Homological Algebra

Dietrich Burde

Lecture Notes 2022

Contents

CHAPTER 1

Introduction

Homological algebra is a branch of mathematics devoted to the study of *homology* in a general algebraic setting. Here "homology" is a general way of associating a sequence of algebraic objects, such as abelian groups or modules, to other mathematical objects such as topological spaces. Homology groups were originally defined in algebraic topology, but then have been generalized to a wide variety of other contexts, such as abstract algebra, algebraic geometry, algebraic number theory, representation theory, mathematical physics and other areas.

CHAPTER 2

Rings and modules

Rings and modules are a prerequisite for areas such as commutative algebra, homological algebra or number theory. Therefore we provide a chapter on it with basic definitions and results.

2.1. Definition of ring and module

In commutative algebra we usually assume that a ring is commutative and has a unit. For homological algebra we consider in addition to commutative rings also other rings like group rings, which are not necessarily commutative.

DEFINITION 2.1.1. A *ring* is an abelian group $(R, +)$ together with a unit element $1 \in R$ and an associative bilinear map $R \times R \to R$, $(x, y) \mapsto x \cdot y$ such that $1 \cdot x = x \cdot 1 = x$ for all $x \in R$ and the distributive laws are satisfied.

Note that this definition excludes non-associative rings like Lie rings or Jordan rings. Recall that a ring homomorphism $\varphi\colon R \to S$ preserves the unit elements, i.e., it satisfies $\varphi(1_R) = 1_S$. The most familiar ring is the ring of integers $\mathbb{Z}$. It is called the *initial ring* in homological algebra for the following reason.

EXAMPLE 2.1.2. *For every ring R, there is a unique ring homomorphism $\varphi\colon \mathbb{Z} \to R$. This says that the ring of integers is an initial object in the category of rings.*

The zero ring $R = \{0\}$ is the only ring with $1_R = 0$. It is called the *terminal ring* for the following reason.

EXAMPLE 2.1.3. *For every ring R, there is a unique ring homomorphism $\varphi\colon R \to 0$, where 0 denotes the zero ring. This says that the zero ring is a terminal object in the category of rings.*

Of course we will give an exact definition for the category of rings lateron. Other typical commutative rings are the fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, or the polynomial ring $R[X]$ over a commutative ring R, and the power series ring $R[[X]]$.

EXAMPLE 2.1.4. *Let R be a commutative ring and G be a group. Then the group ring $R[G]$ is the ring of all finite sums $\sum_{g\in G} r_g[g]$ with $r_g \in R$. The addition is defined by*

$$\sum_{g\in G} r_g[g] + \sum_{g\in G} s_g[g] = \sum_{g\in G} (r_g + s_g)[g],$$

and the multiplication by

$$\left(\sum_{g\in G} r_g[g]\right)\left(\sum_{g\in G} s_g[g]\right) = \sum_{g\in G}\sum_{ab=g} r_a s_b[g].$$

This arises from requiring $[g][h] = [gh]$ and bilinearity over R.

Let G be the infinite cyclic group $\langle t\rangle = \{t^n \mid n \in \mathbb{Z}\}$ and R be a commutative ring. Then $R[G]$ is the ring $R[t, t^{-1}]$ of all Laurent polynomials

$$a_n t^n + a_{n-1}t^{n-1} + \cdots + a_0 + a_{-1}t^{-1} + \cdots + a_{-m}t^{-m}.$$

DEFINITION 2.1.5. Let R be a commutative ring and S be a ring. Then S is called an *R-algebra*, if there is a ring homomorphism $\varphi\colon R \to S$ such that $\varphi(r)s = s\varphi(r)$ for all $r \in R$ and $s \in S$.

Vector spaces are defined over fields. The corresponding notion over a ring is called a *module*. By definition we consider every module as a left module.

DEFINITION 2.1.6. A left R-module is an abelian group $(M, +)$ equipped with a bilinear map $\mu\colon R \times M \to M$ satisfying

$$\mu(1, m) = m,$$
$$\mu(x, \mu(y, m)) = \mu(xy, m)$$

for all $x, y \in R$ and $m \in M$.

When the action μ is fixed, we usually just write $x.m$ or xm for $\mu(x, m)$.

EXAMPLE 2.1.7. *Some basic examples of R-modules are the following.*

1. *Every vector space over a field K is a K-module.*
2. *Every abelian group is a $\mathbb{Z}$-module.*
3. *Every ring is a module over itself, the action given by the ring multiplication.*

DEFINITION 2.1.8. Let M and N be modules over a ring R. Then an R-linear map $f\colon M \to N$ is called an *R-module homomorphism*. So we have

$$f(x + y) = f(x) + f(y),$$
$$f(r.x) = r.f(x)$$

for all $x, y \in M$ and $r \in R$. We denote by $\mathrm{Hom}_R(M, N)$ the abelian group of all R-module homomorphisms.

For a given ring $(R, \cdot)$ the *opposite ring* R^{op} is defined by $(R, \circ)$ with the same underlying abelian group, but with reversed multiplication $r \circ s := s \cdot r$. When R is a commutative ring, it coincides with its opposite ring. Otherwise R may not be isomorpic to R^{op}.

2.2. Actions on rings and modules

There are several ways to construct new rings and modules from given ones. Let I be an index set, which may be finite or infinite.

DEFINITION 2.2.1. Let R be a ring and M_i for $i \in I$ be R-modules. Then the *direct product* $\prod_{i\in I} M_i$ is the R-module $\{(m_i) \mid i \in I\}$ of tuples with componentwise addition and diagonal multiplication $r.(m_i)_{i\in I} = (r.m_i)_{i\in I}$.

The *direct sum* $\bigoplus_{i\in I} M_i$ is defined as the subset of the (m_i) from the direct product, for which $m_i = 0$ for almost all $i \in I$, i.e., for all but finitely many $i \in I$.

The direct sum and direct product differ only for infinite indices, i.e., if I is infinite. There are canonical R-module homomorphisms

$$M_i \xrightarrow{j_i} \bigoplus_{i\in I} M_i \subseteq \prod_{i\in I} M_i \xrightarrow{p_i} M_i$$

given by inclusion of the i-th component and the projection to the i-th component. Note that we can define the direct product of infinitely many rings as well, but not the direct sum, as it would miss an identity element $(1, 1, \ldots, 1)$ with infinitely many 1's. As we will see, the direct product and the direct sum of modules are dual in the sense of category theory: the direct sum is the coproduct, while the direct product is the product in the category of R-modules. We can already be a bit more precise.

LEMMA 2.2.2. *The direct sum satisfies the universal property of a coproduct for R-modules. This means, that we have a bijection, even an isomorphism of abelian groups*

$$\mathrm{Hom}_R\left(\bigoplus_{i\in I} M_i, N\right) \cong \prod_{i\in I} \mathrm{Hom}_R(M_i, N),$$

where the bijective map is given by $f \mapsto (f \circ j_i)_{i\in I}$ for $f \in \mathrm{Hom}_R\left(\bigoplus_{i\in I} M_i, N\right)$.

PROOF. We show that f is bijective by constructing an inverse map, namely $(f_i)_{i\in I} \mapsto \sum_{i\in I} f_i \circ p_i$. Here the sum is finite, because only finitely many $p_i(m)$ are nonzero for $m \in \bigoplus_{i\in I} M_i$. □

Similarly we have the following result for the product.

LEMMA 2.2.3. *The direct product satisfies the universal property of a product for R-modules. This means, that we have a bijection, even an isomorphism of abelian groups*

$$\mathrm{Hom}_R\left(M, \prod_{i\in I} N_i\right) \cong \prod_{i\in I} \mathrm{Hom}_R(M, N_i).$$

We have defined the tensor product of R-modules over a commutative ring R in [**2**]. We will extend this here to rings, which are not necessarily commutative.

DEFINITION 2.2.4. Let M be an R^{op}-module and N be an R-module. The tensor product $M \otimes_R N$ is defined by the free abelian group generated by the pairs $m \otimes n$ for $m \in N$ and $n \in N$ modulo the relations

$$0 \otimes n = m \otimes 0 = 0 \tag{2.1}$$

$$(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n \tag{2.2}$$

$$m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2 \tag{2.3}$$

$$(m.r) \otimes n = m \otimes (r.n) \tag{2.4}$$

for all $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ and $r \in R$.

The tensor product has the following properties.

PROPOSITION 2.2.5. *Let M, M_i be R^{op}-modules and N be an R-module. Let Q be an S-module and P be an R-module, which is at the same time an S^{op}-module with $(r.p).s = r.(p.s)$. Then we have*

(1) $M \otimes_R R \simeq M$ *and* $R \otimes_R N \simeq N$.
(2) $\left(\bigoplus_{i\in I} M_i\right) \otimes_R N \cong \bigoplus_{i\in I}(M_i \otimes_R N)$.
(3) $M \otimes_R \left(\bigoplus_{i\in I} N_i\right) \cong \bigoplus_{i\in I}(M \otimes_R N_i)$.
(4) $(M \otimes_R P) \otimes_S Q \cong M \otimes_R (P \otimes_S Q)$.

PROOF. (1): This follows immediately from (2.4) of Definition 2.2.4.

(2): A morphism

$$\Phi\colon \bigoplus_{i\in I}(M_i \otimes_R N) \to \left(\bigoplus_{i\in I} M_i\right) \otimes_R N$$

is by Lemma 2.2.2 uniquely determined by its restriction to each M_i, where we have $\Phi(m_i \otimes n) = j_i(m_i) \otimes n$. The map is bijective, because we can easily specify an inverse map Ψ as follows. Any element in $\left(\bigoplus_{i\in I} M_i\right) \otimes_R N$ is a sum of elements of the form

$$x = \left(\sum_{i\in I} j_i(m_i)\right) \otimes n,$$

where $m_i \in M_i$ and almost all $m_i = 0$. The define Ψ by

$$\Psi(j_i(m_i) \otimes n) = j_i(m_i \otimes n).$$

(3): This follows the same way as (2).

(4): With the assumptions $M \otimes_R P$ becomes an S^{op}-module via $(m \otimes p).s = m \otimes (p.s)$, and $P \otimes_S Q$ becomes an R-module via $r.(p \otimes q) = (r.p) \otimes q$. Then the claimed associativity follows. □

EXAMPLE 2.2.6. *Let $R^n = R \oplus \cdots \oplus R$ be the free R-module of rank n. Then we have*

$$R^m \otimes_R R^n \cong R^{mn}.$$

This follows directly from (2) respectively (3) of Proposition 2.2.5.

EXAMPLE 2.2.7. *The isomorphism* (2) *does not hold in general for the direct product, i.e.,*

$$\left(\prod_{i\in I} M_i\right) \otimes_R N \ncong \prod_{i\in I}(M_i \otimes_R N).$$

Indeed, consider the $\mathbb{Z}$-module $M = \prod_{n\geq 1} \mathbb{Z}/n$ and the $\mathbb{Z}$-module $N = \mathbb{Q}$. Then we have $M_i \otimes_R N = \mathbb{Z}/n \otimes_{\mathbb{Z}} \mathbb{Q} = 0$ for all $i = n$, because

$$k \otimes q = (kn) \otimes \frac{q}{n} = 0 \otimes \frac{q}{n} = 0.$$

Hence the right side is equal to zero. On the other hand, the element $e \in \prod_{i\in I} M_i = \prod_{n\geq 1} \mathbb{Z}/n$ having each coordinate equal to 1 is not a torsion element, i.e., no multiple of it is zero. So we have

$$0 \neq e \otimes 1 \in \left(\prod_{n\geq 1} \mathbb{Z}/n\right) \otimes_{\mathbb{Z}} \mathbb{Q} = \left(\prod_{i\in I} M_i\right) \otimes_R N.$$

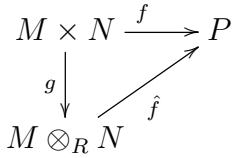
In general, the tensor product $M \otimes_R N$ of two R-modules M and N is an abelian group. If R is commutative, we can also equip it with an R-module structure.

LEMMA 2.2.8. *Let R be a commutative ring and M, N be two R-modules. Then $M \otimes_R N$ becomes an R-module via*

$$r.(m \otimes n) = (r.m) \otimes n = m \otimes (r.n).$$

Furthermore $\mathrm{Hom}_R(M, N)$ *becomes an R-module via $(r.f)(m) = r.f(m)$.*

REMARK 2.2.9. The tensor product of R-modules satisfies the following universal property. Let M be an R^{op}-module, N be an R-module and $g\colon M \times N \to M \otimes_R N$ be given by $g(x, y) = x \otimes y$. For every abelian group P and every R-bilinear map $f\colon M \times N \to P$ there is a unique group homomorphism $\hat{f}\colon M \otimes_R N \to P$ such that $\hat{f} \circ g = f$, i.e., the following diagram commutes:



2.3. Free, projective, injective and flat modules

In this section we will discuss some important classes of R-modules.

DEFINITION 2.3.1. An R-module is called *free*, if it contains a basis, i.e., if it is isomorphic to $\bigoplus_{i \in I} R$ for some index set I.

For $R = \mathbb{Z}$ free R-modules are just free abelian groups.

EXAMPLE 2.3.2. *The $\mathbb{Z}$-module $\mathbb{Q}$ is not free.*

To show this, assume that $\mathbb{Q}$ contains a basis $\{e_\alpha\}_{\alpha \in I}$ over $\mathbb{Z}$. Then we have

$$\frac{1}{1} = n_1 e_{\alpha_1} + \cdots + n_r e_{\alpha_r},$$

for nonzero integers n_i. Chose a nonzero $n \in \mathbb{Z}$ with $n \nmid n_1$. We also have

$$\frac{1}{n} = m_1 e_{\beta_1} + \cdots + m_s e_{\beta_s}.$$

The equation $n \cdot \frac{1}{n} = \frac{1}{1}$ says that

$$n m_1 e_{\beta_1} + \cdots + n m_s e_{\beta_s} = n_1 e_{\alpha_1} + \cdots + n_r e_{\alpha_r}.$$

However, because of the uniqueness of a basis representation, these two representations must coincide. Hence $n m_i = n_1$ for some i. This is a contradiction to $n \nmid n_1$.

DEFINITION 2.3.3. A sequence of R-modules and R-module homomorphisms

$$\cdots \xrightarrow{f_1} M_1 \xrightarrow{f_0} M_0 \xrightarrow{f_{-1}} M_{-1} \cdots$$

is called a *sequence*. It is called an *R-chain complex*, if $f_i \circ f_{i+1} = 0$ for all $i \in \mathbb{Z}$, i.e., if $\mathrm{im}(f_{i+1}) \subseteq \ker(f_i)$ holds. It is called *exact*, if $\mathrm{im}(f_{i+1}) = \ker(f_i)$ for all $i \in \mathbb{Z}$.

We also say, a sequence is exact at a *point M_i*. For example, the sequence is exact at M_1 if $\mathrm{im}(f_1) = \ker(f_0)$. This says that image of the incoming map is the kernel of the outgoing map. Of special interest in homological algebra are *short exact sequences*, which are just exact sequences of the form

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0.$$

The exactness at M' says that $0 = \ker(i)$, so that i is injective. The exactness at M says that $M' = \ker(p)$, and the exactness at M'' says that $\mathrm{im}(p) = M''$, so that p is surjective.

DEFINITION 2.3.4. A short exact sequence of R-modules

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0.$$

is called *split*, if M is isomorphic to $M' \oplus M''$.

PROPOSITION 2.3.5. *Let $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ be a short exact sequence of R-modules. Then then following statements are equivalent.*

(1) *i has a retraction, i.e., there exists a morphism $\pi\colon M \to M'$ such that $\pi \circ i = \mathrm{id}_{M'}$.*

(2) *p has a section, i.e., there exists a morphism $s\colon M'' \to M$ such that $p \circ s = \mathrm{id}_{M''}$.*

(3) *We have $M \cong M' \oplus M''$, so the sequence splits.*

So if the short exact sequence is split then we have

$$M \cong \mathrm{im}(i) \oplus \ker(\pi) \cong \ker(p) \oplus \mathrm{im}(s).$$

Note that the result is not true for short exact sequences of groups.

DEFINITION 2.3.6. An R-module M is called *projective*, if for every surjective R-module homomorphism $g\colon N_1 \to N_2$ and every R-module homomorphism $\gamma\colon M \to N_2$ there exists an R-module homomorphism $\beta\colon M \to N_1$ such that $\gamma = g \circ \beta$.

The definition can be made more transparent as follows. M is projective if for every diagram

$$\begin{array}{ccccc} & & & & M \\ & & & \swarrow & \downarrow \\ N_1 & \longrightarrow & N_2 & \longrightarrow & 0 \end{array}$$

with exact row there exists a lifting, such that the diagram commutes.

This avoids giving names for the mappings. The property says, in the slang of homological algebra, that the map $\mathrm{Hom}_R(M, N_1) \to \mathrm{Hom}_R(M, N_2)$, induced by the surjective map $N_1 \to N_2$, is again surjective.

We have the following equivalent conditions for an R-module to be projective.

PROPOSITION 2.3.7. *Let M be an R-module. Then the following statements are equivalent.*

(1) *M is projective.*

(2) *There exists an R-module N such that $M \oplus N$ is free.*

(3) *Every short exact sequence of R-modules*

$$0 \to N_1 \to N_2 \to M \to 0$$

splits.

(4) *For every short exact sequence* $0 \to T' \to T \to T'' \to 0$ *of* R*-modules the induced sequence*

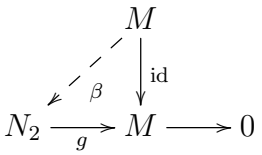
$$0 \to \mathrm{Hom}_R(M, T') \to \mathrm{Hom}_R(M, T) \to \mathrm{Hom}_R(M, T'') \to 0$$

is also exact. We say that the functor $\mathrm{Hom}_R(M, \cdot)$ *is exact.*

PROOF. (1) $\Longrightarrow$ (3): Let

$$0 \to N_1 \to N_2 \xrightarrow{g} M \to 0$$

be a short exact sequence of R-modules. Consider the diagram



Since M is projective, there exists for the R-module homomorphism $g\colon N_2 \to M$ an R-module homomorphism $\beta\colon M \to N_2$ with $g \circ \beta = \mathrm{id}_M$. This says, by using Proposition 2.3.5 that the above sequence splits.

(3) $\Longrightarrow$ (2): For every R-module there is a free R-module F and a surjection $F \to M$. For example, we may take $F = \bigoplus_{m \in M} R$. So let N_2 be such a free R-module with a surjection $N_2 \xrightarrow{g} M$ with kernel N_1. Then we have a short exact sequence

$$0 \to N_1 \to N_2 \to M \to 0.$$

By assumption it splits, so that $N_2 \cong M \oplus N_1$, where N_2 is free. So we have shown (2).

(2) $\Longrightarrow$ (4): Note that $\mathrm{Hom}_R(M, \cdot)$ is always left-exact, i.e., the sequence

$$0 \to \mathrm{Hom}_R(M, T') \to \mathrm{Hom}_R(M, T) \to \mathrm{Hom}_R(M, T'')$$

is alway exact. Then one just needs to show that the last map is surjective, if (2) is satisfied. This is easy. But we will not use this here. We give a different argument. Condition (4) is always satisfied for free R-modules M, because then $\mathrm{Hom}_R(M, N) = \prod_{i \in I} N$, where I is the index set of a basis for M. By assumption $M \oplus N$ is free for some R-module N, so that

$$0 \to \mathrm{Hom}_R(M \oplus N, T') \to \mathrm{Hom}_R(M \oplus N, T) \to \mathrm{Hom}_R(M \oplus N, T'') \to 0$$

is exact. By Lemma 2.2.2, the universal property of a coproduct for R-modules, we have $\mathrm{Hom}_R(M \oplus N, S) \cong \mathrm{Hom}_R(M, S) \times \mathrm{Hom}_R(N, T)$ for $S = T, T', T''$, and we obtain another exact sequence this way. It gives the exactness of the sequence in (4), because the kernel (respectively the image) of a product of maps equals the product of the kernels (the images) of the single maps.

(4) $\Longrightarrow$ (1): Applying (4) with $T'' = N_2$, $T = N_1$ and $T' = \ker(N_2 \to N_1)$ gives that the map

$$\mathrm{Hom}_R(M, N_1) \to \mathrm{Hom}_R(M, N_2)$$

induced by any surjective map $N_1 \to N_2$ is again surjective. But this is just the definition of a projective R-module. □

COROLLARY 2.3.8. *Every free* R*-module is projective.*

PROOF. This follows immediately from Proposition 2.3.7, property (2). □

The converse need not be true.

EXAMPLE 2.3.9. *Let $R = R_1 \oplus R_2$ with non-trivial rings R_1 and R_2, and consider the R-module $M = R_1$ with action $(r_1, r_2).m = r_1 m$. Then M is a projective R-module, which is not free.*

Indeed, R is a free R-module and $M = R_1$ is a direct summand of it, hence projective. Clearly M is not free, because $(0, r_2).m = 0$ for all $r_2 \in R_2$ and hence every $m \in M$ is linearly dependent over R.

REMARK 2.3.10. In the above example, the ring R is not an integral domain. However, one can also find examples of projective, non-free R-modules over integral domains. A typical example is the ring $R = \mathbb{Z}[\sqrt{-5}]$ and its ideal $M = (2, 1 + \sqrt{-5})$, considered as R-module. It is not free since it is not principal and thus any two elements are linearly dependent over R. It is projective since it represents the nontrivial element in the class group of $\mathbb{Q}(\sqrt{-5})$, which is isomorphic to $\mathbb{Z}/2$.

On the other hand we have the following result.

PROPOSITION 2.3.11. *Let M be a projective R-module, where R is a PID. Then M is free.*

PROOF. As a projective module, M is a direct summand of a free module. In particular it is a submodule of a free module and hence is free, because the ring is a PID. □

Hence over a PID, projective modules are just free modules. This is true in particular for the ring $R = \mathbb{Z}$. As an example, there is no nonzero finite abelian group G, which is a projective $\mathbb{Z}$-module. Indeed, G cannot be free, since it has torsion. No element $g \in G$ can be part of a basis because of $|G|g = 0$.

DEFINITION 2.3.12. Let M be an R-module and $0 \to N' \to N \to N'' \to 0$ be a short exact sequence of R-modules. Then M is called *flat*, if the induced sequence

$$0 \to N' \otimes_R M \to N \otimes_R M \to N'' \otimes_R M \to 0$$

is exact. We say that the tensor product functor $\cdot \otimes_R M$ is exact.

Here it is only relevant for flatness, that an injective map $N' \to N$ induces an injective map $N' \otimes_R M \to N \otimes_R M$, since the tensor product functor is generally right-exact for all R-modules, i.e., the sequence

$$N' \otimes_R M \to N \otimes_R M \to N'' \otimes_R M \to 0$$

is always exact for all R-modules M.

PROPOSITION 2.3.13. *Let M be a projective R-module. Then M is flat.*

PROOF. Assume that $N' \to N$ is injective. By the distributivity of $\otimes_R$ and the fact, that M is a direct summand of a free R-module we may assume that M is free. So we have $M \cong \bigoplus_{i \in I} R$. This yields, using distributivity again and $N \otimes_R R \cong N$ for all R-modules N, that

$$\begin{array}{ccc} N' \otimes_R M & \longrightarrow & N \otimes_R M \\ \cong \downarrow & & \downarrow \cong \\ \bigoplus_{i \in I} N' & \longrightarrow & \bigoplus_{i \in I} N \end{array}$$

The lower map is of course injective if the map $N' \to N$ is injective. So we are done. □

The converse statement of the above proposition need not be true.

EXAMPLE 2.3.14. *Show that the $\mathbb{Z}$-module $\mathbb{Q}$ is flat, but not projective.*

We already know that $\mathbb{Q}$ cannot be a projective $\mathbb{Z}$-module, because then it would be free, which contradicts Example 2.3.2.

REMARK 2.3.15. One can show that every *finitely presented* flat R-module (that is the quotient of a finitely generated free R-module by a finitely generated submodule) is always projective. Over a Noetherian ring R, every finitely generated flat R-module is projective, since every finitely generated R-module there is finitely presented.

Now we come to *injective* R-modules. The definition is dual to the one of a projective R-module.

DEFINITION 2.3.16. An R-module M is called *injective*, if for every injective R-module homomorphism $g\colon N_1 \to N_2$ and every R-module homomorphism $\gamma\colon N_1 \to M$ there exists an R-module homomorphism $\beta\colon N_2 \to M$ such that $\gamma = \beta \circ g$.

The short way to express this definition by a diagram is as follows. M is injective if for every diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & N_1 & \longrightarrow & N_2 \\ & & \downarrow & \swarrow & \\ & & M & & \end{array}$$

with exact row there exists a lifting, such that the diagram commutes.

We obtain the following equivalent conditions for an R-module to be injective, which are proved in the same way as for projective R-modules in Proposition 2.3.7.

PROPOSITION 2.3.17. *Let M be an R-module. Then the following statements are equivalent.*

(1) *M is in injective.*

(2) *Any R-module N containing M as a submodule has a submodule P such that $N = M \oplus P$.*

(3) *Every short exact sequence of R-modules*

$$0 \to M \to N_1 \to N_2 \to 0$$

splits.

(4) *For every short exact sequence $0 \to T' \to T \to T'' \to 0$ of R-modules the induced sequence*

$$0 \to \mathrm{Hom}_R(T'', M) \to \mathrm{Hom}_R(T, M) \to \mathrm{Hom}_R(T', M) \to 0$$

is also exact. We say that the functor $\mathrm{Hom}_R(\cdot, M)$ is exact.

Trivially, the zero module $\{0\}$ is injective. To provide more interesting examples we first need Baer's criterion.

THEOREM 2.3.18 (Baer's criterion). *Let R be a ring with unit. Then an R-module M is injective if and only if for every ideal I in R and every R-module homomorphism $f\colon I \to M$ there is an R-module homomorphism $\overline{f}\colon R \to M$ extending f by $\overline{f}_{|I} = f$.*

PROOF. Suppose that M is an injective R-module and I is an ideal in R and $f\colon I \to M$ an R-module homomorphism. Then we see from the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \xrightarrow{\ i\ } & R \\ & & {\scriptstyle f}\downarrow & \swarrow_{\overline{f}} & \\ & & M & & \end{array}$$

that the required map $\overline{f}$ exists by the definition of injectivity for M. Here $i\colon I \to R$ is the inclusion homomorphism.

Conversely assume that M is an R-module such that the lifting property holds for all ideals I of R. We need to show that if N_2 is an R-module, N_1 is a submodule and $f\colon N_1 \to M$ is an R-module homomorphism, then there exists an R-module homomorphism $\overline{f}\colon N_2 \to M$ such that $\overline{f}_{|N_1} = f$. Let S be a set of all pairs (K, f_K) such that

(1) K is a submodule of N_2 such that $N_1 \subseteq K \subseteq N_2$.

(2) $f_K\colon K \to M$ is an R-module homomorphism with $(f_K)_{|N_1} = f$.

Define a partial order on S as follows.

$$(K, f_K) \leq (K', f_{K'}) \iff K \subseteq K' \text{ and } (f_{K'})_K = f_K.$$

By Zorn's Lemma there exists a maximal element (K_0, f_{K_0}). We need to show that $K' = N_2$. Assume, by contradiction, that $K' \neq N_2$, and let $n \in N_2 \setminus K'$. Define

$$I := \{r \in R \mid rn \in K_0\}.$$

This is an ideal of R and the map $g\colon I \to M$, $g(r) = f_{K_0}(rn)$ is an R-module homomorphism. By the assumption on M there exists an R-module homomorphism $\overline{g}\colon R \to M$ such that $\overline{g}_{|I} = g$. Now $K_0 + Rn$ is a submodule of N_2 and the map

$$f'\colon K_0 + Rn \to M,\ f'(k_0 + rn) = f_{K_0}(k) + \overline{g}(r)$$

is a well defined homomorphism of R-modules such that $f'_{|N} = f$. This shows that $(K_0 + Rn, f') \in S$. Obviously we have

$$(K_0, f_{K_0}) < (K_0 + Rn, f'),$$

which is a contradiction to the fact that (K_0, f_{K_0}) is a maximal element. □

COROLLARY 2.3.19. *Let R be an integral domain and let K be the field of fractions of R. Then K is an injective R-module.*

PROOF. Let I be an ideal of R and let $f\colon I \to K$ be a homomorphism of R-modules. For nonzero elements $r, s \in I$ we have

$$rf(s) = f(rs) = sf(r).$$

So we have $\frac{f(r)}{r} = \frac{f(s)}{s}$ in K. Denote this element by x and define $\overline{f}\colon R \to K$ by $\overline{f}(r) = rx$ for $r \in R$. Then $\overline{f}$ is an R-module homomorphism with $\overline{f}_{|I} = f$. By Baer's criterion it folows that K is an injective R-module. □

EXAMPLE 2.3.20. *The $\mathbb{Z}$-module $\mathbb{Q}$ is injective.*

DEFINITION 2.3.21. An R-module M is called *divisible* if for every nonzero $r \in R$, which is not a zerodivisor, and for every $m \in M$ there is an $n \in M$ such that $rn = m$.

For example, if $R = \mathbb{Z}$, then $\mathbb{Q}$, $\mathbb{Q}/\mathbb{Z}$ and the Prüfer group $\mathbb{Z}(p^\infty)$, the subgroup of $\mathbb{Q}/\mathbb{Z}$ generated by the powers of $1/p$, are divisible $\mathbb{Z}$-modules. We have the following relationship between injective and divisible R-modules.

PROPOSITION 2.3.22. *Let R be an integral domain. Then every injective R-module is divisible. Let R be a PID. Then every divisible R-module is injective.*

PROOF. Exercise. □

EXAMPLE 2.3.23. *$\mathbb{Z}$ is not an injective $\mathbb{Z}$-module.*

Indeed, $\mathbb{Z}$ is not divisible.

COROLLARY 2.3.24. *Let R be a PID. Suppose that M is an injective and hence divisible R-module, and that N a submodule of M. Then M/N is an injective and hence divisible R-module.*

PROOF. If $m + N \in M/N$ and $r \neq 0$ in R, then there exists $m' \in M$ such that $m = rm'$. Hence $m + N = rm' + N = r(m' + N)$. Therefore M/N is divisible. But then over a PID, any module is divisible if and only if it is injective by Proposition 2.3.22 , so the claim follows. □

COROLLARY 2.3.25. *The epimorphic image of a divisible $\mathbb{Z}$-module is divisible.*

PROOF. Let $\varphi\colon G \to G'$ be a surjective $\mathbb{Z}$-module homomorphism, where G is a divisible group, i.e., a divisible $\mathbb{Z}$-module. Then $G' \cong G/\ker(\varphi)$ is divisible by the previous corollary. □

CHAPTER 3

Categories and functors

3.1. Categories

We will briefly discuss the language of category theory.

DEFINITION 3.1.1. A *category* $\mathcal{C}$ consists of a class $ob(\mathcal{C})$ of objects and a class $mor(\mathcal{C})$ of morphisms, together with the following structural maps:

(i) An identity map $i\colon ob(\mathcal{C}) \to mor(\mathcal{C})$, which asigns to each object A a morphism id_A, the *identity morphism* of A.

(ii) Two functions $s, t\colon mor(\mathcal{C}) \to ob(\mathcal{C})$, which assign to every morphism its *source* (or domain) and *target* (or codomain),

(iii) A composition map $\circ\colon mor(\mathcal{C}) \times mor(\mathcal{C}) \to mor(\mathcal{C})$, which assigns to any pair of morphisms f, g such that $t(f) = s(g)$ their composite morphism $g \circ f$,

such that the following axioms are satisfied:

(1) $s(g \circ f) = s(f)$ and $t(g \circ f) = t(g)$, i.e., source and target are respected by composition.

(2) $s(\mathrm{id}_A) = A$ and $t(\mathrm{id}_A) = A$, i.e, source and target are respected by identities.

(3) $(h \circ g) \circ f = h \circ (g \circ f)$ whenever $t(f) = s(g)$ and $t(g) = s(h)$, i.e., composition is associative whenever defined.

(4) If $s(f) = A$ and $t(f) = B$, then $\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A$, i.e., composition satisfies the left and right unit laws.

The sets

$$\begin{aligned}\mathrm{Hom}_{\mathcal{C}}(A, B) &= \{f \in mor(\mathcal{C}) \mid s(f) = A,\, t(f) = B\} \\ &= \{f\colon A \to B\}\end{aligned}$$

are called *homsets*.

EXAMPLE 3.1.2. *1. The category $\mathcal{S}et$, with sets as objects and functions as morphisms.*

2. The category $\mathcal{G}\mathfrak{r}\mathfrak{p}$, with groups as objects and group homomorphisms as morphisms.

3. The category $\mathcal{V}ect$, with vector spaces as objects and linear maps as morphisms.

4. The category $\mathcal{T}op$, with topological spaces as objects and continuous functions as morphisms.

5. The category $\mathcal{D}iff$, with smooth manifolds as objects and smooth maps as morphisms.

6. The category $\mathcal{R}ing$, with rings as objects and ring homomorphisms as morphisms.

7. The category $\mathcal{M}od_R$, with R-modules over a ring R as objects and R-module homomorphisms as morphisms.

8. The category $\mathcal{A}lg_R$, with R-algebras as objects and R-algebra homomorphisms as morphisms.

9. The category $\mathcal{CR}ing$, with commutative rings as objects and ring homomorphisms as morphisms.

10. The category $\mathcal{A}ff$, with affine schemes as objects and morphism of locally ringed spaces as morphisms.

The first nine examples are clear, but for the last one we need some definitions.

A *ringed space* is a pair $(X, \mathcal{O}_X)$, where X is a topological space and $\mathcal{O}_X$ is a sheaf of rings on X.

A *morphism* of ringed spaces from $(X, \mathcal{O}_X)$ to $(Y, \mathcal{O}_Y)$ is a pair $(f, f^\#)$, where $f\colon X \to Y$ is a morphism of topological spaces, and $f^\#\colon \mathcal{O}_Y \to f_*\mathcal{O}_X$ is a morphism of sheafes of rings on Y.

A *locally ringed space* is a ringed space $(X, \mathcal{O}_X)$, such that for each $x \in X$ the stalk $\mathcal{O}_{X,x}$ of $\mathcal{O}_X$ at x is a local ring. A morphism of local ringed spaces from $(X, \mathcal{O}_X)$ to $(Y, \mathcal{O}_Y)$ is a morphism of ringed spaces $(f, f^\#)$, such that for all $x \in X$ the induced homomorphism of the local rings

$$f_x^\#\colon \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$$

is *local*, i.e., the image of the maximal ideal of $\mathcal{O}_{Y,f(x)}$ under $f_x^\#$ lies in the maximal ideal of $\mathcal{O}_{X,x}$. This defines the category $\mathcal{LRS}$ of locally ringed spaces.

For $X = \operatorname{spec}(R)$, the set of prime ideals of a commutative ring R with unit, we can consider the Zariski topology together with the structure sheaf $\mathcal{O}_X$ of rings, so that for all $x \in X$ the stalk $\mathcal{O}_{X,x}$ is isomorphis to the local ring $R\mathfrak{p}$, where $\mathfrak{p}$ denotes the prime ideal in R, which belongs to $x \in X$. Then $(X, \mathcal{O}_X)$ is a locally ringed space. Now we can give the following definition.

Definition 3.1.3. An *affine scheme* then is a locally ringed space $(X, \mathcal{O}_X)$, which is isomorphic to $(\operatorname{spec}(R), \mathcal{O}_{\operatorname{spec}(R)}$ for a commutative ring with unit.

We will see later that the category $\mathcal{A}ff$ is "anti-equivalent" to the category $\mathcal{CR}ing$. First we need some more definitions.

Definition 3.1.4. Let $\mathcal{C}$ be a category. A *subcategory* $\mathcal{D}$ consists of a subcollection of the collection of objects of $\mathcal{C}$ and a subcollection of the collection of morphisms of $\mathcal{D}$ such that

(1) If the morphism $f\colon A \to B$ is in $\mathcal{D}$, then so are A and B.

(2) If $f\colon A \to B$ and $g\colon B \to C$ are in $\mathcal{D}$, then so is the composite $g \circ f\colon A \to C$.

(3) If A is in $\mathcal{D}$ then so is the identity morphism id_A.

In addition $\mathcal{D}$ is a *full subcategory* if for any A and B in $\mathcal{D}$, every morphism $f\colon A \to B$ in $\mathcal{C}$ is also in $\mathcal{D}$.

These conditions ensure that $\mathcal{D}$ is a category in its own right and the inclusion $D \hookrightarrow C$ is a *functor*. For example, the category $\mathcal{Ab}$ of abelian groups is a full subcategory of $\mathcal{Grp}$. Here is a table of some categories related to groups:

$\mathcal{C}$	Name
$\mathcal{Grp}$	Groups
$\mathcal{Ab}$	Abelian groups
$\mathcal{Div}$	Divisible abelian groups
$\mathcal{Ab}_f$	Free abelian groups
$\mathcal{Cyc}$	Cyclic groups
$\mathcal{Ab}_{tf}$	Torsion-free abelian groups
$\mathcal{Ab}_{fg}$	Finitely generated abelian groups
$\mathcal{Ab}_{ffg}$	Finitely generated free abelian groups
$\mathcal{grp}$	Finite groups
$\mathcal{ab}$	Finite abelian groups
$\mathcal{Ab}_t$	Torsion abelian groups
$\mathcal{Ab}_p$	Profinite abelian groups

Definition 3.1.5. A *functor* F from a category $\mathcal{C}$ to a category $\mathcal{D}$ is a map sending each object $A \in \mathcal{C}$ to an object $F(A) \in \mathcal{D}$ and each morphism $f\colon A \to B$ in $\mathcal{C}$ to a morphism $F(f) : F(A) \to F(B)$ in $\mathcal{D}$, such that

(1) $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$ for each $A \in ob(\mathcal{C})$.
(2) $F(g \circ f) = F(g) \circ F(f)$, i.e., F is *covariant*, or
(3) $F(g \circ f) = F(f) \circ F(g)$, i.e., F is *contravariant*$(F(f) : F(B) \to F(A))$.

A contravariant functor is a covariant functor from the opposite category C^{op} (see below) to D.

Example 3.1.6. *1. $F\colon \mathcal{Mod}_R \to \mathcal{Ab}$, $N \mapsto \mathrm{Hom}_R(M, N)$ is a functor, denoted by $F = \mathrm{Hom}_R(M, \cdot)$ for a given R-module M.*

2. $F\colon \mathcal{Mod}_R \to \mathcal{Mod}_R$, $N \mapsto M \otimes_R N$ is a functor, denoted by $F = M \otimes_R \cdot$ for a given R-module M over a commutative ring R.

3. $U\colon \mathcal{Mod}_R \to \mathcal{Ab}$, $N \mapsto (N, +)$ is a functor, mapping N to its underlying abelian group. Functors of this kind a called forgetful functors.

Proposition 3.1.7. *Let R be a ring and M be a left R-module. Then $F = \mathrm{Hom}_R(M, \cdot)$ is a covariant functor from $\mathcal{Mod}_R$ to $\mathcal{Ab}$, und $F = \mathrm{Hom}_R(\cdot, M)$ is a contravariant functor from $\mathcal{Mod}_R$ to $\mathcal{Ab}$.*

PROOF. Let $\beta\colon A \to B$ be a morphism in $\mathcal{Mod}_R$. We need to define $F(\beta)$. Let M be a fixed R-module. Consider the sequence $M \xrightarrow{\alpha} A \xrightarrow{\beta} B$ in $\mathcal{Mod}_R$. Then define a homomorphism $\tilde{\beta} = F(\beta)$ of abelian groups

$$F(\beta)\colon \operatorname{Hom}_R(M, A) \to \operatorname{Hom}_R(M, B)$$

by $F(\beta)(\alpha) = \tilde{\beta}(\alpha) = \beta \circ \alpha$. Obviously $\beta = \mathrm{id}$ in $\mathcal{Mod}_R$ implies $F(\beta) = \mathrm{id}$ in $\mathcal{Ab}$. Given a sequence

$$M \xrightarrow{\alpha} A \xrightarrow{\beta} B \xrightarrow{\gamma} C$$

in $\mathcal{Mod}_R$, we obtain

$$F(\gamma \circ \beta)(\alpha) = (\gamma \circ \beta)(\alpha) = \gamma \circ (\beta \circ \alpha) \tag{3.1}$$

$$= F(\gamma)(F(\beta)(\alpha)). \tag{3.2}$$

Hence the functor $F = \operatorname{Hom}_R(M, \cdot)$ is covariant. The second claim follows similarly. □

PROPOSITION 3.1.8. *Let R be a commutative ring and M, N be two R-modules. Then both $F = M \otimes_R \cdot$ and $G = \cdot \otimes_R N$ are covariant functors from $\mathcal{Mod}_R$ to $\mathcal{Mod}_R$.*

PROOF. Given $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ in $\mathcal{Mod}_R$ we put

$$F(\alpha) = 1_M \otimes \alpha\colon M \otimes_R A \to M \otimes_R B,$$

where $(1_M \otimes \alpha)(x \otimes y) = x \otimes \alpha(y)$. Then

$$F(\beta \circ \alpha) = 1_M \otimes (\beta \circ \alpha) = (1_M \otimes \beta) \circ (1_M \otimes \alpha) \tag{3.3}$$

$$= F(\beta)F(\alpha). \tag{3.4}$$

Hence F is covariant. The second claim follows similarly. □

DEFINITION 3.1.9. Given categories $\mathcal{C}$ and $\mathcal{D}$ and a pair of functors $F, G\colon \mathcal{C} \to \mathcal{D}$ a *natural transformation* N from F to G is an assigment N, which gives for every object C in $\mathcal{C}$ a morphism $N(C)\colon F(C) \to G(C)$, so that for every morphism $f \in \operatorname{Hom}_{\mathcal{C}}(C, C')$ the following diagram commutes.

$$\begin{array}{ccc} F(C) & \xrightarrow{N(C)} & G(C) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(C') & \xrightarrow{N(C')} & G(C') \end{array}$$

DEFINITION 3.1.10. An *equivalence* between two categories $\mathcal{C}$ and $\mathcal{D}$ is a pair of functors $F\colon \mathcal{C} \to \mathcal{D}$ and $G\colon \mathcal{D} \to \mathcal{C}$ together with natural isomorphisms $F \circ G \equiv \mathrm{id}_{\mathcal{D}}$ and $G \circ F \equiv \mathrm{id}_{\mathcal{C}}$. Here a natural isomorphism is a a natural transformation with a two-sided inverse.

DEFINITION 3.1.11. For a category $\mathcal{C}$, the *opposite category* $\mathcal{C}^{op}$ has the same objects as $\mathcal{C}$, but a morphism $f : A \to B$ in $\mathcal{C}^{op}$ is the same as a morphism $f : B \to A$ in $\mathcal{C}$, and a composite of morphisms $g \circ f$ in $\mathcal{C}^{op}$ is defined to be the composite $f \circ g$ in $\mathcal{C}$.

In general, the categories $\mathcal{C}$ and $\mathcal{C}^{op}$ need not be equivalent. However, the opposite of an opposite category is the original category, i.e., $(\mathcal{C}^{op})^{op} = \mathcal{C}$.

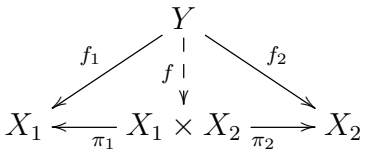
EXAMPLE 3.1.12. *1. The category of affine schemes is equivalent to the opposite of the category of commutative rings, i.e., $\mathcal{A}ff \cong \mathcal{C}\mathcal{R}ing^{op}$.*

2. The Pontryagin duality restricts to an equivalence between the category of compact Hausdorff abelian topological groups and the opposite of the category of abelian groups.

3. The category of profinite abelian groups is equivalent to the opposite of the category of torsion abelian groups.

4. The category of vector spaces is self-dual, i.e., $\mathcal{V}ect \cong \mathcal{V}ect^{op}$. The same is true for the category of finite-dimensional representations of a group (or of a Lie algebra).

DEFINITION 3.1.13. Let $\mathcal{C}$ be a category, and X_1, X_2 two objects in $\mathcal{C}$. A *product* of X_1 and X_2 is an object X, denoted $X_1 \times X_2$, together with a pair of morphisms $\pi_1 : X \to X_1$, $\pi_2 \colon X \to X_2$ that satisfy the following universal property. For every object Y and every pair of morphisms $f_1 : Y \to X_1$, $f_2 : Y \to X_2$ there exists a *unique* morphism $f : Y \to X_1 \times X_2$ such that the following diagram commutes:

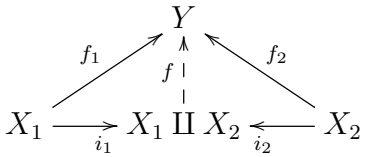


EXAMPLE 3.1.14. *1. In the category of groups, the cartesian product $X_1 \times X_2$ with componentwise multiplication together with the canonical projections $\pi_1 : X_1 \times X_2 \to X_1$, $\pi_2 \colon X_1 \times X_2 \to X_2$ is a categorial product for X_1 and X_2.*

2. The category of cyclic groups does not have a product.

A coproduct in $\mathcal{C}$ is the same as a product in the opposite category $\mathcal{C}^{op}$.

DEFINITION 3.1.15. Let $\mathcal{C}$ be a category, and X_1, X_2 two objects in $\mathcal{C}$. A *coproduct* of X_1 and X_2 is an object X, denoted $X_1 \amalg X_2$, together with a pair of morphisms $i_1 : X_1 \to X_1 \amalg X_2$, $i_2 \colon X_2 \to X_1 \amalg X_2$ that satisfy the following universal property. For every object Y and every pair of morphisms $f_1 : X_1 \to Y$, $f_2 : X_2 \to Y$ there exists a *unique* morphism $f : X_1 \amalg X_2 \to Y$ such that the following diagram commutes:



EXAMPLE 3.1.16. *1. The coproduct in the category of groups is the free product. It is infinite in general. For example, $C_2 * C_3 \cong PSL_2(\mathbb{Z})$.*

2. The coproduct in the category of commutative rings is the tensor product.

3. The category of cyclic groups does not have a coproduct.

DEFINITION 3.1.17. Let $\mathcal{C}$ be a category. An *initial object* in $\mathcal{C}$ is an object X such that for every object Y there is a unique morphism $i \colon X \to Y$.

EXAMPLE 3.1.18. *1. In the category of sets, the empty set is initial.*

2. In the category of groups, the trivial group is initial.

3. In the category of R-modules, the zero module is initial.

DEFINITION 3.1.19. Let $\mathcal{C}$ be a category. An *terminal object* in $\mathcal{C}$ is an object Y such that for every object X there is a unique morphism $t\colon X \to Y$.

EXAMPLE 3.1.20. *1. In the category of sets, any set containg one element is terminal.*

2. In the category of groups, the trivial group is terminal.

3. In the category of R-modules, the zero module is terminal.

DEFINITION 3.1.21. Let $\mathcal{C}$ be a category. A *zero object* in $\mathcal{C}$ is an object which is both initial and terminal.

EXAMPLE 3.1.22. *1. In the category of sets, there is no zero object.*

2. In the category of groups, the trivial group is a zero object.

3. In the category of R-modules, the zero module is a zero object.

4. In the category of rings with unity, there is no zero object.

DEFINITION 3.1.23. A category $\mathcal{C}$ is called *pre-additive*, if each homset is an additive abelian group and composition is bilinear with respect to this addition:

$$(g + g') \circ (f + f') = g \circ f + g \circ f' + g' \circ f + g' \circ f'$$

for all morphisms $f, f'\colon A \to B$, $g, g'\colon B \to C$.

EXAMPLE 3.1.24. *1. The category of groups is not pre-additive (exercise).*

2. The category of R-modules is pre-additive. In particular, for $R = \mathbb{Z}$, the category of abelian groups is pre-additive.

DEFINITION 3.1.25. An *additive category* $\mathcal{C}$ is a pre-additive category with a zero object and a product $A \times B$ for each pair of objects A, B from $\mathcal{C}$.

One can show that this product is also a coproduct for finitely many objects, i.e., product and coproduct are isomorphic.

EXAMPLE 3.1.26. *The category $\mathcal{Mod}_R$ ist additive with product and coproduct $A_1 \oplus A_2$.*

Here is a table with some examples and non-examples. For the definition of an abelian category see below.

$\mathcal{C}$	Additive	Abelian
$\mathcal{S}et$	–	–
$\mathcal{R}ing$	–	–
$\mathcal{A}lg_R$	–	–
$\mathcal{H}il\mathcal{b}$	✓	–
$\mathcal{S}h(X)$	✓	✓
$\mathcal{M}od_R$	✓	✓
$\mathcal{G}rp$	–	–
$\mathcal{A}b$	✓	✓
$\mathcal{D}iv$	✓	–
$\mathcal{A}b_f$	✓	–
$\mathcal{C}yc$	–	–
$\mathcal{A}b_{tf}$	✓	–
$\mathcal{A}b_{fg}$	✓	✓
$\mathcal{A}b_{ffg}$	✓	–
$g\mathcal{r}p$	–	–
$a\mathcal{b}$	✓	✓
$\mathcal{A}b_t$	✓	✓
$\mathcal{A}b_p$	✓	✓

DEFINITION 3.1.27. A morphism $i\colon A \to B$ in an additive category $\mathcal{C}$ is called *monic*, if, whenever $g\colon A' \to A$ is a morphism satisfying $i \circ g = 0$, then $g = 0$.

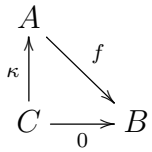
Monics can be cancelled from the left In $\mathcal{S}et$, $\mathcal{G}rp$ and $\mathcal{M}od_R$, monics are just injective maps.

DEFINITION 3.1.28. A morphism $e\colon C \to D$ in an additive category $\mathcal{C}$ is called *epi*, if, whenever $h\colon D \to D'$ is a morphism satisfying $h \circ e = 0$, then $h = 0$.

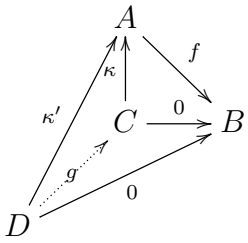
Epis can be cancelled from the right. In $\mathcal{S}et$, $\mathcal{G}rp$ and $\mathcal{M}od_R$, epis are just surjective maps. We define the kernel and the cokernel of a morphism as follows:

DEFINITION 3.1.29. Let $\mathcal{C}$ be an additive category. Suppose that $f\colon A \to B$ is an arbitrary morphism in $\mathcal{C}$. A *kernel of* f is a morphism $\kappa\colon C \to A$ such that

(a) $f \circ \kappa\colon C \to B$ is the zero morphism:

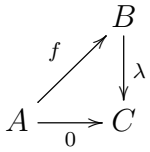


(b) Given any morphism $\kappa' \colon D \to A$ such that $f \circ \kappa'$ is the zero morphism, there is a unique morphism $g \colon D \to C$ such that $\kappa \circ g = \kappa'$:

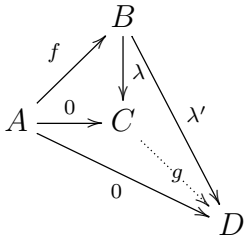


Definition 3.1.30. Let $\mathcal{C}$ be an additive category. Suppose that $f \colon A \to B$ is an arbitrary morphism in $\mathcal{C}$. A *cokernel of* f is a morphism $\lambda \colon B \to C$ such that

(a) $\lambda \circ f \colon A \to C$ is the zero morphism:



(b) Given any morphism $\lambda' \colon B \to D$ such that $\lambda' \circ f$ is the zero morphism, there is a unique morphism $g \colon C \to D$ such that $g \circ \lambda = \lambda'$:



It is easy to see that kernels and cokernels are universal and hence uniquely determined if they exist (they need not exist in general).

Example 3.1.31. *1. In $\mathcal{G}\mathit{rp}$, the usual definition of a kernel, with the inclusion map into A satisfies the above universal property. So kernels always exist in $\mathcal{G}\mathit{rp}$. A cokernel of a morphism $f \colon G \to H$ in $\mathcal{G}\mathit{rp}$ is the quotient of H by the normal closure of the image of f. So cokernels always exist.*

2. In $\mathcal{R}\mathit{ing}$, there is no zero object, so the kernel and the cokernel do not exist.

3. In $\mathcal{M}\mathit{od}_R$, kernels and cokernels always exist.

3.2. Abelian categories

Abelian categories are named after Niels Henrik Abel. They are the most important ones for our lecture. The motivating prototypical example of an abelian category is the category of abelian groups $\mathcal{A}\mathcal{b}$, or more generally of R-modules $\mathcal{M}\mathit{od}_R$.

Definition 3.2.1. An *abelian category* is an additive category $\mathcal{C}$ satisfying the following three conditions:

(AB1) Every morphism in $\mathcal{C}$ has a kernel and a cokernel.

(AB2) Every monic morphism in $\mathcal{C}$ is the kernel of its cokernel, i.e.,

$$i = \ker(\operatorname{coker}(i)).$$

(AB3) Every epi(c) morphism in $\mathcal{C}$ is the cokernel of its kernel, i.e.,

$$e = \operatorname{coker}(\ker(e)).$$

The notion of abelian category is self-dual, i.e., the opposite category of any abelian category is abelian.

EXAMPLE 3.2.2. *1. $\mathcal{M}od_R$ is an abelian category. In particular, $\mathcal{A}b$ is an abelian category.*

2. The category $\mathcal{A}b_f$ of free abelian groups is additive, but not abelian (exercise). In fact, not every morphism has a cokernel.

3. The category $\mathcal{D}iv$ of divisible abelian groups is additive, but not abelian (exercise).

REMARK 3.2.3. Not every abelian category is a concrete category such as $\mathcal{M}od_R$ or $\mathcal{A}b$. But for many proofs in homological algebra it is very convenient to have a concrete abelian category, for that allows one to check the behaviour of morphisms on actual elements of the sets underlying the objects. However, under good conditions an abelian category can be embedded into $\mathcal{A}b$ as a full subcategory by an exact functor, and generally can be embedded this way into $\mathcal{M}od_R$, for some ring R. This is the *Freyd-Mitchell embedding theorem*.

DEFINITION 3.2.4. Let $\mathcal{C}$ be an additive category. A sequence $0 \to A \to B \xrightarrow{\alpha} C$ is called *left-exact* if the sequence of abelian groups

$$0 \to \operatorname{Hom}(T, A) \to \operatorname{Hom}(T, B) \to \operatorname{Hom}(T, C)$$

is exact for all objects T in $\mathcal{C}$. A sequence $A \xrightarrow{\beta} B \to C \to 0$ is *right-exact* if the sequence of abelian groups

$$0 \to \operatorname{Hom}(C, T) \to \operatorname{Hom}(B, T) \to \operatorname{Hom}(A, T)$$

is exact for all objects T.

DEFINITION 3.2.5. A covariant functor $F\colon \mathcal{C} \to \mathcal{D}$ of additive categories is called *exact*, if it takes short exact sequences in $\mathcal{C}$ to short exact sequences in $\mathcal{D}$. That means, given a short exact sequence

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

in $\mathcal{C}$ yields a short exact sequence

$$0 \to F(M_1) \to F(M_2) \to F(M_3) \to 0$$

in $\mathcal{D}$.
The functor is called *left-exact*, if

$$0 \to F(M_1) \to F(M_2) \to F(M_3)$$

is exact. It is called *right-exact*, if

$$F(M_1) \to F(M_2) \to F(M_3) \to 0$$

is exact.

The definition for contravariant functors is analogous. One has to reverse the arrows in $\mathcal{D}$. Hence a contravariant functor F is left-exact if every exact sequence

$$0 \to M_1 \to M_2 \to M_3$$

is taken to an exact sequence

$$0 \to F(M_3) \to F(M_2) \to F(M_1).$$

PROPOSITION 3.2.6. *The contravariant functor* $\mathrm{Hom}_R(\cdot, V)$ *from* $\mathcal{M}od_R$ *to* $\mathcal{A}\mathcal{b}$ *is left-exact, as well as the covariant functor* $\mathrm{Hom}_R(V, \cdot)$.

PROOF. We only show that $\mathrm{Hom}_R(V, \cdot)$ is a left-exact functor. In general, it is not an exact functor. So let

$$0 \to M_1 \xrightarrow{\psi} M_2 \xrightarrow{\varphi} M_3$$

be a short exact sequence of R-modules. We have to show that the sequence

$$0 \to \mathrm{Hom}_R(V, M_1) \xrightarrow{\tilde{\psi}} \mathrm{Hom}_R(V, M_2) \xrightarrow{\tilde{\varphi}} \mathrm{Hom}_R(V, M_3)$$

is exact. Let $\tilde{\psi}\sigma = 0$ for $\sigma \in \mathrm{Hom}_R(V, M_1)$. This means $\psi(\sigma(v)) = 0$ for all $v \in V$. We have $\sigma(v) = 0$, because ψ is injective, and hence $\sigma = 0$. This implies that also $\tilde{\psi}$ is injective.
Now let $\tilde{\varphi}\tau = 0$ with $\tau \in \mathrm{Hom}_R(V, M_2)$. Then $\varphi(\tau(v)) = 0$ for all $v \in V$, and $\tau(v) = \psi(v')$ with some $v' \in M_1$, depending on v. Since ψ is injective, v' is unique. Define $\tau' \in \mathrm{Hom}_R(V, M_1)$ by this v', i.e., let $\tau'(v) = v'$. Then it follows that

$$\tau(v) = \psi(v') = \psi(\tau'(v)) = (\tilde{\psi}\tau')(v).$$

Hence τ is contained in the image of $\tilde{\psi}$. □

REMARK 3.2.7. Let R be a commutative ring. The covariant functors $F = M \otimes_R \cdot$ and $G = \cdot \otimes_R N$ are right-exact, but not exact in general.

CHAPTER 4

Resolutions and derived functors

In this chapter we will use the language of abelian categories. It is useful to think of the category of R-modules as a main example instead.

4.1. Projective and injective resolutions

DEFINITION 4.1.1. Let $\mathcal{C}$ be an abelian category. An object I of $\mathcal{C}$ is *injective* if $\mathrm{Hom}(\cdot, I)$ is an exact functor, i.e., if $0 \to A \to B \to C \to 0$ is exact in $\mathcal{C}$ then also

$$0 \to \mathrm{Hom}(C, I) \to \mathrm{Hom}(B, I) \to \mathrm{Hom}(A, I) \to 0$$

is exact.

This sequence is automatically exact except at $\mathrm{Hom}(A, I)$. Hence to say that I is injective means that every homomorphism $A \to I$ extends to B, i.e., for each injection $f\colon A \to B$ and each $\alpha\colon A \to I$ there exists at least one map $\beta\colon B \to I$ such that $\alpha = \beta \circ f$.

DEFINITION 4.1.2. Let $\mathcal{C}$ be an abelian category. We say that $\mathcal{C}$ has *enough injectives* if for every object A in $\mathcal{C}$ there is an injection $A \to I$ where I is injective.

We have the following result.

THEOREM 4.1.3. *Every R-module can be embedded into an injective R-module, i.e., the category $\mathcal{M}od_R$ has enough injectives.*

PROOF. See [**8**]. □

Let $\mathcal{C}$ be an abelian category. Then $\mathcal{C}^{op}$ is also abelian and injective objects in $\mathcal{C}$ correspond to so called projective objects in $\mathcal{C}^{op}$. We have the following dual definition.

DEFINITION 4.1.4. Let $\mathcal{C}$ be an abelian category. An object P of $\mathcal{C}$ is *projective* if $\mathrm{Hom}(P, \cdot)$ is an exact functor, i.e., if $0 \to A \to B \to C \to 0$ is exact in $\mathcal{C}$ then also

$$0 \to \mathrm{Hom}(P, A) \to \mathrm{Hom}(P, B) \to \mathrm{Hom}(P, C) \to 0$$

is exact.

Indeed, A is injective in $\mathcal{C}$ if and only if A is projective in $\mathcal{C}^{op}$.

EXAMPLE 4.1.5. *Consider the category of all complex vector spaces. Then each object is projective and injective.*

Indeed, every module in this category is free, since it has a basis, and hence projective.

EXAMPLE 4.1.6. *The category of finite abelian groups $\mathfrak{ab}$ is an example of an abelian category that has no nonzero projective objects. Since $\mathfrak{ab}$ is equivalent to $\mathfrak{ab}^{op}$ it has also no nonzero injective objects.*

Since $\mathbb{Z}$ is a PID, a finitely generated projective $\mathbb{Z}$-module is free. But a nonzero finite abelian group cannot be free. On the other hand, an injective module over an integral domain is divisible. Again, a nonzero finite abelian group is not divisible.

DEFINITION 4.1.7. Let $\mathcal{C}$ be an abelian category. We say that $\mathcal{C}$ has *enough projectives* if for every object A in $\mathcal{C}$ there is a surjection $P \to A$ where P is projective.

PROPOSITION 4.1.8. *The category $\mathcal{M}od_R$ has enough projectives.*

PROOF. Every R-module is the homomorphic image of a free, hence projective R-module. □

EXAMPLE 4.1.9. *The category $\mathcal{A}b_{fg}$ of finitely generated abelian groups has enough projectives, but not enough injectives.*

The free group on a finite generating system maps surjectively onto a given finitely generated abelian group. On the other hand, there are no nonzero finitely generated abelian injective groups, because injective means divisible here. So $\mathcal{A}b_{fg}$ has no nonzero injectives at all.

DEFINITION 4.1.10. Let M be an object of an abelian category $\mathcal{C}$. A *projective resolution* of M is a long exact sequence

$$\cdots \to P_r \to P_{r-1} \to \cdots \to P_1 \to P_0 \to M \to 0,$$

also written as $P_\bullet \to M \to 0$, where all P_r are projective objects in $\mathcal{C}$.

An *injective resolution* of M is a long exact sequence

$$0 \to M \to I^0 \to I^1 \to \cdots \to I^r \to \cdots,$$

also written as $0 \to M \to I^\bullet$, where all I^r are injective objects of $\mathcal{C}$.

PROPOSITION 4.1.11. *If the abelian category $\mathcal{C}$ has enough projectives, then every object in $\mathcal{C}$ has an projective resolution. If the abelian category $\mathcal{C}$ has enough injectives, then every object in $\mathcal{C}$ has an injective resolution.*

PROOF. We will prove the first claim. The second one then follows by dualizing. Let M be an object in $\mathcal{C}$. Since $\mathcal{C}$ has enough projectives, there is a projective object P_0 such that there is a surjection $P_0 \to M \to 0$. Let $K_0 = \ker(P_0 \to M)$. This object may not be projective, but we can find again a surjection $P_1 \to K_0 \to 0$, where P_1 is surjective. This yields an exact sequence $P_1 \to P_0 \to M \to 0$. By iterating we obtain a projective resolution of M. □

4.2. Homology and homotopy

Let $\mathcal{C}$ be an abelian category and consider all chain complexes in an abelian category. They form a category $\mathcal{C}h_{\mathcal{C}}$ by taking ladders of morphisms in $\mathcal{C}$ as morphisms, which are commutative diagrams

$$\begin{array}{ccccccccc}
\cdots & \xrightarrow{d_{n+1}} & C_{n+1} & \xrightarrow{d_n} & C_n & \xrightarrow{d_{n-1}} & C_{n-1} & \xrightarrow{d_{n-2}} & \cdots \\
 & & \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \\
\cdots & \xrightarrow{d_{n+1}} & D_{n+1} & \xrightarrow{d_n} & D_n & \xrightarrow{d_{n-1}} & D_{n-1} & \xrightarrow{d_{n-2}} & \cdots
\end{array}$$

Here we have $d_n \circ d_{n+1} = 0$ for all n, which is often just written as $d^2 = 0$. An object in $\mathcal{C}h_{\mathcal{C}}$ then is just denoted by a pair $(C_\bullet, d_\bullet)$. Note that the category $\mathcal{C}h_{\mathcal{C}}$ is again abelian.

DEFINITION 4.2.1. Let $(C_\bullet, d_\bullet) \in \mathcal{Ch}_C$. Denote by $Z_i(C_\bullet, d_\bullet) = \ker(d_{i-1})$ the *i-cycles* and by $B_i(C_\bullet, d_\bullet) = \operatorname{im}(d_i)$ the *i-boundaries*.

Because we have $\operatorname{im}(d_i) \subseteq \ker(d_{i-1})$ for all i, the i-boundaries are a subobject of the i-cycles. In other words, the monomorphism $B_i(C_\bullet, d_\bullet) \to C_i$ factorizes by a monomorphism $B_i(C_\bullet, d_\bullet) \to Z_i(C_\bullet, d_\bullet)$.

DEFINITION 4.2.2. The *homology* of a complex $(C_\bullet, d_\bullet)$ is defined by the quotient

$$H_i(C_\bullet, d_\bullet) = Z_i(C_\bullet, d_\bullet)/B_i(C_\bullet, d_\bullet) = \ker(d_{i-1})/\operatorname{im}(d_i).$$

A chain complex $(C_\bullet, d_\bullet)$ is called *acyclic* in case that $H_i(C_\bullet, d_\bullet) = 0$ for all $i \geq 1$.

REMARK 4.2.3. 1. For every $n \in \mathbb{Z}$ the natural assignment $H_n \colon \mathcal{Ch}_\mathcal{C} \to \mathcal{C}$ is a functor, because it maps kernels of d to kernels of d, and images of d to images of d.

2. Let $P_\bullet \to 0$ be a projective resolution of an object M in $\mathcal{C}$. Then the complex $C_\bullet = P_\bullet \to 0$ is acyclic. Note that

$$H_0(C_\bullet, d_\bullet) = P_0/\operatorname{im}(P_1 \to P_0) = P_0/\ker(P_0 \to M) \cong M.$$

3. Let $C_\bullet$ be a chain complex ending with $\to C_1 \to C_0 \to 0$. We say that it is *concentrated in non-negative degrees*. Then $H_0(C_\bullet) = C_0/\operatorname{im}(C_1 \to C_0)$ and there is a surjective morphism $C_0 \to H_0(C_\bullet)$, so that

$$\cdots \to C_n \to C_{n-1} \to \cdots \to C_0 \to H_0(C_\bullet) \to 0$$

is a complex. This complex is exact if and only if the chain complex $C_\bullet$ is acyclic.

4. A complex is exact if and only if its homology vanishes in all degrees. So homology measures the deviation to being exact.

By dualizing homology one can obtain *cohomology*. Instead of reversing all arrows and so on, one can also just define the cochains by $C^i = C_{-i}$. Then the definition of cohomology is as follows.

DEFINITION 4.2.4. The *cohomology* of a complex $(C_\bullet, d_\bullet)$ is defined by

$$H^i(C_\bullet, d_\bullet) := H_{-i}(C_\bullet, d_\bullet)$$

for all i.

We now return to morphisms of chain complexes.

DEFINITION 4.2.5. A morphism of chain complexes $f_\bullet \colon C_\bullet \to D_\bullet$ is called a *quasi-isomorphism* of chain complexes, if it induces in each degree n an isomorphism $H_n(f) \colon H_n(C_\bullet) \to H_n(D_\bullet)$.

A quasi-isomorphism of chain complexes need not be an isomorphism of chain complexes.

EXAMPLE 4.2.6. *Consider the following map $f_\bullet \colon C_\bullet \to D_\bullet$ in $\mathcal{Ab}$ of chain complexes, given by*

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\times 2} & \mathbb{Z} & \longrightarrow & 0 & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f_{-1}} & & \\
\cdots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z}/2 & \longrightarrow & 0 & \longrightarrow & \cdots
\end{array}$$

This is not an isomorphism of chain complexes, but it induces one in homology.

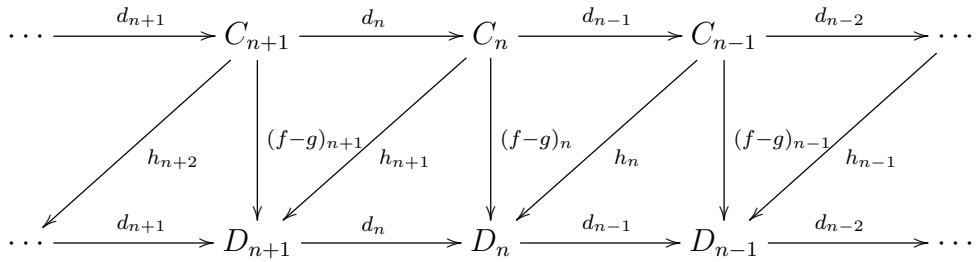
Indeed, we have $H_0(C_\bullet) = H_0(D_\bullet) \cong \mathbb{Z}/2$ and $H_i(C_\bullet) = H_i(D_\bullet) = 0$ for all $i \neq 0$.

DEFINITION 4.2.7. Let $f, g\colon C_\bullet \to D_\bullet$ be two chain maps. A sequence of maps $h_n\colon C_{n-1} \to D_n$ satisfying $f - g = h \circ d + d \circ h$ is called a *chain homotopy* of g to f. We say then that f and g are chain-homotopic and write $f \simeq g$.

More precisely we have

$$(f-g)_n = f_n - g_n = h_n \circ d_{n-1} + d_n \circ h_{n+1}$$

for all n in the diagram (which no longer commutes)



DEFINITION 4.2.8. Let $f\colon C_\bullet \to D_\bullet$ and $g\colon D_\bullet \to C_\bullet$ be chain maps such that $f \circ g \simeq \mathrm{id}_{D_\bullet}$ and $g \circ f \simeq \mathrm{id}_{C_\bullet}$. Then we call $C_\bullet$ and $D_\bullet$ *homotopy-equivalent* and write $C_\bullet \simeq D_\bullet$.

Note that a chain homotopy from g to f is not a chain map in general. This is only true for $f = g$.

PROPOSITION 4.2.9. *Homotopic chain maps $f \simeq g$ induce equal maps on homology. In particular, homotopy equivalences of chain complexes induce isomorphisms of the induced homologies.*

PROOF. The second statement follows immediately from the first by Definition 4.2.8. Let h be a homotopy between f and g. We have to show that $\overline{h} = h \circ d + d \circ h$ induces the zero map in homology. Restricting $\overline{h}_n$ to the cycles we have $\overline{h}_{|\ker(d)} = d \circ h$. So we have $\overline{h}_{|\ker(d)} \subseteq \mathrm{im}(d)$, and hence $\overline{h}_* = 0$. □

4.3. The fundamental theorem of homological algebra

The following theorem, sometimes called fundamental lemma, is very useful for almost all of homological algebra.

THEOREM 4.3.1. *Let $f\colon M \to N$ be a morphism in an abelian category, $P_\bullet \to M \to 0$ be a chain complex with projective objects P_i, and $N_\bullet \to N \to 0$ be an arbitrary exact sequence. Then there exists a lifting of f to a morphism of chain complexes $f_\bullet\colon P_\bullet \to N_\bullet$. Each two such liftings $f_\bullet$ and $f'_\bullet$ are chain-homotopic.*

PROOF. Since P_0 is projective there is a lifting of $f \circ d$ to $P_0 \to N_0$ such that the diagram below commutes:

$$\begin{array}{ccccc} P_0 & \xrightarrow{d} & M & & \\ \vdots & & \downarrow{\scriptstyle f} & & \\ N_0 & \longrightarrow & N & \longrightarrow & 0 \end{array}$$

The lifting need not be unique, though. Let $M' = \ker(P_0 \to M)$ be the kernel of d and $N' = \ker(N_0 \to N)$. Consider the restriction to M' of the map $P_0 \to M_0$. If $x \in \ker(d) = M'$

then $d \circ f)(x) = f(dx) = f(0) = 0$. Thus by restriction we obtain a map $f' \colon M' \to N'$, such that the lower row is again exact in the diagram

$$\begin{array}{ccccc} P_1 & \longrightarrow & M' & & \\ \vdots & & \downarrow{\scriptstyle f'} & & \\ N_1 & \longrightarrow & N' & \longrightarrow & 0 \end{array}$$

Since P_1 is again projective we obtain a morphism $P_1 \to N_1$ in the same way as before. By interating we find a lifting over the complete resolution, and the first part is proved.

For the second part it is enough to show that every lifting $f_\bullet$ of the zero map $M \xrightarrow{0} M$ is homotopic to the zero map on the chain complex, i.e., that there exists a chain homotopy h such that $f = h \circ d + d \circ h$. Consider the ladder diagram

$$\begin{array}{ccccccc} P_1 & \xrightarrow{d} & P_0 & \xrightarrow{d} & M & & \\ & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle 0} & & \\ N_1 & \xrightarrow{d} & N_0 & \xrightarrow{d} & N & \longrightarrow & 0 \end{array}$$

Since $d \circ f_0 = 0 \circ d = 0$ we may view f_0 as a morphism $P_0 \to \ker(N_0 \to N)$. Because $N_\bullet$ is exact, the morphism $N_1 \to \ker(N_0 \to N)$ is surjective. Since P_0 is projective we obtain a lifting

$$\begin{array}{ccccc} & & P_0 & & \\ & \overset{h_0}{\swarrow} & \downarrow{\scriptstyle f_0} & & \\ N_1 & \longrightarrow & \ker(N_0 \to N) & \longrightarrow & 0 \end{array}$$

such that $d \circ h_0 = f_0$. We can now apply the previous argument to $f_1 - h_0 \circ d$ to obtain the diagram

$$\begin{array}{ccccccc} & & P_1 & \xrightarrow{d} & P_0 & & \\ & \overset{h_1}{\swarrow} & \downarrow{\scriptstyle f_1} & \overset{h_0}{\swarrow} & \downarrow{\scriptstyle f_0} & & \\ N_2 & \xrightarrow{d} & N_1 & \xrightarrow{d} & \ker(d) & \longrightarrow & 0 \end{array}$$

where in the square only the lower triangle commutes. But we have

$$d \circ (f_1 - h_0 \circ d) = d \circ f_1 - f_0 \circ d = 0.$$

Thus $f_1 - h_0 \circ d$ lifts to a map h_1 to N_2, so that $d \circ h_1 + h_0 \circ d = f_1$. It follows that we can finish the proof by interating this procedure. □

Corollary 4.3.2. *Each two projective resolutions of an object in $\mathcal{C}$ are chain homotopy-equivalent.*

Proof. Let $P_\bullet$ and $P'_\bullet$ be two projective resolutions of an object M in $\mathcal{C}$. By Theorem 4.3.1 we can lift id_M to morphisms of chain complexes $f \colon P_\bullet \to P'_\bullet$ and $f' \colon P'_\bullet \to P_\bullet$. Then $f \circ f'$ is a lifting of id_M to an endomorphism of the chain complex $P'_\bullet$. Another lifting of id_M is also given by the identity in each degree. By Theorem 4.3.1, these two liftings are chain-homotopic. Hence f, f' represent a chain homotopy equivalence. □

Let F be an additive functor $F \colon \mathcal{C} \to \mathcal{D}$ between two abelian categories, and $N_\bullet$ be a chain complex in $\mathcal{C}h_{\mathcal{C}}$. Then we obtain a chain complex $F(N_\bullet)$ by termwise application of F using

the additivity of F. However, if $N_\bullet$ is exact, $F(N_\bullet)$ need no longer be exact, because the functor may not be exact.

DEFINITION 4.3.3. Let F be an additive functor $F\colon \mathcal{C} \to \mathcal{D}$ between two abelian categories.

1. If $\mathcal{C}$ has enough projectives, then the *left derived* functors $L_nF\colon \mathcal{C} \to \mathcal{D}$ are given by

$$(L_nF)(X) := H_n(F(P_\bullet)),$$

where $P_\bullet \to X$ is an arbitrary projective resolution of X.

2. If $\mathcal{C}$ has enough injectives, then the *right derived* functors $R^nF\colon \mathcal{C} \to \mathcal{D}$ are given by

$$(R^nF)(X) := H^n(F(I_\bullet)),$$

where $X \to I_\bullet$ is an arbitrary injective resolution of X.

REMARK 4.3.4. 1. If F is exact, then the derived functors vanish.

2. The derived functors are well-defined. Indeed, if $P_\bullet$ and $P'_\bullet$ are two different projective resolutions of an object X in $\mathcal{C}$, then there exists by Corollary 4.3.2 a chain homotopy equivalence $P_\bullet \simeq P'_\bullet$. Its image under F yields a chain homotopy equivalence $F(P_\bullet) \simeq F(P'_\bullet)$. By Proposition 4.2.9 the homology groups are isomorphic. The same follows for the right derived functors with injective resolutions.

3. The derived functors are really functors, i.e., they are also defined on morphisms. Indeed, if $f\colon X \to Y$ is a morphism, then f can be lifted uniquely, up to homotopy, to a morphism $f_\bullet\colon P_\bullet \to Q_\bullet$ of projective resolutions $P_\bullet$ and $Q_\bullet$. This yields a morphism $F(f_\bullet)\colon F(P_\bullet) \to F(Q_\bullet)$ of chain complexes, which induces a morphism $F(f_\bullet)_*$ on the homology. By Proposition 4.2.9 this morphism doesn't depend on the choice of $f_\bullet$.

LEMMA 4.3.5. *Let F be a right exact functor. Then we have $L_0F = F$. If F is left exact, then $R^0F = F$. In particular, if F is exact, then $L_0F = R^0F = F$.*

PROOF. It is enough to show the first part here. Let $P_\bullet \to X$ be a projective resolution of X. Since F is right exact, the sequence

$$F(P_1) \to F(P_0) \to F(X) \to 0$$

is exact. By the homomorphism theorem we obtain

$$F(X) \cong F(P_0)/(\ker(F(P_0) \to F(X)) \cong F(P_0)/\operatorname{im}(F(P_1)) = H_0(F(P_\bullet)).$$

□

It makes sense to consider left derived functors now only for right exact functors and right derived functors only for left exact functors.

4.4. The long exact sequence in homology

We know that if the functor F is exact, then the derived functors L_nF and R^nF vanish. If F is not exact, the derived functors may be nonzero. In order to study them we will derive a long exact sequence of derived functors. We start with a lemma which is called *snake lemma*, because of a curved, snake-like arrow in the diagram.

LEMMA 4.4.1. *Let $\mathcal{C}$ be an abelian category and consider the following commutative diagram in $\mathcal{C}$ with exact rows*

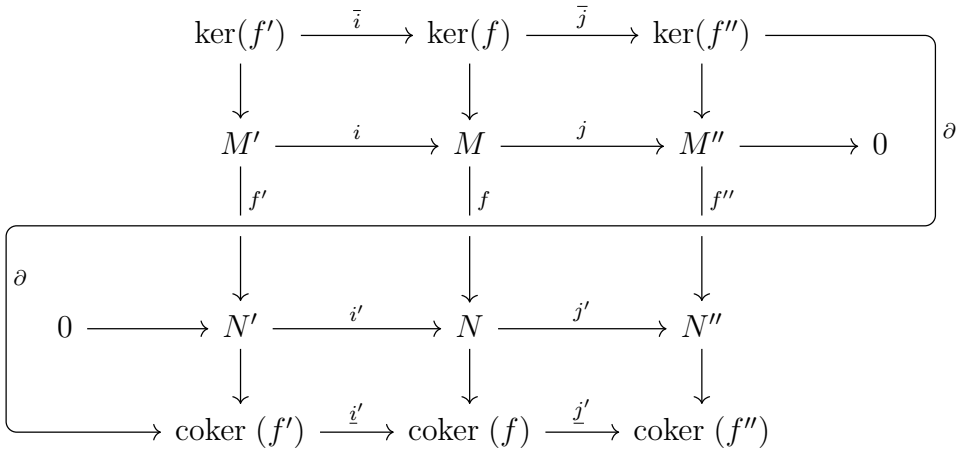
$$\begin{array}{ccccccc} & & M' & \xrightarrow{i} & M & \xrightarrow{j} & M'' \longrightarrow 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} \\ 0 & \longrightarrow & N' & \xrightarrow{i'} & N & \xrightarrow{j'} & N'' \end{array}$$

Then there is an exact sequence

$$\ker(f') \to \ker(f) \to \ker(f'') \xrightarrow{\partial} \operatorname{coker}(f') \to \operatorname{coker}(f) \to \operatorname{coker}(f'').$$

If $M' \to M$ is a monomorphism, so is $\ker(f') \to \ker(f)$, and if $N \to N''$ is an epimorphism, so is $\operatorname{coker}(f) \to \operatorname{coker}(f'')$.

PROOF. Consider the following extended diagram, which shows the snake:



We may assume that $\mathcal{C}$ is an abelian category of modules over a ring R. We prove this result by *diagram chasing*.

1. The construction of ∂: Let $m'' \in \ker(f'')$. Since $j\colon M \to M''$ is surjective, there exists a preimage $m_0 \in M$. By the exactness at M, every other preimage has the form $m = m_0 + i(m')$ for $m' \in M'$. Now $f(m_0)$ is mapped under $j'\colon N \to N''$ to zero, since $j'(f(m_0)) = f''(j(m_0)) = f''(m'') = 0$. Now there is a unique $n_0' \in N'$ such that $i'(n_0) = f(m_0)$ because of the exactness of the N-row. More generally, starting with the preimage $m = m_0 + i(m')$ for $m' \in M'$, the element n_0 is replaced by $n_0' + f'(m')$ with $i'(n_0 + i(m')) = f(m)$. In other words, the class $[n_0']$ of n_0 is well-defined up to an image under f', hence well-defined in $\operatorname{coker}(f')$. So we can define

$$\partial\colon \ker(f'') \to \operatorname{coker}(f'), \quad m'' \mapsto \partial(m'') := [n_0'].$$

By construction, ∂ is a module homomorphism.

2. Exactness at $\ker(f)$: We have $j \circ i = 0$, so that $\overline{j} \circ \overline{i} = 0$, which says that $\operatorname{im}(\overline{i}) \subseteq \ker(\overline{j})$. Conversely let $x \in \ker(\overline{j})$, i.e., $\overline{j}(x) = 0$. Since $x \in M$ we have $x = i(u)$ for some $u \in M'$. Then using $i' \circ f' = f \circ i$,

$$i'(f'(u)) = f(i(u)) = f(x) = 0.$$

By the injectivity of i' we obtain $f'(u) = 0$, hence $u \in \ker(f')$, and thus $x = i(v)$ for some $v \in \ker(f')$, i.e., $x \in \operatorname{im}(\overline{i})$. So $\ker(\overline{j}) \subseteq \operatorname{im}(\overline{i})$.

3. Exactness at $\ker(f'')$: Let $m \in \ker(f)$ and $m'' = \overline{j}(m)$. Then $\partial(m'') = 0$ because of $f(m) = 0$. This yields $\partial \circ \overline{j} = 0$, or $\operatorname{im}(\overline{j}) \subseteq \ker(\partial)$. Conversely let $x \in \ker(f)$ be given with

$x \in \ker(\partial)$. We need to find a preimage in $\ker(f)$. By the exactness of the upper row we find a preimage $m \in M$, which may not yet lie in $\ker(f)$. But $f(m)$ has a preimage $n' \in N'$, since $j'(f(m)) = 0 \in N''$. Since we have $\partial(m'') = 0$ there exists a preimage $m' \in M$ of n', i.e., we have $f'(m') = n'$. Let $m_0 = i(m') \in M$. We claim that the difference $d := m - m_0 \in M$ is the required preimage, which also lies in $\ker(f)$. Indeed, we have

$$\begin{aligned} f(d) &= f(m - i(m')) = f(m) - (f \circ i)(m') \\ &= f(m) - (i' \circ f')(m') \\ &= f(m) - i'(n') \\ &= f(m) - f(m) = 0. \end{aligned}$$

4. Exactness at $\operatorname{coker}(f')$ *and* $\operatorname{coker}(f)$: This follows by passing to the opposite category from above. □

Let $\mathcal{C}$ be an abelian category. Then $\mathcal{C}h_{\mathcal{C}}$ is again an abelian category. So we know what a short exact sequence of chain complexes

$$0 \to M'_\bullet \to M_\bullet \to M''_\bullet \to 0$$

means. In particular we have then a short exact sequence $0 \to M'_n \to M_n \to M''_n \to 0$ for each n.

PROPOSITION 4.4.2. *Let* $0 \to M'_\bullet \to M_\bullet \to M''_\bullet \to 0$ *be a short exact sequence of chain complexes in* $\mathcal{C}$*. Then there exists a long exact sequence*

$$\cdots H_i(M'_\bullet) \to H_i(M_\bullet) \to H_i(M''_\bullet) \xrightarrow{\partial} H_{i-1}(M'_\bullet) \to H_{i-1}(M_\bullet) \to \cdots$$

in homology.

PROOF. We assume again that $\mathcal{C}$ is a subcategory of $\mathcal{M}od_R$. Consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M'_n & \longrightarrow & M_n & \longrightarrow & M''_n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d} & & \\ 0 & \longrightarrow & M'_{n-1} & \longrightarrow & M_{n-1} & \longrightarrow & M''_{n-1} & \longrightarrow & 0 \end{array}$$

and apply the snake lemma to it. Because the kernel of d equals the cycles and the image of d equals the boundaries, we obtain a long exact sequence

$$\begin{aligned} 0 \to Z_n(M'_\bullet) &\to Z_n(M_\bullet) \to Z_n(M''_\bullet) \\ &\to M'_{n-1}/B_{n-1}(M'_\bullet) \to M_{n-1}/B_{n-1}(M_\bullet) \to M''_{n-1}/B_{n-1}(M''_\bullet) \to 0 \end{aligned}$$

Therefore the rows are exact in the following commutative diagram

$$\begin{array}{ccccccccc} & & M'_n/B_n(M'_\bullet) & \longrightarrow & M_n/B_n(M_\bullet) & \longrightarrow & M''_n/B_n(M''_\bullet) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d} & & \\ 0 & \longrightarrow & Z_{n-1}(M'_\bullet) & \longrightarrow & Z_{n-1}(M_\bullet) & \longrightarrow & Z_{n-1}(M''_\bullet) & & \end{array}$$

So we can apply the snake lemma again. This yields the long exact sequence in homology. □

As a consequence we can prove the following result.

PROPOSITION 4.4.3. *Let $\mathcal{C}$ be an abelian category with enough injectives, $\mathcal{D}$ an arbitrary abelian category and $F\colon \mathcal{C} \to \mathcal{D}$ be a left exact additive functor. Let*

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

be a short exact sequence in $\mathcal{C}$. Then there is a long exact sequence in $\mathcal{D}$

$$0 \to (R^0F)(M') \to \cdots \to (R^iF)(M') \xrightarrow{i_*} (R^iF)(M) \xrightarrow{p_*} (R^iF)(M'')$$
$$\xrightarrow{\partial} (R^{i+1}F)(M') \xrightarrow{i_*} (R^{i+1}F)(M) \xrightarrow{p_*} (R^{i+1}F)(M'') \xrightarrow{\partial} \cdots$$

If $\mathcal{C}$ has enough projectives, and the functor F is right exact, then there is a long exact sequence

$$\cdots \to (L_iF)(M') \xrightarrow{i_*} (L_iF)(M) \xrightarrow{p_*} (L_iF)(M'') \xrightarrow{\partial} (L_{i-1}F)(M')$$
$$\xrightarrow{i_*} (L_{i-1}F)(M) \xrightarrow{p_*} (L_{i-1}F)(M'') \xrightarrow{\partial} \cdots \to (L_0F)(M'') \to 0$$

The homomorphism ∂ is called connecting homomorphisms.

PROOF. It is enough to prove one of the two statements, since they are dual to each other. To compute the derived functors we need to construct projective resolutions of $P'_\bullet \to M'$, $P_\bullet \to M$ and $P''_\bullet \to M''$. Then we want to apply Proposition 4.4.2 to them. But for this these resolutions also need to form a short exact sequence of chain complexes $0 \to P'_\bullet \to P_\bullet \to P''_\bullet \to 0$. In other words, the following diagram needs to be commutative:

$$\begin{array}{ccccccc}
 & & P'_n & \longrightarrow & P_n & \longrightarrow & P''_n \\
 & & \downarrow{\scriptstyle d'} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d''} \\
 & & \vdots & & \vdots & & \vdots \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & P'_0 & \longrightarrow & P_0 & \longrightarrow & P''_0 \\
 & & \downarrow{\scriptstyle \varepsilon'} & & \downarrow{\scriptstyle \varepsilon} & & \downarrow{\scriptstyle \varepsilon''} \\
0 & \longrightarrow & M' & \xrightarrow{i} & M & \longrightarrow & M'' \longrightarrow 0
\end{array}$$

To construct this, we chose two arbitrary projective resolutions $P'_\bullet \to M'$ and $P''_\bullet \to M''$ and construct the third one by $P_i := P'_i \oplus P''_i$, taking as differential $d = d' \oplus d''$ the direct sum of the other two differentials. Then $P_\bullet$ is an exact complex consisting of projective objects. The horizontal arrows are given by the canonical injections $P'_i \to P'_i \oplus P''_i$ and the canonical surjections $P'_i \oplus P''_i \to P''_i$. The maps ε' and ε'' are the augmentations of the projective resolutions of M' respectively M''. Then we can define the map $\varepsilon\colon P'_0 \oplus P''_0 \to M$ componentwise. The first component is $i \circ \varepsilon'\colon P'_0 \to M$. For the second component we note that $M \to M''$ is surjective, so that we can use the projectivity of P''_0 to lift ε'' to a morphism $P''_0 \to M$. This finishes the construction and we can apply Proposition 4.4.2 to obtain the result. □

4.5. The functors Tor and Ext

The most important derived functors are the derived functors of the tensor product functor and of the Hom-functor.

DEFINITION 4.5.1. Let R be a ring and X be a right R-module. Let

$$F_X\colon \mathcal{M}od_R \to \mathcal{A}\mathcal{B}$$

be the right exact functor given by $F_X(Y) = X \otimes_R Y$. Its left derived functors are denoted by

$$\mathrm{Tor}_n^R(X,Y) = (L_n F_X)(Y).$$

Note that we have $\mathrm{Tor}_0^R(X,Y) = X \otimes_R Y$. If either X or Y is flat, then we have $\mathrm{Tor}_n^R(X,Y) = 0$ for all $n \geq 1$. In fact, one can compute Tor using a flat resolution of either X or Y. This is more general than a projective (or free) resolution.

Definition 4.5.2. Let R be a ring and X be a left R-module. Let

$$F_X \colon (\mathcal{M}od_R)^{op} \to \mathcal{A}\mathcal{B}$$

be the left exact functor given by $F_X(Y) = \mathrm{Hom}_R(Y,X)$. Its right derived functors are denoted by

$$\mathrm{Ext}_R^n(Y,X) = (R^n F_X)(Y).$$

Note that a injective resolution in $(\mathcal{M}od_R)^{op}$, as used in Ext, is the same as a projective resolution in $\mathcal{M}od_R$. Both functors Tor and Ext are also functors in the other variable. We have $\mathrm{Ext}_R^0(Y,X) = \mathrm{Hom}_R(Y,X)$. If Y is projective, or if X is injective, then $\mathrm{Ext}_R^n(Y,X) = 0$ for all $n \geq 1$.

Example 4.5.3. *We have*

$$\mathrm{Tor}_k^{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Z}/n) = \begin{cases} \mathbb{Z}/gcd(n,m) & \text{for } k = 0,1, \\ 0 & \text{otherwise.} \end{cases}$$

This is an exercise. The same holds for $\mathrm{Ext}_{\mathbb{Z}}^k(\mathbb{Z}/m, \mathbb{Z}/n)$.

Example 4.5.4. *We have*

$$\mathrm{Tor}_k^{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/n) = \begin{cases} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n \cong \mathbb{Z}/n & \text{for } k = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Indeed, since $\mathbb{Z}$ is projective and hence flat, $\mathrm{Tor}_k^{\mathbb{Z}}(\mathbb{Z}, H) = 0$ for all $k \geq 1$ and all $\mathbb{Z}$-modules H. The functor Tor_1 vanishes on finitely generated abelian groups A if and only if A is torisonfree, i.e.,

$$\mathrm{Tor}_1^{\mathbb{Z}}(A, \cdot) = 0 \iff A \text{ is torsionfree } \iff \mathrm{Tor}_1^{\mathbb{Z}}(\cdot, A) = 0$$

This explains the name Tor, comming from torsion.

Example 4.5.5. *We have* $\mathrm{Ext}_{\mathbb{Z}}^n(X,Y) = 0$ *for all abelian groups* X, Y *and all* $n \geq 2$.

We can use a projective resolution of X to compute the right derived functors of $\mathrm{Hom}(-,Y)$, which is a contravariant left exact functor. So take

$$0 \leftarrow F \leftarrow A \leftarrow 0$$

where F is in degree 0. Applying $\mathrm{Hom}(\cdot, Y)$ to this projective resolution, we get a cochain complex

$$0 \to \mathrm{Hom}(F,Y) \to \mathrm{Hom}(A,Y) \to 0$$

where $\mathrm{Hom}(F,Y)$ is in degree 0. Now the group $\mathrm{Ext}^n(X,Y)$ is the n-th cohomology group of this complex. But since the complex is 0 in degrees ≥ 2, this means $\mathrm{Ext}^n(X,Y) = 0$ for all $n \geq 2$.

Remark 4.5.6. Note that $\mathrm{Ext}_{\mathbb{Z}}^1(X,Y)$ need not be zero, e.g., for $X = Y = \mathbb{Z}/p$ for a prime p.

4.6. Double complexes

Let $\mathcal{C}$ be an abelian category. A *double complex* or *bicomplex* is a generalization of a chain complex.

DEFINITION 4.6.1. A double complex is a triple $(X_{i,j}, d_h, d_v)$ consisting of objects $X_{i,j}$ in $\mathcal{C}$ and morphisms $d_h\colon X_{i,j} \to X_{i-1,j}$ and $d_v\colon X_{i,j} \to X_{i,j-1}$, the horizontal and vertical differentials, such that

$$d_h d_v = -d_v d_h, \quad d_h^2 = d_v^2 = 0.$$

The sum $i + j$ is called the *total degree* of $X_{i,j}$.

The equation $d_h d_v = -d_v d_h$ says that the following squares are anticommutative in a bicomplex

$$\begin{array}{ccc} X_{i,j} & \xrightarrow{d_h} & X_{i-1,j} \\ \downarrow{\scriptstyle d_v} & & \downarrow{\scriptstyle d_v} \\ X_{i,j-1} & \xrightarrow{d_h} & X_{i-1,j-1} \end{array}$$

and not commutative. Some readers will probably prefer that these squares commute. But then one can replace d_v by a suitble d'_v such that $d_h d'_v = d'_v d_h$ (and the resulting categories become equivalent). Define a morphism between two double complexes by a family of morphisms $f_{i,j}\colon X_{i,j} \to Y_{i,j}$ commuting with the differentials d_h and d_v, i.e., satisfying

$$d_h f = f d_h,\ d_v f = f d_v.$$

DEFINITION 4.6.2. The double complexes $(X_{i,j}, d_h, d_v)$ together with their morphisms form a category, which is denoted by $\mathcal{BCH}_{\mathcal{C}}$.

The category $\mathcal{BCH}_{\mathcal{C}}$ is again abelian.

DEFINITION 4.6.3. We can associate to every double complex $(X_{i,j}, d_h, d_v)$ two ordinary complexes $|X|$ and $\mathrm{Tot}(X)$ by

$$|X_{\bullet\bullet}|_n := \coprod_{i+j=n} X_{i,j}, \quad (\mathrm{Tot}(X_{\bullet\bullet}))_n = \prod_{i+j=n} X_{i,j},$$

where the differential in both cases is given by $d = d_h + d_v$. Both complexes are called *total complex* of X.

We need to verify that $|X|$ and $\mathrm{Tot}(X)$ are really chain complexes. Indeed, for every $x \in X_{i,j}$ we have

$$\begin{aligned} d^2(x) &= d(d_h(x) + d_v(x)) \\ &= (d_h d_h)(x) + (d_h d_v)(x) + (d_v d_h)(x) + (d_v d_v)(x) = 0. \end{aligned}$$

DEFINITION 4.6.4. Let $(P_\bullet, d)$ be an R^{op}-chain complex and $(Q_\bullet, d)$ be an R-chain complex. Define a bicomplex $(P \otimes_R Q)_{\bullet\bullet}$ of $\mathbb{Z}$-modules by

$$(P \otimes_R Q)_{i,j} := P_i \otimes_R Q_j,$$

where the differentials are given by

$$d_h(p \otimes q) = d(p) \otimes q, \quad d_v(p \otimes q) = (-1)^i p \otimes d(q)$$

for $p \in P_i$ and $q \in Q_j$. The integer i is called the *degree* of p and is denoted by $|p| = i$.

DEFINITION 4.6.5. Let $(P_\bullet, d)$ be an R-chain complex. Define a $\mathbb{Z}$-double complex $\mathrm{Hom}_R(P,Q)_{\bullet\bullet}$ by

$$\mathrm{Hom}_R(P,Q)_{i,j} := \mathrm{Hom}_R(P_i, Q_j),$$

where the differentials are given by

$$(d_h f)(p) = f(d(p)), \quad (d_v f)(p) = (-1)^{|f|+1} d(f(p))$$

for $f\colon P_i \to Q_j$ and $p \in P$. Here $|f|$ is the degree of f.

We can now define a different Tor functor, using the associated total complex of the tensor double complex as follows.

DEFINITION 4.6.6. Let $P_\bullet \to X$ be a projective resolution of R^{op}-modules and $Q_\bullet \to Y$ bne a projective resolution of R-modules. Then define the functor $\overline{\mathrm{Tor}}$ by

$$\overline{\mathrm{Tor}}^R_n(X,Y) := H_n(|P \otimes_R Q|).$$

We want to show that Tor and $\overline{\mathrm{Tor}}$ coincide. For this, we need the following lemma.

LEMMA 4.6.7. *Let $X_{\bullet\bullet}$ be a double complex in an abelian category $\mathcal{C}$. Suppose that the row complex $X_{\bullet,j}$ is exact for every $j \in \mathbb{Z}$. Then the following statements hold.*

1. *If there exists a $N \in \mathbb{Z}$ such that $X_{i,j} = 0$ for all rows $j < N$, then the total complex $|X|$ is exact.*

2. *If there exists a $N \in \mathbb{Z}$ such that $X_{i,j} = 0$ for all columns $i < N$, then the total complex $\mathrm{Tot}(X)$ is exact.*

PROOF. (1): We may assume that $N = 0$. Otherwise we move the complex vertically. It is enough to show the exactness at $|X|_0$, because we can move an arbitrary total degree to the total degree 0 by shifting the complex X horizontally. We have

$$|X|_0 = \bigoplus_{n\in\mathbb{Z}} X_{-n,n} = \bigoplus_{n\geq 0} X_{-n,n}.$$

Let $x = (x_{n_0}, x_{n_0-1}, \dots, x_0) \in |X|_0$ be an arbitrary element with $x_n \in X_{-n,n}$, and let $d(x) = 0$. Because of $d_h(x_n) \in X_{-n-1,n}$ and $d_v(x_n) \in X_{-n,n-1}$ we have

$$\begin{aligned} d_h(x_{n_0}) &= 0, \\ d_v(x_0) &= 0, \\ d_v(x_i) &= -d_h(x_{i-1}) \text{ for } 1 \leq i \leq n_0 \text{ in } X_{-i,i-1} \end{aligned}$$

Since the rows are exact, there exist elements $y_n \in X_{-n+1,n}$ such that

$$\begin{aligned} d_h(y_{n_0}) &= x_{n_0}, \\ d_h(y_i) &= x_i - d_v(y_{i+1}) \text{ for } 0 \leq i \leq n_0 - 1, \end{aligned}$$

because we have, using $d_h(y_{i+1}) = x_{i+1} - d_v(y_{i+2})$ and $d_h(x_i) + d_v(x_{i+1}) = 0$, that

$$\begin{aligned} d_h(x_i - d_v(y_{i+1})) &= d_h(x_i) - d_h(d_v(y_{i+1})) \\ &= d_h(x_i) + d_v(d_h(y_{i+1})) \\ &= d_h(x_i) + d_v(x_{i+1} - d_v(y_{i+2})) \\ &= d_h(x_i) + d_v(x_{i+1}) - d_v^2(y_{i+2}) = 0. \end{aligned}$$

Hence we have found an element $y = (y_{n_0}, \dots, y_0) \in |X|_1$ with $d(y) = x$. So the total complex is exact at $|X|_0$ and we are done.

(2): The proof is similar. □

We can now prove the claimed result concerning the two Tor functors.

PROPOSITION 4.6.8. *Let X be a right R-module and Y a left R-module. Then we have*

$$\mathrm{Tor}_n^R(X,Y) = \overline{\mathrm{Tor}}_n^R(X,Y).$$

PROOF. Let $P_\bullet \to X$ and $Q_\bullet \to Y$ be projective resolutions. Denote by $\overline{P_\bullet}$ the augmented complex with $\overline{P_n} = P_n$ for $n \geq 0$ and $\overline{P_{-1}} = X$. Then $\overline{P}_\bullet$ is exact. Also the double complex $\overline{P} \otimes_R Q$ is exact in each row, since Q_i is projective for each i. By Lemma 4.6.7 the total complex $|\overline{P} \otimes_R Q|$ is exact. Obviously

$$0 \to X[-1] \to \overline{P}_\bullet \to P_\bullet \to 0$$

is a short exact sequence of complexes, where $X[-1]$ denotes the complex having the module X in degree -1 and the zero module otherwise. Since Q_i is projective, tensoring with $Q_\bullet$ yields an exact sequence of double complexes. The functor $|\cdot|$ mapping double complexes to complexes is exact, so that we obtain a short exact sequence of total complexes

$$0 \to |X[-1] \otimes_R Q| \to |\overline{P} \otimes_R Q| \to |P \otimes_R Q| \to 0.$$

Since the complex $|\overline{P} \otimes_R Q|$ is exact, the associated long exact sequence for $n \geq 0$ splits into pieces, which come from the connecting homomorphism

$$0 \to H_n(|P \otimes_R Q|) \to H_{n+1}(|X[-1] \otimes_R Q)| \to 0.$$

So these two homology groups are always isomorphic for all $n \geq 0$. By definition we have

$$H_n(|P \otimes_R Q|) = \overline{\mathrm{Tor}}_n^R(X,Y),$$

and for the second group we have

$$H_{n+1}(|X[-1] \otimes_R Q)| = H_n(X \otimes_R Y) \cong \mathrm{Tor}_n^R(X,Y).$$

So both Tor functors yield isomorphic groups. □

Note that if R is commutative, then also $\mathrm{Tor}_n^R(X,Y) = \mathrm{Tor}_n^R(Y,X)$. We also note, without proof, a corresponding result for Ext functors. Let $Y \to I_\bullet$ be an injective resolution, and $P_\bullet \to X$ be a projective resolution. Define

$$\widetilde{\mathrm{Ext}}_R^n(X,Y) := H^n(\mathrm{Hom}_R(X, I_\bullet)), \quad \overline{Ext}_R^n(X,Y) := H_n(\mathrm{Tot}(\mathrm{Hom}_R(P_\bullet, I_\bullet))).$$

PROPOSITION 4.6.9. *Let X and Y be R-modules. Then we have*

$$\mathrm{Ext}_R^n(X,Y) \cong \widetilde{\mathrm{Ext}}_R^n(X,Y) \cong \overline{\mathrm{Ext}}_R^n(X,Y).$$

4.7. The Yoneda Ext functor

Nobuo Yoneda defined the abelian groups $\mathrm{Ext}^n(M,N)$ for objects M and N in any abelian category $\mathcal{C}$. This agrees with the definition in terms of resolutions if $\mathcal{C}$ has enough projectives or enough injectives. Moreover it shows where the name Ext comes from in this context, namely from extensions. So let $\mathcal{C}$ be an arbitrary abelian category. For $n \geq 1$ consider the set of exact sequences

$$\mathrm{Ext}^n(M,N) := \{0 \to N \to X_{n-1} \to X_{n-2} \to \cdots \to X_0 \to M \to 0\}/\sim$$

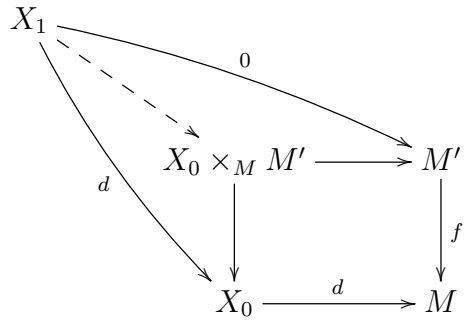
modulo the equivalence relation $E \sim E'$ on the exact sequences if and only if there is a ladder map $E \to E'$, which is the *identity* on the M- and N-entries. We want to show how to obtain a functor $\mathrm{Ext}^n \colon \mathcal{C}^{op} \times \mathcal{C} \to \mathcal{S}et$, $(M, N) \mapsto \mathrm{Ext}^n(M, N)$ from the above definition. We write as a short hand

$$E = (0 \to N \to X_\bullet \to M \to 0) \in \mathrm{Ext}^n(M, N).$$

Let $f \colon M' \to M$ and $g \colon N \to N'$ be morphisms and define the complexes

$$f^*E \colon\ 0 \to N \to X_{n-1} \to \cdots \to X_1 \to X_0 \times_M M' \to M' \to 0$$
$$g_*E \colon\ 0 \to N' \to X_{n-1} \sqcup_N N' \to X_{n-2} \to \cdots \to X_0 \to M \to 0,$$

where $X_0 \times_M M' \to M'$ denotes the *pullback* under M, and $N' \to X_{n-1} \sqcup_N N'$ the *pushout* under N. The pullback diagram for f is given by



The morphism $X_1 \to X_0 \to M$ is from the exact sequence and hence is zero. The pushout diagram for g is dual to the pullback.

LEMMA 4.7.1. *The complexes f^*E and g_*E are exact. Their equivalence class doesn't depend on the choice of a representative for an equivalence class in* Ext^n. *We obtain a functor $F = \mathrm{Ext}^n$.*

PROOF. We have maps

$$\mathrm{Ext}^n(M', N) \to \mathrm{Ext}^n(M, N), \quad E \mapsto f^*E$$
$$\mathrm{Ext}^n(M, N) \to \mathrm{Ext}^n(M, N'), \quad E \mapsto g_*E.$$

1. To show that f^*E and g_*E are well-defined, we need to show that f^*, respectively g_*, doesn't depend on the representative E of the equivalence class. It is enough to consider f^* and then it follows for g_* by duality. So let

$$\begin{array}{ccccccccc} E: & 0 & \longrightarrow & N & \longrightarrow & X_\bullet & \longrightarrow & M & \longrightarrow 0 \\ & & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & \\ E': & 0 & \longrightarrow & N & \longrightarrow & X'_\bullet & \longrightarrow & M & \longrightarrow 0 \end{array}$$

be an elementary equivalence of exact sequences and $f \colon M' \to M$ be a morphism. The functoriality of the pullback yields a map $X_0 \times_M M' \to X'_0 \times_M M'$, which together with the other morphisms $X_i \to X'_i$ yields an elementary equivalence between f^*E and f^*E'.

2. The sequence f^*E is exact. To see this, start with the map $X_0 \times_M M' \to M'$. It is surjective, because for $m' \in M'$ we can find an $x \in X_0$ with $f(m') = d(x)$, since $d \colon X_0 \to M$ is

surjective. Next, the morphism $X_1 \to X_0 \times_M M'$ is given by $x \mapsto (d(x), 0)$, and because of $0 = d(d(x)) = f(0)$ this really lies in $X_0 \times_M M'$. So we have

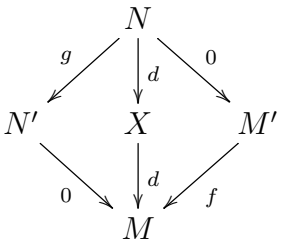
$$\ker(X_1 \to X_0 \times_M M') = \ker(X_1 \to X_0) = \operatorname{im}(X_2 \to X_1).$$

Finally $\ker(X_0 \times_M M' \to M')$ contains the elements of $X_0 \times_M M'$, which are of the form $(x, 0)$. For those we have $d(x) = f(0) = 0$. Because E is exact, $x \in \operatorname{im}(X_1 \to X_0)$ and hence $(x, 0) \in \operatorname{im}(X_1 \to X_0 \times_M M')$. So f^*E is exact. By duality it also follows that g_*E is exact.

3. Functoriality: let $M_2 \xrightarrow{f_1} M_1 \xrightarrow{f_0} M_0$ be two morphisms. Then we need to show that $(f_0 f_1)^* = f_1^* f_0^*$. But this follows form the canonical isomorphism

$$(X_0 \times_{M_0} M_1) \times_{M_1} M_2 \cong X_0 \times_{M_0} M_2.$$

4. For $f\colon M' \to M$ and $g\colon N \to N'$ we need to show that $f^* g_* = g_* f^*$. This is clear for all $n \geq 2$ since then the both functors act on different parts of the exact sequence. For $n = 1$ however, we have the diagram

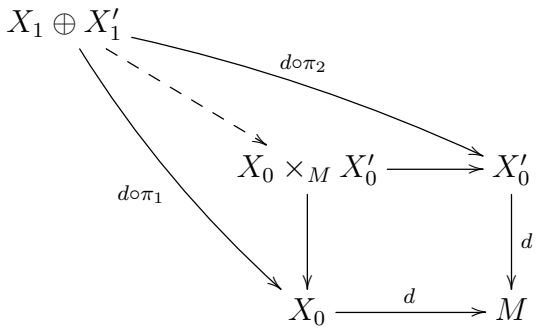


inducing the isomorphism

$$(X \times_M M') \sqcup_N N' \cong (X \sqcup_N N') \times_N M'.$$

This can be verified elementwise. The isomorphism then induces an equivalence of the sequences $f^* g_* E$ and $g_* f^* E$. □

The next step is to equip the Yoneda sets Ext^n with the structure of an abelian group. Let $E, E' \in \operatorname{Ext}^n(M, N)$ For $n \geq 2$ consider the pullback diagram



together with its dual pushout diagram. Then define the sum $E + E'$, the *Baer sum*, as

$$\begin{aligned} E + E' : 0 \to N \to X_{n-1} \sqcup_N X'_{n-1} \to X_{n-2} \oplus X'_{n-2} \to \cdots \\ \to X_1 \oplus X'_1 \to X_0 \times_M X'_0 \to M \to 0. \end{aligned}$$

For $n = 1$ we have to change the middle term of $E + E'$ to

$$\{(x, x') \in X \oplus X' \mid d(x) = d(x')\} / \sim,$$

where the equivalence is given by $(d(a), 0) \sim (0, d(a))$ for all $a \in N$.

LEMMA 4.7.2. *The Yoneda sets* $\mathrm{Ext}^n(M,N)$ *are abelian groups with the above sum* $E+E'$.

PROOF. We will not prove every detail. First note that we have to show that the complexes $E+E'$ are exact. This is clear at the middle direct sum terms. The exactness at M is given by surjectivity. For given $m \in M$ we find an $x_0 \in X_0$ and an $x_0' \in X_0'$ with $d(x_0) = m$, using the surjectivity of the extensions E and E'. Then (x_0, x_0') is the required preimage. To see the exactness at $X_0 \times_M X_0'$ note that the kernel in $X_0 \times_M X_0'$ is given by

$$\ker(X_0 \to M) \times_M \ker(X_0' \to M) = \mathrm{im}(X_1 \oplus X_1' \to X_0 \times_M X_0').$$

The exactness at N and at $X_{n-1} \sqcup_N X_{n-1}'$ follows by duality.

The neutral element is given, for $n \geq 2$, by

$$0 \to N \xrightarrow{\mathrm{id}} N \to 0 \to \cdots \to M \xrightarrow{\mathrm{id}} M \to 0,$$

and by the splitting short exact sequence for $n = 1$. Commutativity and associativity is clear, and the existence of an inverse is left as an exercise. □

Denote now by Ext^n the Yoneda functor, and by $\mathrm{Ext}^n_{\mathcal{C}}$ the usual Ext functor in an (abelian) category $\mathcal{C}$.

PROPOSITION 4.7.3. *Let* $\mathcal{C}$ *be an abelian category with enough projectives. Then there is an isomorphism of functors* $\mathrm{Ext}^n \cong \mathrm{Ext}^n_{\mathcal{C}}$.

PROOF. Let $P_\bullet \to M$ be a projective resolution of M, and $E \in \mathrm{Ext}^n(M,N)$. By the fundamental lemma 4.3.1 the lifting problem for id_M,

$$\begin{array}{ccccccccccccc}
\cdots & \xrightarrow{d_{n+1}} & P_{n+1} & \xrightarrow{d_n} & P_n & \xrightarrow{d_{n-1}} & P_{n-1} & \xrightarrow{d_{n-2}} & P_{n-2} & \longrightarrow \cdots \longrightarrow & P_0 & \longrightarrow & M \longrightarrow 0 \\
 & & \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \downarrow{\scriptstyle f_{n-2}} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle \mathrm{id}} \\
E: & & 0 & \longrightarrow & N & \longrightarrow & X_{n-1} & \longrightarrow & X_{n-2} & \longrightarrow \cdots \longrightarrow & X_0 & \longrightarrow & M \longrightarrow 0
\end{array}$$

has a solution $f_\bullet$. We have $f_n \circ d = 0$ by the commutativity of the left square. So we have

$$f_n \in \ker\big(\mathrm{Hom}(P_n, N) \to \mathrm{Hom}(P_{n+1}, N)\big)$$

and we can define the class

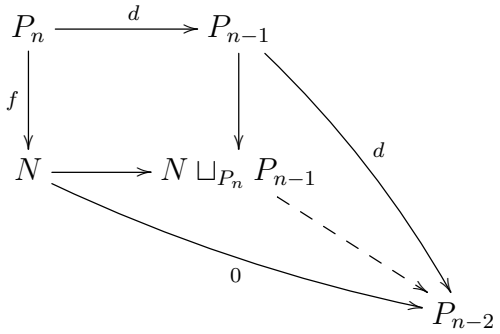
$$\Phi(E) := [f_n] \in \mathrm{Ext}^n_{\mathcal{C}}(M,N).$$

This is indeed well-defined. It doesn't depend on the choice of the lifting $f_\bullet$ of id_M, and on the choice of the extension E in its equivalence class. By the fundamental lemma the lifting $f_n \colon P_n \to N$ is unique up to homotopy. So every other solution is of the form $f_n + H \circ d$, where $H \colon P_{n-1} \to N$ is part of a chain homotopy. This makes no difference in the homology, so the class of f_n in $H^n(\mathrm{Hom}(P_\bullet, N) = \mathrm{Ext}^n_{\mathcal{C}}(M,N)$ is well-defined, if we can also show the second condition, namely that it is invariant under the equivalence relation in Ext^n. So let $E \to E'$ be an elementary equivalence, then we can chose such a lifting $P_\bullet \to E'$, which is the composition of the lifiting of id_M and the equivalence map $E \to E'$. Since this map by definition is id_N, we obtain the same element in $\mathrm{Ext}^n_{\mathcal{C}}$.

Now we want to show that the map

$$\Phi \colon \mathrm{Ext}^n(M,N) \to \mathrm{Ext}^n_{\mathcal{C}}(M,N)$$

is an isomorphism of abelian groups. We define an inverse map Ψ as follows. Let $f\colon P_n \to N$ be a representative in $\operatorname{Ext}^n_{\mathcal{C}}(M,N)$. The by considering the pushout diagram



we obtain an exact sequence

$$0 \to N \to N \sqcup_{P_n} P_{n-1} \to P_{n-2} \to \cdots \to P_0 \to M \to 0$$

in $\operatorname{Ext}^n(M,N)$. It is clear that $\Phi \circ \Psi = \mathrm{id}$. Conversely we have $\Psi \circ \Phi = \mathrm{id}$ by the following diagram

$$\begin{array}{ccccccccccccc}
0 & \longrightarrow & N & \longrightarrow & N \sqcup_{P_n} P_{n-1} & \longrightarrow & P_{n-2} & \longrightarrow & \cdots & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle (d, f_{n-1})} & & \downarrow{\scriptstyle f_{n-2}} & & & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle \mathrm{id}} & & \\
0 & \longrightarrow & N & \xrightarrow{d} & X_{n-1} & \xrightarrow{d} & X_{n-2} & \longrightarrow & \cdots & \longrightarrow & X_0 & \longrightarrow & M & \longrightarrow & 0
\end{array}$$

which gives an equivalence in Ext^n. Finally the bijection Φ is a group homomorphism, which is easy to verify. □

Example 4.7.4. *We have*

$$\operatorname{Ext}^1(\mathbb{Z}/p, \mathbb{Z}/p) \cong \operatorname{Ext}^1_{\mathcal{A}b}(\mathbb{Z}/p, \mathbb{Z}/p) = \operatorname{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/p, \mathbb{Z}/p) \cong \mathbb{Z}_p.$$

Hence there are p equivalence classes of group extensions G of $\mathbb{Z}/p$ by $\mathbb{Z}/p$

$$0 \to \mathbb{Z}/p \to G \to \mathbb{Z}/p \to 0.$$

More generally, $\operatorname{Ext}^1(\mathbb{Z}/m, \mathbb{Z}/n) \cong \mathbb{Z}/d$, *where* $d = \gcd(m,n)$.

The Yoneda functor allows us to define a product of extensions, the so-called *Yoneda product*. For $E \in \operatorname{Ext}^n(M,N)$ and $E' \in \operatorname{Ext}^m(Q,M)$ this will be an element EE' in $\operatorname{Ext}^{n+m}(Q,N)$ for all $n, m \geq 1$. Consider the morphism given by composition $X_0 \to M \to X'_{m-1}$. Since $X_1 \to X_0 \to M$ is the zero map, and $M \to X'_m \to X'_{m-1}$ is the zero map, we obtain an extension

$$0 \to N \to X_{n-1} \to \cdots \to X_0 \to X'_{m-1} \to \cdots \to X'_0 \to Q$$

in $\operatorname{Ext}^{n+m}(Q,N)$. We can also define the product for $n = 0$ or $m = 0$. Let $\operatorname{Ext}^0(M,N) = \operatorname{Hom}(M,N)$, then the product $\operatorname{Ext}^0 \times \operatorname{Ext}^0 \to \operatorname{Ext}^0$ is just the composition of morphisms. For n or m nonzero we define the product by

$$\operatorname{Ext}^0 \times \operatorname{Ext}^m \to \operatorname{Ext}^m, \quad (f, E) \mapsto f^*E,$$
$$\operatorname{Ext}^n \times \operatorname{Ext}^0 \to \operatorname{Ext}^n, \quad (g, E) \mapsto g_*E.$$

This is the Yoneda product, and it is a well-defined bilinear, associative multiplication.

CHAPTER 5

Homology and cohomology of groups

There are at least two different definitions of (co)homology groups. One by means of (co)chains and explicit formulas of the (co)boundary operators, the other by means of derived functors. Of course there is a canonical isomorphism between the two (co)homology groups.

5.1. Functorial definition of group homology and cohomology

For the definition of homology and cohomology of groups we are not using the category of groups. Rather we use the category $\mathcal{M}od_R$ for the *group ring* $R = \mathbb{Z}[G]$.

DEFINITION 5.1.1. Let G be a group. A *G-module* M is an R-module for $R = \mathbb{Z}[G]$.

More explicitly M is an abelian group together with a linear G-action

$$T\colon G \to \mathrm{Aut}(M)$$

given by $T(g)(m) = g.m$ for all $m \in M$. Here T is a group homomorphism, and we have a group action $G \times M \to M$ given by $(g, m) \mapsto g.m$. The *trivial action* of G on M is given by $g.m = m$ for all $g \in G$, $m \in M$.

DEFINITION 5.1.2. Let G be a group. Denote by $\mathcal{M}_G$ the category of G-modules, i.e., of $\mathbb{Z}[G]$-modules. This is an abelian category.

For the trivial group $G = 1$ we obtain the category $\mathcal{A}\mathcal{b}$ of $\mathbb{Z}$-modules.

DEFINITION 5.1.3. Let M be a G-module. Then the G-submodule

$$M^G = \{m \in M \mid g.m = m \text{ for all } g \in G\}$$

is called the *module of G-invariants*. The G-submodule

$$M_G = M/(g.m - m \mid g \in G, m \in M) = M/I_G M$$

is called the *module of G-coinvariants*. Here I_G is the kernel of the augmentation map $\varepsilon\colon \mathbb{Z}[G] \to \mathbb{Z}$.

LEMMA 5.1.4. *The maps $F, G\colon \mathcal{M}_G \to \mathcal{A}\mathcal{b}$ given by $F(M) = M^G$ and $G(M) = M_G$ are additive functors.*

PROOF. Let $f\colon M \to N$ be a $\mathbb{Z}[G]$-module homomorphism, which is a G-equivariant map. We write $f \in \mathrm{Hom}_G(M, N)$ or sometimes $f \in \mathrm{Hom}_{\mathbb{Z}[G]}(M, N)$. Then f restricts to a morphism $f^G\colon M^G \to N^G$. It also induces a morphism $f_G\colon M_G \to N_G$ because of $f(g.m - m) = g.f(m) - f(m)$ □

LEMMA 5.1.5. *Let $\mathbb{Z}$ be a trivial G-module. Then we have*

$$M^G \cong \mathrm{Hom}_G(\mathbb{Z}, M), \quad M_G \cong \mathbb{Z} \otimes_{\mathbb{Z}[G]} M.$$

In particular, the functor $F\colon \mathcal{M}_G \to \mathcal{A}\mathcal{b}$ with $F(M) = M^G$ is left exact, and the functor $G\colon \mathcal{M}_G \to \mathcal{A}\mathcal{b}$ with $G(M) = M_G$ is right exact.

PROOF. Let $f \in \mathrm{Hom}_G(\mathbb{Z}, M)$. Then f is uniquely determined by $f(1)$. Because of $g.f(1) = f(1.g) = f(1)$ we have $f(1) \in M^G$. Conversely every $m \in M^G$ defines an f with $f(1) = m$ by $g.m = m$. This gives the first isomorphism. For the second one, note that in $\mathbb{Z} \otimes_{\mathbb{Z}[G]} M$ we have

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

so that $1 \otimes m$ and $1 \otimes m'$ are equal if and only if m and m' determine the same class in M_G. Clearly the Hom functor is left exact and the tensor product functor is right exact. □

Since the category $\mathcal{M}_G$ has enough injectives and projectives, we can form the right derived functors R^nF of the invariants and the left derived functors L_nG of the coinvariants. So we can define the (co)homology as follows.

DEFINITION 5.1.6. Let M be a G-module. Then the *homology* of G with coefficients in M is defined by

$$H_n(G, M) = (L_nG)(M) = \mathrm{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, M)$$

The *cohomology* of G with coefficients in M is defined by

$$H^n(G, M) = (R^nF)(M) = \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, M)$$

For the trivial G-module $M = \mathbb{Z}$ we write $H_n(G) = H_n(G, \mathbb{Z})$ respectively $H^n(G, \mathbb{Z}) = H^n(G)$. Although the definition of homology and cohomology appears to be symmetric, the properties are quite different. It turns out that group cohomology is often easier to handle and more useful than group homology. For example, group cohomology comes equipped with a natural *cup-product*. Therefore we will prefer cohomology groups to homology groups a bit. We recall a few basic properties of cohomology groups.

(1) We have $H^0(G, M) = F(M) = M^G$.

(2) If I is an injective G-module, then $H^r(G, I) = 0$ for all $r > 0$, because $0 \to I \to I \to 0 \to 0 \to \cdots$ is an injective resolution of I.

(3) A short exact sequence $0 \to N \to M \to V \to 0$ of G-modules gives rise to a long exact sequence

$$\begin{aligned} 0 \to H^0(G, N) \to H^0(G, M) \to H^0(G, V) \to H^1(G, N) \to H^1(G, M) \to \cdots \\ \to H^r(G, N) \to H^r(G, M) \to H^r(G, V) \to H^{r+1}(G, N) \to \cdots \end{aligned}$$

For the homology, we already have computed the case in Exercise 30, where $G = C_n = \langle t \rangle$ is cyclic of order n and $\mathbb{Z}[G] \cong \mathbb{Z}[t]/(t^n - 1)$.

EXAMPLE 5.1.7. *The homology of the cyclic group C_n with trivial coefficients is given by*

$$H_k(C_n) = \mathrm{Tor}_k^{\mathbb{Z}[G]}(\mathbb{Z}, \mathbb{Z}) = \begin{cases} \mathbb{Z} & \text{for } k = 0, \\ \mathbb{Z}/n & \text{for } k \text{ odd}, \\ 0 & \text{for } k > 0 \text{ even}. \end{cases}$$

For the cohomology we obtain a similar result, see Exercise 34.

EXAMPLE 5.1.8. *The cohomology of the cyclic group C_n with trivial coefficients is given by*

$$H^k(C_n) = \mathrm{Ext}^k_{\mathbb{Z}[G]}(\mathbb{Z},\mathbb{Z}) = \begin{cases} \mathbb{Z} & \text{for } k = 0, \\ 0 & \text{for } k \text{ odd}, \\ \mathbb{Z}/n & \text{for } k > 0 \text{ even}. \end{cases}$$

With *sage* one can compute a few more examples, see

`https://sagecell.sagemath.org/`

Using spectral sequences we also can show that

EXAMPLE 5.1.9.

$$H^n(S_3,\mathbb{Z}) = \begin{cases} \mathbb{Z}\,, & \text{for } n = 0 \\ \mathbb{Z}_2 & \text{for } n \equiv 2 \bmod 4, \\ \mathbb{Z}_6 & \text{for } n > 0,\ n \equiv 0 \bmod 4, \\ 0 & \text{for } n \text{ odd}. \end{cases}$$

EXAMPLE 5.1.10. *The group $SL_2(\mathbb{Z})$ is the amalgamated free product*

$$SL_2(\mathbb{Z}) \cong \mathbb{Z}/4 *_{\mathbb{Z}/2} \mathbb{Z}/6.$$

Its homology and cohomology with trivial coefficients is given by

$$H_k(SL_2(\mathbb{Z})) = \begin{cases} \mathbb{Z} & \text{for } k = 0, \\ \mathbb{Z}/12 & \text{for } k \text{ odd}, \\ 0 & \text{for } k > 0 \text{ even}. \end{cases}$$

$$H^k(SL_2(\mathbb{Z})) = \begin{cases} \mathbb{Z} & \text{for } k = 0, \\ 0 & \text{for } k \text{ odd}, \\ \mathbb{Z}/12 & \text{for } k > 0 \text{ even}. \end{cases}$$

Note that $SL_2(\mathbb{Z})$ contains a free group of index 12, which is a reason, why 12 is arising here.

PROPOSITION 5.1.11. *Let F_n be the free group of rank n. Then we have*

$$H^k(F_n) \cong H_k(F_n) = \begin{cases} \mathbb{Z} & \text{for } k = 0, \\ \mathbb{Z}^n & \text{for } k = 1, \\ 0 & \text{for } k \geq 2. \end{cases}$$

PROOF. Let G be the free group F_n of rank n. We can show that there is a length one resolution of the trivial G-module $\mathbb{Z}$ as follows. Let $\varepsilon : \mathbb{Z}[G] \longrightarrow \mathbb{Z}$ be the canonical augmentation that sends every $g \in G \mapsto 1 \in \mathbb{Z}$, and let $K = \ker \varepsilon$. Then K is a free $\mathbb{Z}[G]$-module with basis $\{x - 1 : x \in X\}$ where X is a basis of G, so there is a free resolution of length 1,

$$0 \longrightarrow K \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$$

Thus $H^k(F_n,\mathbb{Z}) = H_k(F_n,\mathbb{Z}) = 0$ for all $k \geq 2$. For $k = 0$ it is clear that we obtain the invariants respectively the coinvariants, and the case $k = 1$ is left as an exercise. □

5.2. The bar resolution

Among the resolutions of a $\mathbb{Z}[G]$-module for computing homology or cohomology there is a concrete one, which is functorial. This is useful for low degrees, but it becomes quite complicated for the explicit computation in general. First we treat the version for homology.

DEFINITION 5.2.1. Let R be a ring and M be an R-module. Define the *bar complex* $B_\bullet(R, M)$ by

$$B_n(R, M) = R^{\otimes(n+1)} \otimes M = R \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} R \otimes_{\mathbb{Z}} M,$$

together with the maps $d\colon B_n(R, M) \to B_{n-1}(R, M)$ with $d = \sum_{i=0}^{n}(-1)^i d_i$, where

$$d_i(r_0 \mid \cdots \mid r_{n+1}) = r_0 \mid \cdots \mid r_i r_{i+1} \mid \cdots \mid r_{n+1}.$$

for $r_i \in R$ with $i \leq n$ and $r_{n+1} \in M$.

The notation $a \mid b := a \otimes b$ has historical reasons and gives the complex its name. The group $B_n(R, M)$ is equipped with an R-module structure by

$$r.(r_0 \mid \cdots \mid r_n \mid m) = r.r_0 \mid r_1 \mid \cdots \mid r_n \mid m.$$

PROPOSITION 5.2.2. *The sequence $B_\bullet(R, M)$ is a resolution of M over R.*

PROOF. We will first show that $d^2 = 0$, so that $B_\bullet(R, M)$ is a complex. Using

$$d_i \circ d_j = d_j \circ d_{i+1} \text{ for all } i \geq j$$

in the third line and splitting up the sum in the second line, we obtain

$$\begin{aligned}
d \circ d &= \sum_{i=0}^{n-1}\sum_{j=0}^{n}(-1)^{i+j} d_i \circ d_j \\
&= \sum_{i=0}^{n-1}\sum_{j=0}^{i}(-1)^{i+j} d_i \circ d_j + \sum_{i=0}^{n-1}\sum_{j=i+1}^{n}(-1)^{i+j} d_i \circ d_j \\
&= \sum_{i=1}^{n}\sum_{j=0}^{i-1}(-1)^{i+j-1} d_j \circ d_i + \sum_{i=0}^{n-1}\sum_{j=i+1}^{n}(-1)^{i+j} d_i \circ d_j \\
&= \sum_{j=0}^{n-1}\sum_{i=j+1}^{n}(-1)^{i+j-1} d_j \circ d_i + \sum_{i=0}^{n-1}\sum_{j=i+1}^{n}(-1)^{i+j} d_i \circ d_j \\
&= 0.
\end{aligned}$$

It remains to show that $B_\bullet(R, M)$ is exact. This will follow from the construction of a *chain contraction* (chain homotopy) $h\colon B_n(R, M) \to B_{n+1}(R, M)$ satisfying

$$h \circ d + d \circ h = \mathrm{id}\,.$$

In fact, let

$$h(r_0 \mid \cdots \mid r_n) = 1 \mid r_0 \cdots \mid r_n.$$

Then one verifies that $h \circ d_i = d_{i+1} \circ h$, so that

$$\begin{aligned}
d \circ h + h \circ d &= \sum_{i=0}^{n+1}(-1)^i d_i \circ h + \sum_{i=0}^{n}(-1)^i h \circ d_i \\
&= d_0 \circ h = \mathrm{id}\,.
\end{aligned}$$

□

REMARK 5.2.3. The R-module $B_n(R, M)$ need not be projective in general. For example, if $R = \mathbb{Z}$ and $M = \mathbb{Z}/m$, then $B_n(R, M) = \mathbb{Z}/m$. However, if R and M are free as abelian groups, so is $B_n(R, M)$.

We can apply the bar resolution for homology groups in low degree.

EXAMPLE 5.2.4. *We have $H_1(G) \cong G/[G, G]$ for every group G.*

To see this, let $\mathbb{Z}$ be the trivial G-module and consider the beginning of the bar resolution

$$\mathbb{Z}[G] \otimes \mathbb{Z}[G] \otimes \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G] \otimes \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G]$$

$$g_0|g_1|g_2 \longrightarrow g_0g_1|g_2 - g_0|g_1g_2 + g_0|g_1$$

$$g_0|g_1 \longrightarrow g_0g_1 - g_0$$

Since $\mathbb{Z}$ is a free module, this is a free resolution. Hence we obtain the homology by tensoring this sequence from the left with the trivial $\mathbb{Z}[G]$-module $\mathbb{Z}$, which gives

$$\mathbb{Z}[G] \otimes \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z}$$

$$g_1|g_2 \longrightarrow g_2 - g_1g_2 + g_1$$

$$g_i \longrightarrow 0$$

So we have

$$H_1(G) = \mathbb{Z}[G]/(g_1 + g_2 - g_1g_2 \mid g_1, g_2 \in G).$$

Now $H_1(G)$ satisfies the universal property of the abelianization, and hence is isomorphic to $G_{ab} = G/[G, G]$. This is proved as follows. The canonical map $G \to H_1(G)$ is a surjective group homomorphism. We need to show that every morphism $f\colon G \to A$ for an abelian group A factorizes uniquely by $H_1(G)$. Since A is abelian, we can extend f uniquely to a homomorphism $\mathbb{Z}[G] \to A$, namely by

$$\sum_{g\in G} a_g[g] \mapsto \sum_{g\in G} a_g f(g).$$

Obvioulsy $g_1 + g_2 - g_1g_2$ lies in the kernel of this map. Hence $H_1(G)$ satisfies the universal property as claimed.

5.3. Group cohomology by explicit coboundary map

As for homology we can use a special resolution to compute the group cohomology. Of course, the definition gives isomrophic cohomology groups, which we have defined by derived functors.

Let A be a G-module and let $C^n(G, A)$ denote the set of functions of n variables

$$f : G \times G \times \cdots \times G \to A$$

into A. For $n = 0$ let

$$C^0(G, A) = \mathrm{Hom}(1, A) \cong A.$$

The elements of $C^n(G, A)$ are called *n-cochains*. The set $C^n(G, A)$ is an abelian group with the usual definitions of addition and the element 0:

$$\begin{aligned}(f + g)(x_1, \ldots, x_n) &= f(x_1, \ldots, x_n) + g(x_1, \ldots, x_n)\\ 0(x_1, \ldots, x_n) &= 0\end{aligned}$$

We now define homomorphisms $\delta = \delta_n : C^n(G, A) \to C^{n+1}(G, A)$.

Definition 5.3.1. If $f \in C^n(G, A)$ then define $\delta_n(f)$ by

$$\begin{aligned}\delta_n(f)(x_1, \ldots, x_{n+1}) = {} & x_1 f(x_2, \ldots, x_{n+1})\\ & + \sum_{i=1}^{n} (-1)^i f(x_1, \ldots, x_{i-1}, x_i x_{i+1}, \ldots, x_{n+1})\\ & + (-1)^{n+1} f(x_1, \ldots, x_n)\end{aligned}$$

For $n = 0, 1, 2, 3$ we obtain

$$(\delta_0 f)(x_1) = x_1 f - f \tag{5.1}$$

$$(\delta_1 f)(x_1, x_2) = x_1 f(x_2) - f(x_1 x_2) + f(x_1) \tag{5.2}$$

$$(\delta_2 f)(x_1, x_2, x_3) = x_1 f(x_2, x_3) - f(x_1 x_2, x_3) + f(x_1, x_2 x_3) - f(x_1, x_2) \tag{5.3}$$

$$\begin{aligned}(\delta_3 f)(x_1, x_2, x_3, x_4) = {} & x_1 f(x_2, x_3, x_4) - f(x_1 x_2, x_3, x_4) + f(x_1, x_2 x_3, x_4)\\ & - f(x_1, x_2, x_3 x_4) + f(x_1, x_2, x_3)\end{aligned} \tag{5.4}$$

For $n = 0$, f is considered as an element of A so that $x_1 f$ makes sense.

We will show that $\delta^2(f) = 0$ for every $f \in C^n(G, A)$, i.e., $\delta_{n+1}\delta_n = 0$ for all $n \in \mathbb{N}$ and hence $\operatorname{im} \delta_n \subseteq \ker \delta_{n+1}$.

Lemma 5.3.2. *It holds $\delta_{n+1}\delta_n(C^n(G, A)) = 0$ for all $n \in \mathbb{N}$. Hence the following sequence is a complex.*

$$A \xrightarrow{\delta_0} C^1(G, A) \xrightarrow{\delta_1} \cdots \xrightarrow{\delta_{n-1}} C^n(G, A) \xrightarrow{\delta_n} C^{n+1}(G, A) \xrightarrow{\delta_{n+1}} \cdots$$

Proof. Let $f \in C^n(G, A)$. We want to show $\delta^2(f)(x_1, \ldots, x_{n+2}) = 0$. Define $g_j \in C^{n+1}(G, A)$ for $0 \le j \le n + 1$ by

$$g_j(x_1, \ldots, x_{n+1}) = \begin{cases} x_1 f(x_2, \ldots, x_{n+1}), & j = 0\\ (-1)^j f(x_1, \ldots, x_j x_{j+1}, \ldots, x_{n+1}), & 1 \le j \le n\\ (-1)^{n+1} f(x_1, \ldots, x_n), & j = n + 1\end{cases}$$

This means

$$(\delta f)(x_1, \ldots, x_{n+1}) = \sum_{j=0}^{n+1} g_j(x_1, \ldots, x_{n+1})$$

Then define $g_{ji} \in C^{n+2}(G, A)$ for $0 \leq i \leq n+2$ by

$$g_{ji}(x_1, \ldots, x_{n+2}) = \begin{cases} x_1 g_j(x_2, \ldots, x_{n+2}), & i = 0 \\ (-1)^i g_j(x_1, \ldots, x_i x_{i+1}, \ldots, x_{n+2}), & 1 \leq i \leq n+1 \\ (-1)^{n+2} g_j(x_1, \ldots, x_{n+1}), & i = n+2 \end{cases}$$

This means

$$(\delta g_j)(x_1, \ldots, x_{n+2}) = \sum_{i=0}^{n+2} g_{ij}(x_1, \ldots, x_{n+2})$$

It follows

$$\delta^2(f)(x_1, \ldots, x_{n+2}) = \sum_{j=0}^{n+1} (\delta g_j)(x_1, \ldots, x_{n+2}) = \sum_{j=0}^{n+1} \sum_{i=0}^{n+2} g_{ij}(x_1, \ldots, x_{n+2})$$

We will show that for all $0 \leq j \leq n+1$ and all $j+1 \leq i \leq n+2$

$$(g_{ji} + g_{i-1,j})(x_1, \ldots, x_{n+2}) = 0 \tag{5.5}$$

This will imply our result as follows. Write down all g_{ji} as an $(n+2) \times (n+3)$ array and cancel out each pair $(g_{ji}, g_{i-1,j})$ starting with $j = 0$ and $i = 1, \ldots, n+2$, then $j = 1$ and $i = 2, \ldots n+2$, until $j = n+1$ and $i = n+2$. Then all entries of the array are cancelled out and we obtain $\delta^2(f) = \sum_{j=0}^{n+1} \sum_{i=0}^{n+2} g_{ij} = 0$.
It remains to show (5.5). Assume first $1 \leq j \leq n$. If $i > j+1$ then

$$\begin{aligned} g_{ji}(x_1, \ldots, x_{n+2}) &= (-1)^i g_j(x_1, \ldots, x_i x_{i+1}, \ldots, x_{n+2}) \\ &= (-1)^i g_j(\tau_1, \ldots, \tau_{n+1}) \\ &= (-1)^{i+j} f(\tau_1, \ldots, \tau_j \tau_{j+1}, \ldots, \tau_{n+1}) \\ &= (-1)^{i+j} f(x_1, \ldots, x_j x_{j+1}, \ldots, x_i x_{i+1}, \ldots, x_{n+2}) \end{aligned}$$

with

$$\begin{gathered} (\tau_1, \ldots, \tau_j, \tau_{j+1}, \ldots, \tau_i, \tau_{i+1}, \ldots, \tau_{n+1}) = \\ (x_1, \ldots, x_j, x_{j+1}, \ldots, x_i x_{i+1}, x_{i+2}, \ldots, x_{n+2}). \end{gathered}$$

On the other hand we have

$$\begin{aligned} g_{i-1,j}(x_1, \ldots, x_{n+2}) &= (-1)^j g_{i-1}(x_1, \ldots, x_j x_{j+1}, \ldots, x_{n+2}) \\ &= (-1)^j g_{i-1}(\sigma_1, \ldots, \sigma_j, \ldots, \sigma_{n+1}) \\ &= (-1)^{i-1+j} f(\sigma_1, \ldots, \sigma_{i-1} \sigma_i, \ldots, \sigma_{n+1}) \\ &= (-1)^{i+j-1} f(x_1, \ldots, x_j x_{j+1}, \ldots, x_i x_{i+1}, \ldots, x_{n+2}) \end{aligned}$$

with

$$\begin{gathered} (\sigma_1, \ldots, \sigma_{j-1}, \sigma_j, \ldots, \sigma_{i-1}, \sigma_i, \ldots, \sigma_{n+1}) = \\ (x_1, \ldots, x_{j-1}, x_j x_{j+1}, \ldots, x_i, x_{i+1}, \ldots, x_{n+2}). \end{gathered}$$

It follows $g_{ij} + g_{i-1,j} = 0$. If $i = j+1$ we obtain in the same way

$$\begin{aligned} g_{ji}(x_1, \ldots, x_{n+2}) &= (-1)^{i+j} f(x_1, \ldots, x_{i-1} x_i x_{i+1}, \ldots, x_{n+2}) \\ &= -g_{i-1,j}(x_1, \ldots, x_{n+2}) \end{aligned}$$

The remaining cases $j = 0$ and $j = n + 1$ follow similarly. □

Define the subgroups $Z^n(G, A) = \ker \delta_n$ and $B^n(G, A) = \operatorname{im} \delta_{n-1}$. For $n = 0$ let $B^0(G, A) = 0$. Since $B^n(G, A) \subseteq Z^n(G, A)$ we can form the factor group:

DEFINITION 5.3.3. The *n-th cohomology group* of G with coefficients in A is given by the factor group

$$H^n(G, A) = Z^n(G, A)/B^n(G, A) = \ker \delta_n / \operatorname{im} \delta_{n-1}$$

These groups coincide with the cohomology groups defined by the right derived functors.

5.4. The zeroth cohomology group

For $n = 0$ we have

$$H^0(G, A) = Z^0(G, A) = \{a \in A \mid xa = a \; \forall \, x \in G\} = A^G$$

Hence $H^0(G, A) = A^G$ is the module of invariants. Let L/K be a finite Galois extension with Galois group $G = Gal(L/K)$. Then L and $L^\times$ are G-modules. Here L is regarded as a group under addition and $L^\times$ is the multiplicative group of units in L. We have

$$H^0(G, L^\times) = (L^\times)^G = K^\times$$

Let p be a prime and C_p the cyclic group of order p.

EXAMPLE 5.4.1. *Let $A = C_p$ be a $G = C_p$-module. Then $xa = a$ for all $x \in C_p$, i.e., A is a trivial C_p-module. We have*

$$H^0(C_p, C_p) = C_p$$

Denote by xa the action of G on A. Let $T : C_p \to \operatorname{Aut}(C_p) \cong C_{p-1}$ be the homomorphism defined by $xa = T(x)a$. Now $\ker T$ being a subgroup of C_p must be trivial or equal to C_p, since p is prime. However $\ker T = 1$ is impossible since T is not injective. In fact, C_p is not contained in $\operatorname{Aut}(C_p)$. Hence it follows $\ker T = C_p$ and $T(C_p) = \{id\}$. This means $xa = T(x)a = a$. Since A is a trivial C_p-module it follows $A^G = A$.

5.5. The first cohomology group

If A is a G-module then the explicit form of the 1-cocycles gives that

$$Z^1(G, A) = \{f : G \to A \mid f(xy) = xf(y) + f(x)\}$$
$$B^1(G, A) = \{f : G \to A \mid f(x) = xa - a \text{ for some } a \in A\}$$

The 1-cocycles are also called crossed homomorphisms of G into A. A 1-coboundary is a crossed homomorphism, i.e., $\delta_1\delta_0 = 0$. For the convenience of the reader we repeat the calculation. Let $f = \delta_0(a)(x_1) = x_1a - a$ and compute

$$\begin{aligned}(\delta_1\delta_0)(a)(x, y) &= \delta_1(f)(x, y) = xf(y) - f(xy) + f(x)\\ &= x(ya - a) - (xy)a + a + xa - a\\ &= 0\end{aligned}$$

Hence $(\delta_1\delta_0)(a) = 0$. Let A be a trivial G-module. Then a crossed homomorphism is just a group homomorphism, i.e., $Z^1(G, A) = \operatorname{Hom}(G, A)$, $B^1(G, A) = 0$ and

$$H^1(G, A) = \operatorname{Hom}(G, A)$$

is the set of group homomorphisms from G into A.

REMARK 5.5.1. We want to consider sometimes right G-modules instead of left G-modules. If A is a left $\mathbb{Z}[G]$-module with action $(x, a) \mapsto xa$, then $a * x = xa$ defines a right module action with multiplication $y * x = xy$ in G: $a * (x * y) = (yx)a = y(xa) = (a * x) * y$. Then the definition of 1-cocycles and 1-coboundaries becomes

$$Z^1(G, A) = \{f : G \to A \mid f(x * y) = f(x) * y + f(y)\}$$
$$B^1(G, A) = \{f : G \to A \mid f(x) = a * x - a \text{ for some } a \in A\}$$

PROPOSITION 5.5.2. *Let A be a G-module. There exists a bijection between $H^1(G, A)$ and the set of conjugacy classes of subgroups $H \leq G \ltimes A$ complementary to A in which the conjugacy class of G maps to zero.*

PROOF. There is a bijection between subgroups $H \leq G \ltimes A$ complementary to A and 1-cocycles $h \in Z^1(G, A)$. If H is complementary to A then $H = \tau(G)$ for a section $\tau : G \to G \ltimes A$ for $\pi : G \ltimes A \to G$. Writing $\tau(x) = (x, h(x))$ with $h : G \to A$ we have $H = \{(x, h(x)) \mid x \in G\}$. We want to show that $h \in Z^1(G, A)$. The multiplication in $G \ltimes A$ is given by the usual formula for the semidirect product. Note that this is a right action. Since we write A additively, the formula becomes

$$(x, a)(y, b) = (xy, ay + b)$$

Since $\tau(xy) = \tau(x)\tau(y)$ we have

$$(xy, h(xy)) = (x, h(x))(y, h(y)) = (xy, h(x)y + h(y))$$

so that $h(xy) = h(x)y + h(y)$. The converse is also clear. Moreover two complements are conjugate precisely when their 1-cocycles differ by a 1-coboundary: for $a \in A \leq G \ltimes A$ the set aHa^{-1} consists of all elements of the form

$$(1, a)(x, h(x))(1, -a) = (x, ax - a - h(x))$$

Hence the cosets of $B^1(G, A)$ in $Z^1(G, A)$ correspond to the A-conjugacy classes of complements H in A, or in $G \ltimes A$ since $G \ltimes A = HA$. □

COROLLARY 5.5.3. *All the complements of A in $G \ltimes A$ are conjugate iff $H^1(G, A) = 0$.*

We have the following result on cohomology groups of *finite* groups.

PROPOSITION 5.5.4. *Let G be a finite group and A be a G-module. Then every element of $H^1(G, A)$ has a finite order which divides $|G|$.*

PROOF. Let $f \in Z^1(G, A)$ and $a = \sum_{y \in G} f(y)$. Then $xf(y) - f(xy) + f(x) = 0$. Summing over this formula we obtain

$$\begin{aligned} 0 &= x \sum_{y \in G} f(y) - \sum_{y \in G} f(xy) + f(x) \sum_{y \in G} 1 \\ &= xa - a + |G| f(x) \end{aligned}$$

It follows that $|G|f(x) \in B^1(G, A)$, which implies $|G|Z^1(G, A) \subseteq B^1(G, A)$. Hence $|G|H^1(G, A) = 0$. □

COROLLARY 5.5.5. *Let G be a finite group and A be a finite G-module such that $(|G|, |A|) = 1$. Then $H^1(G, A) = 0$.*

PROOF. We have $|A|f = 0$ for all $f \in C^1(G, A)$. Then the order of $[f] \in H^1(G, A)$ divides $(|G|, |A|) = 1$. Hence the class $[f]$ is trivial. □

REMARK 5.5.6. We have indeed that $H^n(G, A) = 0$ for all $n \in \mathbb{N}$, provided the conditions of the corollary are satisfied.

We shall conclude this section by proving the following result which can be found already in Hilberts book *Die Theorie der algebraischen Zahlkörper* of 1895. It is called Hilbert's Satz 90 and we present a generalization of it due to Emmy Noether.

PROPOSITION 5.5.7. *Let L/K be a finite Galois extension with Galois group $G = Gal(L/K)$. Then we have $H^1(G, L^\times) = 1$ and $H^1(G, L) = 0$.*

PROOF. We have to show $Z^1 = B^1$ in both cases. Let $f \in Z^1(G, L^\times)$. This implies $f(\sigma) \neq 0$ for all $\sigma \in G$ since $f : G \to L^\times$. The 1-cocycle condition is, written multiplicatively, $f(\sigma\tau) = f(\sigma)\sigma f(\tau)$ or $\sigma f(\tau) = f(\sigma)^{-1} f(\sigma\tau)$. The 1-coboundary condition is $g(\sigma) = \sigma(a)/a$ for a constant a. By a well known result on the linear independence of automorphisms it follows that there exists a $\beta \in L^\times$ such that

$$\alpha := \sum_{\tau \in G} f(\tau)\tau(\beta) \neq 0$$

It follows that for all $\sigma \in G$

$$\begin{aligned}\sigma(\alpha) &= \sum_{\tau \in G} \sigma(f(\tau))\sigma(\tau(\beta)) = \sum_{\tau \in G} f(\sigma)^{-1} f(\sigma\tau)\sigma\tau(\beta) = f(\sigma)^{-1} \sum_{\tau \in G} f(\tau)\tau(\beta) \\ &= f(\sigma)^{-1}\alpha\end{aligned}$$

It follows $f(\sigma) = \frac{\alpha}{\sigma(\alpha)} = \frac{\sigma(\alpha^{-1})}{\alpha^{-1}}$, hence $f \in B^1(G, L^\times)$.
For the second part, let $f \in Z^1(G, L)$. Since L/K is separable there exists a $\beta \in L$ such that

$$a := \sum_{\tau \in G} \tau(\beta) = Tr_{L/K}(\beta) \neq 0$$

Setting $\gamma = a^{-1}\beta$ we obtain $\sum_{\tau \in G} \tau(\gamma) = 1$ since $\tau(a) = a$ and $\tau(a^{-1}) = a^{-1}$. Let

$$x := \sum_{\tau \in G} f(\tau)\tau(\gamma)$$

Hence we obtain for all $\sigma \in G$

$$\begin{aligned}\sigma(x) &= \sum_{\tau \in G} \sigma(f(\tau))\sigma\tau(\gamma) = \sum_{\tau \in G} f(\sigma\tau)\sigma\tau(\gamma) - f(\sigma)\sigma\tau(\gamma) \\ &= x - f(\sigma)\end{aligned}$$

It follows $f(\sigma) = x - \sigma(x) = \sigma(-x) - (-x)$, hence $f \in B^1(G, L)$. □

REMARK 5.5.8. We have $H^n(G, L) = 0$ for all $n \in \mathbb{N}$, but not $H^n(G, L^\times) = 1$ in general.

5.6. The second cohomology group

Let G be a group and A be an abelian group. We recall the definition of a factor system, written additively for A. A pair of functions (f, T), $f : G \times G \to A$ and $T : G \to \mathrm{Aut}(A)$ is

called factor system to A and G if

$$f(xy,z)+f(x,y)z=f(x,yz)+f(y,z) \tag{5.6}$$

$$T(xy)=T(y)T(x) \tag{5.7}$$

$$f(1,1)=0 \tag{5.8}$$

where $f(x,y)z=T(z)(f(x,y))$. Now let

$$0\to A\xrightarrow{\alpha} E\xrightarrow{\beta} G\to 1$$

be an abelian group extension of A by G. This equippes A with a natural G-module structure. We obtain $T(x)(a)=xa$, or $T(x)(a)=ax$, for $x\in G$ and $a\in A$, which is independent of a transversal function. In fact, the extension induces an (anti)homomorphism $T_\tau : G\to \mathrm{Aut}(A)$ with a transversal function $\tau : G\to E$. Since A is abelian it follows $\gamma_{h(x)}=\mathrm{id}_{|A}$ so that $T_{\tau'}(x)=\gamma_{h(x)}T_\tau(x)=T_\tau(x)$. If we fix T and hence the G-module structure on A, then the set of factor systems $f=(f,T)$ to A and G forms an abelian group with respect to addition: $(f+g)(x,y)=f(x,y)+g(x,y)$. It follows from (5.6) that this group is contained in the group

$$Z^2(G,A)=\{f: G\times G\to A \mid f(y,z)-f(xy,z)+f(x,yz)-f(x,y)z=0\}$$

where we have considered A as a right G-module. One has to rewrite the 2-cocycle condition from Definition 5.3.1 for a right G-module according to Remark 5.5.1. Recall that

$$B^2(G,A)=\{f: G\times G\to A \mid f(x,y)=h(y)-h(xy)+h(x)y\}$$

is a subgroup of $Z^2(G,A)$ and the factor group is $H^2(G,A)$. Indeed, a 2-coboundary is a 2-cocycle. The sum of the following terms equals zero.

$$\begin{aligned} f(y,z)&=h(z)-h(yz)+h(y)z\\ -f(xy,z)&=-h(z)+h(xyz)-h(xy)z\\ f(x,yz)&=h(yz)-h(xyz)+h(x)yz\\ -f(x,y)z&=-h(y)z+h(xy)z-h(x)yz \end{aligned}$$

THEOREM 5.6.1. *Let G be a group and A be an abelian group, and let M denote the set of group extensions*

$$0\to A\xrightarrow{\alpha} E\xrightarrow{\beta} G\to 1$$

with a given G-module structure on A. Then there is a $1-1$ correspondence between the set of equivalence classes of extensions of A by G contained in M with the elements of $H^2(G,A)$. The class of split extensions in M corresponds to the class $[0]\in H^2(G,A)$. This class corresponds to the trivial class represented by the trivial factor system $f(x,y)=0$.

PROOF. By Schreier's theorem the set of equivalence classes of such extensions is in bijective correspondence with the equivalence classes of factor systems $f\in Z^2(G,A)$. Two factor systems are equivalent if and only if they differ by a 2-coboundary in $B^2(G,A)$, so we have

$$f_{\tau'}(x,y)=f_\tau(x,y)-h(xy)+h(x)y+h(y)$$

Note that there is exactly one normalized 2-cocycle in each cohomology class, i.e., with $f(1,1)=0$. Hence two extensions of A by G contained in M are equivalent if and only if they determine the same element of $H^2(G,A)$. □

EXAMPLE 5.6.2. *Let $A=\mathbb{Z}/p\mathbb{Z}$ be a trivial $G=C_p$-module. Then*

$$H^2(G,A)\cong\mathbb{Z}/p\mathbb{Z}.$$

Here p is a prime. There are exactly p equivalence classes of extensions

$$0 \to \mathbb{Z}/p\mathbb{Z} \xrightarrow{\alpha} E \xrightarrow{\beta} C_p \to 1$$

EXAMPLE 5.6.3. *Consider the Galois extension $L/K = \mathbb{C}/\mathbb{R}$ with Galois group $G = Gal(\mathbb{C}/\mathbb{R}) \cong C_2$. Then we have*

$$H^2(G, L^\times) \cong \mathbb{Z}/2\mathbb{Z}$$

The proof is left as an exercise. In general we have $H^2(G, L^\times) \cong Br(L/K)$, where $Br(L/K)$ is the relative Brauer group. It consists of equivalence classes of central simple K-algebras S such that $S \otimes_K L \cong M_n(L)$. Two central simple K-algebras are called equivalent if their skew-symmetric components are isomorphic. For any field K the equivalence classes of finite-dimensional central simple K-algebras form an abelian group with respect to the multiplication induced by the tensor product.
The group $Br(\mathbb{C}/\mathbb{R})$ consists of two equivalence classes. The matrix algebra $M_2(\mathbb{R})$ represents the class [0] and the real quaternion algebra $\mathbb{H}$ represents the class [1].
We will now generalize Proposition 5.5.4.

PROPOSITION 5.6.4. *Let G be a finite group and A be a G-module. Then every element of $H^n(G, A)$, $n \in \mathbb{N}$, has a finite order which divides $|G|$.*

PROOF. Let $f \in C^n(G, A)$ and denote

$$a(x_1, \dots, x_{n-1}) = \sum_{y \in G} f(x_1, \dots, x_{n-1}, y)$$

Summing the formula for δf and using

$$\sum_{y \in G} f(x_1, \dots, x_{n-1}, x_n y) = a(x_1, \dots, x_{n-1})$$

we obtain

$$\begin{aligned}\sum_{y \in G} (\delta f)(x_1, \dots, x_n, y) &= x_1 a(x_2, \dots, x_n) \\ &+ \sum_{i=1}^{n-1} (-1)^i a(x_1, \dots, x_i x_{i+1}, \dots, x_n) + (-1)^n a(x_1, \dots, x_{n-1}) \\ &+ (-1)^{n+1} |G| f(x_1, \dots, x_n) \\ &= (\delta a)(x_1, \dots, x_n) + (-1)^{n+1} |G| f(x_1, \dots, x_n)\end{aligned}$$

Hence if $\delta f = 0$, then $|G| f(x_1, \dots, x_n) = \pm(\delta a)(x_1, \dots, x_n)$ is an element of $B^n(G, A)$. Then $|G| Z^n(G, A) \subseteq B^n(G, A)$, so that $|G| H^n(G, A) = 0$. □

COROLLARY 5.6.5. *Let G be a finite group and A be a finite G-module such that $(|G|, |A|) = 1$. Then $H^n(G, A) = 0$ for all $n \geq 1$. In particular, $H^2(G, A) = 0$. Hence any extension of A by G is split.*

The last part is a special case of the Schur-Zassenhaus theorem. We will sketch the proof of the general case.

SCHUR-ZASSENHAUS 5.6.6. *If n and m are relatively prime, then any extension $1 \to A \xrightarrow{\alpha} E \xrightarrow{\beta} G \to 1$ of a group A of order n by a group G of order m is split.*

PROOF. If A is abelian, the extensions are classified by the groups $H^2(G,A)$, one group for every G-module structure on A. These are all zero, hence any extension of A by G is split.
In the general case we use induction on n. It suffices to prove that E contains a subgroup S of order m. Such a subgroup must be isomorphic to G under $\beta : E \to G$. For, if S is such a subgroup, then $S \cap A$ is a subgroup whose order divides $|S| = m$ and $|A| = n$. Then $S \cap A = 1$. Also $AS = E$ since $\alpha(A) = A$ is normal in E so that AS is a subgroup whose order is divided by $|S| = m$ and $|A| = n$ and so is a multiple of $nm = |E|$. It follows that E is a semidirect product and hence the extension of A by G is split.
Choose a prime p dividing n and let P be a p-Sylow subgroup of A, hence of E. Let Z be the center of P. It is well known that $Z \neq 1$, see [**3**], p. 75. Let N be the normalizer of Z in E. A counting argument shows that $AN = E$ and $|N/(A \cap N)| = m$, see [**4**]. Hence there is an extension $1 \to (A \cap N) \to N \to G \to 1$. If $N \neq E$, this extension splits by induction, so there is a subgroup of N, and hence of E, isomorphic to G. If $N = E$, then $Z \lhd E$ and the extension $1 \to A/Z \to E/Z \to G \to 1$ is split by induction. Let G' be a subgroup of E/Z isomorphic to G and let E' denote the set of all $x \in E$ mapping onto G'. Then E' is a subgroup of E, and $0 \to Z \to E' \to G' \to 1$ is an extension. As Z is abelian, the extension splits and there is a subgroup of E', hence of E, isomorphic to $G' \cong G$. □

5.7. The third cohomology group

We have seen that $H^n(G,A)$ for $n = 0, 1, 2$ have concrete group-theoretic interpretations. It turns out that this is also the case for $n \geq 3$. We will briefly discuss the case $n = 3$, which is connected to so called crossed modules. Such modules arise also naturally in topology.

DEFINITION 5.7.1. Let E and N be groups. A *crossed module* (N, α) over E is a group homomorphism $\alpha\colon N \to E$ together with an action of E on N, denoted by $(e,n) \mapsto {}^e n$ satisfying

$$ {}^{\alpha(m)}n = m\,n\,m^{-1} \tag{5.9} $$

$$ \alpha({}^e n) = e\,\alpha(n)\,e^{-1} \tag{5.10} $$

for all $n, m \in N$ and all $e \in E$.

EXAMPLE 5.7.2. *Let $E = \mathrm{Aut}(N)$ and $\alpha(n)$ be the inner automorphism associated to n. Then (N, α) is a crossed module over E.*

By definition we have ${}^{\alpha(m)}n = \alpha(m)(n) = m\,n\,m^{-1}$ and

$$\begin{aligned} \alpha({}^e n)(m) &= \alpha(e(n))(m) = e(n)me(n)^{-1} = e(ne^{-1}(m)n^{-1}) = e(\alpha(n)(e^{-1}(m))) \\ &= (e\alpha(n)e^{-1})(m) \end{aligned}$$

EXAMPLE 5.7.3. *Any normal subgroup $N \lhd E$ is a crossed module with E acting by conjugation and α being the inclusion.*

Let (N, α) be a crossed module over E and $A := \ker \alpha$. Then the sequence $0 \to A \xrightarrow{i} N \xrightarrow{\alpha} E$ is exact. Since $\operatorname{im} \alpha$ is normal in E by (5.10) $G = \operatorname{coker}(\alpha)$ is a group. This means that the sequence $N \xrightarrow{\alpha} E \xrightarrow{\pi} G \to 1$ is exact. Since A is central in N by (5.9), and since the action of E on N induces an action of G on A, we obtain a 4-term exact sequence

$$ 0 \to A \xrightarrow{i} N \xrightarrow{\alpha} E \xrightarrow{\pi} G \to 1 \tag{5.11} $$

where A is a G-module. It turns out that equivalence classes of exact sequences of this form are classified by the group $H^3(G,A)$. Let us explain the equivalence relation. Let G be an

arbitrary group and A be an arbitrary G-module. Consider all possible exact sequences of the form (5.11), where N is a crossed module over E such that the action of E on N induces the given action of G on A. We take on these exact sequences the smallest equivalence relation such that two exact sequences as shown below are equivalent whenever their diagram is commutative:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & N & \xrightarrow{\alpha} & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & A & \longrightarrow & N' & \xrightarrow{\alpha'} & E' & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

Note that f and g need not be isomorphisms. We then have:

THEOREM 5.7.4. *There is a $1-1$ correspondence between equivalence classes of crossed modules represented by sequences as above and elements of $H^3(G, A)$.*

We omit the proof, which can be found in [**9**], Theorem 6.6.13.

5.8. Inflation, restriction and the cup product

DEFINITION 5.8.1. Let G be a group, H a subgroup and M be an H-module. Let

$$\mathrm{Ind}_H^G(M) = \{\varphi\colon G \to M \mid \varphi(hg) = h\varphi(g) \text{ for all } h \in H, g \in G\}$$

Then $\mathrm{Ind}_H^G(M)$ becomes a G-module with the operations

$$(\varphi + \varphi')(x) = \varphi(x) + \varphi'(x)$$
$$(g\varphi)(x) = \varphi(xg)$$

Indeed, $(g, \varphi) \mapsto g\varphi$ defines an action since $(g'g)\varphi = g'(g\varphi)$:

$$((g'g)\varphi)(x) = \varphi(xg'g) = (g\varphi)(xg') = (g'(g\varphi))(x)$$

A homomorphism $\alpha\colon M \to N$ of H-modules defines a homomorphism

$$\alpha_*\colon \mathrm{Ind}_H^G(M) \to \mathrm{Ind}_H^G(N)$$

of G-modules by $\alpha_*(\varphi) = \alpha \circ \varphi$. Hence $\mathrm{Ind}_H^G\colon \mathcal{M}_H \to \mathcal{M}_G$ is a functor.

DEFINITION 5.8.2. A G-module is said to be *induced* if it is isomorphic to $\mathrm{Ind}_1^G(A) = \{\varphi\colon G \to A\}$ for some abelian group A.

Often these modules are called *coinduced*, and denoted by CoInd. Note that the maps φ are just maps, not necessarily homomorphisms. We have $\mathrm{Ind}_H^G(M) = \mathrm{Hom}_H(\mathbb{Z}[G], M)$, where $\mathbb{Z}[G]$ is an H-module as well, with its canonical G-action, and the action of G on an H-module homomorphism $\varphi\colon \mathbb{Z}[G] \to M$ is given by $(\sigma\varphi)(g) := \varphi(g.\sigma)$ for a basis element g of $\mathbb{Z}[G]$.

LEMMA 5.8.3. *For any G-module M and H-module N we have*

$$\mathrm{Hom}_G(M, \mathrm{Ind}_H^G(N)) \cong \mathrm{Hom}_H(M, N)$$

Moreover the functor $\mathrm{Ind}_H^G\colon \mathcal{M}_H \to \mathcal{M}_G$ is exact.

PROOF. Given a G-homomorphism $\alpha\colon M \to \mathrm{Ind}_H^G(N)$, we define $\beta\colon M \to N$ by $\beta(m) = \alpha(m)(1)$, where 1 is the identity in G. Then we have for any $g \in G$

$$\beta(gm) = (\alpha(gm))(1) = (g\alpha(m))(1) = \alpha(m)(g \cdot 1) = \alpha(m)(g)$$

because α is a G-homomorphism and $\alpha(m) \in \mathrm{Ind}_H^G(N)$. Hence for $h \in H$

$$\beta(hm) = \alpha(m)(h) = h(\alpha(m)(1) = h(\beta(m))$$

so that $\beta \in \mathrm{Hom}_H(M, N)$. Conversely, given such a β we define $\alpha\colon M \to \mathrm{Ind}_H^G(N)$ such that $\alpha(m)(g) = \beta(gm)$. It follows similarly that α is a G-homomorphism. These correspondences yield the desired isomorphism of the first part. Given an exact sequence of H-modules

$$0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0$$

we have to prove that the sequence of G-modules

$$0 \to \mathrm{Ind}_H^G(M) \xrightarrow{\alpha_*} \mathrm{Ind}_H^G(N) \xrightarrow{\beta_*} \mathrm{Ind}_H^G(P) \to 0$$

is exact. Let $\varphi \in \mathrm{Ind}_H^G(M)$ and $\alpha_*(\varphi) = \alpha \circ \varphi = 0$. Since α is injective we have $\varphi = 0$, so that α_* is injective. Furthermore $(\beta_*\alpha_*)(\varphi) = \beta \circ \alpha \circ \varphi = 0$ since $\beta \circ \alpha = 0$. Hence $\beta_*\alpha_* = 0$ and $\mathrm{im}\,\alpha_* \subset \ker \beta_*$.
Conversely let $\psi \in \ker \beta_*$, i.e., $\beta_*(\psi) = \beta \circ \psi = 0$. For all $g \in G$ there is an $m \in M$ such that $\psi(g) = \alpha(m)$, because $\psi(g) \in \ker \beta \subset \mathrm{im}\,\alpha$. Define a map $\varphi\colon G \to M$ by $\varphi(g) = m$. This is well defined, since α is injective. Furthermore $\psi = \alpha \circ \varphi = \alpha_*(\varphi)$. We have to show that $\varphi \in \mathrm{Ind}_H^G(M)$, and hence $\psi \in \mathrm{im}\,\alpha_*$. Then $\ker \beta_* \subset \mathrm{im}\,\alpha_*$ and it follows the exactness at $\mathrm{Ind}_H^G(N)$. Since $\psi \in \mathrm{Ind}_H^G(N)$ we have

$$\alpha(\varphi(hg)) = \psi(hg) = h\psi(g) = h\alpha(m) = \alpha(hm) = \alpha(h\varphi(g))$$

and hence $\varphi(hg) = h\varphi(g)$, because α is injective. This shows $\varphi \in \mathrm{Ind}_H^G(M)$.
Finally we have to show that β_* is surjective. Let S be a set of right coset representatives for H in G, i.e., $G = \cup_{s\in S} Hs$, and let $\varphi \in \mathrm{Ind}_H^G(P)$. For each $s \in S$, choose an $n(s) \in N$ mapping under β to $\varphi(s) \in P$, and define $\widetilde{\varphi}(hs) = h{\cdot}n(s)$. Then $\widetilde{\varphi} \in \mathrm{Ind}_H^G(N)$ and $\beta_*(\widetilde{\varphi}) = \beta \circ \widetilde{\varphi} = \varphi$. □

THEOREM 5.8.4 (Shapiro's Lemma). *Let G be a group and H be a subgroup of G. For any H-module N and all $r \geq 0$, there is a canonical isomorphism*

$$H^r(G, \mathrm{Ind}_H^G(N)) \cong H^r(H, N)$$

PROOF. For $r = 0$, the isomorphism is the composite of the following isomorphisms:

$$N^H \cong \mathrm{Hom}_H(\mathbb{Z}, N) \cong \mathrm{Hom}_G(\mathbb{Z}, \mathrm{Ind}_H^G(N)) \cong \mathrm{Ind}_H^G(N)^G$$

The second isomorphism follows from Lemma 5.8.3. $\mathbb{Z}$ is regarded as a trivial module. Now choose an injective resolution $N \to I^\bullet$ of N. By applying the functor Ind_H^G, we obtain an injective resolution $\mathrm{Ind}_H^G(N) \to \mathrm{Ind}_H^G(I^\bullet)$ of the G-module $\mathrm{Ind}_H^G(N)$, because Ind_H^G is exact and preserves injectives. Hence

$$H^r(G, \mathrm{Ind}_H^G(N)) = H^r((\mathrm{Ind}_H^G(I^\bullet))^G) = H^r(I^{\bullet H}) = H^r(H, N)$$

□

COROLLARY 5.8.5. *If M is an induced G-module, then $H^n(G, M) = 0$ for all $n \geq 1$.*

PROOF. If $M = \mathrm{Ind}_1^G(A)$, then $H^n(G, M) = H^n(\{1\}, A) = 0$. □

COROLLARY 5.8.6. *Let L/K be a finite Galois extension and $G = Gal(L/K)$. Then $H^n(G, L) = 0$ for all $n \geq 1$.*

Recall that $H^n(G, L^\times)$ in general need not be trivial.

PROOF. By the normal basis theorem there exists an $\alpha \in L$ such that $\{\sigma\alpha \mid \sigma \in G\}$ is a basis (a "normal" basis) for L as a K-vector space. This means, L is isomorphic to $K[G]$ as a G-module. But $K[G] = \operatorname{Ind}_1^G K$, and hence $H^n(G, L) = H^n(\{1\}, K) = 0$. □

If $\alpha\colon M \to N$ is a homomorphism of G-modules, then it induces a homomorphism

$$H^n(G, M) \to H^n(G, N)$$

of cohomology groups. This can be generalized as follows.

DEFINITION 5.8.7. Let M be a G-module and N be a G'-module. Two homomorphisms $\alpha\colon G' \to G$ and $\beta\colon M \to N$ are said to be *compatible* if

$$\beta(\alpha(g')m) = g'\beta(m) \quad \forall\, g' \in G', m \in M$$

In this case M becomes a G'-module by $g'm = \alpha(g')m$ such that $\beta\colon M \to N$ becomes a homomorphism of G'-modules. Furthermore the map

$$(\alpha, \beta)\colon C^\bullet(G, M) \to C^\bullet(G', N)$$

given by $\varphi \mapsto \beta\circ\varphi\circ\alpha^n$ defines a homomorphism of complexes. It commutes with the coboundary operators, so that it induces a homomorphism of cohomology groups

$$(\alpha, \beta)\colon H^n(G, M) \to H^n(G', N).$$

EXAMPLE 5.8.8. *Let H be a subgroup of G and $\alpha\colon H \hookrightarrow G$ be the inclusion map. For any H-module N let $\beta\colon \operatorname{Ind}_H^G(N) \to N$ be the map defined by $\beta(\varphi) = \varphi(1)$. Then α and β are compatible:*

$$\beta(\alpha(h)\varphi) = \beta(h\varphi) = h\beta(\varphi)$$

The induced homomorphism

$$H^n(G, \operatorname{Ind}_H^G(N)) \to H^n(H, N)$$

is precisely the isomorphism in Shapiro's Lemma.

Similarly, if H is a subgroup of G, $\alpha\colon H \hookrightarrow G$ is the inclusion map and $\beta\colon M \to M$ is the identity, both maps are compatible:

DEFINITION 5.8.9. The induced homomorphisms are called the *restriction homomorphisms*

$$\operatorname{Res}\colon H^n(G, M) \to H^n(H, M)$$

These homomorphisms can also be constructed as follows: let $\varphi_m(g) = gm$. Then $\varphi_m \in \operatorname{Ind}_H^G(M)$ and $\varphi\colon M \to \operatorname{Ind}_H^G(M)$, $m \mapsto \varphi_m$ is a homomorphism of G-modules. Denote by $\widetilde{\varphi}\colon H^n(G, M) \to H^n(G, \operatorname{Ind}_H^G(M))$ the induced homomorphism of cohomology groups. Let $\psi\colon H^n(G, \operatorname{Ind}_H^G(M)) \to H^n(H, M)$ be the isomorphism in Shapiro's Lemma. Then we have

$$\operatorname{Res} = \psi \circ \widetilde{\varphi}$$

Let H be a normal subgroup of G, $\alpha\colon G \to G/H$ be the quotient map and $\beta\colon M^H \hookrightarrow M$ be the inclusion. Then α and β are compatible:

DEFINITION 5.8.10. The induced homomorphisms are called the *inflation homomorphisms*

$$\operatorname{Inf}\colon H^n(G/H, M^H) \to H^n(G, M)$$

There is the following inflation-restriction exact sequence.

THEOREM 5.8.11. *Let G be a group, H be a normal subgroup of G and M be a G-module. Let $n \in \mathbb{N}$. Assume that $H^r(H, M) = 0$ for all r with $1 \leq r < n$. Then the following sequence is exact.*

$$0 \to H^n(G/H, M^H) \xrightarrow{\text{Inf}} H^n(G, M) \xrightarrow{\text{Res}} H^n(H, M)$$

For $n = 1$ the hypothesis on $H^r(H, M)$ is vacuous, so that we always have

$$0 \to H^1(G/H, M^H) \xrightarrow{\text{Inf}} H^1(G, M) \xrightarrow{\text{Res}} H^1(H, M) \tag{5.12}$$

PROOF. Let $n = 1$. We will show that Inf is injective and $\operatorname{im}\text{Inf} = \ker\text{Res}$. Let $\varphi\colon G/H \to M^H$ be a 1-cocycle and $\varphi' = \text{Inf}\varphi$. Then φ' is a 1-cocycle in $H^1(G, M)$ via $G \to G/H \xrightarrow{\varphi} M^H \to M$. Suppose that the class of φ' is trivial, i.e., φ' is a 1-coboundary. Then $\varphi'(g) = gm - m$ for some $m \in M$. Hence $gm - m = ghm - m$ for all $h \in H$, so that $m = hm$ for all $h \in H$, i.e., $m \in M^H$. But then $\varphi(gH) = gHm - m$ is a 1-coboundary in $H^1(G/H, M^H)$ and the class of φ is zero. It follows that Inf is injective. Similarly we see that $\operatorname{im}\text{Inf} = \ker\text{Res}$. For $n > 1$ the result can be proved by induction. □

EXAMPLE 5.8.12. *Let Ω/K and L/K be finite Galois extension with $L \subset \Omega$. Then $H := Gal(\Omega/L)$ is a normal subgroup of $G := Gal(\Omega/K)$, and with $M = \Omega^\times$ we have $M^H = L^\times$. Since we have $H^1(H, \Omega^\times) = 1$, there is an exact sequence*

$$1 \to H^2(G/H, L^\times) \to H^2(G, \Omega^\times) \to H^2(H, \Omega^\times)$$

REMARK 5.8.13. The cohomology groups $H^n(H, M)$ can be equipped with a G-module structure, such that H acts trivially on it. Then $H^n(H, M)$ becomes a G/H-module and it is not difficult to show that the image of $H^n(G, M)$ under Res actually lies in $H^n(H, M)^{G/H}$. Then (5.12) can be extended to the following special case of of the *Hochschild-Serre spectral sequence*

$$\begin{aligned} 0 \to H^1(G/H, M^H) &\xrightarrow{\text{Inf}} H^1(G, M) \xrightarrow{\text{Res}} H^1(H, M)^{G/H} \\ &\to H^2(G/H, M^H) \xrightarrow{\text{Inf}} H^2(G, M) \end{aligned}$$

The result for $n \geq 1$ here is as follows:

THEOREM 5.8.14. *Let G be a group, H be a normal subgroup of G and M be a G-module. Let $n \geq 1$ be an integer and assume that that $H^r(H, M) = 0$ for all r with $1 \leq r < n$. Then there is a natural map*

$$\tau_{n,M}\colon H^n(H, M)^{G/H} \to H^{n+1}(G/H, M^H)$$

fitting into the following exact sequence:

$$\begin{aligned} 0 \to H^n(G/H, M^H) &\xrightarrow{\text{Inf}} H^n(G, M) \xrightarrow{\text{Res}} H^n(H, M)^{G/H} \xrightarrow{\tau_{n,M}} \\ &\to H^{n+1}(G/H, M^H) \xrightarrow{\text{Inf}} H^{n+1}(G, M). \end{aligned}$$

Among many possible topics within techniques from group cohomology we want to mention the *cup-product* (see [**5**]). We will assume that G is a group and A, B are G-modules. A cup-product is an associative product operation

$$\begin{aligned} H^i(G, A) \times H^j(G, B) &\to H^{i+j}(G, A \otimes B), \\ (a, b) &\mapsto a \cup b, \end{aligned}$$

which is graded-commutative, i.e., it satisfies

$$a \cup b = (-1)^{ij}(b \cup a).$$

Here $A \otimes B = A \otimes_{\mathbb{Z}} B$ is the tensor product of A and B over the commutative ring $\mathbb{Z}$, equipped with the G-module structure given by

$$g.(a \otimes b) = g.a \otimes g.b$$

for $g \in G$, $a \in A$ and $b \in B$. Note that in general this is different from the tensor product of A and B over the group ring $\mathbb{Z}[G]$. We begin with a construction of the cup-product with the **first step** as follows: let $A^\bullet$ and $B^\bullet$ be complexes of abelian groups, i.e.,

$$\cdots \to A^{i-1} \xrightarrow{\partial_A^{i-1}} A^i \xrightarrow{\partial_A^i} A^{i+1} \to \cdots,$$

and similarly for $B^\bullet$. Then we define the *tensor product complex* $A^\bullet \otimes B^\bullet$ by first considering the double complex

$$\begin{array}{ccccccc}
 & & \vdots & & \vdots & & \vdots \\
 & & \uparrow & & \uparrow & & \uparrow \\
\cdots & \longrightarrow & A^{i-1} \otimes B^{j+1} & \longrightarrow & A^i \otimes B^{j+1} & \longrightarrow & A^{i+1} \otimes B^{j+1} \longrightarrow \cdots \\
 & & \uparrow & & \uparrow & & \uparrow \\
\cdots & \longrightarrow & A^{i-1} \otimes B^{j} & \longrightarrow & A^i \otimes B^{j} & \longrightarrow & A^{i+1} \otimes B^{j} \longrightarrow \cdots \\
 & & \uparrow & & \uparrow & & \uparrow \\
\cdots & \longrightarrow & A^{i-1} \otimes B^{j-1} & \longrightarrow & A^i \otimes B^{j-1} & \longrightarrow & A^{i+1} \otimes B^{j-1} \longrightarrow \cdots \\
 & & \uparrow & & \uparrow & & \uparrow \\
 & & \vdots & & \vdots & & \vdots
\end{array}$$

where the horizontal maps are given by

$$\partial^h_{i,j} = \partial^i_A \otimes \mathrm{id} \colon A^i \otimes B^j \to A^{i+1} \otimes B^j,$$
$$a \otimes b \mapsto \partial^i_A(a) \otimes b,$$

and the vertical maps are given by

$$\partial^v_{i,j} = \mathrm{id} \otimes (-1)^i \partial^j_B \colon A^i \otimes B^j \to A^i \otimes B^{j+1},$$
$$a \otimes b \mapsto a \otimes (-1)^i \partial^j_B(b).$$

The above squares *anticommute*, i.e., one has

$$\partial^h_{i,j+1} \circ \partial^v_{i,j} = -\partial^v_{i+1,j} \circ \partial^h_{i,j}.$$

Now take the total complex associated with this double complex. This is, by definition, the complex $T^\bullet$ with

$$T^n = \bigoplus_{i+j=n} A^i \otimes B^j$$

and $\partial^n \colon T^n \to T^{n+1}$ given on the component $A^i \otimes B^j$ by $\partial^h_{i,j} + \partial^v_{i,j}$. The above anticommutativity then implies $\partial^{n+1} \circ \partial^n = 0$, i.e., that $T^\bullet$ is really a complex. We define this $T^\bullet$ to be the *tensor product of $A^\bullet$ and $B^\bullet$*, and denote it as above by $A^\bullet \otimes B^\bullet$.

This enables us to proceed to the **second step** of the cup-product construction. In addition to the situation before, assume further given abelian groups A and B. Then we have the complex $\mathrm{Hom}(A^\bullet, A)$ whose degree i term is $\mathrm{Hom}(A^{-i}, A)$ and whose differentials are those induced by the differentials of $A^\bullet$. In the same way we have the complex $\mathrm{Hom}(B^\bullet, B)$. We construct a product operation

$$H^i(\mathrm{Hom}(A^\bullet, A)) \times H^j(\mathrm{Hom}(B^\bullet, B)) \to H^{i+j}(\mathrm{Hom}(A^\bullet \otimes B^\bullet, A \otimes B)) \tag{5.13}$$

as follows. Given homomorphisms of abelian groups $\alpha\colon A^{-i} \to A$ and $\beta\colon B^{-j} \to B$ with $i + j = n$, the tensor product $\alpha \otimes \beta$ is a homomorphism

$$\alpha \otimes \beta\colon A^{-i} \otimes B^{-j} \to A \otimes B,$$

and hence defines an element of the degree $(i+j)$ term in $\mathrm{Hom}(A^\bullet \otimes B^\bullet, A \otimes B)$ via the diagonal embedding

$$\mathrm{Hom}(A^{-i} \otimes B^{-j}, A \otimes B) \to \mathrm{Hom}\left(\bigoplus_{k+l=i+j} A^{-k} \otimes B^{-l}, A \otimes B\right).$$

Here if $\alpha \in Z^i(\mathrm{Hom}(A^\bullet, A))$ and $\beta \in Z^j(\mathrm{Hom}(B^\bullet, B))$, then by construction of $A^\bullet \otimes B^\bullet$ we have

$$\alpha \otimes \beta \in Z^{i+j}(\mathrm{Hom}(A^\bullet \otimes B^\bullet, A \otimes B)).$$

Moreover, if $\alpha \in B^i(\mathrm{Hom}(A^\bullet, A))$, then $\alpha \otimes \beta \in Z^{i+j}(\mathrm{Hom}(A^\bullet \otimes B^\bullet, A \otimes B))$. The same follows if $\beta \in B^j(\mathrm{Hom}(B^\bullet, B))$. This defines the required map (5.13).

If in this construction all abelian groups carry a G-module structure for some group G and G-(module)-homomorphisms α and β, then also $\alpha \otimes \beta$ is a G-homomorphism, hence by restricting to G-homomorphisms the product (5.13) induces a product

$$H^i(\mathrm{Hom}_G(A^\bullet, A)) \times H^j(\mathrm{Hom}_G(B^\bullet, B)) \to H^{i+j}(\mathrm{Hom}_G(A^\bullet \otimes B^\bullet, A \otimes B)),$$

where $A \otimes B$ and $A^\bullet \otimes B^\bullet$ are endowed with the G-module structure defined before.

For the next step we need the following proposition. Recall that the lower numbering in a projective resolution $P_\bullet$ is defined by $P_i := P^{-i}$.

PROPOSITION 5.8.15. *Let G be a group, and let $P_\bullet$ be a complex of G-modules which is a projective resolution of the trivial G-module $\mathbb{Z}$. Then $P_\bullet \otimes P_\bullet$ is a projective resolution of the trivial $\mathbb{Z}[G \times G]$-module $\mathbb{Z}$.*

Here the terms of $P_\bullet \otimes P_\bullet$ are endowed by a $G \times G$-action coming from

$$(g_1, g_2)(p_1 \otimes p_2) = g_1.p_1 \otimes g_2.p_2$$

The proof is based on the following lemma. Recall that a complex $A^\bullet$ is called *acyclic* or *exact*, if $H^i(A^\bullet) = 0$ for all i.

LEMMA 5.8.16. *Let $A^\bullet$ and $B^\bullet$ be complexes of free abelian groups. Then the following holds.*

1. *$A^\bullet \otimes B^\bullet$ is again a complex of free abelian groups.*
2. *If $A^\bullet$ and $B^\bullet$ are acyclic, then so is the complex $A^\bullet \otimes B^\bullet$.*

(3) *If $A^\bullet$ and $B^\bullet$ are concentrated in nonpositive degree, acyclic in negative degrees and having a free abelian group as 0-cohomology, then so is the complex $A^\bullet \otimes B^\bullet$, and in addition*

$$H^0(A^\bullet \otimes B^\bullet) \simeq H^0(A^\bullet) \otimes H^0(B^\bullet).$$

PROOF. (1): As tensor products and direct sums of free abelian groups are again free, it follows that the terms of $A^\bullet \otimes B^\bullet$ are free abelian.

(2): The proof of acyclicity is based on the fact that a subgroup of a free abelian group is again free. This implies that for all i, the subgroups $B^i(A^\bullet)$ are free, and in particular projective. For all i we have the exact sequence

$$0 \to Z^i(A^\bullet) \to A^i \to B^{i+1}(A^\bullet) \to 0,$$

the terms being free abelian groups. Hence the sequence splits. Moreover, we have $Z^i(A^\bullet) = B^i(A^\bullet)$ by the acyclicity of $A^\bullet$. Therefore we may rewrite the above exact sequence as

$$0 \to B^i(A^\bullet) \xrightarrow{\mathrm{id}} B^i(A^\bullet) \oplus B^{i+1}(A^\bullet) \xrightarrow{(0,\mathrm{id})} B^{i+1}(A^\bullet) \to 0.$$

Hence the complex $A^\bullet$ decomposes as an infinite direct sum of complexes of the shape

$$\cdots \to 0 \to 0 \to A \xrightarrow{\mathrm{id}} A \to 0 \to 0 \to \cdots$$

and similarly, the complex $B^\bullet$ decomposes as a direct sum of complexes

$$\cdots \to 0 \to 0 \to B \xrightarrow{\mathrm{id}} B \to 0 \to 0 \to \cdots$$

The construction of tensor products of complexes commutes with arbitrary direct sums. Hence we are reduced to check acyclicity for the tensor product of complexes of the above type. But by definition, these are complexes of the form

$$\cdots \to 0 \to 0 \to A \otimes B \xrightarrow{(\mathrm{id},\pm\mathrm{id})} (A \otimes B) \oplus (A \otimes B) \xrightarrow{(0,\pm\mathrm{id})} A \otimes B \to 0 \to 0 \to \cdots$$

Therefore the claim follows.

(3): The proof goes along the same lines as for (2), and the description of the 0-cohomology follows from the right exactness of the tensor product. □

Proof of Proposition 5.8.15: By definition, the P_i are direct summands in some free G-module, which is in particular a free abelian group, so they are also free abelian groups. Hence we can use (3) of lemma 5.8.16, and we are done if we show that the terms of $P_\bullet \otimes P_\bullet$ are projective as $\mathbb{Z}[G \times G]$-modules. For this, notice first the canonical isomorphism

$$\mathbb{Z}[G \times G] \simeq \mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}[G] :$$

indeed, both abelian groups are free on a basis corresponding to pairs of elements in G. Taking direct sums we obtain that tensor products of free $\mathbb{Z}[G]$-modules are free $\mathbb{Z}[G \times G]$-modules with the above $G \times G$-action. If P_i resp. P_j are projective $\mathbb{Z}[G]$-modules with a direct complement Q_i resp. Q_j in some free $\mathbb{Z}[G]$-module, then the isomorphism

$$(P_i \oplus Q_i) \otimes (P_j \oplus Q_j) \simeq (P_i \otimes P_j) \oplus (P_i \otimes Q_j) \oplus (Q_i \otimes P_j) \oplus (Q_i \otimes Q_j)$$

shows that $P_i \otimes P_j$ is a direct summand in a free $\mathbb{Z}[G \times G]$-module, and hence it is projective. Then the projectivity of the terms of $P_\bullet \otimes P_\bullet$ follows. □

Putting everything together, we can finally construct the cup-product.

Third step: Let A and B be G-modules, and $P_\bullet$ be a projective resolution of the trivial G-module $\mathbb{Z}$. Applying the second step with $A^\bullet = B^\bullet = P_\bullet$ we obtain maps

$$H^i(\mathrm{Hom}(P_\bullet, A)) \times H^j(\mathrm{Hom}(P_\bullet, B)) \to H^{i+j}(P_\bullet \otimes P_\bullet, A \otimes B)).$$

By proposition 5.8.15, the complex $P_\bullet \otimes P_\bullet$ is a projective resolution of $\mathbb{Z}$ as a $G \times G$-module. Hence using the definition of cohomology via projective resolutions we may rewrite the above maps as

$$H^i(G, A) \times H^j(G, B) \to H^{i+j}(G \times G, A \otimes B).$$

On the other hand, the diagonal embedding $G \to G \times G$ induces a restriction map

$$\mathrm{Res}\colon H^{i+j}(G \times G, A \otimes B) \to H^{i+j}(G, A \otimes B).$$

Composing the two maps we finally obtain an operation

$$\begin{aligned} H^i(G, A) \times H^j(G, B) &\to H^{i+j}(G, A \otimes B), \\ (a, b) &\mapsto a \cup b. \end{aligned}$$

which we call the **cup-product** map.
One may check that this construction does not depend on the chosen projective resolution $P_\bullet$.

Remark 5.8.17. The construction is functorial in the following sense. For a given morphism $A \to A'$ of G-modules the diagram

$$\begin{array}{ccc} H^i(G, A) \times H^j(G, B) & \longrightarrow & H^{i+j}(G, A \otimes B) \\ \downarrow & & \downarrow \\ H^i(G, A') \times H^j(G, B) & \longrightarrow & H^{i+j}(G, A' \otimes B) \end{array}$$

commutes. Similarly such a diagram for the second variable commutes.

Remark 5.8.18. For $i = j = 0$ the cup-product map

$$H^0(G, A) \times H^0(G, B) \to H^0(G, A \otimes B)$$

is just the natural map $A^G \otimes B^G \to (A \otimes B)^G$. This follows from the construction of the cup-product.

Remark 5.8.19. There is the following generalization of a cup-product, usually again denoted as cup-product. For a given morphism $A \times B \to C$ of G-modules we obtain pairings

$$H^i(G, A) \times H^j(G, B) \to H^{i+j}(G, C)$$

by composing the cup-product with the natural map

$$H^{i+j}(G, A \otimes B) \to H^{i+j}(G, C).$$

Proposition 5.8.20. *The cup-product is associative and graded-commutative.*

Proof. We leave it to the reader to check associativity. One has to follow carefully the construction. It ultimately boils down to the associativity of the tensor product.

For graded-commutativity, we first work on the level of tensor products of complexes and compare the images of the obvious maps

$$A^i \otimes B^j \to \bigoplus_{k+l=i+j} A^k \otimes B^l,$$
$$B^j \otimes A^i \to \bigoplus_{k+l=i+j} B^l \otimes A^k$$

in the complexes $A^\bullet \otimes B^\bullet$ and $B^\bullet \otimes A^\bullet$ respectively. Given $a \otimes b \in A^i \otimes B^j$, the differential in $A^\bullet \otimes B^\bullet$ acts on it by

$$\partial_A^i \otimes \mathrm{id}_B + (-1)^i \mathrm{id}_A \otimes \partial_B^j,$$

whereas the differential in $B^\bullet \otimes A^\bullet$ acts on $b \otimes a \in B^j \otimes A^i$ by

$$\partial_B^j \otimes \mathrm{id}_A + (-1)^j \mathrm{id}_B \otimes \partial_A^i.$$

Therefore mapping $a \otimes b$ to $(-1)^{ij}(b \otimes a)$ induces an isomorphism of complexes $A^\bullet \otimes B^\bullet \simeq B^\bullet \otimes A^\bullet$. Applying this with $A^\bullet = B^\bullet = P_\bullet$ and performing the rest of the construction of the cup-product, we obtain that both elements $a \cup b$ and $(-1)^{ij}(b \cup a)$ are mapped, via the above isomorphism, to the same element in $H^{i+j}(G, A \otimes B)$. □

The following exactness property holds for the cup-product.

PROPOSITION 5.8.21. *Given an short exact sequence of G-modules*

$$0 \to A_1 \to A_2 \to A_3 \to 0 \tag{5.14}$$

with the property that the tensor product over $\mathbb{Z}$ with a G-module B remains exact, i.e., such that

$$0 \to A_1 \otimes B \to A_2 \otimes B \to A_3 \otimes B \to 0 \tag{5.15}$$

is again exact, we have for all elements $a \in H^i(G, A_3)$ and $b \in H^j(G, B)$ the relation

$$\delta(a) \cup b = \delta(a \cup b)$$

in $H^{i+j+1}(G, A_1 \otimes B)$, where the δ are the connecting maps in the associated long sequence of cohomology.
Similarly, if

$$0 \to B_1 \to B_2 \to B_3 \to 0$$

is a short exact sequence of G-modules such that the tensor product over $\mathbb{Z}$

$$0 \to A \otimes B_1 \to A \otimes B_2 \to A \otimes B_3 \to 0$$

with a G-module A remains exact, we have for all elements $a \in H^i(G, A)$ and $b \in H^j(G, B_3)$ the relation

$$a \cup \delta(b) = (-1)^i \delta(a \cup b)$$

in $H^{i+j+1}(G, A \otimes B_1)$.

PROOF. For the first statement, fix an element $b \in H^j(G, B)$. Take a projective resolution $P_\bullet$ of the trivial G-module $\mathbb{Z}$ and consider the sequences

$$0 \to \mathrm{Hom}(P_\bullet, A_1) \to \mathrm{Hom}(P_\bullet, A_2) \to \mathrm{Hom}(P_\bullet, A_3) \to 0 \tag{5.16}$$

and

$$0 \to \mathrm{Hom}(P_\bullet \otimes P_\bullet, A_1 \otimes B) \to \mathrm{Hom}(P_\bullet \otimes P_\bullet, A_2 \otimes B) \to \mathrm{Hom}(P_\bullet \otimes P_\bullet, A_3 \otimes B) \to 0. \tag{5.17}$$

These are exact sequences of complexes because of the projectivity of the P_i and the exactness of the sequences (5.14) and (5.15). Lifting b to an element $\beta \in \mathrm{Hom}(P_j, B)$ and tensor product with β yields maps

$$\mathrm{Hom}(P_j, A_k) \to \mathrm{Hom}(P_i \otimes P_j, A_k \otimes B)$$

for $k = 1, 2, 3$. Hence proceeding as in the second step of the cup-product construction we obtain maps form the terms in the sequence (5.16) to those of the sequence (5.17), increasing degrees by j, giving rise to a commutative diagram by functoriality of the cup-product construction. The connecting maps δ are obtained by applying the so called snake lemma to the above sequences - we leave out the details. Finally one obtains the first statement by following the image of an element $a \in H^i(G, A)$ by using the above mentioned commutativity. Let us say, that the proof of the second statement is similar, except that one has to replace the differentials in the complexes $\mathrm{Hom}^\bullet(P_\bullet, B_k)$ by their multiples by $(-1)^i$ in order to obtain a commutative diagram, by virtue of the sign convention we have taken in the first step of the cup-product construction. □

Let H be a subgroup of G of finite index, and let A be a G-module. We mention briefly the so called *correstriction maps*

$$\mathrm{Cor}\colon H^i(H, A) \to H^i(G, A),\ i \geq 0$$

which are given by taking cohomology and applying Shapiro's lemma. It satisfies the following property.

PROPOSITION 5.8.22. *Let H be a subgroup of G of finite index $n \geq 1$, and let A be a G-module. Then the composite maps*

$$\mathrm{Cor} \circ \mathrm{Res}\colon H^i(G, A) \to H^i(G, A)$$

are given by multiplication by n for all $i \geq 0$.

Given a subgroup H of G, perhaps a normal subgroup, or a subgroup of finite index if needed, the cup-product satisfies the following compatibility relations with the associated restriction maps, inflation maps and corestriction maps.

PROPOSITION 5.8.23. *For given G-modules A and B we have the following relations.*

(1) *For $a \in H^i(G, A)$ and $b \in H^j(G, B)$ we have*

$$\mathrm{Res}(a \cup b) = \mathrm{Res}(a) \cup \mathrm{Res}(b).$$

(2) *If H is normal in G, $a \in H^i(G/H, A^H)$ and $b \in H^j(G/H, B^H)$, then we have*

$$\mathrm{Inf}(a \cup b) = \mathrm{Inf}(a) \cup \mathrm{Inf}(b).$$

(3) *Let H be a subgroup of G of finite index. Then for $a \in H^i(H, A)$ and $b \in H^j(G, B)$ we have*

$$\mathrm{Cor}(a \cup \mathrm{Res}(b)) = \mathrm{Cor}(a) \cup b.$$

This is called the "projection formula".

PROOF. According to the definition of restriction maps, (1) follows by performing the cup-product construction for the modules

$$\mathrm{Ind}_H^G(A) = \mathrm{Hom}_H(\mathbb{Z}[G], A)$$
$$\mathrm{Ind}_H^G(B) = \mathrm{Hom}_H(\mathbb{Z}[G], B),$$

and using the functoriality of the construction for the natural maps $A \to \mathrm{Ind}_H^G(A)$ and $B \to \mathrm{Ind}_H^G(B)$.
Similarly, (2) follows by performing the cup-product construction simultaneously for the projective resolutions $P_\bullet$ and $Q_\bullet$ considered in the definition of inflation maps (a projective resolution $P_\bullet$ of $\mathbb{Z}$ as a trivial G-module and a projective resolution $Q_\bullet$ of $\mathbb{Z}$ as a trivial G/H-module), and using functoriality.
For (3), consider the diagram

$$\begin{array}{ccc} \mathrm{Hom}_H(\mathbb{Z}[G], A) \times \mathrm{Hom}_H(\mathbb{Z}[G], B) & \longrightarrow & \mathrm{Hom}_{H\times H}(\mathbb{Z}[G\times G], A\otimes B) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_G(\mathbb{Z}[G], A) \times \mathrm{Hom}_G(\mathbb{Z}[G], B) & \longrightarrow & \mathrm{Hom}_{G\times G}(\mathbb{Z}[G\times G], A\otimes B) \end{array}$$

where the horizontal maps are induced by the tensor product, the middle vertical map upwards is the one inducing the restriction and the two others are those inducing the correstriction maps. The diagram is "commutative" in the sense that starting form elements in $\mathrm{Hom}_H(\mathbb{Z}[G], A)$ and $\mathrm{Hom}_G(\mathbb{Z}[G], B)$ we obtain the same elements in $\mathrm{Hom}_{G\times G}(\mathbb{Z}[G\times G], A\otimes B)$ by going through the diagram in the two possible ways; this follows from the definition of the maps. The claim then again follows by performing the cup-product construction for the pairings of the two rows of the diagram and using functoriality. □

Bibliography

[1] K. S. Brown: *Cohomology of groups.* Springer Verlag **1982**.

[2] D. Burde: *Commutative Algebra.* Lecture Notes (2009), 1–87.

[3] N. Jacobson: *Basic algebra I.* San Francisco: Freeman and Co. **1974**.

[4] N. Jacobson: *Basic algebra II.* Second Edition. San Francisco: Freeman and Co. **1989**.

[5] P. Gille, T. Szamuely: *Central simple algebras and Galois cohomology.* Cambridge Studies in advanced mathematics 101 **2006**.

[6] J. C. Jantzen, J. Schwermer: *Algebra.* Springer-Verlag (2006).

[7] H. Koch: *Zahlentheorie.* Vieweg-Verlag (1997).

[8] S. Lang: *Algebra.* Revised third edition. Graduate Texts in Mathematics 211. Springer-Verlag, New York, **2002**.

[9] C. A. Weibel: *An introduction to homological algebra.* Cambridge University Press **1997**.