $\mathbb{Z}$ can be converted into a right one, using inversion rather than any commutativity assumption on the group ring.

Example 4.10 (A first calculation from a short resolution). Let $G = \langle t \rangle \cong \mathbb{Z}$ be infinite cyclic. Its group ring is the Laurent polynomial ring $R = \mathbb{Z}[t, t^{-1}]$, and augmentation is evaluation at $t = 1$. There is a free resolution

$$0 \longrightarrow R \xrightarrow{t-1} R \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0.$$

Multiplication by $t - 1$ is injective because R is an integral domain. Its image is $\ker \varepsilon$: if a Laurent polynomial vanishes at 1, multiplying it by a sufficiently large power of t produces an ordinary polynomial vanishing at 1, which is divisible by $t - 1$; dividing back by that unit proves the claim. The ring is commutative, so this displayed resolution can be used on either side.

Let $M = \mathbb{Z}_-$ with $tm = -m$. Tensoring the right resolution with M gives the chain complex in degrees 1 and 0,

$$0 \longrightarrow \mathbb{Z} \xrightarrow{-2} \mathbb{Z} \longrightarrow 0.$$

Indeed, $(t-1) \otimes m = 1 \otimes (t-1)m$ under the identification $R \otimes_R M \cong M$, so its map is $m \mapsto -2m$. Applying $\text{Hom}_R(-, M)$ to the left resolution gives the same displayed map in cohomological degrees 0 and 1. Under $\text{Hom}_R(R, M) \cong M$, precomposition sends φ to $\varphi \circ (t-1)$, whose value at 1 is $\varphi(t-1) = (t-1)\varphi(1) = -2\varphi(1)$. It follows that

	degree 0	degree 1	degree $n \geq 2$
$H_n(G, \mathbb{Z}_-)$	$\mathbb{Z}/2\mathbb{Z}$	0	0
$H^n(G, \mathbb{Z}_-)$	0	$\mathbb{Z}/2\mathbb{Z}$	0

The kernel and cokernel occur in opposite degrees in the two constructions. For the trivial action on $\mathbb{Z}$, the same map is zero instead, giving $H_0(G, \mathbb{Z}) = H_1(G, \mathbb{Z}) = \mathbb{Z}$ and $H^0(G, \mathbb{Z}) = H^1(G, \mathbb{Z}) = \mathbb{Z}$, with higher groups zero. The general calculation for infinite cyclic groups will be developed in a later Section.

Remark (Which coefficient modules force higher vanishing). The coefficient-variable definitions immediately imply

$$\begin{aligned} M \text{ projective over } R &\implies H_n(G, M) = 0 \quad (n > 0), \\ M \text{ injective over } R &\implies H^n(G, M) = 0 \quad (n > 0). \end{aligned}$$

For projective M , take the length-zero projective resolution with $P_0 = M$ and augmentation id_M . After removing its augmentation target and taking coinvariants, only degree zero remains. For injective M , the length-zero injective resolution with $J^0 = M$ gives the same conclusion after taking invariants. These arguments prove the two positive-degree vanishing assertions directly from the definitions. The hypotheses concern modules over $R = \mathbb{Z}[G]$, not merely the underlying abelian groups.

One should not replace “injective” by “projective” in the second line. For example, for $G = \langle t \rangle$, the left regular module R is free, but the preceding resolution gives

$$H^1(G, R) = R/(t-1)R \cong \mathbb{Z} \neq 0.$$

Using projectives to resolve the *first* argument $\mathbb{Z}$ in $\text{Ext}_R^n(\mathbb{Z}, M)$ does not make a projective *second* argument M acyclic for invariants.

Long exact sequences and the meaning of the higher groups

Proposition 4.11 (Long exact sequences in the coefficients). *Every short exact sequence $0 \rightarrow A \xrightarrow{u} B \xrightarrow{v} C \rightarrow 0$ of G -modules induces natural long exact sequences*

$$\begin{aligned} \cdots \longrightarrow H_n(G, A) &\longrightarrow H_n(G, B) \longrightarrow H_n(G, C) \\ &\xrightarrow{\partial_n} H_{n-1}(G, A) \longrightarrow \cdots \\ \cdots \longrightarrow H_1(G, C) &\xrightarrow{\partial_1} A_G \longrightarrow B_G \longrightarrow C_G \longrightarrow 0 \end{aligned}$$

and

$$\begin{aligned} 0 \longrightarrow A^G &\longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta^0} H^1(G, A) \longrightarrow \cdots \\ \cdots \longrightarrow H^n(G, A) &\longrightarrow H^n(G, B) \longrightarrow H^n(G, C) \\ &\xrightarrow{\delta^n} H^{n+1}(G, A) \longrightarrow \cdots \end{aligned}$$

Naturality here includes commutative diagrams of short exact coefficient sequences.

Proof. Choose a right free resolution $Q_\bullet \rightarrow \mathbb{Z}$. Each Q_n is flat, so tensoring the coefficient sequence with Q_n is exact. These degreewise sequences assemble into a short exact sequence of chain complexes

$$0 \longrightarrow Q_\bullet \otimes_R A \longrightarrow Q_\bullet \otimes_R B \longrightarrow Q_\bullet \otimes_R C \longrightarrow 0.$$

Its long exact homology sequence gives the homology assertion. For cohomology choose a left projective resolution $E_\bullet \rightarrow \mathbb{Z}$. Each functor $\text{Hom}_R(E_n, -)$ is exact, giving a short exact sequence of cochain complexes

$$0 \longrightarrow \text{Hom}_R(E_\bullet, A) \longrightarrow \text{Hom}_R(E_\bullet, B) \longrightarrow \text{Hom}_R(E_\bullet, C) \longrightarrow 0.$$

Its long exact cohomology sequence proves the second assertion.

In either case, the connecting map has the previously established lift–differentiate–lift construction. Lift a cycle in the third complex to the second. Its differential has zero image in the third complex and thus comes from a unique element of the first. That element is a cycle because the differential squares to zero and the first map is injective. Taking its class gives ∂_n in chain degree $n-1$, or δ^n in cochain degree $n+1$. The long exact sequence theorem ensures independence of the lifts and representatives. A morphism of coefficient sequences induces a morphism of these short exact sequences of complexes, and the same construction commutes with that morphism. This gives naturality of the connecting maps, as well as of the other maps. $\square$

These sequences make the exactness failures precise. For an invariant element $c \in C^G$,

$$c \text{ has an invariant lift in } B \iff \delta^0(c) = 0.$$

The image of δ^0 identifies the quotient $C^G / \text{im}(B^G \rightarrow C^G)$ with a subgroup of $H^1(G, A)$. On the homology side,

$$\ker(A_G \rightarrow B_G) = \text{im } \partial_1.$$

Thus $H_1(G, C)$ supplies exactly the classes needed to account for the loss of injectivity at A_G . In Example 4.8, δ^0 injects $\mathbb{F}_2$ into $H^1(C_2, \mathbb{Z}_-)$, and ∂_1 surjects onto $(\mathbb{Z}_-)_G = \mathbb{F}_2$. These claims follow already from exactness; later cyclic-group computations identify the groups themselves.

Remark (Higher information about a group and its coefficient action). The input consists of a group G , an abelian group M , and a specified action $G \rightarrow \text{Aut}_{\mathbf{Ab}}(M)$. Changing the action can change the answer even when the underlying abelian group stays the same, as the infinite cyclic calculation shows.

In degree zero, homology *forces the action to be trivial* by identifying gm with m , while cohomology *selects the elements already fixed*. With G fixed, higher homology and cohomology are the higher derived information of these operations on the entire category of G -modules. The long exact sequences explain precisely how that information records failures of exactness. It is therefore useful to think of the theory as studying higher information carried by the group together with its coefficient action, rather than only by the underlying abelian group.

A trivial coefficient action does not force positive-degree groups to vanish. Both degree-zero constructions return the underlying abelian group on a trivial module, but resolutions are taken over $\mathbb{Z}[G]$: their terms need not have trivial action, and the relations in G still enter the calculation. The computation $H_1(\mathbb{Z}, \mathbb{Z}) = H^1(\mathbb{Z}, \mathbb{Z}) = \mathbb{Z}$ already demonstrates this. With the standard trivial integer coefficients, the resulting groups are invariants of G itself.

Key point. Group homology derives the operation of making an action trivial; group cohomology derives the operation of taking fixed elements. Their Tor and Ext descriptions let us compute both by resolving the trivial module. The next chapter supplies bar resolutions and explicit chain and cochain formulas for every group.

5 Group Homology and Cohomology via Explicit Complexes

The preceding chapter defined group homology and cohomology as derived functors and reduced their calculation to resolutions of the trivial module. We now construct bar resolutions and write the resulting coefficient chain and cochain complexes explicitly. These give equivalent definitions; the later chapters use smaller resolutions for calculations and then interpret the low-degree classes.

5.1 The bar resolution: one construction for every group

The definitions so far do not yet display the elements representing a cohomology class. We now construct a free resolution that works for every group. Its differential records relations among group-ring elements; geometrically, it is the usual boundary of an ordered simplex, expressed using successive steps instead of vertices. Throughout, $R = \mathbb{Z}[G]$ and M is a left G -module.

Starting with generators and their relations

The module to resolve is the trivial module $\mathbb{Z}$. Start with $P_0 = R[\] \cong R$ and the augmentation

$$\varepsilon : P_0 \longrightarrow \mathbb{Z}, \quad \sum_g a_g g[\] \longmapsto \sum_g a_g.$$

As we saw in Chapter 4, its kernel is generated by the elements $(g - 1)[\]$. Indeed, if $\sum_g a_g = 0$, then

$$\sum_g a_g g[\] = \sum_g a_g (g - 1)[\].$$

Introduce a free basis symbol $[g]$ for every $g \in G$ and put

$$P_1 = \bigoplus_{g \in G} R[g], \quad d_1[g] = (g - 1)[\].$$

Thus $\text{im } d_1 = \ker \varepsilon$. Including $g = 1$ introduces a redundant generator with zero image; we will remove this and its higher analogues when normalizing the resolution.

The next step must record relations among these generators of the augmentation ideal. The identity

$$gh - 1 = (g - 1) + g(h - 1)$$

gives the element

$$r(g, h) := g[h] - [gh] + [g] \in \ker d_1.$$

We therefore introduce symbols $[g|h]$ and define

$$P_2 = \bigoplus_{(g, h) \in G^2} R[g|h], \quad d_2[g|h] = r(g, h).$$

The verification is

$$\begin{aligned} d_1 d_2[g|h] &= (g(h - 1) - (gh - 1) + (g - 1))[\] \\ &= (gh - g - gh + 1 + g - 1)[\] = 0. \end{aligned}$$

This explains the proposed second differential. Proving that these relations generate *all* of $\ker d_1$, and doing the same in higher degrees, requires the exactness argument below.

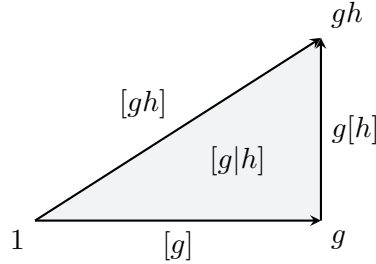
Remark (A coefficient and a label have different roles). The element $g[h]$ means the coefficient $g \in R$ acting on the basis vector $[h]$; the element $[gh]$ is a basis vector with label gh . They are generally different elements of P_1 . Likewise, $r(g, h)$ need not be zero in P_1 : it is a relation because its *image* under d_1 is zero. The next free module supplies a generator whose image is this relation.

The triangle behind the second differential

Regard $[g]$ as the formal oriented edge $(1, g)$. Simultaneous left translation of its vertices gives

$$a[g] \longleftrightarrow (a, ag), \quad a \in G.$$

Its boundary is endpoint minus starting point, so $\partial(1, g) = (g) - (1)$ agrees with $d_1[g] = (g - 1)[\]$. Now regard $[g|h]$ as the ordered triangle $(1, g, gh)$:



The picture shows the three oriented edges; their signs are assigned by the ordered boundary formula

$$\partial(1, g, gh) = (g, gh) - (1, gh) + (1, g).$$

Translate its terms back into bar notation:

face	bar notation	description
(g, gh)	$g[h]$	translate the edge $(1, h)$ by g
$(1, gh)$	$[gh]$	go directly from 1 to gh
$(1, g)$	$[g]$	go from 1 to g .

Hence the boundary is exactly $g[h] - [gh] + [g]$. The coefficient in the first term records the changed starting vertex of that face. In the path $1 \xrightarrow{g} g \xrightarrow{h} gh$, an edge label records *right multiplication* by a step. The module action still acts by *left translation* of all vertices. These two operations are compatible even when G is noncommutative.

These are formal ordered simplices: repeated vertices are allowed, and a picture with distinct corners is only a schematic illustration. We do not identify different orderings of a tuple by an orientation sign. The precise simplicial-space interpretation will appear in a later section.

Vertices, successive steps, and the general formula

For $n \geq 0$, let

$$P_n = \bigoplus_{(g_1, \dots, g_n) \in G^n} R[g_1 | \dots | g_n].$$

The brackets are basis symbols, not products in G ; repetitions and identity labels are allowed. The unique element of G^0 gives the chosen basis of P_0 . Let E_n be the free abelian group on the tuples $(x_0, \dots, x_n) \in G^{n+1}$, with diagonal left action

$$a(x_0, \dots, x_n) = (ax_0, \dots, ax_n).$$

Each orbit has a unique representative starting at 1 and trivial stabilizer, so E_n is free over R . The following are two coordinate systems for the same free module:

$$\begin{aligned} a[g_1 | \dots | g_n] &\longleftrightarrow (a, ag_1, ag_1g_2, \dots, ag_1 \dots g_n), \\ (x_0, \dots, x_n) &\longleftrightarrow x_0[x_0^{-1}x_1 | x_1^{-1}x_2 | \dots | x_{n-1}^{-1}x_n]. \end{aligned}$$

Here $a \in G$; extending additively gives inverse R -linear isomorphisms. Vertex coordinates remember the entire tuple; inhomogeneous bar coordinates remember its starting point and steps $g_i = x_{i-1}^{-1}x_i$.

In vertex coordinates take the usual alternating boundary

$$\partial_n(x_0, \dots, x_n) = \sum_{i=0}^n (-1)^i (x_0, \dots, \widehat{x_i}, \dots, x_n),$$

where the hat means omission. The maps are R -linear because deleting a vertex commutes with simultaneous left translation. To express this boundary on $[g_1 | \dots | g_n]$, start with

$$(1, g_1, g_1 g_2, \dots, g_1 \cdots g_n)$$

and distinguish the three possible locations of the deleted vertex:

1. **Delete the first vertex.** The remaining tuple is

$$(g_1, g_1 g_2, \dots, g_1 \cdots g_n) = g_1(1, g_2, \dots, g_2 \cdots g_n).$$

Its starting point has moved to g_1 , giving the term $g_1[g_2 | \dots | g_n]$.

2. **Delete an interior vertex x_i .** The starting point remains 1, but the two successive steps through x_i become a single step, since

$$x_{i-1}^{-1}x_{i+1} = (x_{i-1}^{-1}x_i)(x_i^{-1}x_{i+1}) = g_i g_{i+1}.$$

This gives $[g_1 | \dots | g_i g_{i+1} | \dots | g_n]$ with sign $(-1)^i$, for $1 \leq i \leq n-1$.

3. **Delete the last vertex.** Only the last step is lost, giving $[g_1 | \dots | g_{n-1}]$ with sign $(-1)^n$.

Thus the differential in bar coordinates is

$$\begin{aligned} d_n[g_1 | \dots | g_n] &= g_1[g_2 | \dots | g_n] \\ &\quad + \sum_{i=1}^{n-1} (-1)^i [g_1 | \dots | g_i g_{i+1} | \dots | g_n] \\ &\quad + (-1)^n [g_1 | \dots | g_{n-1}]. \end{aligned} \tag{4}$$

Extend this formula R -linearly. The apparent difference between its first, middle, and last terms comes entirely from expressing the same operation—deleting a vertex—in step coordinates.

For example, the four faces of $(1, g, gh, ghk)$ give

$$d_3[g|h|k] = g[h|k] - [gh|k] + [g|hk] - [g|h].$$

This records a relation among the relations introduced in degree two:

$$g r(h, k) - r(gh, k) + r(g, hk) - r(g, h) = 0 \quad \text{in } P_1.$$

Indeed, substituting $r(u, v) = u[v] - [uv] + [u]$ cancels every term; associativity identifies $(gh)k$ with $g(hk)$. Thus $d_3[g|h|k]$ is in $\ker d_2$, and the process of recording relations continues in higher degrees.

Why this is a complex, and why it is a resolution

In vertex coordinates, every term of $\partial_{n-1}\partial_n$ deletes two vertices. Fix their original indices $i < j$. Deleting j and then i has sign $(-1)^{j+i}$, whereas deleting i and then the shifted index $j-1$ has sign $(-1)^{i+j-1}$. The resulting tuples are equal and the signs opposite. Hence $\partial^2 = 0$, and therefore $d^2 = 0$ in bar coordinates. Also $\varepsilon d_1 = 0$.

Being a chain complex does not yet imply exactness. To establish exactness, augment E_0 by $(x_0) \mapsto 1$ and define additive maps

$$s_n(x_0, \dots, x_n) = (1, x_0, \dots, x_n), \quad s_{-1}(1) = (1).$$

Here $s_{-1} : \mathbb{Z} \rightarrow E_0$ is extended additively. Deleting the new first vertex gives the original tuple, while all other terms cancel those in $s_{n-1}\partial_n$. Consequently

$$\partial_{n+1}s_n + s_{n-1}\partial_n = \text{id}_{E_n}, \quad \varepsilon s_{-1} = \text{id}_{\mathbb{Z}},$$

where $\partial_0 = \varepsilon$ in this augmented equation. If $z \in \ker \partial_n$, then $z = \partial_{n+1}s_n z$. This proves exactness at every E_n , including E_0 ; the last identity proves surjectivity onto $\mathbb{Z}$. The coordinate isomorphisms respect the augmentations, so $P_\bullet \rightarrow \mathbb{Z}$ is a free resolution, called the *unnormalized bar resolution*.

Geometrically, s adds the fixed vertex 1 to cone off a simplex. It is generally *not* R -linear:

$$\begin{aligned} s_n(a(x_0, \dots, x_n)) &= (1, ax_0, \dots, ax_n), \\ a s_n(x_0, \dots, x_n) &= (a, ax_0, \dots, ax_n). \end{aligned}$$

This causes no problem for exactness, which can be checked on the underlying abelian groups. It does mean that s cannot in general be passed through $\text{Hom}_R(-, M)$ or tensor over R to contract the resulting coefficient complexes. The resolution can therefore be exact while group homology and cohomology are nonzero.

Normalization removes redundant identity labels

In homogeneous coordinates let $D_n \subseteq E_n$ be generated by tuples with two adjacent coordinates equal. Deleting either member of an equal adjacent pair gives equal tuples with opposite signs; every other deletion retains a repeated adjacent pair. Therefore $\partial D_n \subseteq D_{n-1}$, so these groups form a subcomplex. The operation of prepending 1 preserves such a repetition, hence $s_n(D_n) \subseteq D_{n+1}$. The additive contraction above therefore descends to the augmented quotient complex $E_\bullet/D_\bullet \rightarrow \mathbb{Z}$ and proves it exact.

In inhomogeneous coordinates this quotient has the basis $[g_1 | \dots | g_n]$ with *all* $g_i \neq 1$. Its differential is the same formula, with every term containing an identity label interpreted as zero. The quotient is still free over R because the discarded symbols were part of an R -basis. It is the *normalized bar resolution*, denoted $\bar{P}_\bullet \rightarrow \mathbb{Z}$. The projection $P_\bullet \rightarrow \bar{P}_\bullet$ lifts $\text{id}_{\mathbb{Z}}$ and is a chain homotopy equivalence by the comparison theorem. Thus either resolution computes the same group cohomology.⁵

Key point. The bar differential is the alternating simplex boundary written in starting-point and step coordinates. Its group coefficient records a translated face, its products combine adjacent steps, and its signs are the ordinary boundary signs. Exactness is a separate consequence of the additive contracting homotopy.

⁵For the bar resolutions and their applications, compare Weibel, Section 6.5, especially Definition 6.5.1 and Theorem 6.5.3.

5.2 The right bar resolution and the coefficient chain complex

For homology with left coefficients we use a *right* bar resolution. Let Q_n be free as a right R -module on the same strings, with

$$\begin{aligned} d_n^r[g_1 | \cdots | g_n] &= [g_2 | \cdots | g_n] \\ &+ \sum_{i=1}^{n-1} (-1)^i [g_1 | \cdots | g_i g_{i+1} | \cdots | g_n] \\ &+ (-1)^n [g_1 | \cdots | g_{n-1}] g_n. \end{aligned}$$

The group-ring coefficient is on the right in the last term. This follows from homogeneous tuples with diagonal right action, using the representative $(g_1 \cdots g_n, g_2 \cdots g_n, \dots, g_n, 1)$ for a basis string. Deleting the first vertex drops the first step without changing the chosen last vertex 1. Deleting the last vertex instead leaves

$$(g_1 \cdots g_n, g_2 \cdots g_n, \dots, g_n) = (g_1 \cdots g_{n-1}, g_2 \cdots g_{n-1}, \dots, 1) g_n.$$

Thus the coefficient occurs in the *last* face and on the *right*. Interior deletions again multiply adjacent step labels. This explains the displayed formula with our right-module convention. Prepending 1 gives an additive contraction of the augmentation. Thus it is a free right resolution of $\mathbb{Z}$. Its first differential is $[g] \mapsto [] - [g]$; on tensoring with an arbitrary left module, this sends $[g] \otimes m$ to $m - gm$. This fixes our right-module sign convention.

Define the chain groups

$$C_n(G, M) = Q_n \otimes_R M \cong \bigoplus_{(g_1, \dots, g_n) \in G^n} M.$$

An element is a finite sum of symbols $[g_1 | \cdots | g_n] \otimes m$, additive in the coefficient m . Unlike a cochain, a chain has finite support in its tuple labels. Here $C_0(G, M) \cong M$ and $C_n = 0$ for $n < 0$. The differential $\partial_n = d_n^r \otimes 1$ is explicitly

$$\begin{aligned} \partial_n([g_1 | \cdots | g_n] \otimes m) &= [g_2 | \cdots | g_n] \otimes m \\ &+ \sum_{i=1}^{n-1} (-1)^i [g_1 | \cdots | g_i g_{i+1} | \cdots | g_n] \otimes m \\ &+ (-1)^n [g_1 | \cdots | g_{n-1}] \otimes g_n m. \end{aligned} \tag{5}$$

The last action follows from the balancing relation $(x g_n) \otimes m = x \otimes g_n m$. In the first two degrees,

$$\begin{aligned} \partial_1([g] \otimes m) &= m - gm, \\ \partial_2([g|h] \otimes m) &= [h] \otimes m - [gh] \otimes m + [g] \otimes hm. \end{aligned}$$

For example, applying ∂_1 to the second line gives $(m - hm) - (m - ghm) + (hm - ghm) = 0$. The equation $(d^r)^2 = 0$ proves $\partial^2 = 0$ in every degree. Set $\partial_0 = 0$; the augmentation target $\mathbb{Z}$ is not a term of this coefficient complex.

The normalized right bar resolution is obtained by discarding strings with an identity label, just as for the left resolution. Its additive homogeneous contraction descends, and the projection from the full resolution is a homotopy equivalence of right resolutions. Tensoring therefore gives the same homology with the normalized chain complex. The sign $m - gm$ is the convention for this right bar model; other convenient resolutions may use a first differential $T - 1$ instead. Comparison of resolutions justifies both choices.

5.3 Cochains as functions and the equivalent definitions

A map $P_n \rightarrow M$ is determined by arbitrary values on its basis, so the cochain groups are

$$C^n(G, M) = \text{Hom}_R(P_n, M) \cong \text{Map}(G^n, M).$$

These are all functions, with pointwise addition. They need not be group homomorphisms, and for infinite G no finite-support restriction is imposed. In degree zero, $C^0(G, M) = M$. Precomposition with d_{n+1} gives

$$\begin{aligned} (\delta^n f)(g_1, \dots, g_{n+1}) &= g_1 f(g_2, \dots, g_{n+1}) \\ &\quad + \sum_{i=1}^n (-1)^i f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1}) \\ &\quad + (-1)^{n+1} f(g_1, \dots, g_n). \end{aligned} \tag{6}$$

In particular,

$$\begin{aligned} (\delta^0 a)(g) &= ga - a, \\ (\delta^1 f)(g, h) &= gf(h) - f(gh) + f(g), \\ (\delta^2 c)(g, h, k) &= gc(h, k) - c(gh, k) + c(g, hk) - c(g, h). \end{aligned}$$

The action in the first term is forced by R -linearity. For example, let $\tilde{f}: P_1 \rightarrow M$ correspond to the function $f: G \rightarrow M$, so that $f(g) = \tilde{f}([g])$. Then

$$\begin{aligned} (\delta^1 f)(g, h) &= \tilde{f}(d_2[g|h]) \\ &= \tilde{f}(g[h] - [gh] + [g]) \\ &= gf(h) - f(gh) + f(g). \end{aligned}$$

The triangle of Section 5.1 now expresses compatibility of values along its edges: $\delta^1 f = 0$ says

$$f(gh) = f(g) + gf(h).$$

The value on the route $1 \rightarrow g \rightarrow gh$ agrees with the value on the direct edge $1 \rightarrow gh$; translating the second edge by g translates its coefficient value by the action on M . For trivial action this reduces to $f(gh) = f(g) + f(h)$, the homomorphism condition from G to the additive group of M . We return to these crossed homomorphisms in a later Chapter.

The equation $d^2 = 0$ implies $\delta^{n+1}\delta^n = 0$, and

$$H^n(G, M) = Z^n(G, M)/B^n(G, M), \quad Z^n = \ker \delta^n, \quad B^n = \text{im } \delta^{n-1},$$

with $B^0 = 0$. A cochain is *normalized* if it vanishes whenever one argument equals 1. These form the Hom complex of $\bar{P}_\bullet$, and its inclusion into the full cochain complex induces isomorphisms on cohomology by Section 5.1.

The homogeneous description is equally explicit: a degree- n cochain is an equivariant function $\phi: G^{n+1} \rightarrow M$ satisfying

$$\phi(gx_0, \dots, gx_n) = g\phi(x_0, \dots, x_n),$$

and its differential is the alternating sum of coordinate deletions. The two descriptions correspond by

$$\begin{aligned} \phi(x_0, \dots, x_n) &= x_0 f(x_0^{-1}x_1, \dots, x_{n-1}^{-1}x_n), \\ f(g_1, \dots, g_n) &= \phi(1, g_1, g_1g_2, \dots, g_1 \cdots g_n). \end{aligned}$$

They describe the same cochain complex in different coordinates.

Proposition 5.1 (The explicit complexes compute the derived definitions). *For a left G -module M , the complexes just constructed give natural isomorphisms*

$$\begin{aligned} H_n(C_\bullet(G, M)) &\cong \operatorname{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, M) = H_n(G, M), \\ H^n(C^\bullet(G, M)) &\cong \operatorname{Ext}_{\mathbb{Z}[G]}^n(\mathbb{Z}, M) = H^n(G, M). \end{aligned}$$

The normalized complexes give the same groups. Thus these concrete kernel-modulo-image constructions are equivalent definitions of group homology and cohomology.

Proof. The augmented right bar complex $Q_\bullet \rightarrow \mathbb{Z}$ is a free resolution, so the balanced computation of Tor identifies the homology of $Q_\bullet \otimes_R M$ with the first derived definition. The left bar complex $P_\bullet \rightarrow \mathbb{Z}$ is a free resolution, so the equivalent projective computation of Ext identifies the cohomology of $\operatorname{Hom}_R(P_\bullet, M)$ with the second. These are exactly the complexes whose differentials we displayed. Normalization follows from the comparison homotopy equivalences and preservation of homotopies by tensor and Hom.

If $u : M \rightarrow N$ is a coefficient map, the induced chain map sends $[g_1 | \cdots | g_n] \otimes m$ to $[g_1 | \cdots | g_n] \otimes u(m)$; the cochain map sends f to $u \circ f$. Equivariance of u makes both commute with the displayed differentials. The resolution identifications commute with these maps, giving naturality. $\square$

Key point. We now have both definitions and explicit complexes. The next chapter chooses smaller resolutions for cyclic and free groups. After computing their groups, we will return to the bar formulas to interpret low-degree classes.

To be completed.