University of Helsinki
Faculty of Science
Department of Mathematics and Statistics

Master's thesis

A peek at homological algebra via group cohomology

Tapio Saarinen

Supervisor: Marja Kankaanrinta 22.10.2019

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta — Fakultet — Faculty	Koulutusohjelma — Utbildningsprogram — Degree programme
Matemaattis-luonnontieteellinen	Geometria, algebra ja topologia

Tekijä — Författare — Author

Tapio Saarinen

Työn nimi — Arbetets titel — Title

A peek at homological algebra via group cohomology

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Pro gradu -tutkielma	Lokakuu 2019	74 s.

Tiivistelmä — Referat — Abstract

Tutkielman tarkoituksena on johdattaa lukija Ext-funktorin ja ryhmien kohomologian määritelmien ja teorian äärelle ja siten tutustuttaa lukija homologisen algebran keskeisiin käsitteisiin.

Ensimmäisessä luvussa esitellään tutkielman olettamia taustatietoja, algebran ja algebrallisen topologian peruskurssien sisältöjen lisäksi.

Toisessa luvussa esitellään ryhmien laajennosongelma ja ratkaistaan se tapauksessa, jossa annettu aliryhmä on vaihdannainen. Ryhmälaajennosten näytetään olevan yksi yhteen -vastaavuudessa tietyn ryhmän alkioiden kanssa, ja lisäksi tutkitaan erityisesti niitä ryhmälaajennoksia, jotka ovat annettujen ryhmien puolisuoria tuloja. Vastaan tulevien kaavojen todetaan vastaavan eräitä singulaarisen koketjukompleksin määritelmässä esiintyviä kaavoja.

Kolmannessa luvussa määritellään viivaresoluutio sekä normalisoitu viivaresoluutio, sekä niiden pohjalta ryhmien kohomologia. Aluksi määritellään teknisenä sivuseikkana G-modulin käsite, jonka avulla ryhmien toimintoja voi käsitellä kuten moduleita. Luvun keskeisin tulos on se, että viivaresoluutio ja normalisoitu viivaresoluutio ovat homotopiaekvivalentit – tuloksen yleistys takaa muun muassa, että Ext-funktori on hyvin määritelty. Luvun lopuksi lasketaan syklisen ryhmän kohomologiaryhmät.

Neljännessä luvussa määritellään resoluutiot yleisyydessään, sekä projektiiviset että injektiiviset modulit ja resoluutiot. Viivaresoluutiot todetaan projektiivisiksi, ja niiden homotopiatyyppien samuuden todistuksen todetaan yleistyvän projektiivisille ja injektiivisille resoluutioille. Samalla ryhmien kohomologian määritelmä laajenee, kun viivaresoluution voi korvata millä tahansa projektiivisella resoluutiolla. Luvussa määritellään myös funktorien eksaktisuus, ja erityisesti tutkitaan Hom-funktorin eksaktiuden yhteyttä projektiivisiin ja injektiivisiin moduleihin.

Viidennessä luvussa määritellään oikealta johdetun funktorin käsite, ja sen erikoistapauksena Ext-funktori, joka on Hom-funktorin oikealta johdettu funktori. Koska Hom-funktori on bifunktori, on sillä kaksi oikealta johdettua funktoria, ja luvun tärkein tulos osoittaa, että ne ovat isomorfiset. Ryhmien kohomologian määritelmä laajenee entisestään, kun sille annetaan määritelmä Ext-funktorin avulla, mikä mahdollistaa ryhmien kohomologian laskemisen myös injektiivisten resoluutioiden kautta.

Viimeiseen lukuun on koottu aiheeseen liittyviä asioita, joita tekstissä hipaistaan, mutta joiden käsittely jäi rajaussyistä tutkielman ulkopuolelle.

Avainsanat — Nyckelord — Keywords

homologinen algebra, ryhmien kohomologia, Ext-funktori

Säilytyspaikka — Förvaringsställe — Where deposited

Elektroninen opinnäytearkisto E-thesis

Muita tietoja — Övriga uppgifter — Additional information

Contents

Introduction **3**

1 Preliminaries **5**
1.1 Conventions 5
1.2 Abelian categories in brief 5
1.3 Modules and bimodules, hom and tensor 7

2 Group extensions **10**
2.1 Split extensions 12
2.2 Nonsplit extensions 17

3 A first definition **21**
3.1 Group rings and G-modules 21
3.2 Motivating observations 24
3.3 The bar resolution 27
3.4 A first definition 30
3.5 The normalised bar resolution 31
3.6 Connecting the bar resolutions 34
3.7 The low-dimensional cohomology groups 39

4 Resolutions and exact functors **41**
4.1 Resolutions 41
4.2 Projective modules 45
4.3 Exact functors 48
4.4 Injective modules 53
4.5 Injective resolutions 60

5 Derived functors and Ext **62**
5.1 Right derived functors 62
5.2 The Ext functors 70

Further avenues **74**

Introduction

Homological algebra arose from (or along) the field of algebraic topology, as a development of the "algebraic" side. In algebraic topology one takes spaces, assigns to them algebraic objects called chain complexes, and calculates their cohomology groups: in homological algebra one concentrates on the chain complexes and their cohomology. Group cohomology is the application of cohomology theory, both topological and algebraic, to group theoretic questions.

The cohomology theory of groups has topological origins. In a 1936 paper, Hurewicz proved that any two spaces having isomorphic fundamental groups π, and all higher homotopy groups trivial, have the same homotopy type, and thus the same (co)homology. He then defined the (co)homology of the group π to be the (co)homology of any such space.

The second homology group was the first to receive a purely algebraical description, by Hopf in 1942, after which it was noticed that the other low-dimensional (co)homology groups had also appeared in earlier algebraic literature. The second cohomology group, for example, consisted of "factor sets", which had been defined in the study of the group extension problem by Schur in 1904, and Schreier and Brauer in 1926. For precise references and a more elaborate historical account, see the introduction to the book [1].

This thesis ignores the topological side of group cohomology, focusing on the algebraic side. We present a sequence of equivalent but increasingly refined definitions for group cohomology, starting from the explicit definition derived from the group extension problem, up to the very compact definition via the Ext functor. Along the way, we come upon several key concepts of basic homological algebra: we hope that the reader finds every new topic and definition a natural continuation of the previous ones. In short, this thesis attempts to be an (entirely ahistorical) account of how one, previously uninitiated, might come to arrive at the definition of the Ext functor. The two main sources are the book [1] for group cohomology in particular, and the book [2] for homological algebra in general.

The first chapter contains a brief overview of abelian categories and (bi)modules for the reader unfamiliar with the topics. We presume that the reader is acquainted with algebraic topology, having seen a development of some form of (co)homology

for some class of topological spaces. As such, we also assume that the reader is familiar with the basic category theory involved, including the snake lemma. For algebraic topology, the reader can refer to [3], and for category theory, to [4].

The second chapter presents the group extension problem. After restricting to the case where the given subgroup is abelian, it is resolved in two steps. First, the extensions that split are shown to correspond to semidirect products, and the possible splittings are classified by an auxiliary group. Then, the extensions without splittings are shown to correspond to elements of another auxiliary group (these will turn out to be the first and second cohomology groups).

The third chapter takes the expressions encountered in the previous chapter and intuits from them a definition of group cohomology. First, G-modules are defined to turn group actions into module multiplication, digestible by the machinery of cohomology. The rest of the chapter defines (two variations of) a cochain complex that defines group cohomology, first examining the chain complexes – known as bar resolutions – laying behind the cochain complexes. Lastly, the two cochain complexes are shown to be chain homotopy equivalent so that they produce the same cohomology, and the first and second cohomology groups are shown to be the auxiliary groups.

The fourth chapter begins by generalising from the bar resolutions, defining resolutions in general. Then, projective modules and resolutions are defined, as suggested by the proof of equivalence of the bar resolutions. Their properties and connection to the Hom functor are explored, from which the concept of exact functors pops up naturally. The chapter then folds in on itself, defining injective modules and resolutions as dual to their projective counterparts.

The fifth chapter generalises the process of taking a resolution, functoring and calculating cohomology by defining right derived functors. The right derived functors of Hom are then examined in detail, which leads to a very succinct definition of group cohomology. The last section details topics that could well have been included if not for length limitations, suggesting further topics to study.

Chapter 1

Preliminaries

1.1 Conventions

Unless otherwise mentioned, rings are always assumed to be unital (but not commutative). In an algebraic context, a map is implicitly assumed to be homomorphic, as with topological spaces and (continuous) maps; when a map is only a set function it will be explicitly pointed out. Regarding group actions, a group element g acting on an element x is denoted either $g.x$ or gx, if it is clear from the context.

The presence of the symbol $-$ indicates a function (or functor, or natural transformation...) that takes a value and puts it in place of $-$. For example, $(f \circ -)$ is the function $g \mapsto f \circ g$, with appropriate domain, and $\mathrm{Hom}(-, \mathbf{Z})$ is the functor taking, say, an abelian group A to $\mathrm{Hom}(A, \mathbf{Z})$ and a map $f\colon A \to B$ to $\mathrm{Hom}(f, \mathbf{Z}) = - \circ f\colon \mathrm{Hom}(B, \mathbf{Z}) \to \mathrm{Hom}(A, \mathbf{Z})$.

1.2 Abelian categories in brief

An abelian category is a category tailored for homology. It is defined in three stages:

Definition 1.1. A category $\mathcal{C}$ is called *preadditive* if the following hold:

i) The hom-set $\mathrm{Hom}(A, B)$ is an abelian group for all objects A, B in $\mathcal{C}$

ii) Composition is bilinear in the following sense: for all morphisms f in $\mathcal{C}$, the maps $f_* = (f \circ -)$ and $f^* = (- \circ f)$ between hom-sets are homomorphic.

In a preadditive category, the product $A \times B$ and coproduct $A \coprod B$ of two objects A and B are always isomorphic: the common value is called the *biproduct* of A and B, denoted $A \oplus B$.

Definition 1.2. A preadditive category $\mathcal{C}$ is *additive* if the following hold:

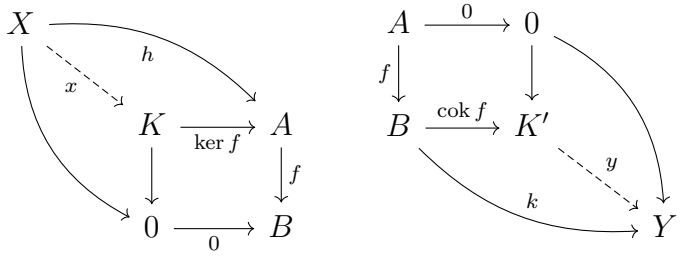
i) $\mathcal{C}$ has a zero object 0

ii) Each pair A, B of objects in $\mathcal{C}$ has a biproduct $A \oplus B$.

A functor $F\colon \mathcal{C} \to \mathcal{D}$ between additive categories is *additive* if $F(f+g) = Ff + Fg$ for each pair of morphisms f, $g\colon A \to B$ for all objects A, B in $\mathcal{C}$.

An additive functor sends zero objects to zero objects, and preserves biproducts.

Definition 1.3. Given an additive category $\mathcal{C}$ and a morphism $A \xrightarrow{f} B$ in $\mathcal{C}$, its *kernel* and *cokernel* are defined as follows.



The kernel is the pair $(K, \ker f)$ in the pullback of $A \xrightarrow{f} B$ and $0 \xrightarrow{0} B$: dually, the cokernel is the pair $(K', \operatorname{cok} f)$ in the pushout of $A \xrightarrow{f} B$ and $A \xrightarrow{0} 0$.

Since morphisms can be thought to implicitly include their source and target, $\ker f$ and $\operatorname{cok} f$ here refer to only the morphisms: $\operatorname{Ker} f$ and $\operatorname{Cok} f$ (capitalised) refer to the objects K and K', which are unique up to (unique) isomorphisms, as they are defined by universal properties.

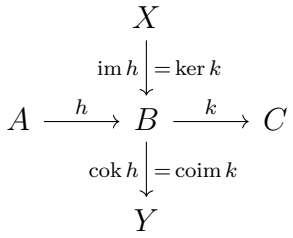
A morphism f is monic if and only if $\ker f = 0$, and $\ker f$ itself is always monic. Also, $\ker(jf) = \ker f$ if j is monic. The dual statements for cok are also true.

Definition 1.4. Given an additive category $\mathcal{C}$ and a morphism $A \xrightarrow{f} B$ in $\mathcal{C}$, its *image* and *coimage* are $\operatorname{im} f = \ker(\operatorname{cok} f)$ and $\operatorname{coim} f = \operatorname{cok}(\ker f)$.

$$\begin{array}{ccccccc} K & \xrightarrow{\ker f} & A & \xrightarrow{f} & B & \xrightarrow{\operatorname{cok} f} & K' \\ & & {\scriptstyle \operatorname{coim} f}\downarrow & & \uparrow{\scriptstyle \operatorname{im} f} & & \\ & & I' & & I & & \end{array}$$

It turns out that the objects I and I' above are always isomorphic, and thus any morphism $A \xrightarrow{f} B$ always factors as $f = (\operatorname{im} f) \circ \operatorname{coim} f$ (given that the kernels and cokernels exist): this is a categorical form of the first isomorphism theorem.

Definition 1.5. A sequence $A \xrightarrow{h} B \xrightarrow{k} C$ in $\mathcal{C}$ is *exact* if $\operatorname{im} h = \ker k$.



Equivalently, the above sequence is exact if $\operatorname{cok} h = \operatorname{coim} k$. Yet another equivalent condition is $kh = 0$ and $(\operatorname{cok} h) \circ \ker k = 0$ (both the horizontal and vertical sequences compose to 0).

Definition 1.6. An additive category $\mathcal{C}$ is called *abelian*, if the following hold:

i) Every morphism has a kernel and a cokernel

ii) Every monomorphism is a kernel and every epimorphism is a cokernel.

The prototypical abelian categories are the category $\mathbf{Ab} = {}_{\mathbf{Z}}\mathbf{Mod}$ of abelian groups, and the module categories ${}_R\mathbf{Mod}$ for a ring R.

Only the skeletal bare minimum has been mentioned here: for proofs and more details, consult chapter 5.5 of [2], or the book [5].

1.3 Modules and bimodules, hom and tensor

When R is a noncommutative ring, R-modules come in two chiral flavours: *left* and *right* R-modules. Left R-modules write scalar multiplication on the left as rx, satisfying $(rr')x = r(r'x)$ for $r, r' \in R$, whereas right R-modules write scalar multiplication on the right as xr, satisfying $x(rr') = (xr)r'$ for $r, r' \in R$. Note the difference: left multiplication by rr' applies first r', then r: right multiplication applies r first, then r'. Of course, for a commutative ring R the left-right distinction between modules vanishes. The unspecified term R-module shall refer to a left R-module, with right modules explicitly named when needed.

An R, S-*bimodule* M is both a left R-module and a right S-module in a compatible manner, satisfying $r(xs) = (rx)s$ for $r \in R$, $s \in S$ and $x \in M$, and maps between R, S-bimodules are simultaneously R- and S-linear. Every left R-module is an $R, \mathbf{Z}$-bimodule by setting $xn = nx$: this is because multiples of the ring unit commute with every element of R. The same goes for right R-modules and $\mathbf{Z}, R$-bimodules. The ring R is naturally an R, R-bimodule via left and right multiplication.

Given left (or right) R-modules M and N, the hom-set $\mathrm{Hom}_R(M,N)$ is naturally an abelian group (so a $\mathbf{Z}$-module) with pointwise addition, but it fails to receive an R-module structure in general. Attempting to define left scalar multiplication by $(rf)(x) = f(rx)$ runs into trouble as the resulting map rf may fail to be R-linear. The function values

$$(rf)(r'x) = f(rr'x) \quad \text{and} \quad r'(rf)(x) = r'f(rx) = f(r'rx)$$

should be equal, but $rr'x$ and $r'rx$ have no reason to coincide unless the ring R is commutative; the left R-multiplication in M and the left R-multiplication in $f(r\cdot -)$ interfere with each other

But given an R', R-bimodule M and an R', S-bimodule N, then $\mathrm{Hom}_{R'}(M,N)$ is naturally an R,S-bimodule via setting $(rf)(x) = f(xr)$ and $(fs)(x) = f(x)s$: here both rf and fs remain R'-linear, and $((rf)s)(x)$ and $(r(fs))(x)$ both equal $f(xr)s$.

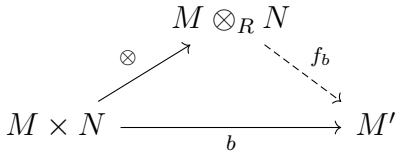
Furthermore, the Hom functors are of type $\mathrm{Hom}_{R'}(M,-)\colon {}_{R'}\mathbf{Mod}_S \to {}_R\mathbf{Mod}_S$ and $\mathrm{Hom}_{R'}(-,N)\colon {}_{R'}\mathbf{Mod}_R \to {}_R\mathbf{Mod}_S$ (a priori the target category is $\mathbf{Ab}$, so the point is that the functors yield not only $\mathbf{Z}$-linear but even R,S-linear maps). For example, if $g\colon N \to N'$ is R', S-linear, then $g_*\colon \mathrm{Hom}_{R'}(M,N) \to \mathrm{Hom}_{R'}(M,N')$ is R,S-linear: it satisfies

$$g_*(rfs)(x) = g(rfs(x)) = g(f(xr)s) = g(f(xr))s = g_*(f)(xr)s = (rg_*(f)s)(x)$$

for all $x \in M$, so $g_*(rfs) = rg_*(f)s$ for all $f\colon M \to N$, $r \in R$ and $s \in S$.

The tensor product $M \otimes_R N$ of two left R-modules M and N is generated by elements $x \otimes y$ where $x \in M$, $y \in N$ so that $\otimes$ is R-bilinear: then $M \otimes_R N$ inherits a left R-module structure by setting $r(x \otimes y) = rx \otimes y = x \otimes ry$. The same goes for two right R-modules.

The universal property satisfied by this tensor product is that R-bilinear maps $b\colon M \times N \to M'$ correspond bijectively to R-linear maps $f_b\colon M \otimes_R N \to M'$ with $f_b \circ \otimes = b$ for any left R-module M'.



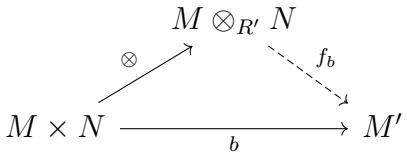
As bilinear maps $M \times N \to M'$ correspond to elements of $\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, M'))$, this gives the adjunction

$$\mathrm{Hom}_R(M \otimes N, M') \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, M'))$$

between $- \otimes_R N\colon {}_R\mathbf{Mod} \to {}_R\mathbf{Mod}$ and $\mathrm{Hom}_R(N,-)\colon {}_R\mathbf{Mod} \to {}_R\mathbf{Mod}$.

In the case of an R, R'-bimodule M and an R', S-bimodule N, the tensor product $M \otimes_{R'} N$ is generated by elements $x \otimes y$ so that $\otimes$ is R'-*biadditive* (that is, $\otimes$ is $\mathbf{Z}$-bilinear and satisfies $xr' \otimes y = x \otimes r'y$). It inherits a natural R, S-module structure by setting $r(x \otimes y)s = rx \otimes ys$, making $\otimes$ an R-linear map in the first component, and S-linear in the second.

The universal property satisfied by this tensor product is as follows: for M' an R, S-module, R'-biadditive maps $b\colon M \times N \to M'$ that are R-linear in the first and S-linear in the second component, correspond bijectively to R, S-linear maps $f_b\colon M \otimes_{R'} N \to M'$ with $f_b \circ \otimes = b$.



As R'-biadditive functions that are R-linear in the first and S-linear in the second component correspond to elements of $\mathrm{Hom}_R(M, \mathrm{Hom}_S(N, M'))$, this gives the adjunction

$$\mathrm{Hom}_{R,S}(M \otimes_{R'} N, M') \cong \mathrm{Hom}_{R,R'}(M, \mathrm{Hom}_S(N, M'))$$

between $- \otimes_{R'} N\colon {}_R\mathbf{Mod}_{R'} \to {}_R\mathbf{Mod}_S$ and $\mathrm{Hom}_S(N, -)\colon {}_R\mathbf{Mod}_S \to {}_R\mathbf{Mod}_{R'}$.

Chapter 2

Group extensions

Consider a short exact sequence of groups

$$0 \to N \xrightarrow{i} G \xrightarrow{p} G/N \to 0,$$

where p is the quotient map and $i = \ker p$ is the inclusion map. Furthermore, from the right half $G \xrightarrow{p} G/N \to 0$, the subgroup N is recovered as $\operatorname{Ker} p$ (up to isomorphism), and given $0 \to N \xrightarrow{i} G$, the quotient group is readily formed as $\operatorname{Cok} i$. We are thus led to investigate the third case: given only the two extremal groups N and $Q = G/N$, to what degree can we recover G? This is the group extension problem.

Remark 2.1. The maps i and p are important in specifying how the given subgroup sits inside the given group, and how the group lies over the given quotient. For example, $\mathbf{Z}$ and $2\mathbf{Z}$ are isomorphic normal subgroups of $\mathbf{Z}$, but the quotients $\mathbf{Z}/\mathbf{Z}$ and $\mathbf{Z}/2\mathbf{Z}$ are not isomorphic.

Two nonisomorphic subgroups can also produce isomorphic quotients. Given any pair of groups $N \trianglelefteq G$, we have $G \times 1$, $N \times G/N \trianglelefteq G \times G/N$ and

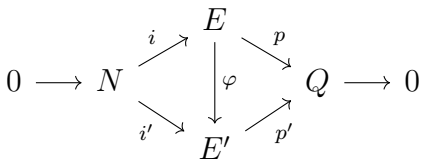
$$\frac{G \times G/N}{G \times 1} \cong \frac{G}{G} \times \frac{G/N}{1} \cong G/N, \quad \frac{G \times G/N}{N \times G/N} \cong \frac{G}{N} \times \frac{G/N}{G/N} \cong G/N$$

but of course $G \ncong N \times G/N$ in general. (Take G to be any semidirect product with normal factor N and nontrivial action, for example.)

Definition 2.2. A *group extension* of Q by N is a short exact sequence

$$0 \to N \xrightarrow{i} E \xrightarrow{p} Q \to 0.$$

Two such extensions E, E' are *equivalent* if there is a homomorphism $\varphi\colon E \to E'$ making the diagram



commute.

Because (an isomorphic copy of) the group N is present as a subgroup of E, it would also be natural to call E an extension of N by Q, but the opposite convention seems to be more frequent.

Remark 2.3. Any homomorphism between extensions in Definition 2.2 is necessarily an isomorphism, which follows from the five lemma; even though **Grp** is not an abelian category, the diagram chase goes through. Also conversely, given an extension $0 \to N \xrightarrow{i} E \xrightarrow{p} Q \to 0$ and isomorphism $E \xrightarrow{\varphi} E'$, the extension

$$0 \to N \xrightarrow{\varphi \circ i} E' \xrightarrow{p \circ \varphi^{-1}} Q \to 0$$

is equivalent to the original extension via φ.

An immediate observation is that the size of E is determined by N and Q, even if they are not finite.

Lemma 2.4. *If* $0 \to N \xrightarrow{i} E \xrightarrow{p} Q \to 0$ *is an extension, then* $|E| = |N \times Q|$.

Proof. By exactness, $E/iN \cong Q$ so there are as many cosets of iN as there are elements of Q. The cosets partition E, and each coset has $|N|$ many elements, so $|E| = |N \times Q|$. □

Remark 2.5. Consider an extension $0 \to N \to E \to Q \to 0$, and suppose for simplicity that N is a subgroup and Q is a quotient of E. Since N is normal in E, E acts on N by conjugation: $\hat{g}.n = \hat{g}n\hat{g}^{-1}$. If N is abelian, then the whole coset $\hat{g}N \in Q$ acts on n the same way: for $\hat{g}h \in \hat{g}N$, we have that

$$(\hat{g}h).n = \hat{g}.(h.n) = \hat{g}.(hnh^{-1}) = \hat{g}.(nhh^{-1}) = \hat{g}.n,$$

so the group Q also acts on N. This group action is a shadow of the group law in E, and is of use when reconstructing E.

Thus for the rest of the section, we restrict to the case where N is abelian, fix an action of the group Q on N and aim to find all the extensions E that induce the given Q-action. The terminology is borrowed from [2].

Remark on notation. Since N is abelian, it is customary to use additive notation for it, and $0 \in N$ is the identity; subsequently, since E will contain N as a subgroup, E will also be written additively even though it may well not be abelian. However, when E is some concrete group where N appears only as an isomorphic copy, for example a semidirect product, we use multiplicative notation. The group law in Q will be written multiplicatively, and $1 \in Q$ is the identity.

As for elements, since N is abelian, we will consistently use letters $g, h, \dots$ for elements of Q and $x, y, \dots$ for elements of N. For arbitrary elements of E, we use hatted letters $\hat{g}, \hat{h}, \dots$ to avoid confusion with elements of Q.

For the actions, we usually write the Q-action on N as gx without the dot. The conjugation action of Q on E as seen below will be written with the dot.

Definition 2.6. Given a group Q acting on an abelian group N, we say an extension $0 \to N \xrightarrow{i} E \xrightarrow{p} Q \to 0$ *realises the operators* if the E/iN-action on iN (as in Remark 2.5) coincides with the Q-action on N. That is,

$$i(p(\hat{g}).x) = \hat{g} + i(x) - \hat{g} = \hat{g}iN.i(x)$$

for all $x \in N$ and $\hat{g} \in E$.

Remark 2.7. If we make no distinction between the group N and its image in E, the condition becomes less unsightly:

$$p(\hat{g}).x = \hat{g} + x - \hat{g} = \hat{g}N.x$$

for all $x \in N$ and $\hat{g} \in E$. Since the conjugation action depends only on the coset and not on any particular representative, we might alternatively choose a (not necessarily homomorphic) section $s\colon Q \to E$ for p, and the condition becomes

$$i(gx) = s(g) + i(x) - s(g)$$

for all $x \in N, g \in Q$. This is evidently an alternative for Definition 2.6. It can also be written as a commutation rule: $s(g) + i(x) = i(gx) + s(g)$.

2.1 Split extensions

The extensions where the section s can be chosen to be homomorphic have a special name.

Definition 2.8. An extension $0 \to N \xrightarrow{i} E \xrightarrow{p} Q \to 0$ is called *split* if the short exact sequence splits. This means the map p has a homomorphic section, that is a homomorphism $s\colon Q \to E$ satisfying $ps = \mathrm{id}_Q$. The section s is called a *splitting*.

Two split extensions are *equivalent* if they are equivalent extensions and the vertical map and the splittings form a commuting triangle.

Example 2.9. Suppose Q acts trivially on N, that is $gx = x$ for all $x \in N, g \in Q$. Evidently $0 \to N \to N \times Q \to Q \to 0$ is then an extension realizing the operators, with the canonical inclusion and projection maps. This is because the conjugation action (and thus the induced action) is trivial:

$$(y, g).(x, 1) = (y, g)(x, 1)(y, g)^{-1} = (y + x - y, g1g^{-1}) = (x, 1).$$

Any extension E that realises the operators for a trivial action has conjugation acting trivially on N, meaning any element of N commutes with every element of E, meaning N is a subgroup of the center of E. These are called *central extensions*.

Example 2.10. Suppose Q acts on N. We can then form the *semidirect product* $N \rtimes Q$ with respect to this action: the base set is $N \times Q$ with the group law $(x, g)(y, h) = (x + gy, gh)$. It is associative, because

$$(x, g)(y, h) \cdot (z, k) = (x + gy, gh)(z, k) = (x + gy + ghz, ghk),$$

$$(x, g) \cdot (y, h)(z, k) = (x, g)(y + hz, hk) = (x + g(y + hz), ghk)$$

and these are equal. The identity element is $(0, 1)$:

$$(0, 1)(x, g) = (0 + 1x, 1g) = (x, g) = (x + g0, g1) = (x, g)(0, 1),$$

and the inverse of (x, g) is $(-g^{-1}x, g^{-1})$:

$$(x, g)(-g^{-1}x, g^{-1}) = (x - gg^{-1}x, gg^{-1}) = (0, 1),$$

$$(-g^{-1}x, g^{-1})(x, g) = (-g^{-1}x + g^{-1}x, g^{-1}g) = (0, 1).$$

Since 1 acts as identity, the map $i\colon N \to N \rtimes Q, i(x) = (x, 1)$ is homomorphic, and $p\colon N \rtimes Q \to Q, p(x, g) = g$ is homomorphic because of the group law on the second component. Also, $\operatorname{Im} i = N \times 1 = \operatorname{Ker} p$ holds so $0 \to N \xrightarrow{i} N \rtimes Q \xrightarrow{p} Q \to 0$ is an extension.

The function $s\colon Q \to N \rtimes Q$ defined by $s(g) = (0, g)$ is a section of p, and it is homomorphic since $g0 = 0$ for any $g \in Q$ so the extension is a split extension. Finally, taking $x \in N$ and $g \in Q$, we calculate $s(g) + i(x) - s(g)$ to be

$$(0, g)(x, 1)(0, g)^{-1} = (0 + gx, g1)(0, g^{-1}) = (gx + g0, gg^{-1}) = (gx, 1) = i(gx)$$

so we see that this extension realises the operators. Note that in case the Q-action is trivial, the semidirect product is just the direct product.

The above example shows that the natural semidirect product extensions $0 \to N \xrightarrow{i} N \rtimes Q \xrightarrow{p} Q \to 0$ are split extensions. The converse is also true: a split extension is isomorphic to the semidirect product of N and Q with the action induced from conjugation in E.

Theorem 2.11. *Semidirect products are split extensions of the factors*

$$0 \longrightarrow N \xrightarrow{i} N \rtimes Q \underset{s}{\overset{p}{\rightleftarrows}} Q \longrightarrow 0$$

with the natural maps $i(x) = (x, 1)$, $p(x, g) = g$ *and* $s(g) = (0, g)$. *Conversely, a split extension with splitting* s *is equivalent to a semidirect product under the* Q*-action on* N *defined by* $i(gx) = s(g) + i(x) - s(g) = s(g).i(x)$ *(the action induced by conjugation in* E*).*

Proof. One direction is given by Example 2.10, and we are left to verify that splittings yield semidirect products.

Suppose the extension $0 \to N \xrightarrow{i} E \xrightarrow{p} Q \to 0$ has a splitting s. Define an action of Q on N as follows:

$$gx = y \quad \text{if} \quad i(y) = s(g) + i(x) - s(g) = s(g).i(x),$$

where the dot denotes the conjugation action. This is well defined, because $iN = \operatorname{Im} i = \operatorname{Ker} p$ is normal in E, so the conjugate $s(g) + i(x) - s(g)$ is in iN, and since i is injective it has only one preimage. So, for every $x \in N$ and $g \in Q$ such a $y \in N$ exists and is unique. We then check that it is an action:

i) $1x = x$ holds because $i(1x) = s(1).i(x) = 0.i(x) = i(x)$ holds for all $x \in N$

ii) $(gh)x = g(hx)$ holds because

$$\begin{aligned} i((gh)x) &= s(gh).i(x) = (s(g) + s(h)).i(x) \\ &= s(g).s(h).i(x) = s(g).i(hx) = i(g(hx)) \end{aligned}$$

holds for all $n \in N$ and $g, h \in Q$

iii) $g(x + y) = gx + gy$ holds because

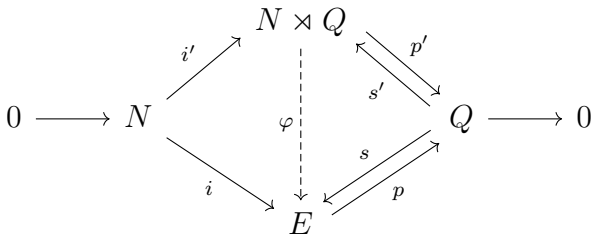
$$\begin{aligned} i(g(x + y)) &= s(g).i(x + y) = s(g).(i(x) + i(y)) \\ &= s(g).i(x) + s(g).i(y) = i(gx) + i(gy) = i(gx + gy) \end{aligned}$$

holds for all $x, y \in N$ and $g \in Q$.

The above calculations all amount to the fact that the Q-action is a kind of pullback along i of conjugation on E.

We can then form the semidirect product of N and Q with this action, which makes a split extension with inclusion $i'(x) = (x, 1)$, projection $p'(x, g) = g$ and

splitting $s'(g) = (0, g)$ all having their natural forms.



Now define $\varphi\colon N \rtimes Q \to E$ by $\varphi(x, g) = i(x) + s(g)$. We check that it is a homomorphism: for any $x, y \in N$ and $g, h \in Q$, we have

$$\begin{aligned}\varphi((x, g)(y, h)) &= \varphi(x + gy, gh) = i(x + gy) + s(gh) = i(x) + i(gy) + s(gh)\\ &= i(x) + s(g) + i(y) - s(g) + s(g) + s(h)\\ &= i(x) + s(g) + i(y) + s(h) = \varphi(x, g) + \varphi(y, h)\end{aligned}$$

so φ is homomorphic. Lastly, we verify that φ makes the three triangles commute: for $x \in N$ and $g \in Q$, we have

i) $\varphi(i'(x)) = \varphi(x, 1) = i(x)$

ii) $p(\varphi(x, g)) = p(i(x) + s(g)) = p(i(x)) + p(s(g)) = 0 + g = p'(x, g)$

iii) $\varphi(s'(g)) = \varphi(0, g) = i(0) + s(g) = s(g)$,

so φ is an equivalence between E and $N \rtimes Q$. □

Thus split extensions correspond to extensions by semidirect products, and as seen in Theorem 2.11, different splittings correspond to different ways of representing the middle group as a semidirect product of the left and right groups. Since a section is necessarily injective, splittings are embeddings of the non-normal factor into the semidirect product.

Definition 2.12. Given a group G and a subgroup H, a *complement* of H is a subgroup K so that $H \cap K = \{e\}$ and $G = HK = \{hk \mid h \in H, k \in K\}$.

Remark 2.13. The definition is clearly symmetric. By the definition, each element of G can be written as a product hk, and it turns out this factorisation is unique: if $hk = h'k'$ with $h, h' \in H$ and $k, k' \in K$, then $h'^{-1}h = k'k^{-1} \in H \cap K = \{e\}$ so $h = h'$ and $k = k'$.

The two factors $N \times 1$ and $0 \times Q$ are complementary in the semidirect product $N \rtimes Q$, as their intersection is $\{(0, 1)\}$ and $(x, 1)(0, g) = (x, g)$ for all $x \in N$ and $g \in G$. Theorem 2.11 further shows that given any split extension, $\operatorname{Im} i = iN$ and $\operatorname{Im} s$ are complementary subgroups in E, so any splitting yields a complement of iN. Conversely, any complement of iN yields a splitting, as we shall see next.

Lemma 2.14. *Suppose $0 \to N \xrightarrow{i} E \xrightarrow{p} Q \to 0$ is an extension, and $Q' \leq E$ is a complement of iN. Then Q and Q' are isomorphic, and the extension splits.*

Proof. We can restrict p to get a homomorphism $p{\restriction}Q' \colon Q' \to Q$. We then verify that it is bijective. For injectivity, suppose $p(g') = 1$ for some $g' \in Q'$. Then $g \in \operatorname{Ker} p = iN$, and since Q' and iN are complements, $g' \in Q' \cap iN = \{0\}$ so $g' = 0$ and $p{\restriction}Q'$ is injective.

To see that $p{\restriction}Q'$ is surjective, take any $g \in Q$ and choose a $\hat{g} \in E$ with $p(\hat{g}) = g$. Since Q' is a complement of iN, we find a $x \in N$ and $g' \in Q'$ so that $\hat{g} = i(x) + g'$: now $g = p(\hat{g}) = p(i(x) + g') = p(i(x)) + p(g') = 0 + p(g')$. Thus $p{\restriction}Q'$ is also surjective. This shows that Q' and Q are isomorphic via $p{\restriction}Q'$, so $(p{\restriction}Q')^{-1}$ is a splitting of p. □

We thus see that splittings correspond to complements of iN, so it is interesting to classify different splittings. A generic section of the generic split extension $0 \to N \xrightarrow{i} N \rtimes Q \xrightarrow{p} Q \to 0$ has the form $s(g) = (dg, g)$ for some function $d \colon Q \to N$, where we write dg for $d(g)$. In order for s to be homomorphic, the elements

$$s(gh) = (d(gh), gh) \quad \text{and} \quad s(g)s(h) = (dg, g)(dh, h) = (dg + g.dh, gh)$$

must be the same, so s is a splitting precisely when d satisfies $d(gh) = dg + g.dh$.

Definition 2.15. Given a group Q acting on an abelian group N, a *derivation* is a function $d \colon Q \to N$ satisfying $d(gh) = dg + g.dh$.

The reason for the name 'derivation' becomes apparent if we let Q act trivially on N on the right in addition to the given left action. Then the derivation condition can be written as

$$d(gh) = (dg).h + g.(dh),$$

since $(dg).h = dg$ by the trivial right action. It is now manifestly analogous to the product rule for derivatives. Derivations are also called *crossed homomorphisms*, since d satisfies not the usual homomorphicity rule $d(gh) = dg + dh$ but a version twisted by the Q-action.

The derivations $Q \to N$ form an abelian group $\operatorname{Der}(Q, N)$ under pointwise sum: the zero derivation corresponds to the natural splitting of the semidirect product, and sums and negatives are readily verified. If $d, \delta \in \operatorname{Der}(Q, N)$, then

$$(d - \delta)(gh) = d(gh) - \delta(gh) = dg + g.dh - \delta g - g.\delta h = (d - \delta)g + g.(d - \delta)h,$$

so $d - \delta$ also satisfies the derivation condition. Also, $\operatorname{Der}(Q, N)$ is abelian since N is; note that if N is not abelian, the elements $g.dh$ and δg may not commute, so

$\mathrm{Der}(Q, N)$ would fail to be a group. However, it would still be a pointed set with the zero derivation as the distinguished element.

In summary, any split extension of a group Q by an abelian group N that Q acts on is equivalent to the semidirect product $N \rtimes Q$ with the natural inclusion, quotient and splitting maps, and other splittings differ in the choice of complementary subgroup for $N \times 1$, or equivalently in the choice of derivation for the splitting $s(g) = (dg, g)$.

2.2 Nonsplit extensions

We now turn to investigate extensions without splittings.

Definition 2.16. Given an extension $0 \to N \xrightarrow{i} E \xrightarrow{p} Q \to 0$, a *normalised section* for p is a (not necessarily homomorphic) section s such that $s(1) = 0$.

Since p maps $0 \in E$ to $1 \in Q$, normalised sections always exist, and there are no natural choices to make for the other elements. Groups are naturally pointed sets with identity as the basepoint, so we require that s should at least be a pointed map, if not a homomorphism.

Since s has no reason to be homomorphic, we can define a correction factor that turns out to be fruitful. In general, $s(gh) \neq s(g) + s(h)$ for all $g, h \in Q$, but since they both map to gh under p, they differ by an element of $\operatorname{Ker} p = iN$. Thus the following definition is justified:

Definition 2.17. Given an extension $0 \to N \xrightarrow{i} E \xrightarrow{p} Q \to 0$ and a normalised section $s\colon Q \to E$, define the *factor set* associated to the section s to be the function $f\colon Q \times Q \to N$ defined by

$$s(g) + s(h) = i(f(g, h)) + s(gh)$$

for $g, h \in Q$.

Note that since $s(1) = 0$, factor sets satisfy $f(1, g) = f(g, 1) = 0$ for all $g \in Q$, and factor sets that are identically zero correspond to splittings. We now show that from a factor set f the whole extension is recovered:

Lemma 2.18. *Given an extension $0 \to N \xrightarrow{i} E \xrightarrow{p} Q \to 0$, a normalised section s and the associated factor set f, there is a group E' that depends only on f and the Q-action on N that forms an extension equivalent to E.*

Proof. By Lemma 2.4, we know any extension E' will have size $|N \times Q|$ so we might as well take $N \times Q$ to be the base set. In fact, as s bijects Q onto the cosets of iN, the lemma shows that $\varphi\colon E' \to E$, $\varphi(x, g) = i(x) + s(g)$ is a bijection.

There is precisely one group law on E' that will make φ an isomorphism: it helps to recall the commutation rule from Remark 2.7. Given $(x,g),(y,h) \in E'$, the element $\varphi((x,g)(y,h))$ should be equal to the element

$$\begin{aligned}
\varphi(x,g)+\varphi(y,h) &= i(x)+s(g)+i(y)+s(h) \\
&= i(x)+i(gy)+s(g)+s(h) && \text{(commutation rule)} \\
&= i(x)+i(gy)+i(f(g,h))+s(gh) && \text{(factor set definition)} \\
&= i(x+gy+f(g,h))+s(gh) \\
&= \varphi(x+gy+f(g,h),gh),
\end{aligned}$$

so we see that the correct group law is $(x,g)(y,h) = (x+gy+f(g,h),gh)$. This only depends on the factor set f and the action of Q on N.

The equivalent extension is then, as seen in Remark 2.3, the exact sequence $0 \to N \xrightarrow{i'} E' \xrightarrow{p'} Q \to 0$ where $i' = \varphi^{-1} \circ i$ and $p' = p \circ \varphi$. These turn out to be

$$i'(x) = \varphi^{-1}(i(x)) = \varphi^{-1}(i(x)+s(1)) = (x,1)$$

and

$$p'(x,g) = p(\varphi(x,g)) = p(i(x)+s(g)) = p(i(x))+p(s(g)) = 0+g = g$$

for all $x \in N$, $g \in Q$: they are the natural inclusion and projection maps. □

A natural continuation is then to characterise which functions can be factor sets. Given a group Q acting on an abelian group N and a function $f\colon Q \times Q \to N$, we attempt to define a group law on $N \times Q$ by the formula that appeared above: set $(x,g)(y,h) = (x+gy+f(g,h),gh)$ for $(x,g),(y,h) \in N \times Q$. We then verify the group axioms, keeping track of what each axiom requires of f.

i) Identity: for $(x,g) \in N \times Q$, we have

$$\begin{aligned}
(0,1)(x,g) &= (0+1.x+f(1,g),1g) = (x+f(1,g),g) = (x,g), \\
(x,g)(0,1) &= (x+g.0+f(g,1),g1) = (x+f(g,1),g) = (x,g)
\end{aligned}$$

if and only if $f(1,g) = f(g,1) = 0$ holds for all $g \in Q$.

ii) Associativity: for $(x,g),(y,h),(z,k) \in N \times Q$, we have

$$\begin{aligned}
(x,g)(y,h)\cdot(z,k) &= (x+g.y+f(g,h),gh)(z,k) \\
&= (x+g.y+gh.z+f(g,h)+f(gh,k),ghk), \\
(x,g)\cdot(y,h)(z,k) &= (x,g)(y+h.z+f(h,k),hk) \\
&= (x+g.y+gh.z+g.f(h,k)+f(g,hk),ghk)
\end{aligned}$$

and these are equal if and only if $f(g,h)+f(gh,k) = g.f(h,k)+f(g,hk)$ for all $f,g,h \in Q$.

iii) Inverses: for $(x, g) \in N \times Q$, let $y, z \in N$ be such that $x + gy + f(g, g^{-1}) = 0$ and $z + g^{-1}x + f(g^{-1}, g) = 0$, whence

$$(x, g)(y, g^{-1}) = (x + gy + f(g, g^{-1}), gg^{-1}) = (0, 1),$$
$$(z, g^{-1})(x, g) = (z + g^{-1}x + f(g^{-1}, g), g^{-1}g) = (0, 1)$$

so the element (x, g) has a left and a right inverse. They coincide as long as the operation is associative, so inverses make no further requirements of f.

The above group law then makes $N \times Q$ into a group, which we call E_f: it is reminiscent of a semidirect product, but further twisted by a factor set.

Next, we show that E_f is an extension of Q by N having f as a factor set. As the end of Lemma 2.18 suggests, we define $i\colon N \to E_f$ and $p\colon E_f \to Q$ to be the natural maps $i(x) = (x, 1)$ and $p(x, g) = g$ for $x \in N$, $g \in Q$.

The verification that i and p are homomorphic is nearly exactly the same as in the case of semidirect products: for i the fact that $f(g, 1) = f(1, g) = 0$ for all $g \in G$ is needed so that $f(1, 1) = 0$. Similarly, $\operatorname{Ker} p = N \times 1 = \operatorname{Im} i$ holds, so $0 \to N \xrightarrow{i} E_f \xrightarrow{p} Q \to 0$ is an extension.

Lastly, letting $s\colon Q \to E_f$ be the natural section $s(g) = (0, g)$ for all $g \in Q$ (which is normalised), we see that

$$s(g)i(x) = (0, g)(x, 1) = (0 + gx + f(g, 1), g1) = (gx, g)$$
$$i(gx)s(g) = (gx, 1)(0, g) = (gx + 1.0 + f(1, g), 1g) = (gx, g)$$

for all $x \in N$ and $g \in G$, so the commutation rule of Remark 2.7 holds and E_f realises the operators, and

$$\begin{aligned} i(f(g, h))s(gh) &= (f(g, h), 1)(0, gh) = (f(g, h) + 1.0 + f(1, gh), gh) \\ &= (f(g, h), gh) = (0 + g.0 + f(g, h), gh) = (0, g)(0, h) = s(g)s(h) \end{aligned}$$

for all $g, h \in Q$ so f is the factor set of the section s. All in all, we have showed the following:

Theorem 2.19. *Suppose Q acts on N. A function $f\colon Q \times Q \to N$ is a factor set of some extension realising the operators if and only if it satisfies the conditions*

i) $f(1, g) = 0 = f(g, 1)$ *for all* $g \in Q$

ii) $f(g, h) + f(gh, k) = g.f(h, k) + f(g, hk)$ *for all* $g, h, k \in Q$.

One such extension is $0 \to N \xrightarrow{i} E_f \xrightarrow{p} Q \to 0$ *as constructed above.* □

Conditions i) and ii) are called the normalisation condition and (perhaps teleologically) the cocycle condition.

Much like derivations, factor sets turn out to form an abelian group under pointwise sum, because the zero function is a factor set and the expressions in conditions i) and ii) are linear in f.

Definition 2.20. Given a group Q acting on an abelian group N, the set of factor sets $Q \times Q \to N$ is an abelian group called $\mathcal{F}(Q, N)$.

The last question to answer is when two factor sets define the same extension. Factor sets correspond to normalised sections, and if two extensions are isomorphic then one section can be transported into the other extension via the isomorphism. Thus we want to set two factor sets to be equivalent if they arise from normalised sections of the same extension.

Given an extension $0 \to N \xrightarrow{i} E \xrightarrow{p} Q \to 0$ and a normalised section $s\colon Q \to E$, any other section differs from it by a choice of coset representatives (except at 0), so a generic section is of the form $s'(g) = i(c(g)) + s(g)$ for a function $c\colon Q \to N$ with $c(1) = 0$ (so that s' is normalised). Let f be the factor set associated to s. The factor set f' associated to s' is defined by

$$\begin{aligned} s'(g) + s'(h) &= i(c(g)) + s(g) + i(c(h)) + s(h) \\ &= i(c(g)) + i(g.c(h)) + s(g) + s(h) \\ &= i(c(g)) + i(g.c(h)) + i(f(g,h)) - i(c(gh)) + i(c(gh)) + s(gh) \\ &= i\Big(c(g) + g.c(h) + f(g,h) - c(gh)\Big) + s'(gh), \end{aligned}$$

so the factor set is $f'(g,h) = g.c(h) - c(gh) + c(g) + f(g,h)$, and f and f' differ by $g.c(h) - c(gh) + c(h)$. This motivates the following definition.

Definition 2.21. Two factor sets $f, f'\colon Q \times Q \to N$ are said to be *equivalent* if $f(g,h) - f'(g,h) = g.c(h) - c(gh) + c(g)$ for some function $c\colon Q \to N$ with $c(1) = 0$. Factor sets equivalent to the zero set – that is, of the form $g.c(h) - c(gh) + c(g)$ – are called *split*, and their subgroup is denoted $\mathcal{S}(Q, N)$.

Split factor sets get their name from the fact that they correspond split extensions. This is because split factor sets are equivalent to the zero factor set – which corresponds to the semidirect product extension – and equivalent factor sets define equivalent extensions, as seen above.

To summarise, given a group Q acting on an abelian group N, inequivalent extensions $0 \to N \to E \to Q \to 0$ are in one-to-one correspondence to elements of $\mathcal{F}(Q, N)/\mathcal{S}(Q, N)$, which has the structure of an abelian group.

Chapter 3

A first definition

To prepare for the machinery of homology, we first need to convert the Q-action on the abelian group N into a module structure on N. This is done by extending the acting group Q into a ring.

3.1 Group rings and G-modules

Definition 3.1. Given a group G, the *group ring* $\mathbf{Z}G$ is defined to be the free $\mathbf{Z}$-algebra with basis G where multiplication of basis elements is given by the group law.

To elaborate, the elements of $\mathbf{Z}G$ are formal $\mathbf{Z}$-linear combinations of elements of G, and multiplication in $\mathbf{Z}G$ is simply the group law of G extended bilinearly. Because the group law of G is associative and unital, so is the algebra $\mathbf{Z}G$; as associative, unital $\mathbf{Z}$-algebras correspond to rings and vice versa, this means that $\mathbf{Z}G$ is a ring, with unity being $1e$. Note that $\mathbf{Z}G$ is commutative precisely when G is abelian, since the coefficient ring $\mathbf{Z}$ is commutative.

As $\mathbf{Z}G$ is a free algebra, to define a map out of $\mathbf{Z}G$ it is enough to specify it on the basis G, and in order for it to preserve multiplication, the map on the basis should be homomorphic. This is codified in the following lemma.

Lemma 3.2. *For a group G and a ring R there is a bijection*

$$\mathrm{Hom}_{\mathbf{Ring}}(\mathbf{Z}G, R) \cong \mathrm{Hom}_{\mathbf{Grp}}(G, R^*)$$

where R^* is the group of units of R. Furthermore, this is an adjunction between the functors $\mathbf{Z}-$ and $-^*$.

Proof. Take a ring map $f\colon \mathbf{Z}G \to R$. Since $f(g)f(g^{-1}) = f(e) = 1$ for all $g \in G$, we have that $fG \subseteq R^*$, so f restricts to $f\restriction G\colon G \to R^*$.

Conversely, any group homomorphism $g\colon G \to R^*$ extends linearly to a ring map $\hat{g}\colon \mathbf{Z}G \to R$ defined by $\hat{g}(\sum_i n_i g_i) = \sum_i n_i g(g_i)$. This is because $\mathbf{Z}G$ is a free algebra with basis G, and $\hat{g}$ preserves multiplication since g does.

To see the naturality of the isomorphisms, consider a group map $h\colon H \to G$ and a ring map $k\colon R \to S$. The functor $\mathbf{Z}-$ extends h linearly to $\hat{h}\colon \mathbf{Z}H \to \mathbf{Z}G$, and the functor $-^*$ restricts k to $k{\restriction}R^*\colon R^* \to S^*$. We want to show that the below square commutes.

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbf{Ring}}(\mathbf{Z}G, R) & \xrightarrow{-\restriction G} & \mathrm{Hom}_{\mathbf{Grp}}(G, R^*) \\ {\scriptstyle k \circ - \circ \hat{h}}\downarrow & & \downarrow{\scriptstyle k\restriction R^* \circ - \circ h} \\ \mathrm{Hom}_{\mathbf{Ring}}(\mathbf{Z}H, S) & \xrightarrow[-\restriction H]{} & \mathrm{Hom}_{\mathbf{Grp}}(H, S^*) \end{array}$$

Taking $f\colon \mathbf{Z}G \to R$, we should have that $k{\restriction}R^* \circ f{\restriction}G \circ h = (k \circ f \circ \hat{h}){\restriction}H$. Indeed, since $\hat{h}{\restriction}H = h$, we see that

$$(k \circ f \circ \hat{h})\restriction H = k \circ f \circ \hat{h}\restriction H = k \circ f \circ h = k\restriction R^* \circ f\restriction G \circ h,$$

as desired. □

Definition 3.3. Given a group G, a *G-module* M is a left $\mathbf{Z}G$-module. Similarly, a map of G-modules is a $\mathbf{Z}G$-module homomorphism.

Unwrapping the definition, it says that M is an abelian group that comes equipped with scalar multiplication by elements of $\mathbf{Z}G$, satisfying the usual laws for all $g, g' \in \mathbf{Z}G$ and $m, m' \in M$:

i) $1m = m$,

ii) $g'(gm) = (g'g)m$,

iii) $g(m + m') = gm + gm'$,

iv) $(g + g')m = gm + g'm$.

Taking $g, g' \in G$, we see that the first two conditions define an action of G on M, the third says that the action should respect the addition on M, and the fourth says that the action should extend to $\mathbf{Z}G$ linearly. So, we see that a G-module M is an abelian group M equipped with an action of G on M that respects the group structure (that is, the maps $m \mapsto gm$ are homomorphisms).

In the other direction, a G-action on a $\mathbf{Z}$-module M that respects addition in M is readily linearised: the action is a group homomorphism $G \to \mathrm{Aut}(M)^*$, and by the above lemma this extends to a ring homomorphism $\mathbf{Z}G \to \mathrm{Aut}(M)$, and this map defines scalar multiplication satisfying conditions i–iv) above. Thus G-modules are effectively linearised group actions on abelian groups.

The collection of maps between G-modules M and N is denoted by $\mathrm{Hom}_G(M, N)$ (instead of $\mathrm{Hom}_{\mathbf{Z}G}(M, N)$, for slight brevity). A G-linear map is of course $\mathbf{Z}$-linear,

and a $\mathbf{Z}$-linear map is G-linear if and only if it is equivariant with respect to the G-actions.

Example 3.4. A natural example is given by Galois extensions $K \supset k$ and the associated Galois groups $\mathrm{Gal}(K/k)$ acting on K: by linearising the action, K becomes a $\mathrm{Gal}(K/k)$-module.

Example 3.5. G-modules also arise naturally from normal subgroups. Suppose $N \trianglelefteq G$: then G acts on N by conjugations as $g.n = gng^{-1}$. This action respects the group law in N: if $n, n' \in N$ and $g \in G$, then

$$g.(nn') = gnn'g^{-1} = gng^{-1}gn'g^{-1} = (g.n)(g.n').$$

Thus, if N is abelian, then it is naturally a G-module. In this case, N is also a G/N-module by defining $gN.n = g.n$. This does not depend on the choice of representative for the coset: for any $n \in N$ and any other representative $gh \in gN$, n and h commute so $h.n = n$ and $gh.n = g.(h.n) = g.n$.

Example 3.6. Any G-set X can be linearised and turned into a G-module by extending X into the free abelian group $X^{(\mathbf{Z})}$, extending the G-action linearly into $X^{(\mathbf{Z})}$, and then extending this into a $\mathbf{Z}G$-action as above.

Note that the resulting G-module $X^{(\mathbf{Z})}$ above is rarely the same as the free G-module on X: for example, if $g \in G_x$ is not 1, then $(g-1)x = 0$ is a nontrivial linear combination.

Example 3.7. Any G-set X can be extended into a free G-module, say Y, with basis X without losing the original G-action.

Observe that by freeness, the G-action that Y receives must be free: if $g.y = h.y$ for some $y \in Y \setminus \{0\}$, then it must be that $g = h$ lest $(g-h).y = 0$ be a nontrivial linear combination. Also, X must be a basis, so any $y \in Y$ must be expressible as $\sum_{x \in X} k_x g_x.x$ for $k_x \in \mathbf{Z}, g_x \in G$. Thus each $x \in X$ must have a trivial isotropy group, and the orbits Gx, $x \in X$ must span Y over coefficients from $\mathbf{Z}$.

To keep isotropy groups trivial we turn to the set $G \times X$, intending the pair (g, x) to represent gx. This would be accomplished by setting the G-action to be $g.(g', x) = (gg', x)$, but note that it does not depend at all on the original group action, $G \times X \to X, (g, x) \mapsto gx$, only turning it into a G-equivariant map. Another natural action is the diagonal action $g.(g', x) = (gg', gx)$: it has the advantage that the original group action is now intrinsic in the structure, and it turns the second projection $\mathrm{pr}_2 \colon G \times X \to X$ into a G-equivariant map.

We thus choose to endow $G \times X$ with the diagonal action. Now letting Y be the free abelian group on $G \times X$ (and extending the G-action linearly) makes Y a free $\mathbf{Z}G$-module on $\{1\} \times X$.

Firstly, we note that $\{1\} \times X$ is a $\mathbf{Z}G$-basis. Indeed, if $\sum_{i<n} k_i g_i.(1, x_i) = 0$ is a linear combination without repetition – that is $x_i \neq x_j$ when $i \neq j$ – then we may write it as

$$\sum_{i<n} k_i g_i.(1, x_i) = \sum_{i<n} k_i (g_i, g_i x_i)$$

which is again a sum without repetition: if $(g_i, g_i x_i) = (g_j, g_j x_j)$, then $g_i = g_j$ whence $x_i = g_i^{-1} g_i x_i = g_j^{-1} g_j x_j = x_j$. Now, since Y is a $\mathbf{Z}$-module over $G \times X$, it follows that $k_i = 0$ for all $i < n$, affirming freeness of $\{1\} \times X$ over $\mathbf{Z}G$.

Since $G \times X$ spans Y over $\mathbf{Z}$, we have that for any $y \in Y$,

$$y = \sum_{i<n} k_i (g_i, x_i) = \sum_{i<n} k_i g_i.(1, g_i^{-1} x_i).$$

This means that $\{1\} \times X$ spans Y over $\mathbf{Z}G$. Thus we obtain a concrete description of a free G-module over a G-set X.

Remark 3.8. Note that there is nothing special about the ring $\mathbf{Z}$: the same constructions would work replacing $\mathbf{Z}$ by any commutative ring. (The category **Ring** in Lemma 3.2 should be replaced with the category $\mathbf{Alg}_R$.)

3.2 Motivating observations

Recall that the defining formula of a derivation $d\colon Q \to N$, by Definition 2.15, is $d(gh) = d(g) + g.d(h)$. It can be rearranged into the form

$$0 = g.d(h) - d(gh) + d(g).$$

Notice how similar this is to the defining formula of a split factor set. By Definition 2.21, they are functions $Q \times Q \to N$ of the form

$$f(g, h) = g.c(h) - c(gh) + c(g).$$

These equations have right sides of exactly the same form! The equations suggest that d belongs to the kernel of some operator, and that f belongs in its image.

Furthermore, compare these to the characterisation of a factor set given by Theorem 2.19. Factor sets are functions $f\colon Q \times Q \to N$ satisfying the identity $f(g, h) + f(gh, k) = g.f(h, k) + f(g, hk)$, which can be rearranged to

$$0 = g.f(h, k) - f(gh, k) + f(g, hk) - f(g, h),$$

which is a natural generalisation of the corresponding formula for derivations. Thus, factor sets can be seen as functions lying in the kernel of an operator, split factor sets can be seen as the image of another analogous operator, and their quotient $\mathcal{F}(Q, N)/\mathcal{S}(Q, N)$ is an interesting group: it is reminiscent of a cohomology group of a cochain complex.

Remark on notation. Moving away from group extensions, we start denoting groups by G instead of Q and G-modules by M instead of N: for element names we still use $g, h, \ldots \in G$ and $x, y, \ldots \in M$.

Emcouraged by the similarity of these equations, we set out to form a cochain complex of the form

$$0 \to \mathrm{Hom}(G^0, M) \xrightarrow{d^0} \mathrm{Hom}(G, M) \xrightarrow{d^1} \mathrm{Hom}(G^2, M) \xrightarrow{d^2} \cdots,$$

where the coboundary operators are defined by

$$\begin{aligned} d^n(f)(g_0, \ldots, g_n) &= g_0.f(g_1, \ldots, g_n) \\ &\quad + \sum_{i=1}^{n} (-1)^i f(g_0, \ldots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \ldots, g_n) \\ &\quad + (-1)^{n+1} f(g_0, \ldots, g_{n-1}). \end{aligned}$$

Note that for $n = 1$ and $n = 2$, we get the formulas

$$\begin{aligned} d^1(c)(g, h) &= g.c(h) - c(gh) + c(g) \\ d^2(f)(g, h, k) &= g.f(h, k) - f(gh, k) + f(g, hk) - f(g, h) \end{aligned}$$

as special cases. The zeroth coboundary deserves a comment: it is the function $d^0\colon \mathrm{Hom}(G^0, M) \to \mathrm{Hom}(G, M)$ taking a constant (rather, a nullary function) $x \in M$ to the function $d^0(x)(g) = g.x() - x() = g.x - x$.

However, there is a slight aesthetic flaw: here M is a G-module while G is a group and the hom-sets are those of **Set**, made into abelian groups by recalling that the target M was also an abelian group. This can be remedied by replacing the sets G^n with free G-modules with bases G^n.

Definition 3.9. Let G be a group and let it act on G^n diagonally for $n \in \mathbf{N}$. We define B_n to be the free G-module on G^n as constructed in Example 3.7: thus B_n is the free abelian group on $G \times G^n$ equipped with the diagonal G-action extended to $\mathbf{Z}G$. The basis elements $(1, g_1, \ldots, g_n) \in \{1\} \times G^n$ are customarily denoted by $[g_1 | \ldots | g_n]$.

Remark 3.10. Derivations and factor sets did not involve a G-action on G^n, so the choice of action is somewhat arbitrary: the trivial and diagonal actions are two natural candidates. Remark 3.11 shows the value of choosing the diagonal action.

We could now define a cochain complex as before, but using B_n in place of G^n:

$$0 \to \mathrm{Hom}_G(B_0, M) \xrightarrow{d^0} \mathrm{Hom}_G(B_1, M) \xrightarrow{d^1} \mathrm{Hom}_G(B_2, M) \xrightarrow{d^2} \cdots,$$

where the hom-sets are of G-module maps, and the coboundary maps are defined on the bases as before by

$$\begin{aligned} d^n(f)([g_1|\dots|g_{n+1}]) &= g_1.f([g_2|\dots|g_{n+1}]) \\ &\quad + \sum_{i=1}^{n}(-1)^i f([g_1|\dots|g_{i-1}|g_ig_{i+1}|g_{i+2}|\dots|g_{n+1}]) \\ &\quad + (-1)^{n+1}f([g_1|\dots|g_n]) \end{aligned}$$

and extended linearly. It is starting to look a lot like a cochain complex obtained from an application of $\mathrm{Hom}_G(-, M)$. Since f is now a map of G-modules, the first term equals $f(g_1.[g_2|\dots|g_{n+1}])$, and we can pull all the sums inside f as

$$d^n(f)([g_1|\dots|g_{n+1}]) = f(g_1.[g_2|\dots|g_{n+1}] - [g_1g_2|\dots|g_{n+1}] + \dots \pm [g_1|\dots|g_n]).$$

It is now evident that if we define $\delta_{n,i}\colon B^n \to B^{n-1}$ by

$$\delta_{n,i}([g_1|\dots|g_n]) = \begin{cases} g_1.[g_2|\dots|g_n], & i = 0, \\ [g_1|\dots|g_{i-1}|g_ig_{i+1}|g_{i+2}|\dots|g_n], & 0 < i < n, \\ [g_1|\dots|g_{n-1}], & i = n, \end{cases}$$

and let $\partial_{n+1}\colon B^{n+1} \to B^n$ be the alternating sum $\partial_{n+1} = \sum_{i\le n+1}(-1)^i\delta_{n+1,i}$, then the coboundary map becomes $d^n(f)(x) = f(\partial_{n+1}(x))$, that is

$$d^n(f) = f \circ \partial_{n+1} = (- \circ \partial_{n+1})(f) = \mathrm{Hom}_G(\partial_{n+1}, M)(f).$$

All of this means that the cochain complex written above is obtained from the chain complex

$$\dots \to B_2 \xrightarrow{\partial_2} B_1 \xrightarrow{\partial_1} B_0 \to 0$$

by applying to it the contravariant functor $\mathrm{Hom}_G(-, M)$. It turns out that this is almost an exact complex, which becomes exact once ∂_1 is followed by its cokernel: this is called the *bar resolution* of G, and its exactness will turn out to be very useful.

Remark 3.11. Again, the maps ∂_n are slightly asymmetric in the first and last terms, which can be remedied by adding a trivial right G-action on M and adjusting $\delta_{n,n} = [g_1|\dots|g_{n-1}].g_n$. However, there is another way of restoring symmetry.

If we change bases by $[g_1|\dots|g_n] = (1, g_1, g_1g_2, \dots, \prod_{i\le n} g_i)$, the converse is $(1, g_1, g_2, \dots, g_n) = [g_1|g_1^{-1}g_2|g_2^{-1}g_3|\dots|g_{n-1}^{-1}g_n]$. Recall that G acts on G^{n+1} diagonally. With these choices, in the alternate basis the maps $\delta_{n,i}$ become

$$\begin{aligned} \delta_{n,0}(1, g_1, \dots, g_n) &= \delta_{n,0}([g_1|g_1^{-1}g_2|g_2^{-1}g_3|\dots|g_{n-1}^{-1}g_n]) \\ &= g_1.[g_1^{-1}g_2|g_2^{-1}g_3|\dots|g_{n-1}^{-1}g_n] \\ &= g_1.(1,\ g_1^{-1}g_2,\ g_1^{-1}g_2g_2^{-1}g_3, \dots,\ g_1^{-1}g_2g_2^{-1}g_3\cdots g_{n-1}^{-1}g_n) \\ &= (g_1, g_2, \dots, g_n), \end{aligned}$$

$$\begin{aligned}\delta_{n,1}(1, g_1, \ldots, g_n) &= \delta_{n,1}([g_1|g_1^{-1}g_2|g_2^{-1}g_3|\ldots|g_{n-1}^{-1}g_n]) \\ &= [g_2|g_2^{-1}g_3|\ldots|g_{n-1}^{-1}g_n] \\ &= (1, g_2, \ldots, g_n),\end{aligned}$$

and similarly $\delta_{n,i}(1, g_1, \ldots, g_n) = (1, g_1, \ldots, \hat{g}_i, \ldots, g_n)$ for $2 \leq i \leq n$, where the hat denotes omission. This is directly comparable to the defining alternating sum of simplicial homology!

The astute reader will recall one more detail that has been swept aside. While inspecting the defining formulae of derivations and factor sets, we neglected to take into account the conditions $d(1) = 0$ and $f(1, g) = f(g, 1) = 0$ that factor sets must satisfy. The general condition for a function $f\colon G^n \to M$ is evidently $f(g_1, \ldots, g_n) = 0$ if $g_i = 1$ for some i.

This restriction can be taken into account in the bar complex by dividing out the tuples containing 1. Define $D_n \subseteq B_n$ to be the submodule generated by the degenerate tuples containing a 1: one can then use the quotient complex B_n/D_n. (Taking the submodules B'_n generated by tuples not containing a 1 will not work because $\delta_{n,i}$ does not map B'_n into B'_{n-1}.)

We hope the reader has been thoroughly motivated: it is time to proceed to verifying the claims made here.

3.3 The bar resolution

Definition 3.12. Let G be a group. For $n \in \mathbf{N}$, let B_n be the free G-module on G^n with basis elements denoted by $[g_1|\ldots|g_n]$. The *bar resolution* of G, denoted $B_\bullet(G)$, is the complex

$$\cdots \to B_2 \xrightarrow{\partial_2} B_1 \xrightarrow{\partial_1} B_0 \xrightarrow{\varepsilon} \mathbf{Z}_t \to 0,$$

where $\partial_n = \sum_{i \leq n} (-1)^i \, \delta_{n,i}$ with the G-linear maps $\delta_{n,i}\colon B_n \to B_{n-1}$ being defined on bases as

$$\delta_{n,i}([g_1|\ldots|g_n]) = \begin{cases} g_1.[g_2|\ldots|g_n], & i = 0 \\ [g_1|\ldots|g_{i-1}|g_ig_{i+1}|g_{i+2}|\ldots|g_n], & 0 < i < n \\ [g_1|\ldots|g_{n-1}], & i = n. \end{cases}$$

Here, $\mathbf{Z}_t$ is the free $\mathbf{Z}$-module on one generator with trivial G-action, and $\varepsilon\colon B_0 \to \mathbf{Z}_t$ is the G-linear map defined by $\varepsilon([\,]) = 1$. The map ε is called the *augmentation map*.

Remark 3.13. Note that as B_0 is the free $\mathbf{Z}G$-module on one generator, it is isomorphic to $\mathbf{Z}G$, and ε can be viewed as the $\mathbf{Z}$-linear map sending $g \mapsto 1$ for all $g \in G$.

Lemma 3.14. *For a group G, the bar resolution $B_\bullet(G)$ is exact, so it is an acyclic complex.*

Proof. As constructed in Example 3.7, we can take B_n to be the free $\mathbf{Z}$-module with basis G^{n+1} and diagonal G-action, and $\mathbf{Z}G$-basis $\{1\} \times G^n$. We first verify that $B_\bullet(G)$ is a chain complex, and then construct a contracting homotopy.

Since the function $\tau\colon \{[g_1|\dots|g_n] \mid g_1,\dots,g_n \in G\} \to \{1\} \times G^n$ defined by $[g_1|\dots|g_n] \mapsto (1, g_1, g_1g_2, \dots, g_1g_2\cdots g_n)$ is a bijection (with the inverse being $(1, g_1, \dots, g_n) \mapsto [g_1|g_1^{-1}g_2|\dots|g_{n-1}^{-1}g_n]$), we can set $[g_1|\dots|g_n] = (1, g_1, \dots, g_n)$ to lighten the notation. We can then calculate the values $\delta_{n,i}(1, g_1, \dots, g_n) = \delta_{n,i}([g_1|g_1^{-1}g_2|\dots|g_{n-1}^{-1}g_n])$ in the alternate basis. Firstly,

$$\begin{aligned}
&\delta_{n,0}([g_1|g_1^{-1}g_2|g_2^{-1}g_3|\dots|g_{n-1}^{-1}g_n]) \\
&= g_1.[g_1^{-1}g_2|g_2^{-1}g_3|\dots|g_{n-1}^{-1}g_n] \\
&= g_1.(1,\ g_1^{-1}g_2,\ g_1^{-1}g_2g_2^{-1}g_3, \dots, g_1^{-1}g_2\cdots g_{n-1}^{-1}g_n) \\
&= (g_1, g_2, \dots, g_n),
\end{aligned}$$

where the products first telescope down to $g_1^{-1}g_i$ in each coordinate, and lastly g_1^{-1} is cancelled by the g_1 acting diagonally. Then, setting $g_0 = 1$ so that $g_1 = g_0^{-1}g_1$ for uniformity,

$$\begin{aligned}
&\delta_{n,i}([g_0^{-1}g_1|g_1^{-1}g_2|\dots|g_{n-1}^{-1}g_n]) \\
&= [g_0^{-1}g_1|\dots|g_{i-2}^{-1}g_{i-1}|g_{i-1}^{-1}g_ig_i^{-1}g_{i+1}|g_{i+1}^{-1}g_{i+2}|\dots|g_{n-1}^{-1}g_n] \\
&= [g_0^{-1}g_1|\dots|g_{i-2}^{-1}g_{i-1}|g_{i-1}^{-1}g_{i+1}|g_{i+1}^{-1}g_{i+2}|\dots|g_{n-1}^{-1}g_n] \\
&= (1, g_1, g_2, \dots, g_{i-1}, g_{i+1}, \dots, g_n)
\end{aligned}$$

for $1 \le i < n$, and lastly

$$\begin{aligned}
&\delta_{n,n}([g_1|g_1^{-1}g_2|\dots|g_{n-2}^{-1}g_{n-1}|g_{n-1}^{-1}g_n]) \\
&= [g_1|g_1^{-1}g_2|\dots|g_{n-2}^{-1}g_{n-1}] \\
&= (1, g_1, \dots, g_{n-1}).
\end{aligned}$$

So all in all $\delta_{n,i}(1, g_1, \dots, g_n) = (1, g_1, \dots, \hat{g}_i, \dots, g_n)$ with the omission of g_0 understood to be omission of the 1 in front. The omission formula holds even if the first element of the tuple is $g_0 \neq 1$, because

$$\begin{aligned}
\delta_{n,i}(g_0, g_1, \dots, g_n) &= \delta_{n,i}(g_0.(1, g_0^{-1}g_1, \dots, g_0^{-1}g_n)) = g_0.\delta_{n,i}(1, g_0^{-1}g_1, \dots, g_0^{-1}g_n) \\
&= g_0.(1, g_0^{-1}g_1, \dots, \hat{g}_0^{-1}\hat{g}_i, \dots, g_0^{-1}g_n) = (g_0, \dots, \hat{g}_i, \dots, g_n).
\end{aligned}$$

To calculate ∂^2, we need to first calculate δ^2:

$$\begin{aligned}\delta_{n+1,i}(\delta_{n,j}(1,g_1,\ldots,g_n)) &= \delta_{n+1,i}(1,g_1,\ldots,\hat{g}_j,\ldots,g_n)\\ &= \begin{cases}(1,g_1,\ldots,\hat{g}_i,\ldots,\hat{g}_j,\ldots,g_n), & i<j\\ (1,g_1,\ldots,\hat{g}_j,\ldots,\hat{g}_{i+1},\ldots,g_n), & i\geq j\end{cases}\\ &= \begin{cases}\delta_{n+1,j-1}(\delta_{n,i}(1,g_1,\ldots,g_n)), & j-1\geq i\\ \delta_{n+1,j}(\delta_{n,i+1}(1,g_1,\ldots,g_n)), & j<i+1.\end{cases}\end{aligned}$$

We then get

$$\begin{aligned}\partial_{n+1}\,\partial_n &= \sum_{i=0}^{n+1}(-1)^i\,\delta_{n+1,i}\left(\sum_{j=0}^{n}(-1)^j\,\delta_{n,j}\right) = \sum_{\substack{0\leq i\leq n+1\\ 0\leq j\leq n}}(-1)^{i+j}\,\delta_{n+1,i}\,\delta_{n,j}\\ &= \sum_{0\leq j<i\leq n+1}(-1)^{i+j}\,\delta_{n+1,i}\,\delta_{n,j} + \sum_{0\leq i\leq j\leq n}(-1)^{i+j}\,\delta_{n+1,i}\,\delta_{n,j}:\end{aligned}$$

in the first sum we apply the identity $(-1)^{i+j}\,\delta_{n+1,i}\,\delta_{n,j} = (-1)^{i+1+j-1}\,\delta_{n+1,j}\,\delta_{n,i+1}$ and rename $i+1$ to k ranging between j and n to get

$$\partial_{n+1}\partial_n = \sum_{0\leq j\leq k\leq n}(-1)^{k+j-1}\,\delta_{n+1,j}\,\delta_{n,k} + \sum_{0\leq i\leq j\leq n}(-1)^{i+j}\,\delta_{n+1,i}\,\delta_{n,j} = 0,$$

whence the sums evidently cancel out. Also,

$$\varepsilon(\partial_0([g])) = \varepsilon(g.[\,] - [\,]) = g.\varepsilon([\,]) - \varepsilon([\,]) = 0,$$

because the G-action on $\mathbf{Z}_t$ is trivial. Thus $B_\bullet(G)$ is a chain complex.

To show that the complex is acyclic, we find a contracting homotopy s satisfying $s\partial + \partial s = \mathrm{id}$. However, the components of s will not be $\mathbf{Z}G$-linear maps, but only $\mathbf{Z}$-linear, so the whole complex will have to be considered as a complex of $\mathbf{Z}$-modules: this is not a problem, because this does not change the kernels and images of ∂. Note that because $\{1\}\times G^n$ is a $\mathbf{Z}G$-basis of B_n, the orbits G^{n+1} form a $\mathbf{Z}$-basis.

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & B_2 & \xrightarrow{\partial_2} & B_1 & \xrightarrow{\partial_1} & B_0 & \xrightarrow{\varepsilon} & \mathbf{Z}_t & \longrightarrow & 0\\
 & \swarrow & \downarrow{\scriptstyle \mathrm{id}} & \swarrow{\scriptstyle s_1} & \downarrow{\scriptstyle \mathrm{id}} & \swarrow{\scriptstyle s_0} & \downarrow{\scriptstyle \mathrm{id}} & \swarrow{\scriptstyle s_{-1}} & \downarrow{\scriptstyle \mathrm{id}} & \swarrow{\scriptstyle 0} & \\
\cdots & \longrightarrow & B_2 & \xrightarrow[\partial_2]{} & B_1 & \xrightarrow[\partial_1]{} & B_0 & \xrightarrow[\varepsilon]{} & \mathbf{Z}_t & \longrightarrow & 0
\end{array}$$

Caveat stated, define $s_n\colon B_n \to B_{n+1}$ on bases by $s_n(g_0,\ldots,g_n) = (1,g_0,\ldots,g_n)$ for $n\geq 0$ and $s_{-1}(1) = (1)$. Now, for $n\geq 1$,

$$\begin{aligned}\partial_{n+1}(s_n(g_0,\ldots,g_n)) &= \partial_{n+1}(1,g_0,\ldots,g_n)\\ &= (g_0,\ldots,g_n) - \sum_{0\leq i\leq n}(-1)^i(1,g_0,\ldots,\hat{g}_i,\ldots,g_n)\end{aligned}$$

and

$$\begin{aligned} s_{n-1}(\partial_n(g_0,\dots,g_n)) &= s_{n-1}\left(\sum_{0\le j\le n}(-1)^j(g_0,\dots,\hat{g}_j,\dots,g_n)\right) \\ &= \sum_{0\le j\le n}(-1)^j s_{n-1}(g_0,\dots,\hat{g}_j,\dots,g_n) \\ &= \sum_{0\le j\le n}(-1)^j(1,g_0,\dots,\hat{g}_j,\dots,g_n) \end{aligned}$$

so the alternating sums cancel out and $s_{n-1}\partial_n + \partial_{n+1}s_n = \mathrm{id}_{B_n}$. For $n = 0$,

$$s_{-1}(\varepsilon(g)) + \partial_1(s_0(g)) = s_{-1}(1) + \partial_1(1,g) = (1) + (g) - (1) = (g)$$

so $s_{-1}\circ\varepsilon + \partial_1\circ s_0 = \mathrm{id}_{B_0}$, and lastly for the case $n = -1$, $\varepsilon(s_{-1}(1)) = \varepsilon(1) = 1$ so $\varepsilon\circ s_{-1} = \mathrm{id}_{\mathbf{Z}_t}$. Thus s is a contraction and $B_\bullet(G)$ is acyclic. □

Remark 3.15. The trivial G-module $\mathbf{Z}_t$ and augmentation map ε are there to make the bar resolution exact at B_0: the exactness of the bar resolution will turn out to be very useful.

3.4 A first definition

Now is as good a time as any to set in stone a definition of group cohomology.

Definition 3.16. Let G be a group, $\cdots \to B_2 \xrightarrow{\partial_2} B_1 \xrightarrow{\partial_1} B_0 \xrightarrow{\varepsilon} \mathbf{Z}_t \to 0$ the bar resolution of G and M a G-module. The n-th *cohomology group* of G with coefficients in M, denoted $H^n(G,M)$, is the n-th cohomology group of the cochain complex

$$0 \to \mathrm{Hom}_G(B_0,M) \xrightarrow{\delta^0} \mathrm{Hom}_G(B_1,M) \xrightarrow{\delta^1} \mathrm{Hom}_G(B_2,M) \to \cdots$$

obtained by deleting the $\mathbf{Z}_t$-term in the bar resolution and then applying the contravariant Hom functor $\mathrm{Hom}_G(-,M)$. Explicitly, for $n \ge 0$,

$$H^n(G,M) = \frac{\mathrm{Ker}\,\delta^n}{\mathrm{Im}\,\delta^{n-1}} = \frac{\mathrm{Ker}\,\mathrm{Hom}_G(\partial_{n+1},M)}{\mathrm{Im}\,\mathrm{Hom}_G(\partial_n,M)} = \frac{\mathrm{Ker}\,\partial_{n+1}^*}{\mathrm{Im}\,\partial_n^*},$$

where δ^{-1} is the zero map.

Example 3.17. Let G be a group and M a G-module. We can now calculate $H^0(G,M)$. The map $\delta^0 = \partial_1^* = (-\circ\partial_1)\colon \mathrm{Hom}_G(B_0,M) \to \mathrm{Hom}_G(B_1,M)$ has the formula

$$\delta^0(f)([g]) = f(\partial_1([g])) = f(g.[\,] - [\,]) = g.f([\,]) - f([\,]) = (g-1).f([\,]).$$

Since B_0 is the free G-module on one generator $[\,]$, we have that $\mathrm{Hom}_G(B_0, M)$ is isomorphic to M by identifying $f\colon B_0 \to M$ with the element $f([\,]) \in M$. Under this identification, the map δ^0 looks like $\delta^0(x)([g]) = (g-1).x$.

Since $x \in \operatorname{Ker}\delta^0$ if and only if $\delta^0(x)$ maps the basis $\{[g] \mid g \in G\}$ of B_1 to 0, we see that $\operatorname{Ker}\delta^0$ consists of those $x \in M$ for which $g.x - x = 0$ for all $g \in G$, or equivalently $g.x = x$ for all $g \in G$. These elements form a submodule M^G of M, and they are the *fixed points* of the action of G on M. Thus $H^0(G, M) = M^G$. That the 0-th cohomology group also turned out meaningful adds to the merit of the definition.

Remark 3.18. Why was the augmentation map dropped from the defining cochain complex? The map $\varepsilon^* = (- \circ \varepsilon)\colon \mathrm{Hom}_G(\mathbf{Z}_t, M) \to \mathrm{Hom}_G(B_0, M)$ has the formula

$$\varepsilon^*(f)([\,]) = f(\varepsilon([\,])) = f(1)$$

so under the identification $\mathrm{Hom}_G(B_0, M) \cong M$ as in the previous example, $\varepsilon^*\colon \mathrm{Hom}_G(\mathbf{Z}_t, M) \to M$ is simply the map $\varepsilon^*(f) = f(1)$. It is injective because $\mathbf{Z}$ is a free $\mathbf{Z}$-module with basis $\{1\}$.

As for the group $\mathrm{Hom}_G(\mathbf{Z}_t, M)$, recall that $\mathbf{Z}_t$ has G acting trivially on it. A map in $\mathrm{Hom}_G(\mathbf{Z}_t, M)$ satisfies $g.f(1) = f(g1) = f(1)$ for all $g \in G$, so $f(1) \in M^G$. Conversely, any $\mathbf{Z}$-linear map sending 1 to an element of M^G is clearly G-equivariant (and thus G-linear), so $\mathrm{Hom}_G(\mathbf{Z}_t, M) \cong M^G$ under the identification $f \mapsto f(1)$.

These observations taken together mean that $\operatorname{Im}\varepsilon^* \cong M^G$, and considered as maps into $\mathrm{Hom}_G(B_0, M)$, also $\operatorname{Im}\varepsilon^* = \operatorname{Ker}\delta^0$. Thus, if ε was not removed from the defining cochain complex, the 0-th cohomology group would be identically 0, which is much less interesting than the alternative M^G.

We cannot yet show the first and second cohomology groups are what they should be. Currently the functions in, say, $\mathrm{Hom}_G(B_2, M)$ which we mean to represent factor sets with, have no reason to satisfy the conditions $f([1|g]) = 0 = f([g|1])$ for all $g \in G$. We next modify the bar resolution to take this into account.

3.5 The normalised bar resolution

Definition 3.19. Let G be a group and $B_\bullet(G) = \cdots \to B_1 \xrightarrow{\partial_1} B_0 \xrightarrow{\varepsilon} \mathbf{Z}_t \to 0$ its bar resolution. For each $n \geq 0$, let $U_n \subseteq B_n$ be the submodule generated by $\{[g_1|\ldots|g_n] \mid g_i = 1 \text{ for some } i\}$. These form a subcomplex of the bar resolution.

The *normalised bar resolution* $B^*_\bullet(G)$ is the quotient complex in the bottom row

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & U_2 & \xrightarrow{\partial_2 \restriction U_2} & U_1 & \xrightarrow{\partial_1 \restriction U_1} & U_0 & \xrightarrow{\varepsilon \restriction U_0} & 0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & B_2 & \xrightarrow{\partial_2} & B_1 & \xrightarrow{\partial_1} & B_0 & \xrightarrow{\varepsilon} & \mathbf{Z}_t & \longrightarrow & 0 \\
 & & {\scriptstyle q_2}\downarrow & & {\scriptstyle q_1}\downarrow & & {\scriptstyle q_0}\downarrow & & {\scriptstyle \mathrm{id}}\downarrow & & \\
\cdots & \longrightarrow & B_2/U_2 & \xrightarrow{\partial'_2} & B_1/U_1 & \xrightarrow{\partial'_1} & B_0/U_0 & \xrightarrow{\varepsilon'} & \mathbf{Z}_t & \longrightarrow & 0
\end{array}$$

where the equivalence classes $q_n([g_1|\dots|g_n]) = [g_1|\dots|g_n] + U_n$ are denoted by $[g_1, \dots, g_n]$, and the maps ∂'_n are the induced maps defined by

$$\partial'_n([g_1, \dots, g_n]) = q_{n-1}(\partial_n([g_1|\dots|g_n]))$$

and $\varepsilon'([\,] + U_0) = 1$.

We remark that this definition is what it claims to be.

Remark 3.20. In order for $\partial_n \colon B_n \to B_{n-1}$ to induce $\partial'_n \colon B_n/U_n \to B_{n-1}/U_{n-1}$, we should check that ∂_n maps U_n into U_{n-1}. Suppose $(g_0, \dots, g_n)$ has $g_{i-1} = g_i$. In the alternating sum $\partial_n(g_0, \dots, g_n)$, the terms $(-1)^{i-1}(g_0, \dots, g_{i-2}, g_i, g_{i+1}, \dots, g_n)$ and $(-1)^i(g_0, \dots, g_{i-2}, g_{i-1}, g_{i+1}, \dots, g_n)$ have opposite signs, so they cancel, and the rest of the terms contain both g_{i-1} and g_i, so they are in U_{n-1}. Thus $\partial_n U_n \subseteq U_{n-1}$, and $B^*_\bullet(G)$ is the quotient of the bar complex by the degenerate complex

$$\cdots \to U_2 \xrightarrow{\partial_2 \restriction U_2} U_1 \xrightarrow{\partial_1 \restriction U_1} U_0 \xrightarrow{\varepsilon \restriction U_0} 0 \to 0$$

as claimed; for the restricted augmentation map, note that $U_0 = \{0\}$. The map q is a chain map by definition.

Remark 3.21. Note that the quotient B_n/U_n is still a free G-module with the evident G-basis $\{(1, g_1, \dots, g_n) + U_n \mid g_1 \neq 1, g_{i-1} \neq g_i \text{ for } 2 \leq i \leq n\}$ in terms of tuples, $\{[g_1, \dots, g_n] \mid g_i \neq 1 \text{ for all } i\}$ in terms of brackets, and as a free $\mathbf{Z}$-module it has the $\mathbf{Z}$-basis $\{(g_0, \dots, g_n) \mid g_{i-1} \neq g_i \text{ for } 1 \leq i \leq n\}$. Also, $B_0/U_0 = B_0$ since $U_0 = \{0\}$.

The normalised bar complex is also acyclic, as the contracting homotopy defines another such in the quotient.

Lemma 3.22. *For a group G, the normalised bar resolution $B^*_\bullet(G)$ is exact, so it is an acyclic complex.*

Proof. As when proving that $B_\bullet(G)$ is acyclic in Lemma 3.14, we treat $B^*_\bullet(G)$ as a complex of $\mathbf{Z}$-modules. Recall that the contracting homotopy s of $B_\bullet(G)$ was defined on bases as

$$s_{-1}\colon \mathbf{Z}_t \to B_0,\ 1 \mapsto (1) \quad \text{and} \quad s_n\colon B_n \to B_{n+1},\ (g_0,\dots,g_n) \mapsto (1,g_0,\dots,g_n)$$

for $n \geq 0$. We show that the homotopy s descends to a contracting homotopy t of $B^*_\bullet(G)$ in the quotient, the defining squares depicted below.

$$\begin{array}{ccc} \mathbf{Z}_t & \xrightarrow{s_{-1}} & B_0 \\ \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle q_0} \\ \mathbf{Z}_t & \xrightarrow[t_{-1}]{} & B_0/U_0 \end{array} \qquad \begin{array}{ccc} B_n & \xrightarrow{s_n} & B_{n+1} \\ \downarrow{\scriptstyle q_n} & & \downarrow{\scriptstyle q_{n+1}} \\ B_n/U_n & \xrightarrow[t_n]{} & B_{n+1}/U_{n+1} \end{array}$$

In degree -1, defining $t_{-1}\colon \mathbf{Z} \to B_0/U_0$, $t_{-1} = q_0 s_{-1}$ makes the quotient square commute. For $n \geq 0$, we only need to check that s_n maps U_n into U_{n+1}. As U_n has the set $\{(g_0,g_1,\dots,g_n) \mid g_{i-1} = g_i \text{ for some } i\}$ as a $\mathbf{Z}$-basis, this is evident: thus s_n defines $t_n\colon B_n/U_n \to B_{n+1}/U_{n+1}$ so that it satisfies $t_n q_n = q_{n+1} s_n$.

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & B_2/U_2 & \xrightarrow{\partial'_2} & B_1/U_1 & \xrightarrow{\partial'_1} & B_0/U_0 & \xrightarrow{\varepsilon'} & \mathbf{Z}_t & \longrightarrow & 0 \\ & \swarrow & \downarrow{\scriptstyle \mathrm{id}} & \swarrow{\scriptstyle t_1} & \downarrow{\scriptstyle \mathrm{id}} & \swarrow{\scriptstyle t_0} & \downarrow{\scriptstyle \mathrm{id}} & \swarrow{\scriptstyle t_{-1}} & \downarrow{\scriptstyle \mathrm{id}} & \swarrow{\scriptstyle 0} & \\ \cdots & \longrightarrow & B_2/U_2 & \xrightarrow[\partial'_2]{} & B_1/U_1 & \xrightarrow[\partial'_1]{} & B_0/U_0 & \xrightarrow[\varepsilon']{} & \mathbf{Z}_t & \longrightarrow & 0 \end{array}$$

To show that t satisfies the chain homotopy equations, we show that the squares below commute. It is not hard, but requires keeping in mind all the relevant equations from the definitions of t and the normalised bar resolution, collected below.

$$t_{-1} = q_0 s_{-1}, \qquad t_n q_n = q_{n+1} s_n, \qquad \varepsilon = \varepsilon' q_0, \qquad q_{n-1}\partial_n = \partial'_n q_n.$$

$$\begin{array}{ccc} \mathbf{Z}_t & \xrightarrow[=\mathrm{id}_{\mathbf{Z}_t}]{\varepsilon s_{-1}} & \mathbf{Z}_t \\ \downarrow{\scriptstyle \mathrm{id}_{\mathbf{Z}_t}} & & \downarrow{\scriptstyle \mathrm{id}_{\mathbf{Z}_t}} \\ \mathbf{Z}_t & \xrightarrow[\varepsilon' t_{-1}]{} & \mathbf{Z}_t \end{array} \qquad \begin{array}{ccc} B_0 & \xrightarrow[=\mathrm{id}_{B_0}]{s_{-1}\varepsilon + \partial_1 s_0} & B_0 \\ \downarrow{\scriptstyle q_0} & & \downarrow{\scriptstyle q_0} \\ B_0/U_0 & \xrightarrow[t_{-1}\varepsilon' + \partial'_1 t_0]{} & B_0/U_0 \end{array} \qquad \begin{array}{ccc} B_n & \xrightarrow[=\mathrm{id}_{B_n}]{s_{n-1}\partial_n + \partial_{n+1} s_n} & B_n \\ \downarrow{\scriptstyle q_n} & & \downarrow{\scriptstyle q_n} \\ B_n/U_n & \xrightarrow[t_{n-1}\partial'_n + \partial'_{n+1} t_n]{} & B_n/U_n \end{array}$$

For the first diagram, we have that $\mathrm{id}_{\mathbf{Z}} = \varepsilon s_{-1} = \varepsilon' q_0 \circ s_{-1} = \varepsilon' \circ q_0 s_{-1} = \varepsilon' t_{-1}$, so it commutes. For the second,

$$\begin{aligned} (t_{-1}\varepsilon' + \partial'_1 t_0) q_0 &= t_{-1} \circ \varepsilon' q_0 + \partial'_1 t_0 q_0 \\ &= q_0 s_{-1} \circ \varepsilon + \partial'_1 q_1 s_0 \\ &= q_0 s_{-1}\varepsilon + q_0 \partial_1 s_0 \\ &= q_0 (s_{-1}\varepsilon + \partial_1 s_0) \\ &= q_0 \end{aligned}$$

so the second diagram commutes, and for $n \geq 1$,

$$\begin{aligned}(t_{n-1}\partial'_n + \partial'_{n+1}t_n)q_n &= t_{n-1}\partial'_n q_n + \partial'_{n+1}t_n q_n \\ &= t_{n-1}q_{n-1}\partial_n + \partial'_{n+1}q_{n+1}s_n \\ &= q_n s_{n-1}\partial_n + q_n \partial_{n+1}s_n \\ &= q_n(s_{n-1}\partial_n + \partial_{n+1}s_n) \\ &= q_n\end{aligned}$$

so the third diagram commutes too. Now, because q_n is a surjection for $n \geq 0$, it follows that $t_{-1}\varepsilon' + \partial'_1 t_0 = \mathrm{id}_{B_0}$ and $t_{n-1}\partial'_n + \partial'_{n+1}t_n = \mathrm{id}_{B_n}$ for $n \geq 1$, so t is a contraction and $B^*_\bullet(G)$ is acyclic. □

3.6 Connecting the bar resolutions

We have defined two complexes for defining group cohomology. Soon we will see that the two variations of the bar resolution are have the same homotopy type: the following observation guarantees that they define the same cohomology.

Lemma 3.23. *Suppose R, S are rings and (C, ∂), (D, d) are two (co)chain complexes of R-modules that are homotopy equivalent via the maps $f\colon C_\bullet \to D_\bullet$ and $g\colon D_\bullet \to C_\bullet$, and let $F\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ be a co- or contravariant additive functor. Then the (co)chain complexes $(FC, F\partial)$ and (FD, Fd) are homotopy equivalent via Ff and Fg.*

Proof. Suppose, without loss of generality, that $C_\bullet$ and $D_\bullet$ are chain complexes and F is contravariant. Since f and g are homotopy equivalences, there are homotopies $h_n\colon C_n \to C_{n+1}$ and $k_n\colon D_n \to D_{n+1}$ satisfying the equations

$$\begin{aligned}h_{n-1}\partial_n + \partial_{n+1}h_n &= g_n f_n - \mathrm{id}_{C_n} \\ k_{n-1}d_n + d_{n+1}k_n &= f_n g_n - \mathrm{id}_{D_n}\end{aligned}$$

for all n. Now, applying the additive functor F to both equations, we get that

$$\begin{aligned}Fh_{n-1}\,F\partial_n + F\partial_{n+1}\,Fh_n &= Fg_n\,Ff_n - \mathrm{id}_{FC_n} \\ Fk_{n-1}\,Fd_n + Fd_{n+1}\,Fk_n &= Ff_n\,Fg_n - \mathrm{id}_{FD_n}\end{aligned}$$

for all n, so we see that Ff and Fg make a homotopy equivalence between $FC_\bullet$ and $FD_\bullet$ witnessed by the homotopies Fh and Fk. □

The worth of the above observation is as follows. It is obvious that any cochain complex with the same homotopy type as the defining cochain complex

$$0 \to \mathrm{Hom}_G(B_0, M) \to \mathrm{Hom}_G(B_1, M) \to \cdots$$

will have the same cohomology as the group G, but the above states that one may substitute any chain complex homotopy equivalent to the bar resolution *before* applying the Hom functor. This hints at a great flexibility in calculating cohomology for groups, as the bar resolution will turn out to be rather easy to construct homotopies to and from. Before we present the general method, it is instructive to attempt a special case.

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & B_2 & \xrightarrow{\partial_2} & B_1 & \xrightarrow{\partial_1} & B_0 & \xrightarrow{\varepsilon} & \mathbf{Z}_t & \longrightarrow & 0 \\
 & & {\scriptstyle q_2}\downarrow\uparrow{\scriptstyle s_2} & & {\scriptstyle q_1}\downarrow\uparrow{\scriptstyle s_1} & & {\scriptstyle q_0}\downarrow\uparrow{\scriptstyle s_0} & & {\scriptstyle \mathrm{id}}\downarrow\uparrow{\scriptstyle \mathrm{id}} & & \\
\cdots & \longrightarrow & B_2/U_2 & \xrightarrow[\partial_2']{} & B_1/U_1 & \xrightarrow[\partial_1']{} & B_0/U_0 & \xrightarrow[\varepsilon']{} & \mathbf{Z}_t & \longrightarrow & 0
\end{array}$$

Consider showing that for a group G, the bar resolution $B_\bullet(G)$ and normalised bar resolution $B_\bullet^*(G)$ are homotopy equivalent. In one direction, there is the natural quotient map $q\colon B_\bullet(G) \to B_\bullet^*(G)$. In the other direction, note that the maps s_n defined by $[g_1, \ldots, g_n] \mapsto [g_1 | \ldots | g_n]$ will not form a chain map, because $\operatorname{Im} s_n$ does not contain any tuples containing a 1, whereas $\operatorname{Im} \partial_n$ certainly does, so the commutation identity $\partial_n s_n = s_{n-1}\partial_n'$ cannot hold.

Thus the tentative homotopy inverse s needs to be chosen more carefully. In degrees -1 and 0 there are the natural choices of $s_{-1} = \mathrm{id}_{\mathbf{Z}_t}$ and s_0 defined by $s_0([\,]) = [\,]$. Inductively, having defined s_n, we wish to define s_{n+1} so that it is at least a chain map.

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & B_{n+1}/U_{n+1} & \xrightarrow{\partial_{n+1}'} & B_n/U_n & \xrightarrow{\partial_n'} & B_{n-1}/U_{n-1} & \longrightarrow & \cdots \\
 & & \vdots{\scriptstyle s_{n+1}} & & \downarrow{\scriptstyle s_n} & & \downarrow{\scriptstyle s_{n-1}} & & \\
\cdots & \longrightarrow & B_{n+1} & \xrightarrow[\partial_{n+1}]{} & B_n & \xrightarrow[\partial_n]{} & B_{n-1} & \longrightarrow & \cdots
\end{array}$$

It is a standard diagram chase: for each basis element $b \in B_{n+1}/U_{n+1}$, one defines $s_{n+1}(b)$ by mapping b into B_n as $b' = s_n(\partial_{n+1}'(b))$ and choosing an element from the preimage $\partial_{n+1}^{-1}\{b'\}$ to be the value $s_{n+1}(b)$. The preimage has elements because $\partial_n(b') = \partial_n(s_n(\partial_{n+1}'(b))) = s_{n-1}(\partial_n'(\partial_{n+1}'(b))) = 0$ so $b' \in \operatorname{Ker} \partial_n = \operatorname{Im} \partial_{n+1}$.

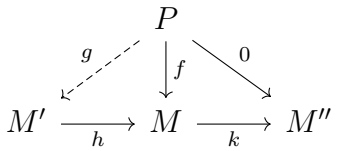
Examining the above argument, the condensed diagram looks as below.

$$\begin{array}{ccccc}
 & & B_{n+1}/U_{n+1} & & \\
 & {\scriptstyle s_{n+1}}\swarrow & \downarrow{\scriptstyle s_n\partial_{n+1}'} & \searrow{\scriptstyle 0} & \\
B_{n+1} & \xrightarrow[\partial_{n+1}]{} & B_n & \xrightarrow[\partial_n]{} & B_{n-1}
\end{array}$$

All it takes to define a chain map s between the two complexes is the freeness of the top complex and exactness of the bottom complex, so it is just as well to present the construction in full generality.

Even the freeness of the top complex can be relaxed: the modules B_n/U_n only need to be such that the map s_{n+1} can be defined off of the composite $s_n\partial'_{n+1}$ given that the above diagram commutes and has an exact bottom row. We thus name this property and return to examine it more fully later.

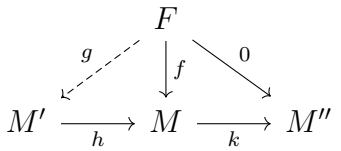
Definition 3.24. Let R be a ring.



An R-module P is called *projective* if for any exact sequence $M' \xrightarrow{h} M \xrightarrow{k} M''$ of R-modules and for any map $P \xrightarrow{f} M$ making the triangle on the right commute, there is a map $P \xrightarrow{g} M'$ making the triangle on the left commute.

Lemma 3.25. *Free modules are projective.*

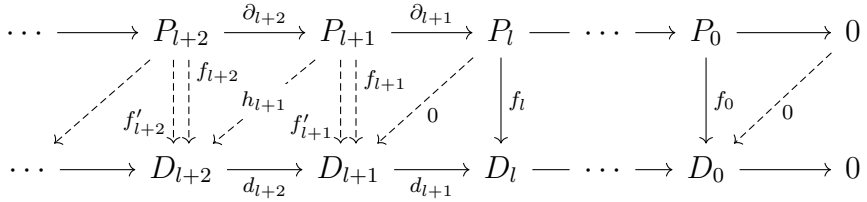
Proof. The proof goes as seen above. Let F be a free module with basis B, let $M' \xrightarrow{h} M \xrightarrow{k} M''$ be exact and $F \xrightarrow{f} M$ be such that $kf = 0$.



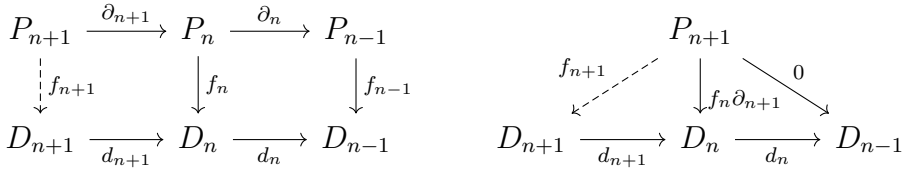
Because $kf = 0$, we have that $\operatorname{Im} f \subseteq \operatorname{Ker} k = \operatorname{Im} h$. We define the function $g\colon F \to M'$ as follows: for each basis element $b \in B$, we may choose a preimage $g(b) \in h^{-1}\{f(b)\}$. This means that $h(g(b)) = f(b)$ for each $b \in B$, so $hg = f$ since they agree on a basis of F. □

This is the general method of constructing chain maps. In a refined form it is called the *method of acyclic models*.

Theorem 3.26. *Let R be a ring. Let (P, ∂) and (D, d) be chain complexes of R-modules, and for $i \leq l$, suppose there are maps $f_i\colon P_i \to D_i$ so that $d_i f_i = f_{i-1}\partial_i$. If P_n is projective for all $n \geq l+1$ and $D_\bullet$ is acyclic, then the maps f_i, $i \leq l$ extend to a chain map $f\colon P_\bullet \to D_\bullet$. Furthermore, the map f is unique in that any two such extensions f and f' are homotopic via a homotopy h having $h_i = 0$ for $i \leq l$. The chain maps and the homotopy are illustrated below.*



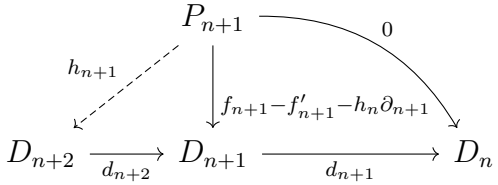
Proof. First we extend the maps f_i, $i \leq l$ into a chain map inductively. Suppose we have defined f_i so that $f_{i-1}\partial_i = d_i f_i$ up to $i \leq n$ for some $n \geq l$. We want to define f_{n+1} so that the leftmost square below commutes.



Because in particular the chain map square involving f_n and f_{n-1} commutes, we have that $d_n \circ f_n\partial_{n+1} = f_{n-1}\partial_n\partial_{n+1} = 0$ so the triangle on the right commutes. Because the bottom row is exact and P_{n+1} is projective, there is a map f_{n+1} filling in the left triangle. But the fact that this triangle commutes means that the chain map square involving f_{n+1} and f_n commutes. Continuing inductively, we get a chain map extending the given maps.

Now suppose $f' \colon C_\bullet \to D_\bullet$ is another chain map extending the given maps, so $f'_i = f_i$ for $i \leq l$. This means that defining $h_i = 0$ for $i \leq l$ works, because then $d_{i+1}h_i + h_{i-1}\partial_i = 0 = f_i - f'_i$ for $i \leq l$.

Inductively, suppose then we have defined h_i satisfying $d_{i+1}h_i + h_{i-1}\partial_i = f_i - f'_i$ for $i \leq n$ for some $n \geq l$.



Since we wish for h_{n+1} to satisfy $d_{n+2}h_{n+1} + h_n\partial_{n+1} = f_{n+1} - f'_{n+1}$ or equivalently $d_{n+2}h_{n+1} = f_{n+1} - f'_{n+1} - h_n\partial_{n+1}$, we only need to show that the composite $d_{n+1} \circ (f_{n+1} - f'_{n+1} - h_n\partial_{n+1})$ is 0. By the inductive assumption and the fact that f and f' are chain maps, we have

$$\begin{aligned} d_{n+1}h_n\partial_{n+1} &= (f_n - f'_n - h_{n-1}\partial_n) \circ \partial_{n+1} \\ &= f_n\partial_{n+1} - f'_n\partial_{n+1} - h_{n-1}\partial_n\partial_{n+1} \\ &= d_{n+1}f_{n+1} - d_{n+1}f'_{n+1} \end{aligned}$$

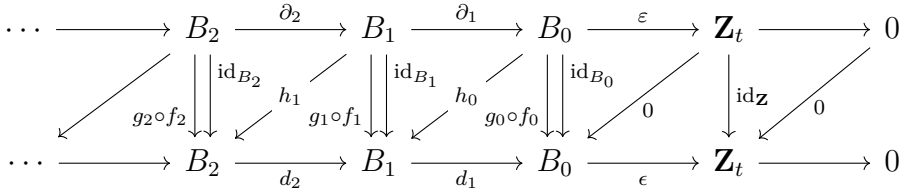
so $d_{n+1}f_{n+1} - d_{n+1}f'_{n+1} - d_{n+1}h_n\partial_{n+1} = 0$ and the triangle on the right commutes. Again, by exactness of the bottom row and projectivity of P_{n+1} we find a map h_{n+1} satisfying $d_{n+1}h_{n+1} = f_{n+1} - f'_{n+1} - h_n\partial_{n+1}$ as desired, and by continuing inductively we get a homotopy between f and f'. □

Corollary 3.27. *Let G be a group, M a G-module and $\cdots \to B_1 \xrightarrow{\partial_1} B_0 \xrightarrow{\varepsilon} \mathbf{Z} \to 0$ the bar resolution of G. If $P_\bullet = \cdots \to P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} \mathbf{Z} \to 0$ is an acyclic chain complex with P_n projective for $n \geq 0$, then the chain complexes $\cdots \to B_1 \xrightarrow{\partial_1} B_0 \to 0$ and $\cdots \to P_1 \xrightarrow{d_1} P_0 \to 0$ are homotopy equivalent and the cohomology groups of $\mathrm{Hom}_G(P_\bullet, M)$ are the group cohomology groups $H^\bullet(G, M)$.*

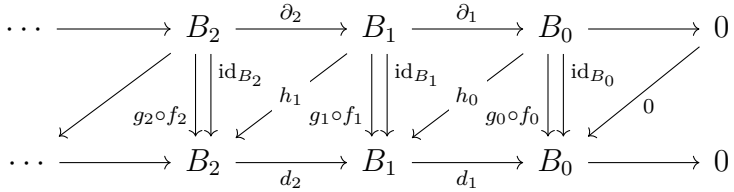
Proof. Lemma 3.25 assures us that $B_\bullet(G)$ is a complex of projective G-modules for $n \geq 0$, since B_n is free for $n \geq 0$, and Lemma 3.14 shows that $B_\bullet(G)$ is acyclic. We thus have two projective, acyclic chain complexes $B_\bullet(G)$ and $P_\bullet$, and the existence part of Theorem 3.26 gives us chain maps $f\colon B_\bullet(G) \to P_\bullet$ and $g\colon P_\bullet \to B_\bullet(G)$ both extending $\mathrm{id}_{\mathbf{Z}}$, depicted below.

$$\begin{array}{ccccccccccccc}
\cdots & \longrightarrow & B_2 & \xrightarrow{\partial_2} & B_1 & \xrightarrow{\partial_1} & B_0 & \xrightarrow{\varepsilon} & \mathbf{Z}_t & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_2} \uparrow{\scriptstyle g_2} & & \downarrow{\scriptstyle f_1} \uparrow{\scriptstyle g_1} & & \downarrow{\scriptstyle f_0} \uparrow{\scriptstyle g_0} & & \downarrow{\scriptstyle \mathrm{id}} \uparrow{\scriptstyle \mathrm{id}} & & \\
\cdots & \longrightarrow & P_2 & \xrightarrow[d_2]{} & P_1 & \xrightarrow[d_1]{} & P_0 & \xrightarrow[\epsilon]{} & \mathbf{Z}_t & \longrightarrow & 0
\end{array}$$

Now the composite $g \circ f\colon B_\bullet(G) \to B_\bullet(G)$ too is a chain map extending $\mathrm{id}_{\mathbf{Z}_t}$, as is $\mathrm{id}_{B_\bullet(G)}$. Thus by the uniqueness part of Theorem 3.26, they are chain homotopic so $g \circ f \simeq \mathrm{id}_{B_\bullet(G)}$, and similarly, $f \circ g \simeq \mathrm{id}_{P_\bullet}$. Thus $B_\bullet(G)$ and $P_\bullet$ are homotopy equivalent, with the homotopy shown below.



Since the homotopy $h\colon g \circ f \simeq \mathrm{id}_{B_\bullet(G)}$ supplied by Theorem 3.26 has $h_{-1}\colon \mathbf{Z} \to B_0$ identically zero, we see that h remains a chain homotopy between $g \circ f$ and the identity chain map if we delete the $\mathbf{Z}_t$ terms, as below.



As the same holds for the homotopy witnessing $f \circ g \simeq \mathrm{id}_{P_\bullet}$, we get that the chain complexes $\cdots \to B_2 \xrightarrow{\partial_2} B_1 \xrightarrow{\partial_1} B_0 \to 0$ and $\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to 0$ are homotopy equivalent, which was the first claim to be shown. The other claim is then the content of Lemma 3.23, since the Hom functor $\mathrm{Hom}_G(-, M)$ is additive. □

Corollary 3.28. *For a group G, the truncated versions $\cdots \to B_1 \to B_0 \to 0$ and $P_\bullet = \cdots \to B_1/U_1 \to B_0/U_0 \to 0$ of the bar resolution $B_\bullet(G)$ and normalised bar resolution $B^*_\bullet(G)$ are homotopy equivalent. For a G-module M, the cohomology groups of $\mathrm{Hom}_G(P_\bullet, M)$ are the group cohomology groups $H^\bullet(G, M)$.*

Proof. Like $B_\bullet(G)$, the normalised bar resolution $B^*_\bullet(G)$ is acyclic as seen in Lemma 3.22, and it is a complex of projective G-modules for $n \geq 0$ since B_n/U_n is free for $n \geq 0$, and free modules are projective by Lemma 3.25. This is then just a special case of the previous Corollary 3.27. □

3.7 The low-dimensional cohomology groups

Now that we are free to use the normalised bar resolution, we can return to the first and second cohomology groups; $H^0(G, M)$ was calculated in Example 3.17. Let G be a group and M a G-module. We are going to calculate $H^2(G, M)$ and $H^1(G, M)$ from the cochain complex

$$0 \to \mathrm{Hom}_G(B_0/U_0, M) \xrightarrow{\delta^0} \mathrm{Hom}_G(B_1/U_1, M) \xrightarrow{\delta^1} \mathrm{Hom}_G(B_2/U_2, M) \to \cdots$$

defined from $B^*_\bullet(G) = \cdots \to B_1/U_1 \xrightarrow{\partial_1} B_0/U_0 \xrightarrow{\varepsilon} \mathbf{Z}_t \to 0$ in place of $B_\bullet(G)$. Note that we drop the primes from the map names in $B^*_\bullet(G)$.

The map $\delta^2 = (-\circ\partial_3)\colon \mathrm{Hom}_G(B_2/U_2, M) \to \mathrm{Hom}_G(B_3/U_3, M)$ has the formula

$$\begin{aligned}\delta^2(f)([g,h,k]) &= f(\partial_3([g,h,k])) \\ &= f(g.[h,k] - [gh,k] + [g,hk] - [g,h]) \\ &= g.f([h,k]) - f([gh,k]) + f([g,hk]) - f([g,h])\end{aligned}$$

and similarly δ^1 and δ^0 have formulae

$$\delta^1(f)([g,h]) = f(\partial_2([g,h])) = f(g.[h] - [gh] + [g]) = g.f([h]) - f([gh]) + f([g])$$

and $\delta^0(f)([g]) = g.f([\,]) - f([\,])$, as seen before in Example 3.17.

To see that $\mathrm{Ker}\,\delta^2/\,\mathrm{Im}\,\delta^1 \cong \mathcal{F}(G, M)/\mathcal{S}(G, M)$ (Definitions 2.20 and 2.21), define

$$\varphi\colon \mathrm{Hom}_G(B_2/U_2, M) \to \mathrm{Hom}(G^2, M), \quad \varphi(f)(g,h) = f([g,h])$$

where $\mathrm{Hom}(G^2, M)$ is a hom-set of set-functions. Observe that since $[g|1], [1|g] \in U_2$, it holds that $[1,g] = [g,1] = 0$ in B_2/U_2. We then see that the functions $\varphi(f)$ in $\mathrm{Im}\,\varphi$ satisfy $\varphi(f)(1,g) = 0 = \varphi(f)(g,1)$ for all $g \in G$, because

$$\varphi(f)(g,1) = f([g,1]) = f(0) = 0 = f(0) = f([1,g]) = \varphi(f)(1,g)$$

for all $g \in G$ and $f \in \mathrm{Hom}_G(B_2/U_2, M)$. Also, for all $g, h, k \in G$ it holds that

$$\begin{aligned} &g.\varphi(f)(h,k) - \varphi(f)(gh,k) + \varphi(f)(g,hk) - \varphi(f)(g,h) \\ &= g.f([h,k]) - f([gh,k]) + f([g,hk]) - f([g,h]) \\ &= f(g.[h,k] - [gh,k] + [g,hk] - [g,h]) \\ &= f(\partial^3([g,h,k])) \end{aligned}$$

so $\varphi(f)$ satisfies the cocycle condition – and is in $\mathcal{F}(G,M)$ by Theorem 2.19 – if and only if $f \in \operatorname{Ker}\delta^2$. Thus φ maps $\operatorname{Ker}\delta^2$ into $\mathcal{F}(G,M)$.

The restriction $\varphi\restriction \operatorname{Ker}\delta^2$ is bijective, as given any factor set $f' \in \mathcal{F}(G,M)$, one can define a function $f\colon B_2/U_2 \to M$ by $f([g,h]) = f'(g,h)$: this is well defined, because $f'(g,h) = 0$ if $[g,h] \in U_2$ (if $g = 1$ or $h = 1$), and f' satisfying the cocycle condition guarantees that $f \in \operatorname{Ker}\varphi$. Similarly, φ bijects $\operatorname{Im}\delta^1$ onto $\mathcal{S}(G,M)$.

Lastly, φ is homomorphic, as the group operation is pointwise addition on both sides. As promised, we get the below theorem.

Theorem 3.29. *For a group G and a G-module M, $H^2(G,M)$ is isomorphic to $\mathcal{F}(G,M)/\mathcal{S}(G,M)$.* □

Analogously, one sees that $\operatorname{Ker}\delta^1 \cong \mathrm{Der}(G,M)$ (see Definition 2.15) via

$$\varphi\colon \mathrm{Hom}_G(B_1/U_1, M) \to \mathrm{Hom}(G,M), \quad \varphi(f)(g) = f([g] + U_1).$$

A function in $\operatorname{Im}\delta^0$ is of the form $\delta^0(f)([g]) = gx - x$ (where $x = f([\,])$) for some $f\colon B_0/U_0 \to M$, and it is identified with the set function $\varphi(\delta^0(f))\colon G \to M$ taking g to $(g-1)x$. Because functions $f\colon B_0/U_0 \to M$ and elements $x \in M$ are in bijection, $\operatorname{Im}\delta^0$ is identified with the subgroup

$$\{d \in \mathrm{Der}(G,M) \mid dg = gx - x \text{ for some } x \in M\} = \mathrm{PDer}(G,M);$$

the derivations in $\mathrm{PDer}(G,M)$ are called *principal derivations*. Thus the first cohomology group is as below.

Theorem 3.30. *For a group G and a G-module M, $H^1(G,M)$ is isomorphic to $\mathrm{Der}(G,M)/\mathrm{PDer}(G,M)$.* □

Recall that by Section 2.1, the group of derivations $\mathrm{Der}(Q,N)$ classifies the different splittings of the semidirect product extension $0 \to N \to N \rtimes Q \to Q \to 0$, or equivalently the different complements of $N \times 1 \trianglelefteq N \rtimes Q$: explicitly, a derivation d specifies a splitting $s(g) = (dg, g)$, and a splitting s specifies a complement $\operatorname{Im} s$.

To the zero derivation corresponds the natural splitting $s_0(g) = (0,g)$, and the natural complement $0 \times Q$. To the principal derivation $dg = gx - x$, associated to $x \in N$, corresponds the splitting $s_x(g) = (gx - x, g) = (-x,1)(0,g)(x,1)$, which is obtained from s_0 by conjugation with $(x,1) \in N \times 1$ and so the corresponding complement is the conjugate complement $(-x,1)(0 \times Q)(x,1)$.

Thus the group $H^1(N,Q)$ classifies the different splittings, or complements, of the semidirect product extension $N \rtimes Q$ up to conjugation by an element of N.

Chapter 4

Resolutions and exact functors

4.1 Resolutions

The theorems and corollaries of Section 3.6 were rather clumsy to state, and heavily suggest defining a general analogue of the bar resolutions. Here it is:

Definition 4.1. Let R be a ring and M an R-module.

i) A *resolution* of M is a long exact sequence

$$\cdots \to F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\varepsilon} M \to 0$$

of R-modules ending at M. The map ε is called the *augmentation map*.

The above resolution is denoted $F_\bullet \to M$ if one wishes to emphasise the module being resolved, or just $F_\bullet$ for short (with the convention $F_{-1} = M$).

ii) A *deleted resolution* of M is a resolution of M with the M-term deleted:

$$\cdots \to F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \to 0.$$

iii) A map between resolutions $C_\bullet \to M$ and $D_\bullet \to N$ is a chain map $f\colon C_\bullet \to D_\bullet$:

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & C_2 & \xrightarrow{\partial_2} & C_1 & \xrightarrow{\partial_1} & C_0 & \xrightarrow{\varepsilon} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f_{-1}} & & \\
\cdots & \longrightarrow & D_2 & \xrightarrow[\partial_2']{} & D_1 & \xrightarrow[\partial_1']{} & D_0 & \xrightarrow[\varepsilon']{} & N & \longrightarrow & 0
\end{array}$$

A chain map f extending a given map $g\colon M \to N$ is said to be *over* g. The same goes for deleted resolutions: a chain map f between two deleted resolutions $C_\bullet$ and $D_\bullet$ is said to be *over* the map $g\colon M \to N$ if f remains a chain map between the resolutions $C_\bullet \to M$ and $D_\bullet \to N$ when extended by g in degree -1.

iv) A (deleted) resolution is said to be *free* if all the modules F_n for $n \geq 0$ are free (but the module M does not have to be). The same definition is made for any other property a module might have.

v) The same definitions are made for the dual case of long exact sequences

$$0 \to M \xrightarrow{\eta} E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} E^2 \to \cdots .$$

These are sometimes called *coresolutions*, but we will simply call both variations resolutions, unless disambiguation between the two is needed.

Remark 4.2. Note that the deleted resolution $\cdots \to F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \to 0$ is no longer exact (unless M was the zero module), but the original module M is easily recovered as $\operatorname{cok} \partial_1$. The reason for defining deleted resolutions is that in Definition 3.16, group cohomology was defined off of a deleted version of the bar resolution. On the other hand, Theorem 3.26 requires an acyclic chain complex as the target, so a non-deleted resolution must be used there. Thus both kinds of resolution are needed.

We rephrase the consequences of Theorem 3.26 in terms of resolutions: these are the forms worth remembering.

Corollary 4.3. *Suppose R is a ring and M, N are R-modules. If $P_\bullet \to M$ is a projective resolution and $D_\bullet \to N$ is any resolution, then any map of modules $f_{-1} \colon M \to N$ extends to a chain map $f \colon P_\bullet \to D_\bullet$, and is unique up to homotopy.*

Corollary 4.4. *Suppose R is a ring and M is an R-module. Then any two projective resolutions of M are homotopy equivalent.*

Recall that the G-module $\mathbf{Z}_t$ is the $\mathbf{Z}$-module $\mathbf{Z}$ with trivial G-action.

Corollary 4.5. *Let G be a group and M a G-module. If $P_\bullet$ is any deleted projective resolution of $\mathbf{Z}_t$, then the cohomology groups of $\operatorname{Hom}_G(P_\bullet, M)$ are the group cohomology groups $H^\bullet(G, M)$.*

Remark 4.6. Given an R-module M, one may consider the category of deleted resolutions of M, with the maps being homotopy equivalence classes of chain maps over id_M. The above then says that deleted projective resolutions are initial objects in this category, and so any two of them have the same homotopy type. This is the categorical way to say that any deleted projective resolution of $\mathbf{Z}_t$ may be used in place of the deleted bar resolution.

As an example of the usefulness of general projective resolutions, and as an example in itself, we calculate the cohomology of a cyclic group of order n. For more details, consult theorem 9.27 of [2].

Example 4.7. Let $G = \langle t \rangle = \{1, t, t^2, \ldots, t^{n-1}\}$ be the cyclic group of order n with generator t, written multiplicatively. The ring $\mathbf{Z}G$ is evidently isomorphic to the polynomial ring $\mathbf{Z}[t]/\langle t^n - 1 \rangle$.

Let $D = t - 1 \in \mathbf{Z}G$ and $N = 1 + t + \cdots + t^{n-1} \in \mathbf{Z}G$. The following is then a projective resolution of $\mathbf{Z}_t$,

$$\cdots \to \mathbf{Z}G \xrightarrow{N\cdot -} \mathbf{Z}G \xrightarrow{D\cdot -} \mathbf{Z}G \xrightarrow{N\cdot -} \mathbf{Z}G \xrightarrow{D\cdot -} \mathbf{Z}G \xrightarrow{\varepsilon} \mathbf{Z}_t \to 0$$

where ε is the usual augmentation map defined by $\varepsilon(g) = 1$ for all $g \in G$, and D and N alternate indefinitely ($D \cdot -$ denotes multiplication by D, as with N).

Deleting the $\mathbf{Z}_t$ term and applying $\mathrm{Hom}_G(-, M)$ then yields the cochain complex

$$0 \to \mathrm{Hom}_G(\mathbf{Z}G, M) \xrightarrow{-\circ(D\cdot -)} \mathrm{Hom}_G(\mathbf{Z}G, M) \xrightarrow{-\circ(N\cdot -)} \mathrm{Hom}_G(\mathbf{Z}G, M) \to \cdots .$$

which is naturally isomorphic, via $f \mapsto f(1)$, to the cochain complex

$$0 \to M \xrightarrow{D\cdot -} M \xrightarrow{N\cdot -} M \xrightarrow{D\cdot -} M \xrightarrow{N\cdot -} M \to \cdots$$

from which the cohomology groups are readily calculated. We have that

$$\mathrm{Ker}(D \cdot -) = \{x \in M \mid Dx = (t-1)x = 0\} = M^G,$$

as $(t-1)x = 0$ guarantees $tx = x$ and thus $t^k x = x$ for all k. Also,

$$\mathrm{Ker}(N \cdot -) = \{x \in M \mid Nx = (1 + t + \cdots + t^{n-1})x = 0\} = {}_N M$$

is the submodule ${}_N M$ of elements annihilated by multiplication by N. Note that as Nx is the sum of all elements in the orbit Gx, the condition "$Nx = 0$" could be could be interpreted as "the average of Gx is 0."

Thus we have that for $n \geq 1$,

i) $H^0(G, M) \cong \mathrm{Ker}(D \cdot -) = M^G$,

ii) $H^{2n}(G, M) \cong \mathrm{Ker}(D \cdot -)/\,\mathrm{Im}(N \cdot -) = M^G/NM$,

iii) $H^{2n-1}(G, M) \cong \mathrm{Ker}(N \cdot -)/\,\mathrm{Im}(D \cdot -) = {}_N M/DM$.

It is then natural to ask whether every module has a projective resolution. In fact, every module has a free resolution: the proof goes by taking presentations, and gives another natural way of arriving at the concept of resolutions.

Let R be a ring and M an R-module. Recall that a *presentation* of M is a surjective map $\pi\colon F \to M$, where F is a free R-module. This is also denoted by

$$\langle S \mid R \rangle = \left\langle b_1, b_2, \ldots \;\middle|\; \sum_{b \in S} r_b^1 b, \sum_{b \in S} r_b^2 b, \ldots \right\rangle,$$

where $S = \{b_1, b_2, \ldots\}$ is the π-image of a basis of F and $R = \{\sum_b r_b^1 b, \sum_b r_b^2 b, \ldots\}$ is the π-image of a generating set for $\operatorname{Ker}\pi \subseteq F$. Conversely, the map π is recovered from a presentation $\langle S \mid R\rangle$ by taking F to be the free R-module on S and letting $\pi\colon F \to M$ take each basis element $b_i \in F$ to the actual element $b_i \in M$.

Remark 4.8. Note that every module has a presentation, as one can take the free module F to be the free module on any generating set of M, and letting π take each basis element in F to the actual corresponding element in M. For a canonical choice, one can take the generating set to be all of M.

Lemma 4.9. *Every module has a free (and thus also a projective) resolution.*

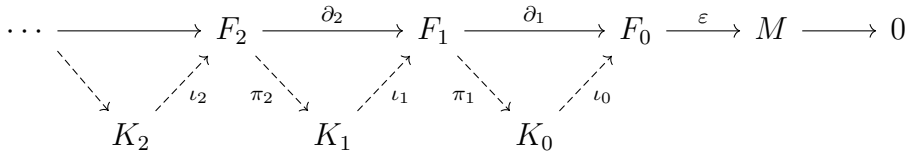
Proof. Let R be a ring and M an R-module. The proof is an iteration of the above remark.

Let $\pi_0\colon F_0 \to M$ be a presentation of M, let $K_0 = \operatorname{Ker}\pi_0$ be the kernel, and let $\iota_0\colon K_0 \to F_0$ be the inclusion map. Then, inductively, let $\pi_{n+1}\colon F_{n+1} \to K_n$ be a presentation of K_n, let K_{n+1} be the kernel $\operatorname{Ker}\pi_{n+1}$ and let $\iota_{n+1}\colon K_{n+1} \to F_{n+1}$ be the inclusion. This gets us a sequence

$$\cdots \to K_n \xrightarrow{\iota_n} F_n \xrightarrow{\pi_n} K_{n-1} \xrightarrow{\iota_{n-1}} F_{n-1} \to \cdots \to F_1 \xrightarrow{\pi_1} K_0 \xrightarrow{\iota_0} F_0 \xrightarrow{\pi_0} M \to 0$$

which is not necessarily yet exact: exactness holds at M and every F_n by definition, but not at any K_n as the composite $F_{n+1} \xrightarrow{\pi_{n+1}} K_n \xrightarrow{\iota_n} F_n$ is not 0 unless $K_n = 0$.

This is remedied by contracting the problem maps by defining $\partial_n\colon F_n \to F_{n-1}$, $\partial_n = \iota_{n-1}\pi_n$ for $n \geq 1$: the picture becomes



where we rename $\pi_0 = \varepsilon$ to match conventions. Now, because π_n is surjective for $n \geq 0$, we have that

$$\operatorname{Im}\partial_n = \operatorname{Im}(\iota_{n-1}\pi_n) = \iota_{n-1}\pi_n F_n = \iota_{n-1}K_{n-1} = \operatorname{Im}\iota_{n-1},$$

and because ι_n is injective for $n \geq 0$, we have that

$$\operatorname{Ker}\partial_n = \operatorname{Ker}(\iota_{n-1}\pi_n) = \pi_n^{-1}\iota_{n-1}^{-1}\{0\} = \pi_n^{-1}\{0\} = \operatorname{Ker}\pi_n.$$

Because $\operatorname{Im}\iota_n = \operatorname{Ker}\pi_n$ by definition, this means that $\operatorname{Im}\partial_{n+1} = \operatorname{Ker}\partial_n$ for $n \geq 1$, and $\operatorname{Im}\partial_1 = \operatorname{Ker}\pi_0 = \operatorname{Ker}\varepsilon$, so the sequence is exact at every F_n. Exactness at M follows from the surjectivity of $\varepsilon = \pi_0$. Since every F_n is free, this is a free resolution for M. □

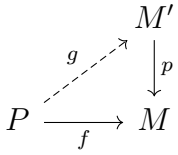
4.2 Projective modules

We now take a moment to look at projective modules. There is a host of equivalent conditions for projectiveness, some are collected below.

Lemma 4.10. *For a ring R and an R-module P, the following are equivalent:*

i) The module P is projective.

ii) For every surjective map $p\colon M' \to M$, every map $f\colon P \to M$ has a lift $g\colon P \to M'$ over p making the diagram below commute.



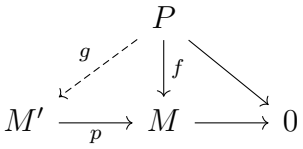
iii) Every surjective map $p\colon M \to P$ has a section.

iv) Every short exact sequence $0 \to M' \to M \xrightarrow{p} P \to 0$ splits.

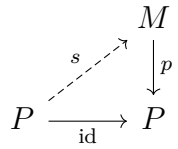
v) The module P is a direct summand of a free module.

Proof.

i) $\implies$ ii): Flip the diagram over and add 0: as p is surjective, the bottom row is exact so g exists per definition.



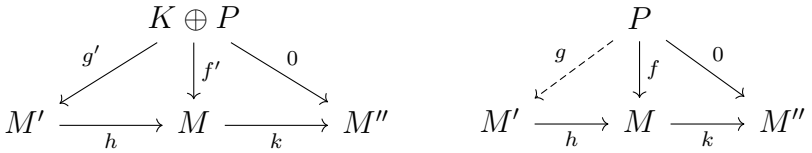
ii) $\implies$ iii): A lift s of id over the surjective map p satisfies $ps = \mathrm{id}$, so it is a desired section.



iii) $\implies$ iv): By exactness p is surjective, so it has a section, so the sequence splits.

iv) $\implies$ v): Let $F \xrightarrow{\pi} P$ be a presentation of P, let $K = \operatorname{Ker}\pi$ and let $K \xrightarrow{i} F$ be the inclusion. These make a short exact sequence $0 \to K \to F \to P \to 0$ which then splits, so $F \cong K \oplus P$.

v) $\implies$ i): Suppose $K \oplus P$ is free. Let $M' \xrightarrow{h} M \xrightarrow{k} M''$ be exact and suppose there is a map $f\colon P \to M'$ with $kf = 0$.



Extend the map f into $f' = 0 \oplus f\colon K \oplus P \to M$. The composite kf' is still 0, as $k \circ (0 \oplus f) = k0 \oplus kf = 0 \oplus 0 = 0$. As free modules are projective (Lemma 3.25), there is a map $g'\colon K \oplus P \to M'$ so that $hg' = 0 \oplus f$. Restricting both sides of the equation into P, we get that $h \circ g' \restriction P = (0 \oplus f) \restriction P = f$, so the desired map is $g = g' \restriction P$. □

The last condition is perhaps the most useful form for ring theory. For example, it yields the following corollaries.

Corollary 4.11. *Any direct summand of a projective module is projective, and any direct sum of projective modules is projective.*

Proof. This follows immediately from condition v) in Lemma 4.10. □

Corollary 4.12. *Suppose P is finitely generated. Then it is projective if and only if it is a direct summand of a finitely generated free module.*

Proof. Any direct summand of a finitely generated free module is a direct summand of a free module, hence projective. In the other direction, as P is finitely generated, we can take the free module F in the presentation $p\colon F \to P$ in the proof of Lemma 4.10, condition v) to be finitely generated. □

Corollary 4.13. *The module P is projective if and only if it is a direct summand of a free module with another free module: that is, there is a free module F so that $P \oplus F$ is free.*

Proof. As P is projective, there is a module Q so that $P \oplus Q \cong F'$ is free. Then, the module

$$F = \bigoplus_{n \in \mathbf{N}} F' = \bigoplus_{n \in \mathbf{N}} (P \oplus Q) \cong P \oplus Q \oplus P \oplus Q \oplus \cdots$$

is also free. But now $P \oplus F$ is free, as it is isomorphic to F:

$$\begin{array}{ccccccccc} P & \oplus & P & \oplus & Q & \oplus & P & \oplus & Q \oplus \cdots \\ \downarrow & & \searrow\swarrow & & & & \searrow\swarrow & & \\ P & \oplus & Q & \oplus & P & \oplus & Q & \oplus & P \oplus \cdots \end{array}$$

the isomorphism swaps the n-th and $(n+1)$-st coordinates for $n \geq 1$. □

Remark 4.14. Note that if R is such a ring that submodules of free R-modules are free, then projective modules are automatically free: for example, if R is a principal ideal domain (see Corollary 4.15 in [2]).

There is also a version internal to the module of the direct summand condition.

Definition 4.15. Let R be a ring and M an R-module. A *projective basis* of M is a collection of elements $b_i \in M$ and module maps $f_i \colon M \to R$ indexed over a common set I satisfying the following:

i) for each $x \in M$, $f_i(x) \neq 0$ for only finitely many i, and

ii) for each $x \in M$, $x = \sum_{i \in I} f_i(x) b_i$.

Note that condition i) implies that the sum in condition ii) is finite.

Lemma 4.16. *For a ring R, an R-module P is projective if and only if it has a projective basis.*

Proof. First suppose that P is projective, and let K be such that $F = K \oplus P$ is free: let $p \colon K \oplus P \to P$ be the projection map, so $p \restriction P = \mathrm{id}$.

Let $\{c_i \mid i \in I\}$ be a basis of F and let $g_i \colon F \to R$ be the function taking $\sum_i r_i c_i$ to r_i for each $i \in I$. The choice of basis yields an isomorphism $F \cong R^{(I)}$ of modules: the maps g_i are compositions of this map with projection to a coordinate.

Now set $b_i = p(c_i)$ and $f_i = g_i \restriction P$. Take $x \in P$. As $x = p(x)$, we have

$$x = p(x) = p\left(\sum_{i \in I} g_i(x) c_i\right) = \sum_{i \in I} g_i(x) p(c_i) = \sum_{i \in I} f_i(x) b_i,$$

where only a finite number of the scalars $f_i(x)$ are nonzero, so we have a projective basis.

In the other direction, suppose the elements $b_i \in P$ and maps $f_i \colon P \to R$ for $i \in I$ form a projective basis for P. By Lemma 4.10 iii), it suffices to find a section for an arbitrary surjective map $p \colon M \to P$.

Define $s \colon P \to M$ by choosing a preimage $a_i \in p^{-1}\{b_i\}$ for each $i \in I$ and setting

$$s(x) = \sum_{i \in I} f_i(x) a_i$$

for each $x \in P$. Writing s in the form $s = \sum_i (- \cdot a_i) \circ f_i$ makes it evident that s is well defined and homomorphic. It is also a section of p, because

$$p(s(x)) = p\left(\sum_{i \in I} f_i(x) a_i\right) = \sum_{i \in I} f_i(x) p(a_i) = \sum_{i \in I} f_i(x) b_i = x$$

holds for all $x \in P$ (the last equality comes from the definition of a projective basis). □

Now we can give examples of projective nonfree modules.

Example 4.17. Consider the ring $\mathbf{Z}/6\mathbf{Z} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$. As a module over itself, it is free. Both submodules $\langle 3 \rangle \cong \mathbf{Z}/2\mathbf{Z}$ and $\langle 2 \rangle \cong \mathbf{Z}/3\mathbf{Z}$ are projective as they are direct summands of a free module, but neither is free as $2 \cdot 3 = 3 \cdot 2 = 0$ in $\mathbf{Z}/6\mathbf{Z}$.

Of course, the same works with any two nonzero rings R, S. The submodule $R \times 0 \subseteq R \times S$ is a projective but nonfree $R \times S$-module, as is $0 \times S$.

Example 4.18. For a more interesting example, consider an integral domain R.

An *invertible ideal* of R is an ideal $I \subseteq R$ so that there is an ideal $J \subseteq R$ so that $JI = \langle \gamma \rangle$ for some nonzero $\gamma \in R$. In particular, $\gamma = \sum_i a_i b_i$ for some $a_i \in J$ and $b_i \in I$ for $i < n$. As R-modules, $\langle \gamma \rangle \cong R$, the isomorphism being $- \cdot \gamma \colon R \to \langle \gamma \rangle$. Note that is injective because R has no zero divisors. This isomorphism takes I to $I\gamma$, which is projective. This is because given any $x\gamma \in I\gamma$, we can write

$$x\gamma = x \sum_{i<n} a_i b_i = \sum_{i<n} x a_i b_i = \sum_{i<n} (- \cdot a_i)(x) b_i = \sum_{i<n} f_i(x\gamma) b_i$$

where f_i is the composite $(- \cdot a_i) \circ (- \cdot \gamma)^{-1}$, so the elements b_i and maps $(- \cdot a_i)$ for $i < n$ form a projective basis. Thus the ideal I is a projective R-module.

The ideals which are free as R-modules are precisely the principal ideals. Clearly principal ideals are free with dimension one: suppose I is nonprincipal but free, so it has no sole generator and thus has dimension at least two. However, any two elements a, b in an ideal are linearly dependent, as $a \cdot b + (-b) \cdot a = 0$, which is a contradiction.

Thus any invertible nonprincipal ideal is an example of a nonfree projective module over an integral domain. In algebraic number theory one runs into *Dedekind domains*, which are integral domains where every ideal is invertible, so their nonprincipal ideals provide a whole class of examples of nonfree projective modules.

4.3 Exact functors

There is one more important condition on projectiveness. Recall the alternative defining diagram:

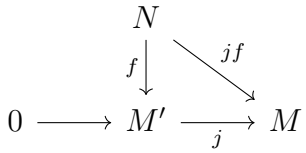
$$\begin{array}{ccccc} & & P & & \\ & \overset{g}{\swarrow} & \downarrow{\scriptstyle f} & & \\ M' & \xrightarrow[p]{} & M & \longrightarrow & 0 \end{array}$$

This can be phrased in terms of Hom functors as follows: if $p \colon M' \to M$ is surjective, then so is the map $p \circ - = p_* = \mathrm{Hom}_R(P, p) \colon \mathrm{Hom}_R(P, M') \to \mathrm{Hom}_R(P, M)$.

The corresponding result for injectiveness requires no conditions on the module:

Lemma 4.19. *For a ring R, R-modules N, M', M and an injection $j\colon M' \to M$, the map $j_*\colon \operatorname{Hom}_R(N, M') \to \operatorname{Hom}_R(N, M)$ is injective.*

Proof. As the hom-sets are abelian groups, it is enough to verify that j_* has trivial kernel.



Suppose jf is identically zero: as j is injective, f is identically zero. □

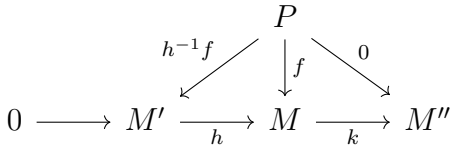
This heavily suggests that if $0 \to M' \xrightarrow{h} M \xrightarrow{k} M'' \to 0$ is an exact sequence of R-modules, then $0 \to \operatorname{Hom}_R(P, M') \xrightarrow{h_*} \operatorname{Hom}_R(P, M) \xrightarrow{k_*} \operatorname{Hom}_R(P, M'') \to 0$ is an exact sequence of abelian groups, if P is projective. This is indeed the case.

Lemma 4.20. *If R is a ring, $0 \to M' \xrightarrow{h} M \xrightarrow{k} M'' \to 0$ is an exact sequence of R-modules and P is a projective R-module, then*

$$0 \to \operatorname{Hom}_R(P, M') \xrightarrow{h_*} \operatorname{Hom}_R(P, M) \xrightarrow{k_*} \operatorname{Hom}_R(P, M'') \to 0$$

is an exact sequence of abelian groups.

Proof. Since k is surjective, so is k_* (because P is projective), and as h is injective, so is h_* as seen above. Because $kh = 0$, also $(kh)_* = k_*h_* = 0$, so the only thing left to check is that $\operatorname{Ker} k_* \subseteq \operatorname{Im} h_*$.



Suppose $f\colon P \to M$ is such that $k_*(f) = kf = 0$: then $\operatorname{Im} f \subseteq \operatorname{Ker} k$, and by exactness $\operatorname{Ker} k = \operatorname{Im} h$ so $\operatorname{Im} f \subseteq \operatorname{Im} h$. Since h is injective, it inverts on $\operatorname{Im} h$ so the map $h^{-1}f$ is well defined. Then $h_*(h^{-1}f) = hh^{-1}f = f$, so $f \in \operatorname{Im} h_*$. □

Remark 4.21. Notice that the projectiveness of P was needed only for the surjectiveness of k. Thus, if we replace P by a not necessarily projective module N in the above, we get the exact sequence

$$0 \to \operatorname{Hom}_R(N, M') \xrightarrow{h_*} \operatorname{Hom}_R(N, M) \xrightarrow{k_*} \operatorname{Hom}_R(N, M'')$$

which falls short of being short exact, but only barely: exactness on the injective side remains.

What of the contravariant Hom functor? The above readily dualises:

Lemma 4.22. *If N is an R-module and $0 \to M' \xrightarrow{h} M \xrightarrow{k} M'' \to 0$ is an exact sequence of R-modules, then*

$$0 \to \operatorname{Hom}_R(M'', N) \xrightarrow{k^*} \operatorname{Hom}_R(M, N) \xrightarrow{h^*} \operatorname{Hom}_R(M', N)$$

is an exact sequence of abelian groups.

Proof. To see that k^* is injective, suppose $k^*(f) = fk = 0$ for some $f\colon M'' \to N$.

$$\begin{array}{ccccc} M & \xrightarrow{k} & M'' & \longrightarrow & 0 \\ & \searrow^{kf} & \downarrow{\scriptstyle f} & & \\ & & N & & \end{array}$$

This means that f is zero on $\operatorname{Im} k = M''$, so $f = 0$ and k^* is injective. Because $kh = 0$, also $(kh)^* = h^*k^* = 0$, so the only thing left to check is that $\operatorname{Ker} h^* \subseteq \operatorname{Im} k^*$.

$$\begin{array}{ccccccc} M' & \xrightarrow{h} & M & \underset{s}{\overset{k}{\rightleftarrows}} & M'' & \longrightarrow & 0 \\ & \searrow^{0} & \downarrow{\scriptstyle f} & \swarrow_{fs} & & & \\ & & N & & & & \end{array}$$

Suppose $f\colon M \to N$ is such that $h^*(f) = fh = 0$: then $\operatorname{Im} h \subseteq \operatorname{Ker} f$, and by exactness $\operatorname{Im} h = \operatorname{Ker} k$ so $\operatorname{Ker} k \subseteq \operatorname{Ker} f$. Letting s be any (not necessarily homomorphic) section of k, the map fs is homomorphic. This is because

$$k(s(x) + s(y) - s(x + y)) = k(s(x)) + k(s(y)) - k(s(x + y)) = x + y - (x + y) = 0$$

so we have that $s(x) + s(y) - s(x + y) \in \operatorname{Ker} k \subseteq \operatorname{Ker} f$. Thus also

$$f(s(x)) + f(s(y)) - f(s(x + y)) = f(s(x) + s(y) - s(x + y)) = 0,$$

so fs is homomorphic. Then $k(sk - \mathrm{id}_M) = ksk - k = \mathrm{id}_M k - k = 0$, so $\operatorname{Im}(sk - \mathrm{id}_M) \subseteq \operatorname{Ker} k \subseteq \operatorname{Ker} f$, which means that $0 = f(sk - \mathrm{id}_M) = fsk - f$, so $k^*(fs) = fsk = f$. Thus k^* is surjective. □

The two properties are interesting enough to be named.

Definition 4.23. Suppose $\mathcal{C}$ and $\mathcal{D}$ are abelian categories. Let $F, G\colon \mathcal{C} \to \mathcal{D}$ be additive functors, F covariant and G contravariant. Let $0 \to A \to B \to C \to 0$ range over all the short exact sequences in $\mathcal{C}$.

i) If $0 \to FA \to FB \to FC$ is always exact, F is said to be *left exact*.

ii) If $FA \to FB \to FC \to 0$ is always exact, F is said to be *right exact*.

iii) If $0 \to FA \to FB \to FC \to 0$ is always exact, F is said to be *exact*.

iv) If $0 \to GC \to GB \to GA$ is always exact, G is said to be *left exact*.

v) If $GC \to GB \to GA \to 0$ is always exact, G is said to be *right exact*.

vi) If $0 \to GC \to GB \to GA \to 0$ is always exact, G is said to be *exact*.

Remark 4.24. The (left, right) exactness of a contravariant functor $G\colon \mathcal{C} \to \mathcal{D}$ can also be defined in terms of the covariant definition: considered as a covariant functor $G'\colon \mathcal{C}^{\mathrm{op}} \to \mathcal{D}$, G is (left, right) exact if G' is. As a rule of thumb, the adjectives left and right indicate which side of the exact sequence retains a 0 after being mapped with the functor.

Remark 4.25. An exact functor is evidently left and right exact, and conversely a left and right exact functor is exact as the two truncated short exact sequences can be overlapped to form a whole short exact sequence.

Lemma 4.26. *Suppose $\mathcal{C}$ and $\mathcal{D}$ are categories where kernels and images are defined. Let $F, G\colon \mathcal{C} \to \mathcal{D}$ be additive functors, F covariant and G contravariant.*

i) F is left exact if and only if exactness of $0 \to A \to B \to C$ implies $0 \to FA \to FB \to FC$ is exact.

ii) F is right exact if and only if exactness of $A \to B \to C \to 0$ implies $FA \to FB \to FC \to 0$ is exact.

iii) F is exact if and only if exactness of $A \to B \to C$ implies $FA \to FB \to FC$ is exact.

iv) G is left exact if and only if exactness of $A \to B \to C \to 0$ implies $0 \to GC \to GB \to GA$ is exact.

v) G is right exact if and only if exactness of $0 \to A \to B \to C$ implies $GC \to GB \to GA \to 0$ is exact.

vi) G is exact if and only if exactness of $A \to B \to C$ implies $GC \to GB \to GA$ is exact.

Proof. First, the "only if" directions: for i), if $0 \to A \to B \to C \to 0$ is a short exact sequence, then so is $0 \to A \to B \to C$, whence $0 \to FA \to FB \to FC$ is exact, and F is left exact. The cases ii, iv, v) are entirely similar.

For vi), suppose $0 \to A \to B \to C \to 0$ is exact: then the three pieces $0 \to A \to B$, $A \to B \to C$ and $B \to C \to 0$ are also all exact, and thus so are $GB \to GA \to 0$, $GC \to GB \to GA$ and $0 \to GC \to GB$, and the exact sequence $0 \to GC \to GB \to GA \to 0$ assembles from these. The case of v) is entirely similar.

For the other directions: for iv), suppose G is left exact and $A \xrightarrow{h} B \xrightarrow{k} C \to 0$ is exact. By writing $h = \operatorname{im} h \circ \operatorname{coim} h$, and using the fact that $\operatorname{coim} h$ is epi and $\operatorname{im} h$ is mono, we get the diagram

$$\begin{array}{ccccccccc} & & & & A & \xrightarrow{h} & B & \xrightarrow{k} & C & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \operatorname{coim} h} & & \downarrow{\scriptstyle \mathrm{id}_B} & & \downarrow{\scriptstyle \mathrm{id}_C} & & \\ 0 & \longrightarrow & \operatorname{Im} h & \xrightarrow[\operatorname{im} h]{} & B & \xrightarrow[k]{} & C & \longrightarrow & 0 & & \\ & & \downarrow & & & & & & & & \\ & & 0 & & & & & & & & \end{array}$$

with exact column (which is $0 \to \operatorname{Ker} \operatorname{coim} h \to A \to \operatorname{Im} h \to 0$ in full) and exact rows. Applying the functor G to the diagram gives

$$\begin{array}{ccccccccc} & & & & & & & & 0 & & \\ & & & & & & & & \downarrow & & \\ 0 & \longrightarrow & GC & \xrightarrow{Gk} & GB & \xrightarrow{G \operatorname{im} h} & G \operatorname{Im} h & & & & \\ & & \downarrow{\scriptstyle \mathrm{id}_{GC}} & & \downarrow{\scriptstyle \mathrm{id}_{GB}} & & \downarrow{\scriptstyle G \operatorname{coim} h} & & & & \\ 0 & \longrightarrow & GC & \xrightarrow[Gk]{} & GB & \xrightarrow[Gh]{} & GA & & & & \end{array}$$

with exact top row and right column (by left exactness of G): this means Gk and $G \operatorname{coim} h$ are monic, so the bottom row is exact at GB, and we also get that

$$\begin{aligned} \operatorname{im}(Gk) &= \ker(G \operatorname{im} h) && \text{(as the top row is exact)} \\ &= \ker(G \operatorname{coim} h \circ G \operatorname{im} h) && \text{(as } G \operatorname{coim} h \text{ is monic)} \\ &= \ker(G(\operatorname{im} h \circ \operatorname{coim} h)) \\ &= \ker(Gh). \end{aligned}$$

So the bottom row is exact also at GB, so the bottom row is exact as desired. The other cases are entirely similar: for iii) and vi), factorise both h and k. □

Remark 4.27. Because kernels and cokernels are uniquely characterised by exact sequences as

$$0 \to K \xrightarrow{\ker f} A \xrightarrow{f} B \quad \text{and} \quad A \xrightarrow{f} B \xrightarrow{\operatorname{cok} f} K' \to 0,$$

it follows that a covariant additive functor F is left (right) exact if and only if it preserves kernels (cokernels), and a contravariant additive functor G is left (right) exact if it turns cokernels into kernels (kernels into cokernels).

It even turns out that left (right) exact covariant functors preserve all finite limits (colimits), and left (right) exact contravariant functors turn finite colimits

into limits (limits into colimits). The reverse implication is clear, since kernels are finite limits and cokernels are finite colimits: the limit characterisation is taken as a definition in non-abelian contexts.

The upshot is that in an adjoint pair $F \dashv G$, F commutes with limits and G commutes with colimits, so F is left and G is right exact. For more details, see section 4.5 of the book [4].

For Hom functors, the above amounts to the following:

Lemma 4.28. *For a ring R and an R-module M, the co- and contravariant Hom functors $\mathrm{Hom}_R(M,-)$ and $\mathrm{Hom}_R(-,M)$ are left exact. Furthermore, $\mathrm{Hom}_R(P,-)$ is exact if and only if P is projective.*

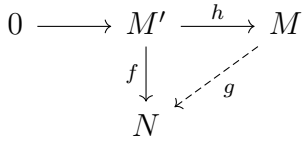
Proof. The two first statements were shown earlier, as with the implication that projectiveness of P implies exactness of $\mathrm{Hom}_R(P,-)$.

On the other hand, if $\mathrm{Hom}_R(P,-)$ is exact and $p\colon M' \to M$ is surjective, then the sequence $0 \to \operatorname{Ker} p \to M' \xrightarrow{p} M \to 0$ is exact, whence

$$0 \to \mathrm{Hom}_R(P, \operatorname{Ker} p) \to \mathrm{Hom}_R(P, M') \xrightarrow{p_*} \mathrm{Hom}_R(P, M) \to 0$$

is too. In particular, p_* is surjective, which is condition ii) in Lemma 4.10. □

What of the exactness of the contravariant Hom functor $\mathrm{Hom}_R(-,N)$? By Lemma 4.22, the only thing missing is that h^* be surjective – that is, for every $f\colon M' \to N$ there is $g\colon M \to N$ so that $f = gh$.

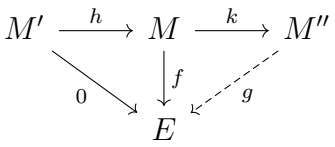


Unsurprisingly, this diagram is the dual of the alternative defining diagram of a projective module. Next, we shall define and examine these modules.

4.4 Injective modules

For aesthetic consistency, we define injective modules by dualising the projective Definition 3.24.

Definition 4.29. Let R be a ring.



An R-module is called *injective* if for any exact sequence $M' \xrightarrow{h} M \xrightarrow{k} M''$ of R-modules and for any map $M \xrightarrow{f} E$ making the triangle on the left commute, there is a map $M'' \xrightarrow{g} E$ making the triangle on the right commute.

The equivalent definitions are largely dual to those in Lemma 4.10, save for condition v), which does not readily dualise. However, the proof of equivalence is more involved.

Lemma 4.30. *For a ring R and an R-module E, the following three conditions are equivalent:*

i) E is injective

ii) For every injective map $M' \xrightarrow{i} M$, every map $f\colon M' \to E$ has an extension $g\colon M \to E$ along i making the diagram below commute

$$\begin{array}{ccc} M' & \xrightarrow{i} & M \\ & \searrow^{f} & \downarrow{\scriptstyle g} \\ & & E \end{array}$$

iii) The contravariant Hom functor $\mathrm{Hom}_R(-, E)$ is exact.

Any of the above imply either of the below conditions, which are equivalent:

iv) Every injective map $i\colon E \to M$ has a retraction

v) Every short exact sequence $0 \to E \xrightarrow{i} M \to M'' \to 0$ splits.

Proof.

i) $\implies$ ii): Since i is an injection, the sequence $0 \to M' \xrightarrow{i} M$ is exact, so g exists by definition.

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \xrightarrow{i} & M \\ & & {\scriptstyle f}\downarrow & \swarrow_{g} & \\ & & E & & \end{array}$$

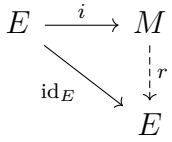
ii) $\implies$ iii): By Lemma 4.28, it is enough to show that if $0 \to M' \xrightarrow{h} M \xrightarrow{k} M'' \to 0$ is exact, then $h^* = \mathrm{Hom}_R(h, E)$ is surjective. Let $f\colon M' \to E$ be any map.

$$\begin{array}{ccc} M' & \xrightarrow{h} & M \\ & \searrow^{f} & \downarrow{\scriptstyle g} \\ & & E \end{array}$$

Since h is injective, there exists a $g\colon M \to E$ so that $f = gh = h^*(g)$, so h^* is surjective and $\mathrm{Hom}_R(-, E)$ is exact.

iii) $\implies$ i): Suppose $M' \xrightarrow{h} M \xrightarrow{k} M''$ is exact and that $f\colon M \to E$ is a map satisfying $0 = fh = h^*(f)$: this means that $f \in \operatorname{Ker} h^* = \operatorname{Im} k^*$, so $f = k^*(g) = gk$ for some $g\colon M'' \to E$. This g is as desired.

ii) $\implies$ iv): Given an injective map $i\colon E \to M$, the identity map id_E has an extension r along i making the diagram below commute.



Because $ri = \mathrm{id}_E$, this is the desired section.

iv) $\implies$ v): Suppose $0 \to E \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ is exact, whence i is injective and has a retraction r that satisfies $ri = \mathrm{id}_E$. We show $p\restriction \operatorname{Ker} r$ is an isomorphism.

For surjectivity, given $y \in M''$, the surjectivity of p implies there is an $x \in M$ with $p(x) = y$. Now, $x - i(r(x))$ is the desired preimage: it is a preimage of y because $p(x - i(r(x))) = p(x) - p(i(r(x)) = y - 0 = y$, and it is in $\operatorname{Ker} r$ because $r(x - i(r(x))) = r(x) - r(i(r(x))) = r(x) - r(x) = 0$.

For injectivity, if $p(x) = 0$, then $x \in \operatorname{Ker} p = \operatorname{Im} i$, so $x = i(x')$ for some $x' \in E$, but $x' = r(i(x')) = r(x) = 0$ as $x \in \operatorname{Ker} r$, so also $x = i(x') = 0$.

Thus $p\restriction \operatorname{Ker} r$ has an inverse s, which is the desired section of p.

v) $\implies$ iv): Any injective map $i\colon E \to M$ fits into an exact sequence $0 \to E \xrightarrow{i} M \xrightarrow{p} \operatorname{Cok} i \to 0$, which splits so p has a section s. Now define $r\colon M \to E$ by $r(x) = x'$ where $i(x') = x - s(p(x))$ (so $x = s(p(x)) + i(x')$).

To see that r is well defined, observe that $x - s(p(x))$ is in $\operatorname{Im} i = \operatorname{Ker} p$ because $p(x - s(p(x))) = p(x) - p(s(p(x)) = p(x) - p(x) = 0$, and the element x' is unique as i is injective.

To see that r is homomorphic, suppose $r(x) = x'$ and $r(y) = y'$. Then $x + y = s(p(x)) + i(x') + s(p(y)) + i'(y) = s(p(x + y)) + i(x' + y')$, so $r(x + y) = x' + y'$.

Lastly, $r(i(x)) = x$ because $i(x) = 0 + i(x) = s(p(i(x)) + i(x)$, so r is a retraction of i. □

Just like projective modules make lifting problems easy, injective modules make extension problems easy. The extension criterion ii) in Lemma 4.30 can be specialised even further, known as *Baer's criterion*:

Lemma 4.31. *For a ring R, an R-module E is injective if and only if any module map $f\colon I \to E$, where I is a left ideal of R, extends to a map $g\colon R \to E$.*

Proof. Necessity is clear, as ideals of a ring R amount to submodules of the R-module R. For sufficiency, suppose $\iota\colon M' \to M$ is injective and $f\colon M' \to E$ is any map: to simplify notation, we discard ι and treat M' as a submodule of M. Set $M_0 = M'$ and $f_0 = f$: we are going to construct an increasing transfinite sequence of modules $M' \subseteq M_i \subseteq M$ and functions $f_i\colon M_i \to E$ so that $f_i{\restriction}M_j = f_j$ for $j < i$.

Having defined M_i and f_i, if $M_i = M$ we are done: otherwise choose $x_i \in M \setminus M_i$, and set $I_i = \{r \in R \mid rx_i \in M_i\}$. Then I_i is an ideal, because it is the preimage of the submodule $M_i \subseteq M$ under the module map $(- \cdot x_i)\colon R \to E$. Then the map $f_i(- \cdot x_i)\colon I_i \to E$ is well defined: by assumption, it extends to a function $g_i\colon R \to E$.

$$\begin{array}{ccc} I_i & \longrightarrow & R \\ {\scriptstyle f_i(-\cdot x_i)}\downarrow & \swarrow_{g_i} & \\ E & & \end{array}$$

Now, set the next module to be $M_{i+1} = \langle M_i, x_i\rangle = \{y + rx_i \mid y \in M_i, r \in R\}$ and define $f_{i+1}\colon M_{i+1} \to E$ by

$$f_{i+1}(y + rx_i) = f_i(y) + g_i(r) \quad \text{for } y \in M_i \text{ and } r \in R.$$

To see that f_{i+1} is well defined, suppose $y, y' \in M_i$ and $r, r' \in R$ are such that $y + rx_i = y' + r'x_i$: then $(r - r')x_i = y' - y \in M_i$ so $r - r' \in I_i$. As g_i extends $f_i(- \cdot x_i)$ on I_i, we have

$$g_i(r) - g_i(r') = g_i(r - r') = f_i((r - r')x_i) = f_i(y' - y) = f_i(y') - f_i(y),$$

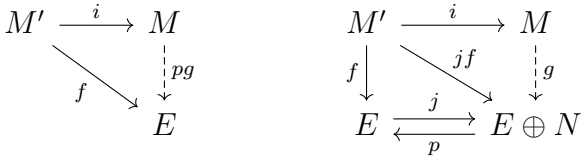
meaning that $f_i(y) + g_i(r) = f_i(y') + g_i(r')$ after rearranging, so f_{i+1} is well defined. Also, as $y = y + 0x_i$ for all $y \in M_i$, we have that $f_{i+1}(y) = f_i(y) + g_i(0) = f_i(y)$, meaning that f_{i+1} extends f_i, and so also any f_j for $j < i + 1$, as desired.

For limit stages, set $M_i = \bigcup_{j<i} M_j$ and $f_i = \bigcup_{j<i} f_j$: we verify that M_i is a submodule of M and f_i is a homomorphism. If $x, y \in M_i$, then $x \in M_j$ and $y \in M_k$ for some $j, k < i$: as $M_j, M_k \subseteq M_l$ where $l = \max(j, k)$, it follows that all of $x, y, x + y$ and rx are in $M_l \subseteq M_i$ for any $r \in R$, as M_l is a submodule of M. Also, for f_i it holds that $f_i(x + y) = f_l(x + y) = f_l(x) + f_l(y) = f_i(x) + f_i(y)$ and $f_i(rx) = f_j(rx) = rf_j(x) = rf_i(x)$, so it is homomorphic. □

To see that conditions iv) and v) imply i), ii) and iii) in Lemma 4.30 takes some more work. Recall that condition v) implies that $M \cong E \oplus M'$, so E is a direct summand of M. We will show that any module can be embedded in an injective module (dualising the fact that any module is the quotient of a projective – even free – module), and that a direct summand of an injective module is injective. The latter is simple.

Lemma 4.32. *For a ring R, suppose E' is an injective R-module and E is a direct summand of E'. Then E is injective.*

Proof. Suppose $E' \cong E \oplus N$, and let $j\colon E \to E \oplus N$ and $p\colon E \oplus N \to E$ be the inclusion and projection maps. We use condition ii) in Lemma 4.30. Let $i\colon M' \to M$ be injective and $f\colon M' \to E$ be any map. We find a map g so that pg is the desired extension of f, as shown below.



Since $E \oplus N$ is injective, the map jf extends to a map g along i making the top right triangle commute, so $jf = gi$. As $pj = \mathrm{id}_E$, it follows that $pgi = pjf = f$, so the triangle on the left commutes and pg extends f along i. □

To see what it takes for an R-module E to be injective, consider a module M such that there is a homomorphism $f\colon rM \to E$ where $r \in R$. Any extension g of f from rM to all of M must take care that $x = g(m)$ is such an element that $rx = rg(m)$ equals $f(rm) = g(rm) = rg(m)$; that is, one has to solve the equation $rx = y$ for each $y \in f(rM)$. This motivates the following definition.

Definition 4.33. Let R be an integral domain and M an R-module. An element $m \in M$ is *divisible by* r if the equation $rx = m$ has a solution $x \in M$. The module M is *divisible* if every $m \in M$ is divisible by every nonzero $r \in R$.

Example 4.34. The $\mathbf{Z}$-module $\mathbf{Q}$ is divisible, as is the R-module $\mathrm{Frac}(R)$ for any integral domain R, as it is designed to enable solving $rx = y$ with $x = y/r$ for any $r \in R \setminus \{0\}$ and $y \in \mathrm{Frac}(R)$.

Lemma 4.35. *Any direct sum of divisible modules is divisible, and any quotient module of a divisible module is divisible.*

Proof. Suppose M_i is a divisible R-module for each $i \in I$, and let $M = \bigoplus_{i \in I} M_i$. Now the equation $rx = y$ where $y \in M$, $r \in R \setminus \{0\}$ can be solved componentwise, and the componentwise solutions assemble into a solution $x \in M$: we can arrange $x_i = 0$ for all but finitely many i, since already $y_i = 0$ for all but finitely many i.

Suppose then that M is a divisible R-module and M/M' is a quotient module. To find a solution to the equation $r[x] = [y]$ with $[y] \in M/M'$ and $r \in R \setminus \{0\}$, we first find an $x \in M$ satisfying $rx = y$. Taking equivalence classes, we get that $r[x] = [rx] = [y]$, so M/M' is also divisible. □

For some rings R, the above is all it takes for an R-module to be injective.

Lemma 4.36. *Let R be a principal ideal domain. Then an R-module is injective if and only if it is divisible.*

Proof. First, suppose M is a divisible R-module. By Baer's criterion (Lemma 4.31), it suffices to extend a given map $f\colon I \to M$ from an ideal $I \subseteq R$ to all of R. Since R is a principal ideal domain, $I = \langle s \rangle$ for some $s \in R$. If $s = 0$, then $I = \{0\}$ so the zero function suffices. If $s \neq 0$, consider the equation $sy = f(s)$. Since M is divisible, this equation has a solution $y \in M$: define $g\colon R \to M$ by $g(1) = y$ so $g(r) = rg(1) = ry$ for $r \in R$. Now g extends f since $g(s) = sg(1) = sy = f(s)$.

Then suppose M is an injective R-module, and fix $m \in M$ and $r \in R \setminus \{0\}$. To find a solution to $rx = m$, define the map $f\colon \langle r \rangle \to M$ by $f(r) = m$ and extending linearly. By injectivity of M, the map f extends to a map $g\colon R \to M$. The element $g(1) \in M$ satisfies $rg(1) = g(r) = f(r) = m$, so $g(1)$ is a solution to $rx = m$ as desired. □

As $\mathbf{Z}$ is a principal integral domain, the injective abelian groups ($\mathbf{Z}$-modules) are precisely the divisible abelian groups. Working towards embedding any module into an injective module, we now show that any abelian group embeds into a divisible (equally, injective) abelian group.

Lemma 4.37. *Every abelian group G embeds into a divisible abelian group.*

Proof. Let $F \xrightarrow{\pi} G$ be a presentation of G and $K = \operatorname{Ker} \pi$, so $G \cong F/K$. Since F is a free abelian group, $F \cong \mathbf{Z}^{\oplus \kappa} = \bigoplus_{i<\kappa} \mathbf{Z}$ for some cardinal κ. Since $\mathbf{Z}^{\oplus\kappa}$ embeds into $\mathbf{Q}^{\oplus\kappa}$, as does $K \subseteq \mathbf{Z}^{\oplus\kappa}$, we have that

$$G \cong \mathbf{Z}^{\oplus\kappa}/K \subseteq \mathbf{Q}^{\oplus\kappa}/K$$

so G embeds into the divisible abelian group $\mathbf{Q}^{\oplus\kappa}/K$, which is divisible by Lemma 4.35 as $\mathbf{Q}$ is divisible. □

The covariant Hom functor $\operatorname{Hom}_{\mathbf{Z}}(R, -)\colon \mathbf{Ab} \to {}_R\mathbf{Mod}$ takes divisibles to injectives:

Lemma 4.38. *For a ring R and a divisible abelian group D, the R-module $\operatorname{Hom}_{\mathbf{Z}}(R, D)$ is injective.*

Proof. Consider R as a $\mathbf{Z}, R$-bimodule and D as a $\mathbf{Z}, \mathbf{Z}$-bimodule, so $\operatorname{Hom}_{\mathbf{Z}}(R, D)$ becomes an $R, \mathbf{Z}$-bimodule (so an R-module). To show that $\operatorname{Hom}_{\mathbf{Z}}(R, D)$ is injective, we show that the contravariant Hom functor $\operatorname{Hom}_R(-, \operatorname{Hom}_{\mathbf{Z}}(R, D))$ is exact, by condition iii) of Lemma 4.30. The tensor-hom adjunction gives

$$\operatorname{Hom}_R(-, \operatorname{Hom}_{\mathbf{Z}}(R, D)) \cong \operatorname{Hom}_{\mathbf{Z}}(R \otimes_R -, D)$$

and as $R \otimes_R M \cong M$ is naturally isomorphic to the identity functor, we get that

$$\mathrm{Hom}_R(-, \mathrm{Hom}_{\mathbf{Z}}(R, D)) \cong \mathrm{Hom}_{\mathbf{Z}}(-, D)$$

which is an exact functor, as D is a divisible abelian group (so an injective $\mathbf{Z}$-module). □

Putting the last two results together:

Lemma 4.39. *Any R-module can be embedded into an injective R-module.*

Proof. Let M be an R-module. Consider M first as an abelian group: Lemma 4.37 says there is an embedding $i\colon M \to D$ of M into a divisible abelian group D. Since the covariant Hom functor $\mathrm{Hom}_{\mathbf{Z}}(R, -)\colon \mathbf{Ab} \to {}_R\mathbf{Mod}$ is left exact by Lemma 4.28, the map $i_*\colon \mathrm{Hom}_{\mathbf{Z}}(R, M) \to \mathrm{Hom}_{\mathbf{Z}}(R, D)$ is also injective. As $\mathrm{Hom}_{\mathbf{Z}}(R, D)$ is injective by Lemma 4.38, we are left to show that M embeds into $\mathrm{Hom}_{\mathbf{Z}}(R, M)$.

Define $f\colon M \to \mathrm{Hom}_{\mathbf{Z}}(R, M)$ by $f(x) = - \cdot x$, that is $f(x)(r) = rx$ for $x \in M$ and $r \in R$: then $f(x)$ is $\mathbf{Z}$-linear (so f is well defined) and f is $\mathbf{Z}$-linear because scalar multiplication is $\mathbf{Z}$-bilinear. Also, f is even R-linear because

$$rf(x)(r') = f(x)(r'r) = r'rx = f(rx)(r')$$

for all $r' \in R$, so $f(rx) = rf(x)$ for all $x \in M$, $r \in R$. (Recall the R-scalar multiplication in $\mathrm{Hom}_{\mathbf{Z}}(R, M)$ is $rg(r') = g(r'r)$, stemming from R as a $\mathbf{Z}, R$-bimodule.) Finally, f is injective, because $f(x) = 0$ implies in particular that $f(x)(1) = 1x = 0$, so $x = 0$.

Thus M embeds into $\mathrm{Hom}_{\mathbf{Z}}(R, M)$, which embeds into $\mathrm{Hom}_{\mathbf{Z}}(R, D)$, which is injective, proving the claim. □

We can now show that all five conditions of Lemma 4.30 are equivalent by showing that condition v) implies condition i):

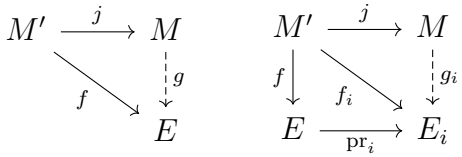
Lemma 4.40. *Suppose E is an R-module so that every short exact sequence $0 \to E \xrightarrow{i} M \to M'' \to 0$ splits. Then E is injective.*

Proof. By Lemma 4.39, E embeds into an injective R-module E', call the embedding $i\colon E \to E'$. It then fits into the short exact sequence $0 \to E \xrightarrow{i} E' \xrightarrow{\mathrm{cok}\, i} K' \to 0$, which splits by assumption, meaning that $E' \cong E \oplus K'$. By Lemma 4.32, E is injective as it is a direct summand of an injective module. □

There is one more useful property of injective modules to mention. It is dual to the fact that any direct sum of projective modules is projective:

Lemma 4.41. *Let R be a ring, and suppose E_i is an injective module for $i \in I$. Then $E = \prod_{i \in I} E_i$ is injective.*

Proof. Suppose $j\colon M' \to M$ is an injection of R-modules and $f\colon M' \to E$ is a module map. Let $f_i\colon M' \to E_i$ be the composition of f with the i-th projection $E \to E_i$. Since E_i is injective, f_i extends into $g_i\colon M \to E_i$ satisfying $g_i j = f_i$.



The maps g_i for $i \in I$ assemble into a map $g\colon M \to E$. It satisfies $gj = f$ since this happens componentwise: $f_i = g_i j = (gj)_i$. Thus g is the desired extension for f and E is injective by Lemma 4.30, condition ii). □

4.5 Injective resolutions

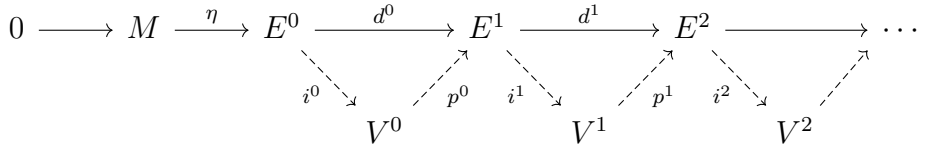
Since injective modules are dual to projective modules, one would hope that the results about projective resolutions also dualise. This is indeed true: first we prove the dual of Lemma 4.9, showing that every module has an injective resolution.

Lemma 4.42. *Every R-module M has an injective resolution, that is, there is a long exact sequence*

$$0 \to M \xrightarrow{\eta} E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^2} E^2 \to \cdots$$

with every module E^i, $i \geq 0$ injective.

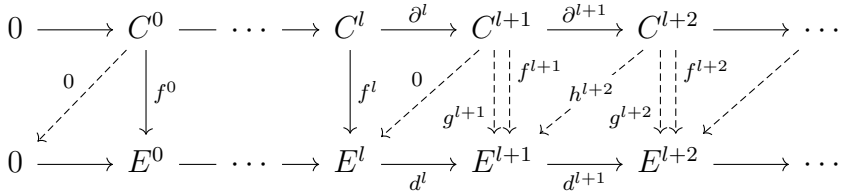
Proof. The proof goes as the proof of the dual statement, Lemma 4.9: there is an embedding $\eta\colon M \to E^0$ of M into an injective module E^0, which has cokernel $p^0\colon E^0 \to V^0 = \operatorname{Cok} \eta$. Then, inductively, there is an embedding $i^n\colon V^n \to E^{n+1}$ of V^n into an injective module E^{n+1} with cokernel $p^{n+1}\colon E^{n+1} \to V^{n+1} = \operatorname{Cok} i^n$.



Defining $d^n = p^n i^n$ then yields a long exact sequence, as before. □

The dual of Remark 4.6 says that deleted injective resolutions of a module M are final in the category of deleted (co)resolutions of M and homotopy equivalence classes of maps over id_M. This is also true, and the proof is dual to the proof of Theorem 3.26.

Theorem 4.43. *Let R be a ring. Let (C, ∂) and (E, d) be cochain complexes of R-modules, and for $i \leq l$, suppose there are maps $f^i \colon C^i \to E^i$ so that $d^i f^i = f^{i+1}\partial^i$. If E^n is injective for all $n \geq l+1$ and $C^\bullet$ is acyclic, then the maps f^i, $i \leq l$ extend to a cochain map $f \colon C^\bullet \to E^\bullet$. Furthermore, the map f is unique in that any two such extensions f and g are homotopic via a homotopy h having $h^i = 0$ for $i \leq l+1$.*



Specifically, if M and N are R-modules, $M \to C^\bullet$ is any (co)resolution and $N \to E^\bullet$ is an injective resolution, then any map of modules $f^{-1} \colon M \to N$ extends to a cochain map $f \colon C^\bullet \to E^\bullet$ and is unique up to homotopy. □

Corollary 4.44. *If R is a ring and M is an R-module, then any two injective resolutions of M are homotopy equivalent.*

Chapter 5

Derived functors and Ext

Recall that our current recipe for group cohomology $H^\bullet(G, M)$ is as follows. First, take a deleted projective resolution $P_\bullet$ of the trivial G-module $\mathbf{Z}_t$, apply to it the contravariant Hom functor $\mathrm{Hom}_G(-, M)$ to get the cochain complex

$$0 \to \mathrm{Hom}_G(P_0, M) \to \mathrm{Hom}_G(P_1, M) \to \mathrm{Hom}_G(P_2, M) \to \cdots,$$

and then take cohomology. What happens if we instead take a deleted injective resolution $E^\bullet$ of M and apply to it the covariant Hom functor $\mathrm{Hom}_G(\mathbf{Z}_t, -)$ to get the cochain complex

$$0 \to \mathrm{Hom}_G(\mathbf{Z}_t, E^0) \to \mathrm{Hom}_G(\mathbf{Z}_t, E^1) \to \mathrm{Hom}_G(\mathbf{Z}_t, E^2) \to \cdots ?$$

Do these two complexes have the same cohomology? It is worth it to abstract away the specifics and look at what the constructions have in common. They both start with a pair of modules $\mathbf{Z}_t$, M, choose a projective/injective resolution for one module, apply a functor depending on the other module, and then take cohomology. This motivates the following definitions.

5.1 Right derived functors

Definition 5.1. Let $\mathcal{C}$ be an abelian category. An object of $\mathcal{C}$ is said to be *projective*, if it satisfies the Definition 3.24. Similarly, an object of $\mathcal{C}$ is said to be *injective*, if it satisfies Definition 4.29. The category $\mathcal{C}$ is said to have *enough projectives* if for any object C of $\mathcal{C}$ there is an epimorphism $P \to C$ with P projective. Similarly, the category $\mathcal{C}$ is said to have *enough injectives* if for any object C of $\mathcal{C}$ there is a monomorphism $C \to E$ with E injective.

Note that Definitions 3.24 and 4.29 make sense in any abelian category, as they are diagrammatical. Similarly, all the definitions pertaining to resolutions

are easily extended to any abelian category. Note that the definitions for having enough projectives or injectives generalise the fact that every module is a quotient of a projective module, and embeds in an injective module.

As such, if an abelian category has enough projectives, then the proof of Lemma 4.9 shows that any object has a projective resolution (using the guaranteed epimorphisms from projectives in place of presentations). Similarly, if an abelian category has enough injectives, then the proof of Lemma 4.42 shows that every object has an injective resolution.

Finally, the proofs of Theorems 3.26 and 4.43 about chain maps between projective resolutions and acyclic chain complexes, and between acyclic cochain complexes and injective resolutions go through just as well.

Definition 5.2. Let $\mathcal{C}$ and $\mathcal{D}$ be abelian categories and $F, G\colon \mathcal{C} \to \mathcal{D}$ additive co- and contravariant functors, respectively.

If $\mathcal{C}$ has enough injectives, then the *right derived functors* of the *covariant* functor F, denoted $R^nF\colon \mathcal{C} \to \mathcal{D}$ for $n \geq 0$, are defined as follows.

For each object C in $\mathcal{C}$, choose a deleted injective resolution $E^\bullet_C$ of C. This defines a functor $\mathrm{Cch}\colon \mathcal{C} \to \mathrm{Cch}(\mathcal{C})$ into the category of cochain complexes and homotopy classes of cochain maps over $\mathcal{C}$: each object is taken to its chosen (co)resolution, and a morphism $f\colon C \to C'$ in $\mathcal{C}$ defines a chain map $E^\bullet_C \to E^\bullet_{C'}$ over f, which is unique up to homotopy.

The functor $F\colon \mathcal{C} \to \mathcal{D}$ then determines a functor $\hat{F}\colon \mathrm{Cch}(\mathcal{C}) \to \mathrm{Cch}(\mathcal{D})$ that applies F to each cochain complex and cochain map componentwise:

$$\hat{F}\Big(0 \to C^0 \xrightarrow{d^0} C^1 \to \cdots\Big) \quad = \quad 0 \to FC^0 \xrightarrow{Fd^0} FC^1 \to \cdots .$$

The functor R^nF is then defined to be the composite $H^n \circ \hat{F} \circ \mathrm{Cch}\colon \mathcal{C} \to \mathcal{D}$, where H^n is the n-th chain cohomology functor.

If $\mathcal{C}$ has enough projectives, then the *right derived functors* of the *contravariant* functor G, denoted $R^nG\colon \mathcal{C} \to \mathcal{D}$ for $n \geq 0$, are similarly defined. The choice of projective resolutions determines a functor $\mathrm{Ch}\colon \mathcal{C} \to \mathrm{Ch}(\mathcal{C})$ into the category of chain complexes and homotopy classes of chain maps. Similarly, G determines a functor $\hat{G}\colon \mathrm{Ch}(\mathcal{C}) \to \mathrm{Cch}(\mathcal{D})$ that applies G to each chain complex and morphism componentwise, turning them into cochain complexes:

$$\hat{G}\Big(\cdots \to D_1 \xrightarrow{\partial_1} D_0 \to 0\Big) \quad = \quad 0 \to GD_0 \xrightarrow{G\partial_1} GD_1 \to \cdots .$$

The functor R^nG is then defined to be the composite $H^n \circ \hat{G} \circ \mathrm{Ch}\colon \mathcal{C} \to \mathcal{D}$.

Remark 5.3. To see that the right derived functors are well defined, one must verify that Ch and Cch are additive functors and that the choice of resolutions

does not affect the end result, although it affects the Ch and Cch functors. The latter is simple: Corollary 4.44 says that any two (deleted) injective resolutions of the same module are homotopy equivalent, so they have isomorphic cohomology, and Corollary 4.4 says the same for projective resolutions.

For the former, the functoriality and additivity of Ch and Cch follows from the uniqueness of extensions to chain maps from projective and to injective (deleted) resolutions. For example, for morphisms $f\colon C \to C'$ and $g\colon C' \to C''$, taking extensions $h\colon E_C \to E_{C'}$ over f and $k\colon E_{C'} \to E_{C''}$ over g, the chain map $k \circ h$ is over $g \circ f$, so uniqueness up to homotopy deems that $\mathrm{Cch}(g \circ f) = \mathrm{Cch}(g) \circ \mathrm{Cch}(f)$.

Lastly, the right derived functors are additive because H^n, $\hat{F}$, $\hat{G}$, Ch and Cch all are.

As they are derived via cohomology, right derived functors inherit the long exact sequence property: they make long exact sequences of short exact sequences.

Lemma 5.4. *Let $\mathcal{C}$ and $\mathcal{D}$ be abelian categories, and $F, G\colon \mathcal{C} \to \mathcal{D}$ be additive co- and contravariant functors, respectively. Suppose $0 \to A \xrightarrow{h} B \xrightarrow{k} C \to 0$ is a short exact sequence in $\mathcal{C}$. Then, if $\mathcal{C}$ has enough injectives so that R^nF, $n \in \mathbf{N}$ are defined, there is the long exact sequence*

$$0 \to (R^0F)A \xrightarrow{(R^0F)h} (R^0F)B \xrightarrow{(R^0F)k} (R^0F)C \xrightarrow{\Delta^0_F} (R^1F)A \xrightarrow{(R^1F)h} (R^1F)B \to \cdots$$

and if $\mathcal{C}$ has enough projectives so that R^nG, $n \in \mathbf{N}$ are defined, there is the long exact sequence

$$0 \to (R^0G)C \xrightarrow{(R^0G)k} (R^0G)B \xrightarrow{(R^0G)h} (R^0G)A \xrightarrow{\Delta^0_G} (R^1G)C \xrightarrow{(R^1G)k} (R^1G)B \to \cdots$$

where Δ^n_F and Δ^n_G are connecting homomorphisms defined in the proof.

Proof. We prove the claim for F, as the proof for G is dual. It is enough to show that there are deleted injective resolutions for $A \to E^\bullet_A$, $B \to E^\bullet_B$ and $C \to E^\bullet_C$ and chain maps over h and k respectively, so that each row in the resulting diagram is exact (that is, it is an exact sequence of cochain complexes): this is done in the lemma below.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E^0_A & \xrightarrow{f^0} & E^0_B & \xrightarrow{g^0} & E^0_C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d^0_A} & & \downarrow{\scriptstyle d^0_B} & & \downarrow{\scriptstyle d^0_C} & & \\
0 & \longrightarrow & E^1_A & \xrightarrow{f^1} & E^1_B & \xrightarrow{g^1} & E^1_C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

Supposing that this has been done, observe that each row splits by Lemma 4.30, as the objects E_A^n are injective. This means that $E_B^n \cong E_A^n \oplus E_C^n$, so as additive functors preserve biproducts, also $FE_B^n \cong FE_A^n \oplus FE_C^n$, and so the rows remain exact after applying F to each resolution.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & FE_A^0 & \xrightarrow{Ff^0} & FE_B^0 & \xrightarrow{Fg^0} & FE_C^0 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle Fd_A^0} & & \downarrow{\scriptstyle Fd_B^0} & & \downarrow{\scriptstyle Fd_C^0} & & \\
0 & \longrightarrow & FE_A^1 & \xrightarrow{Ff^1} & FE_B^1 & \xrightarrow{Fg^1} & FE_C^1 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

As the values of the right derived functors of F are the cohomologies of the columns, taking cohomology along the columns gives the usual long exact sequence

$$\begin{array}{ccccccc}
 & & & & & & 0 \\
 & & & & & \swarrow & \\
(R^0F)A & \xrightarrow{(R^0F)f^0} & (R^0F)B & \xrightarrow{(R^0F)g^0} & (R^0F)C & & \\
 & & & & & \swarrow{\scriptstyle \Delta_F^0} & \\
(R^1F)A & \xrightarrow{(R^1F)f^1} & (R^1F)B & \xrightarrow{(R^1F)g^1} & (R^1F)C & & \\
 & & & & & \swarrow & \\
\vdots & & & & & &
\end{array}$$

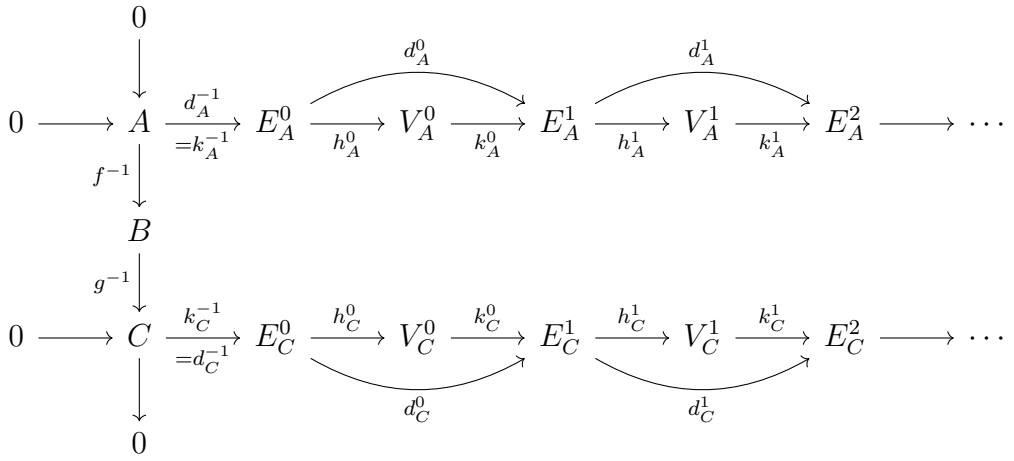
with the usual connecting maps Δ_F^n, obtained e.g. from the snake lemma. □

Lemma 5.5. *Suppose R is a ring and $0 \to A \xrightarrow{f^{-1}} B \xrightarrow{g^{-1}} C \to 0$ is a short exact sequence of R-modules. Let $A \to E_A^\bullet$ and $C \to E_C^\bullet$ be any injective resolutions for A and C respectively. Then there is an injective resolution $B \to E_B^\bullet$ and chain maps f over f^{-1} and g over g^{-1} so that each row $0 \to E_A^n \xrightarrow{f^n} E_B^n \xrightarrow{g^n} E_C^n \to 0$ is short exact.*

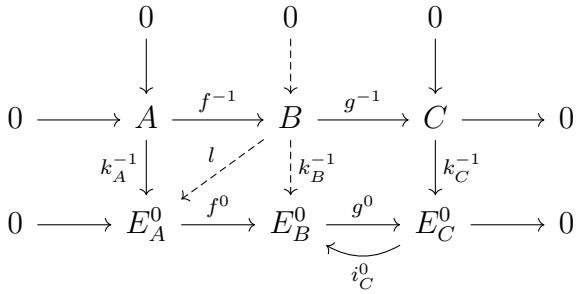
Note that the superscripts in f^{-1} and g^{-1} are not inverses but indices. The proof below contains no inverse morphisms, all the superscripts $^{-1}$ that appear below are indices.

Proof. Let $d_A^\bullet$ be the coboundary map of $E_A^\bullet$, and $d_A^{-1} \colon A \to E_A^0$ the coaugmentation map. Also, let $V_A^n = \operatorname{Cok} d_A^{n-1} = \operatorname{Coim} d_A^n$, so that each d_A^n decomposes into

$E_A^n \xrightarrow{h_A^n} V_A^n \xrightarrow{k_A^n} E_A^{n+1}$ where $h_A^n = \operatorname{coim} d_A^n$ is epi and $k_A^n = \operatorname{im} d_A^n$ is mono (so $d_A^{-1} = k_A^{-1}$). Make the same definitions for C.



Define $E_B^n = E_A^n \oplus E_C^n$, which is injective as the product of E_A^n and E_C^n by Lemma 4.41. Let $f^n = i_A^n \colon E_A^n \to E_B^n$ and $g^n = p_C^n \colon E_B^n \to E_C^n$ be the canonical inclusion and projection maps (together with $i_C^n \colon E_C^n \to E_B^n$ and $p_A^n \colon E_B^n \to E_A^n$), which makes $0 \to E_A^n \xrightarrow{f^n} E_B^n \xrightarrow{g^n} E_C^n \to 0$ (split) short exact.



Because E_A^0 is injective, the morphism k_A^{-1} extends into $l \colon B \to E_A^0$ along f^{-1} so that $lf^{-1} = k_A^{-1}$. Define $k_B^{-1} = f^0 l + i_C^0 k_C^{-1} g^{-1}$. Now

$$k_B^{-1} f^{-1} = f^0 l f^{-1} + i_C^0 k_C^{-1} g^{-1} f^{-1} = f^0 k_A^{-1} + 0 = f^0 k_A^{-1}$$

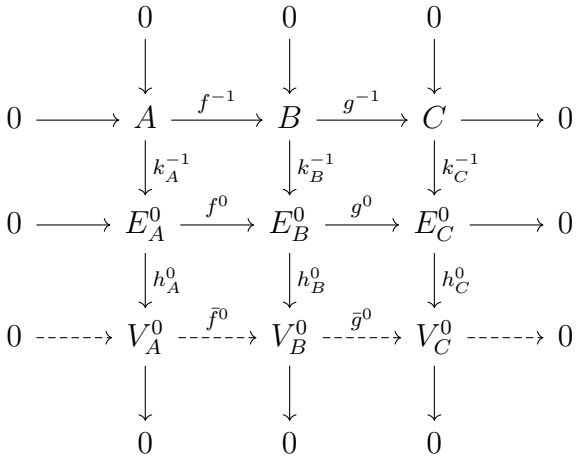
and

$$g^0 k_B^{-1} = g^0 f^0 l + g^0 i_C^0 k_C^{-1} g^{-1} = 0 + k_C^{-1} g^{-1} = k_C^{-1} g^{-1}$$

so the two squares formed by k_B^{-1} commute.

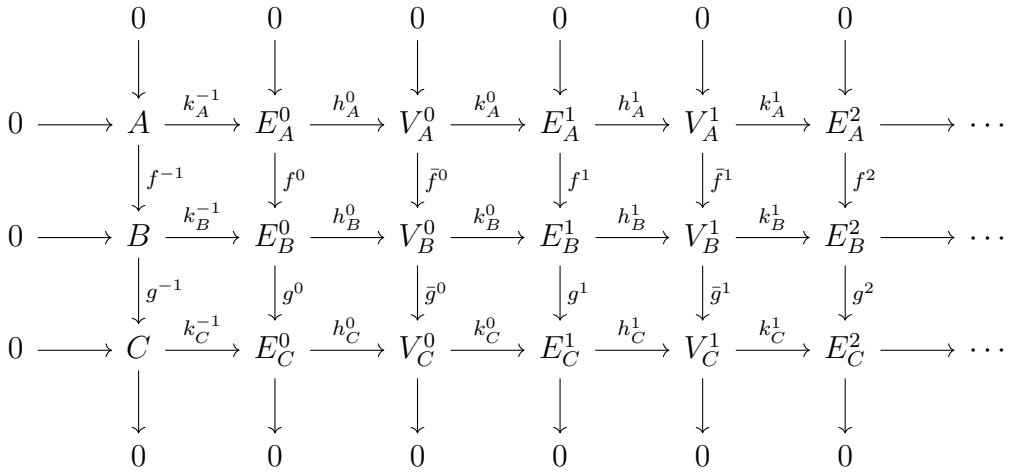
Define $V_B^0 = \operatorname{Cok} k_B^{-1}$ and let $h_B^0 = \operatorname{cok} k_B^{-1}$ be the quotient morphism, as with A and C. Then, because the top squares commute, f^0 and g^0 descend into the quotient as $\bar{f}^0 \colon V_A^0 \to V_B^0$ and $\bar{g}^0 \colon V_B^0 \to V_C^0$ and the two bottom squares commute,

as illustrated below.



Now, since all but the bottom row are known to be exact, the bottom row is also exact by the nine lemma.

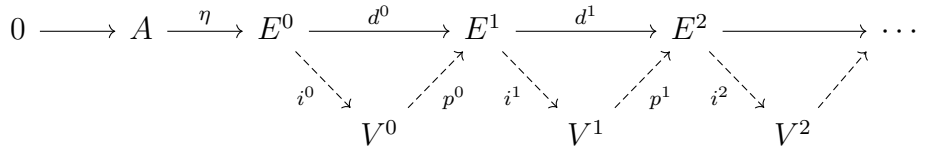
This process can then be iterated, with $0 \to V_A^0 \xrightarrow{\bar{f}^0} V_B^0 \xrightarrow{\bar{g}^0} V_C^0 \to 0$ in place of $0 \to A \xrightarrow{f^{-1}} B \xrightarrow{g^{-1}} C \to 0$ to define k_B^0 and then h_B^1, and continued. We define the coboundary maps $d_B^\bullet$ by $d_B^{-1} = k_B^{-1}$ and $d_B^n = k_B^n h_B^n$ for $n \geq 0$, which makes $0 \to A \to E_B^\bullet$ long exact, as in Lemma 4.9. This yields the below diagram.



The maps f^n and g^n assemble into cochain maps between the injective resolutions as every square in the above diagram commutes, and the maps are evidently over f^{-1} and g^{-1}. Lastly, the sequences $0 \to E_A^n \xrightarrow{f^n} E_B^n \xrightarrow{g^n} E_C^n \to 0$ are short exact by construction. □

The objects V_X^n above are called *cosyzygies* of the corresponding coresolution $X \to E_X^\bullet$ (where $X = A$ or B or C), and similarly the objects K_n appearing in Lemma 4.9 are called *syzygies*.

Lemma 5.6. *Let $\mathcal{C}$ and $\mathcal{D}$ be abelian categories, let $F, G\colon \mathcal{C} \to \mathcal{D}$ be co- and contravariant additive functors, and let A be an object of $\mathcal{C}$. Suppose $\mathcal{C}$ has enough injectives so that R^nF are defined for $n \in \mathbf{N}$.*



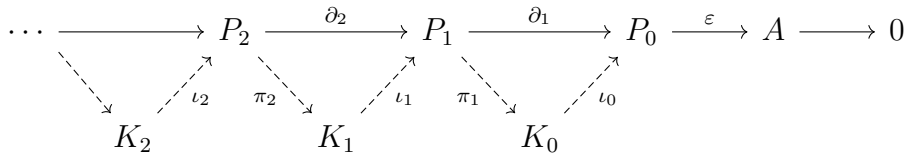
If $0 \to A \xrightarrow{\eta} E^0 \xrightarrow{d^0} E^1 \to \cdots$ is an injective resolution with cosyzygies $V^0 = \operatorname{Cok}\eta$ and $V^n = \operatorname{Cok} d^{n-1}$ for $n \geq 1$, then

$$(R^{n+1}F)A \cong (R^nF)V^0 \cong (R^{n-1}F)V^1 \cong \cdots \cong (R^1F)V^{n-1}$$

for all $n \in \mathbf{N}$. Similarly, if $\mathcal{C}$ has enough projectives so that R^nG are defined for $n \in \mathbf{N}$, then

$$(R^{n+1}G)A \cong (R^nG)K_0 \cong (R^{n-1}G)K_1 \cong \cdots \cong (R^1G)K_{n-1}$$

for any syzygies $K_0 = \operatorname{Ker}\varepsilon$, $K_n = \operatorname{Ker}\partial_n$ for $n \geq 1$ of any projective resolution $\cdots \to P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\varepsilon} A \to 0$.



Proof. Let $0 \to A \xrightarrow{\eta} E^0 \xrightarrow{d^0} E^1 \to \cdots$ be an injective resolution. The object $(R^{n+1}F)A$ is the $(n+1)$-st cohomology group of the deleted, functored resolution

$$0 \to FE^0 \xrightarrow{Fd^0} FE^1 \to \cdots \to FE^n \xrightarrow{Fd^n} FE^{n+1} \xrightarrow{Fd^{n+1}} FE^{n+2} \to \cdots$$

so $(R^{n+1}F)A = \operatorname{Ker} Fd^{n+1} / \operatorname{Im} Fd^n$.

For a $j \in \mathbf{N}$ with $j \leq n-1$, we can cut off the injective resolution of A at E^j by factoring $d^j\colon E^j \to E^{j+1}$ as $E^j \xrightarrow{\operatorname{coim} d^j} V^j \xrightarrow{\operatorname{im} d^j} E^{j+1}$. Since $\operatorname{im} d^j$ is mono, this yields the long exact sequence

$$0 \to \underset{-1}{V^j} \xrightarrow{\operatorname{im} d^j} \underset{0}{E^{j+1}} \xrightarrow{d^{j+1}} \underset{1}{E^{j+2}} \to \cdots \to \underset{n-j-1}{E^n} \xrightarrow{d^n} \underset{n-j}{E^{n+1}} \xrightarrow{d^{n+1}} \underset{n-j+1}{E^{n+2}} \to \cdots$$

which is an injective resolution for the cosyzygy V^j. The indexing is now offset from the degrees, which are displayed below the objects. The object in degree

$k \geq 0$ is E^{j+1+k}, and in particular E^{n+1} is sitting in degree $n-j$. The object $(R^{n-j}F)V^j$ is the $(n-j)$-th cohomology group of the functored, deleted resolution

$$0 \to \underset{0}{FE^{j+1}} \xrightarrow{Fd^{j+1}} \underset{1}{FE^{j+2}} \to \cdots \to \underset{n-j-1}{FE^{n}} \xrightarrow{Fd^{n}} \underset{n-j}{FE^{n+1}} \xrightarrow{Fd^{n+1}} \underset{n-j+1}{FE^{n+2}} \to \cdots$$

which is $\operatorname{Ker} Fd^{n+1} / \operatorname{Im} Fd^n = (R^{n+1}F)A$, as desired.

The case of the contravariant functor G is entirely similar. □

Note that the chain of isomorphisms in the above lemma does not reach $(R^0F)V^n$, because in the truncated resolution $0 \to V^n \to E^{n+1} \to E^{n+2} \to \cdots$, the object E^{n+1} is no longer flanked by E^n on the left. However, the zeroth derived functor is special:

Lemma 5.7. *Let $\mathcal{C}$ and $\mathcal{D}$ be abelian categories, and $F, G \colon \mathcal{C} \to \mathcal{D}$ be additive co- and contravariant left exact functors. Then $R^0F \cong F$ if $\mathcal{C}$ has enough injectives, and $R^0G \cong G$ if $\mathcal{C}$ has enough projectives.*

Proof. For the covariant functor F, let A be an object in C and $0 \to A \to E^\bullet$ an injective resolution for A. By exactness of the sequence, $A \cong \operatorname{Ker} d^0$. Because covariant left exact functors preserve kernels by Remark 4.27, we also have that $FA \cong \operatorname{Ker} Fd^0$. Thus $(R^0F)A = \operatorname{Ker} Fd^0 / \operatorname{Im} 0 \cong FA$.

To see naturality, consider a morphism $A \xrightarrow{f} B$. Take injective resolutions $0 \to A \xrightarrow{\eta_A} E^\bullet_A$ and $0 \to B \xrightarrow{\eta_B} E^\bullet_B$, fill f into a chain map g over f and apply F. Below are the first square of the functored chain map diagram, which is known to commute, and the naturality square we wish to show to commute.

$$\begin{array}{ccc} FA & \xrightarrow{F\eta_A} & FE^0_A \\ \downarrow{\scriptstyle Ff} & & \downarrow{\scriptstyle Fg^0} \\ FB & \xrightarrow[F\eta_B]{} & FE^0_B \end{array} \qquad \begin{array}{ccc} FA & \xrightarrow{\cong} & (R^0F)A \\ \downarrow{\scriptstyle Ff} & & \downarrow{\scriptstyle (R^0F)f} \\ FB & \xrightarrow[\cong]{} & (R^0F)B \end{array}$$

Now, $(R^0F)f \colon (R^0F)A \to (R^0F)B$ is the morphism induced by Fg^0 in cohomology. It is obtained by restricting Fg^0 into $\operatorname{Ker} Fd^0_A$ (and quotienting by $\operatorname{Im} 0$, so doing nothing). Thus restricting Fg^0 into $\operatorname{Ker} Fd^0_A$ and shrinking the target of Fg^0 into $\operatorname{Ker} Fd^0_B$ in the commuting square on the left gives the naturality square on the right, which commutes.

The case of a contravariant left exact additive functor G is similar, which converts the cokernel in a projective resolution into a kernel. □

Corollary 5.8. *Putting the previous lemma together with the long exact sequence Lemma 5.4 shows that a left exact covariant additive functor F turns the short exact sequence $0 \to A' \to A \to A'' \to 0$ into a long exact sequence*

$$0 \to FA' \to FA \to FA'' \to (R^1F)A' \to (R^1F)A \to (R^1F)A'' \to (R^2F)A' \to \cdots$$

and a left exact additive contravariant functor G has the long exact sequence

$$0 \to GA'' \to GA \to GA' \to (R^1G)A'' \to (R^1G)A \to (R^1G)A' \to (R^2G)A'' \to \cdots$$

so the right derived functors can be seen as a way of repairing the loss of short exactness of the original short exact sequence.

5.2 The Ext functors

We now return to look at the Hom functor in specific. The derived functors of Hom have special names: since Hom is a functor of two variables, we may hold either one constant and derive on the other.

Definition 5.9. Let R be a ring, $n \in \mathbf{N}$, and let M and N be R-modules. We define $\operatorname{Ext}^n_R(M, -)$ to be the n-th right derived functor R^nF of $F = \operatorname{Hom}_R(M, -)$, and $\operatorname{ext}^n_R(-, N)$ to be the n-th right derived functor R^nG of $G = \operatorname{Hom}_R(-, N)$.

Example 5.10. Let G be a group and M be a G-module. Note that $\operatorname{ext}^n_{\mathbf{Z}G}(\mathbf{Z}_t, M)$ is simply $H^n(G, M)$: both take a deleted projective resolution of the trivial G-module $\mathbf{Z}_t$, apply to it the functor $\operatorname{Hom}_G(-, M)$ and calculate the n-th cohomology.

Recall that in Example 3.17 and Remark 3.18, we calculated $H^0(G, M) = \operatorname{ext}^0_{\mathbf{Z}G}(\mathbf{Z}_t, M)$ to be $M^G \cong \operatorname{Hom}_G(\mathbf{Z}_t, M)$, the fixed points of the G-action on M. Together with Lemma 5.7, which says that the zeroth derived functor is isomorphic to the original functor, these suggest that the groups $H^n(G, M) = \operatorname{ext}^n_{\mathbf{Z}G}(\mathbf{Z}_t, M)$ are also the values of the derived functors $\operatorname{Ext}^n_{\mathbf{Z}G}(\mathbf{Z}_t, M)$.

We thus set out to prove that $\operatorname{Ext}_R(M, N) \cong \operatorname{ext}_R(M, N)$. First, we observe that projective and injective modules make Ext and ext trivial.

Lemma 5.11. *Let R be a ring, let M, P and E be R-modules and let $n \geq 1$. Then $\operatorname{Ext}^n_R(M, E) = 0 = \operatorname{ext}^n_R(M, E)$ if E is injective and $\operatorname{ext}^n_R(P, M) = 0 = \operatorname{Ext}^n_R(P, M)$ if P is projective.*

Proof. Suppose E is injective. Then $0 \to E \xrightarrow{\cong} E \to 0 \to \cdots$ is an injective resolution of E, so $\operatorname{Ext}^n_R(M, E)$ is the n-th cohomology of the deleted, functored resolution $0 \to \operatorname{Hom}_R(M, E) \to 0 \to \cdots$, which is 0, as $n \geq 1$.

Consider then $\operatorname{Ext}^n_R(P, M)$ where P is projective. Let $0 \to M \to E^\bullet$ be an injective resolution of M. Ext is calculated as the n-th cohomology of the deleted, functored resolution

$$0 \to \operatorname{Hom}_R(P, E^0) \xrightarrow{d^0_*} \operatorname{Hom}_R(P, E^1) \xrightarrow{d^1_*} \operatorname{Hom}_R(P, E^2) \to \cdots$$

which is exact everywhere except in degree 0 – because the left-flanking term M was deleted – as $\operatorname{Hom}_R(P,-)$ is an exact functor, per the projectiveness of P. Thus $\operatorname{Ext}^n_R(P,M) = 0$ as $n \geq 1$.

The case of ext^n_R is entirely similar. □

Theorem 5.12. *Let R be a ring, let M and N be R-modules and let $n \in \mathbf{N}$. Then* $\operatorname{ext}^n_R(M,N) \cong \operatorname{Ext}^n_R(M,N)$.

Proof. The case $n = 0$ is Lemma 5.7: it says that $\operatorname{ext}^0_R(-,N) \cong \operatorname{Hom}_R(-,N)$ and $\operatorname{Ext}^0_R(M,-) \cong \operatorname{Hom}_R(M,-)$ since both Hom functors are left exact by Lemma 4.28, so putting these together gives $\operatorname{ext}^0_R(M,N) \cong \operatorname{Hom}_R(M,N) \cong \operatorname{Ext}^0_R(M,N)$.

Let $\cdots \to P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\varepsilon} M \to 0$ and $0 \to N \xrightarrow{\eta} E^0 \xrightarrow{d^0} E^1 \to \cdots$ be projective and injective resolutions, respectively. Introduce the syzygies and cosyzygies by setting $K_j = \operatorname{Im}\partial_{j+1}$ and $V^j = \operatorname{Im} d^j$ for $j \in \mathbf{N}$, and set $K_{-1} = M$ and $V^{-1} = N$ for uniformity. This splits the resolutions into short exact sequences

$$0 \to K_j \xrightarrow{\operatorname{im}\partial_{j+1}} P_j \xrightarrow{\operatorname{coim}\partial_j} K_{j-1} \to 0 \quad \text{and} \quad 0 \to V^{j-1} \xrightarrow{\operatorname{im} d^{j-1}} E^j \xrightarrow{\operatorname{coim} d^j} V^j \to 0$$

as seen in Lemma 5.5, for any $j \geq 0$; for $j = 0$, replace $\operatorname{coim}\partial_0$ with ε and $\operatorname{im} d^{-1}$ with η.

These may be woven into a 3×3 square with the Hom functor, denoted by $[X,Y] = \operatorname{Hom}_R(X,Y)$ to save space. The columns are obtained by applying $\operatorname{Hom}_R(-,X)$ on $0 \to K_i \to P_i \to K_{i-1} \to 0$ with $X = V^{j-1}, E^j, V^j$, and the rows are obtained by applying $\operatorname{Hom}_R(Y,-)$ on $0 \to V^{j-1} \to E^j \to V^j \to 0$ with $Y = K_{i-1}, P_i, K_i$.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & [K_{i-1},V^{j-1}] & \longrightarrow & [K_{i-1},E^j] & \xrightarrow{a} & [K_{i-1},V^j] & \longrightarrow & \operatorname{Ext}^1_R(K_{i-1},V^{j-1}) \to 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & [P_i,V^{j-1}] & \longrightarrow & [P_i,E^j] & \xrightarrow{b} & [P_i,V^j] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle e} & & \downarrow{\scriptstyle f} & & \\
0 & \longrightarrow & [K_i,V^{j-1}] & \longrightarrow & [K_i,E^j] & \xrightarrow{c} & [K_i,V^j] & \longrightarrow & \operatorname{Ext}^1_R(K_i,V^{j-1}) \to 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \operatorname{ext}^1_R(K_{i-1},V^{j-1}) & & 0 & & \operatorname{ext}^1_R(K_{i-1},V^j) & & \\
 & & \downarrow & & & & \downarrow & & \\
 & & 0 & & & & 0 & &
\end{array}$$

As P_i is projective and E^j is injective, the functors $\operatorname{Hom}_R(P_i,-)$ and $\operatorname{Hom}_R(-,V^j)$ are exact so the middle row and column are exact. The extremal rows and columns are also exact, as obtained from Corollary 5.8: the zeroes after the Ext terms are

Ext terms that contain the injective module E^j, and thus zero by Lemma 5.11, and the zeroes below the ext terms are ext terms containing the projective module P_i. Lastly, the diagram commutes as Hom is a bifunctor. We shall show that $\operatorname{ext}^1_R(K_{i-1}, V^j) \cong \operatorname{Ext}^1_R(K_i, V^{j-1})$ and $\operatorname{ext}^1_R(K_{i-1}, V^{j-1}) \cong \operatorname{Ext}^1_R(K_{i-1}, V^{j-1})$ hold for any $i, j \geq 0$.

For the first isomorphism, the functions b and e are surjective by exactness, so $\operatorname{Im} f = \operatorname{Im}(fb)$ and $\operatorname{Im} c = \operatorname{Im}(ce)$. As the diagram commutes, we have $fb = ce$, so $\operatorname{Im} f = \operatorname{Im} c$ and $\operatorname{Cok} f = \operatorname{Cok} c$. But the cokernels are $\operatorname{ext}^1_R(K_{i-1}, V^j)$ and $\operatorname{Ext}^1_R(K_i, V^{j-1})$ by exactness, so $\operatorname{ext}^1_R(K_{i-1}, V^j) \cong \operatorname{Ext}^1_R(K_i, V^{j-1})$.

For the second isomorphism, applying the snake lemma to the two bottom rows of the 3×3 square gives the exact sequence

$$\operatorname{Ker} d \to \operatorname{Ker} e \xrightarrow{a} \operatorname{Ker} f \to \operatorname{Cok} d \to \operatorname{Cok} e \to \operatorname{Cok} f$$

with $\operatorname{Ker} e \cong \operatorname{Hom}_R(K_{i-1}, E^j)$, $\operatorname{Ker} f \cong \operatorname{Hom}_R(K_{i-1}, V^j)$, $\operatorname{Cok} d \cong \operatorname{ext}^1_R(K_{i-1}, V^{j-1})$ and $\operatorname{Cok} e = 0$. Thus the four middle terms are

$$\operatorname{Hom}_R(K_{i-1}, E^j) \xrightarrow{a} \operatorname{Hom}_R(K_{i-1}, V^j) \to \operatorname{ext}^1_R(K_{i-1}, V^{j-1}) \to 0$$

which means that $\operatorname{Cok} a \cong \operatorname{ext}^1_R(K_{i-1}, V^{j-1})$. On the other hand, the exactness of the top row of the diagram implies that $\operatorname{Cok} a \cong \operatorname{Ext}^1_R(K_{i-1}, V^{j-1})$, so we get that $\operatorname{ext}^1_R(K_{i-1}, V^{j-1}) \cong \operatorname{Ext}^1_R(K_{i-1}, V^{j-1})$.

Next, we show by induction on n that the isomorphisms

$$\operatorname{ext}^n_R(K_{i-1}, V^j) \overset{\text{A}}{\cong} \operatorname{Ext}^n_R(K_i, V^{j-1}) \quad \text{and} \quad \operatorname{ext}^n_R(K_{i-1}, V^{j-1}) \overset{\text{B}}{\cong} \operatorname{Ext}^n_R(K_{i-1}, V^{j-1})$$

hold for any $i, j \geq 0$ and $n \geq 1$. The base case of $n = 1$ was handled above: suppose now that it holds for some $n \geq 1$ so that we may show it holds for $n + 1$. Let $i, j \geq 0$ be arbitrary. We then have the isomorphisms

$$\begin{aligned}
\operatorname{ext}^{n+1}_R(K_{i-1}, V^j) &\cong \operatorname{ext}^n_R(K_i, V^j) && \text{(by Lemma 5.6 on } \operatorname{Hom}_R(-, V^j)) \\
&\cong \operatorname{Ext}^n_R(K_i, V^j) && \text{(by isomorphism B)} \\
&\cong \operatorname{Ext}^{n+1}_R(K_i, V^{j-1}) && \text{(by Lemma 5.6 on } \operatorname{Hom}_R(K_i, -))
\end{aligned}$$

and

$$\begin{aligned}
\operatorname{ext}^{n+1}_R(K_{i-1}, V^{j-1}) &\cong \operatorname{ext}^n_R(K_i, V^{j-1}) && \text{(by Lemma 5.6 on } \operatorname{Hom}_R(-, V^{j-1})) \\
&\cong \operatorname{Ext}^n_R(K_i, V^{j-1}) && \text{(by isomorphism B)} \\
&\cong \operatorname{ext}^n_R(K_{i-1}, V^j) && \text{(by isomorphism A)} \\
&\cong \operatorname{Ext}^n_R(K_{i-1}, V^j) && \text{(by isomorphism B)} \\
&\cong \operatorname{Ext}^{n+1}_R(K_{i-1}, V^{j-1}) && \text{(by Lemma 5.6 on } \operatorname{Hom}_R(K_{i-1}, -))
\end{aligned}$$

which complete the induction step. As $K_{-1} = M$ and $V^{-1} = N$, we have in particular in the case $i = j = -1$ that $\operatorname{ext}^n_R(M, N) \cong \operatorname{Ext}^n_R(M, N)$ for all $n \in \mathbf{N}$. $\square$

Thus the distinction between the two functors can be ignored, and Ext^n_R is used to denote either functor, with the understanding that $\mathrm{Ext}^n_R(M,N)$ can be calculated by choosing a resolution for either module.

Remark 5.13. As foreseen at the start of this section, we have yet another way to calculate $H^n(G,M) = \mathrm{Ext}^n_{\mathbf{Z}G}(\mathbf{Z}_t, M)$, which is to choose an injective resolution $0 \to M \to E^\bullet$ of the G-module M, then delete M and apply the functor $\mathrm{Hom}_G(\mathbf{Z}_t, -)$ (which is isomorphic to the fixed-point functor $-^G$, as seen in Remark 3.18) and calculate the n-th homology group.

$$0 \to (E^0)^G \to (E^1)^G \to (E^2)^G \to \cdots$$

This also explains why $H^n(G,M)$ is just an abelian group, and not a G-module as it a priori would be. It is a G-module, but we see from the above cochain complex that the G-action it inherits is trivial, so it may as well not be.

Further avenues

A lot of good topics have been left out in order to keep the scope suitably narrow. Perhaps the most glaring omission is that of *left derived functors* and Tor; the story of left derived functors runs parallel to Section 5.1, where homology replaces cohomology (and the resolutions to be used are arranged so that functoring yields a chain complex). Tor is the left derived functor of the tensor product, and it is used analogously to Ext to define group homology.

Ext and Tor can also be characterised axiomatically, which yields a nice set of rules for calculating them, at least on finitely generated abelian groups. They can also be computed by taking a resolution for each variable and twining them into a double complex, which is then collapsed into a single total complex. Computing its cohomology leads to the concept of *spectral sequences*.

Projective and injective modules were defined to make the co- and contravariant Hom functors exact. The missing third concept is that of a *flat module*, which makes tensoring an exact functor. One can also define flat resolutions in analogy. Considering the shortest possible resolution of each type for an arbitrary module leads to the concept of *projective*, *injective*, and *flat dimensions*.

Also of interest is the topological side of group cohomology. Originally, the cohomology of a group was defined as the cohomology of a certain topological space, called a *classifying space*, having that group as its *fundamental group*. Topology also provides means to generate projective resolutions for calculations. A fuller treatment of group cohomology would also include a description of the *ring structure* it enjoys, a *Künneth formula* for products, and descriptions on how the cohomology changes as the group is shrunk or quotiented, or the coefficients are changed.

Bibliography

[1] Kenneth S. Brown. *Cohomology of groups*. Graduate texts in mathematics. New York: Springer, 1982.

[2] Joseph J. Rotman. *An introduction to homological algebra*. Second edition. Universitext. New York: Springer, 2009.

[3] Allen Hatcher. *Algebraic topology*. Cambridge: Cambridge University Press, 2002.

[4] Emily Riehl. *Category Theory in Context*. Aurora: Dover Modern Math Originals. Dover Publications, 2017.

[5] Peter Freyd. *Abelian categories: an introduction to the theory of functors*. New York: Harper & Row, 1964.