Advanced Algebra: Representation theory and homological algebra

Summer semester 2023

Christoph Schweigert
Universität Hamburg
Fachbereich Mathematik
Bereich Algebra und Zahlentheorie

(Stand: 22.09.2023)

Contents

Literatur:

Some literature I used for the preparation of this lecture:

- Wolfgang Soergel, Lecture notes on algebra (in German), available at
  `http://home.mathematik.uni-freiburg.de/soergel/`
- Jens Carsten Jantzen, Joachim Schwermer: Algebra, Springer, 2006
- Peter J. Hilton, Urs Stammbach: A course in homological algebra, Springer Graduate Texts in Mathematics, 1997
- Kenneth S. Brown: Cohomology of groups, Springer Graduate Texts in Mathematics, 1982
- Charles Weibel, An Introduction to Homological Algebra, Cambridge University Press, 1995
  To fill possible gaps in linear algebra, I recommend [A15].

These lecture notes are the result of lectures that I gave in the winter terms 2008/09, 2010/11, 2013/14 and 2014/15 and the summer terms 2017, 2020 and 2023 at the University of Hamburg. The present version of these lecture notes can be found at
`http://www.math.uni-hamburg.de/home/schweigert/skripten/a2skript.pdf`
Please send corrections and remarks to `christoph.schweigert@uni-hamburg.de`.

I am grateful to Simon Lentner, Catherine Meusburger and Thomas Nikolaus for many remarks on the notes and discussions. I am also grateful to the students in Hamburg for remarks, in particular to Rüdiger Brecht, Max Demirdilek, Pascal Gollin, Alea Hofstetter, Johannes Lederich, David Lindemann, Nils Matthes, Svea-Nora Mierach, Christoph Nehring, Cora Welsch and Jan-Ole Willprecht.

1 Modules over rings

1.1 Foundational definitions

Rings will play a central role in this lecture. We thus recall some concepts:

Definition 1.1.1

1. A ring is an abelian group with group operation denoted additively $(R, +)$, equipped with a map
$$\begin{array}{rcl} R \times R & \to & R \\ (x, y) & \mapsto & xy \equiv x \cdot y \ , \end{array}$$
called multiplication, for which the associative law
$$(xy)z = x(yz) \quad \text{for all } x, y, z \in R$$
and the two distributive laws hold:
$$(x_1 + x_2) \cdot y = x_1 \cdot y + x_2 \cdot y \qquad \text{and} \quad x \cdot (y_1 + y_2) = x \cdot y_1 + x \cdot y_2$$
for all $x, x_1, x_2, y, y_1, y_2 \in R$. Note that $(R, \cdot)$ is an associative monoid. The existence of multiplicative inverses is not required.

2. A ring with unit (or unital ring) is a ring with a unit element $1 \in R$, such that $1 \cdot x = x \cdot 1 = x$ for all $x \in R$ holds. In this case, $(R, \cdot)$ is a unital associative monoid.

3. A ring $(R, +, \cdot)$ is called commutative , if the monoid $(R, \cdot)$ is abelian, i.e. for all $x, y \in R$ the equation $x \cdot y = y \cdot x$ holds.

4. If R, S are rings, then a ring homomorphism $f \colon R \to S$ is a map $f \colon R \to S$, which respects both the abelian group and monoid structures on R and S:
$$f(x + y) = f(x) + f(y) \quad \text{and} \quad f(xy) \ = \ f(x)\, f(y) \quad \text{for all } x, y \in R \ .$$
For unitary rings we additionally require morphisms of rings to send
$$f(1_R) \ = \ 1_S \, .$$
We denote the set of all ring homomorphisms by $\mathrm{Hom}(R, S)$.

In this lecture we adopt that convention that by a ring we mean an associative, not necessarily commutative ring with unit.

Examples 1.1.2 Important examples for rings are:

1. The ring $\mathbb{Z}$ of the integers (and, more generally, the ring of integers in an algebraic number field).

2. Fields such as the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$ or the complex numbers $\mathbb{C}$ are (commutative) rings.

3. For every commutative ring R, the polynomial ring $R[X]$ is again a ring; more about this later.

4. For every associative unital ring R, we also have the ring $\mathrm{Mat}_n(R)$ of $n \times n$-matrices with entries in R.

5. Let $U \subset \mathbb{R}^n$ be an open subset. Then the real-valued functions on U as well as the differentiable and analytic functions on U form rings. More generally, one can also consider functions on manifolds.

6. The ring $\mathbb{Z}$ of integers is the initial unital ring: for every (unital) ring R there exists a unique (unital) ring homomorphism $f\colon \mathbb{Z} \to R$ and it is determined by $f(1) = 1_R$. To see the latter, note that

$$f(n) = f(\underbrace{1 + \ldots + 1}_{n-\text{times}}) = \underbrace{f(1) + \ldots + f(1)}_{n-\text{times}}$$

determines the ring homomorphism uniquely.

7. The terminal unital ring is the null ring $\{0\}$, the unique unital ring in which $1 = 0$ holds. For every ring R there exists a unique ring homomorphism $f\colon R \to \{0\}$

We will need the appropriate generalization of vector spaces and linear maps over rings instead of fields. In the case of non-commutative rings we have to be more careful and distinguish three concepts:

Definition 1.1.3

1. A left module over a ring R is an abelian group $(M, +)$, equipped with a map

$$\begin{array}{rccl} \mu\colon & R \times M & \to & M \\ & (r, m) & \mapsto & \mu(r, m) \equiv r.m \equiv rm\ , \end{array}$$

the (scalar-)multiplication, such that for all $x, y \in R$ and $m, n \in M$ we have:

$$\begin{array}{rcl} \mu(x, m+n) = \mu(x, m) + \mu(x, n) & \text{resp.} & x.(m+n) = x.m + x.n \\ \mu(x+y, m) = \mu(x, m) + \mu(y, m) & \text{resp.} & (x+y).m = x.m + y.m \\ \mu(x, \mu(y, m)) = \mu(xy, m) & \text{resp.} & x.(y.m) = (x \cdot y).m \end{array}$$

The first two equations express that the scalar multiplication is bilinear (or rather: bi-additive). The third equation is a mixed associativity law. For modules of unital rings we additionally require

$$\mu(1, m) = m \quad \text{resp.} \quad 1.m = m$$

for all $m \in M$.

2. If M, N are left modules over the same ring, then we call a map $f\colon M \to N$ a module homomorphism, if it is compatible with addition and scalar multiplication:

$$\begin{array}{rcl} f(m+n) & = & f(m) + f(n) \\ f(r.m) & = & r.f(m) \end{array}$$

We also call such a map an R-linear map. A bijective homomorphism of modules is called an isomorphism. We denote by $\mathrm{Hom}_R(M, N)$ the set of all such morphisms. If the ring is obvious from the context, we also write $\mathrm{Hom}(M, N)$.

3. A right module over a ring R is an abelian group $(M, +)$, equipped with a (scalar) multiplication

$$\begin{array}{rccl} \mu\colon & M \times R & \to & M \\ & (m, r) & \mapsto & \mu(m, r) \equiv m.r \equiv mr\ , \end{array}$$

such that for all $x, y \in R$ and $m, n \in M$ we have:

$$\begin{array}{rcl} \mu(m+n,x) = \mu(m,x) + \mu(n,x) & \text{i.e.} & (m+n).x = m.x + n.x \\ \mu(m,x+y) = \mu(m,x) + \mu(m,y) & \text{i.e.} & m.(x+y) = m.x + m.y \\ \mu(m,x\cdot y) = \mu(\mu(m,x),y) & \text{i.e.} & m.(x\cdot y) = (m.x).y \end{array}$$

For unital rings we additionally require

$$\mu(m,1) \;=\; m \;\text{ i.e. }\; m.1 = m$$

for all $m \in M$.

4. Let R, S be two rings, not necessarily distinct. An R-S-bimodule is an abelian group M, that carries that structures of an R-left module (M, μ) and an S-right module $(M, \tilde{\mu})$, such that the condition
$$\tilde{\mu}(\mu(\alpha, m), \beta) = \mu(\alpha, \tilde{\mu}(m, \beta))$$
is satisfied for all $m \in M, \alpha \in R, \beta \in S$. In other notation:
$$(\alpha.m).\beta = \;\alpha.(m.\beta)\;.$$

5. Morphisms of right modules and of bimodules are defined analogously as in the case of left modules.

Remarks 1.1.4

1. We will use the familiar order of operations "multiplication/division before addition/subtraction".

2. The ring multiplication exhibits every ring as a left module, a right module, and a bimodule over itself. This module is called the regular left/right/bimodule.

3. If R is a field, then the left R-modules are exactly the R-vector spaces.

4. As in the case of vector spaces, one shows for all rings R and left modules M
$$0_R m = 0_M \qquad \text{for all} \quad m \in M$$
and deduces $(-1)m = -m$. Analogous equations hold for right modules and bimodules.

Linear maps form a vector space themselves. Now let R be a ring and let M and N be two R-modules. The sum of two module homomorphisms $\varphi_1, \varphi_2 \in \mathrm{Hom}_R(M, N)$ is defined (as in the case of vector spaces) pointwise

$$(\varphi_1 + \varphi_2)(m) := \varphi_1(m) + \varphi_2(m) \quad \text{for all} \quad m \in M$$

which equips the set $\mathrm{Hom}_R(M, N)$ with the structure of an abelian group. In the following, we will always consider $\mathrm{Hom}_R(M, N)$ as abelian group. One might be tempted to extend this definition by

$$(r.\varphi)(m) := r.\varphi(m) \quad \text{for all} \quad m \in M \text{ and } r \in R$$

to a (left) R-module. But for $\lambda \in R$ one has

$$(r\varphi)(\lambda m) = r\varphi(\lambda m) = r\lambda\varphi(m)$$

and this would have to equal

$$\lambda(r.\varphi)(m) = \lambda r\varphi(m)$$

for $r.\varphi$ to be R-linear. Unless the ring R is commutative, this will not be true, in general. In summary:

Theorem 1.1.5 Let R be a ring and M, N two R-modules. Then $\mathrm{Hom}_R(M,N)$ carries the structure of an abelian group. If R is commutative, then $\mathrm{Hom}_R(M,N)$ carries a natural R-module structure.

We add a few remarks about the connection between left modules and right modules:

Remarks 1.1.6

1. For a ring R, we denote by R^{opp} the opposite ring : this is the ring with the same underlying abelian group, but with multiplication

$$(x,y) \mapsto \mu(y,x) \ .$$

One can show: every R-right module (M,μ) can be considered via

$$\begin{array}{rccl} \mu^{\mathrm{opp}}\colon & R^{\mathrm{opp}} \times M & \to & M \\ & (r,m) & \mapsto & m.r := \mu(m,r) \end{array}$$

as an R^{opp}-left module. Conversely, every R^{opp}-left module determines an R-right module.

2. If R, S are rings and $f\colon R \to S$ is a homomorphism of abelian groups, which satisfies

$$f(xy) \ = \ f(y)\ f(x) \text{ for all } x,y \in R\,,$$

then f is called an antihomomorphism. An antihomomorphism is a homomorphism from R^{opp} to S or, equivalently, a homomorphism from R to S^{opp}. The rings R and R^{opp} are thus always anti-isomorphic.

3. A ring R is commutative, if and only if the identity is an isomorphism from R to R^{opp}. For a commutative ring R, remark (1) implies that every R-left module is naturally an R-right module and vice versa. Indeed, every R-left module has even the structure of an R-bimodule. For commutative rings R, we thus often drop "left" or "right" and simply speak of R-modules, see e.g. Theorem 1.1.5.

4. There are non-commutative rings that are *isomorphic* to their opposite, albeit via a non-trivial isomorphism. For example, the ring $M(R, n\times n)$ of quadratic $n \times n$ matrices over a commutative ring R via the transposition, which switches the order of multiplication:

$$(AB)^t = \ B^t \cdot A^t \ .$$

Modules already carry an addition by their definition; now we consider modules over a commutative ring R with the additional structure of a multiplication of module elements:

Definition 1.1.7

1. Let R be a commutative ring. An (associative) R-algebra is an R-module A, which carries the structure of an (associative but, not necessarily unital) ring, such that the ring addition agrees with the module addition and the compatibility condition

$$r(xy) \ = (rx)y = x(ry) \qquad (*)$$

holds for all $x, y \in A$ and $r \in R$. We call such a ring multiplication R-bilinear.

2. An algebra A is called unital, if it is unital as ring.

Remarks 1.1.8

1. For example the polynomial ring $K[X]$ over a field K is a unital K-algebra. For a field extension E/K, the field E is also a unital K-algebra.

2. The definition of a unital R-algebra A can also equivalently be expressed as: there exists a ring homomorphism $\Phi\colon R \to A$ with the property that $\Phi(r)a = a\Phi(r)$ holds for all $r \in R$ and $a \in A$.

   For a unital R-algebra A we may define $\Phi(r) = r.1_A$ and find

   $$\Phi(r)a \overset{\text{def}}{=} (r.1_A) \cdot a \overset{(*)}{=} r.(1_A \cdot a) \ = r.a = r.(a \cdot 1_A) \overset{(*)}{=} a \cdot (r.1_A) \overset{\text{def}}{=} \ a \cdot \Phi(r) \ .$$

   Conversely, given the ring homomorphism Φ, we define an R-module structure on ring A by

   $$r.a := \Phi(r) \cdot a \ ,$$

   which is indeed R-bilinear, i.e. $(*)$ holds

   $$r.(ab) = \Phi(r)(ab) = a\Phi(r)b = a(r.b) \ .$$

Examples 1.1.9

1. Every abelian group $(G, +)$ can be seen as a $\mathbb{Z}$-module with scalar multiplication given by:

   $$\begin{array}{rcl} \mathbb{Z} \times G & \to & G \\ (n, x) & \mapsto & nx = \begin{cases} \underbrace{x + \ldots + x}_{n-\text{times}} & n > 0 \\ 0 & n = 0 \\ -|n|x & n < 0 \, . \end{cases} \end{array}$$

2. Let M be an R-module. Then the map

   $$\begin{array}{rcl} M & \to & \mathrm{Hom}_R(R, M) \\ m & \mapsto & (\varphi_m\colon r \mapsto rm) \end{array}$$

   is an isomorphism of abelian groups. If the ring R is *commutative*, then $\mathrm{Hom}_R(R, M)$ also carries an R-module structure and the above map is an isomorphism of R-modules since:

   $$\varphi_{rm}(s) = s.(r.m) = (s \cdot r).m = (r \cdot s).m = r.(s.m) = r\varphi_m(s)$$

   The inverse sends a morphism $\varphi \in \mathrm{Hom}_R(R, M)$ to its image $\varphi(1) \in M$ on the unit.

We now take a closer look at Example 1.1.9 (1). For every abelian group $(M, +)$ the group endomorphisms $\mathrm{End}(M)$ form a ring, the endomorphism ring. The addition in this ring is defined pointwise,

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m) \, .$$

The multiplication in the endomorphism ring is the composition of maps, $\varphi\psi := \varphi \circ \psi$, with unit given by the identity on M. Many endomorphism rings are non-commutative.

Lemma 1.1.10 Let M be an abelian group and R a ring.

1. If $\varphi\colon R \to \mathrm{End}(M)$ is a ring homomorphism, then

   $$r.m := \varphi(r) \, .m$$

   equips M with the structure of a (left) R-module.

2. If M is even an R-module, then the map

$$\begin{array}{rccl} \varphi\colon & R & \to & \text{Maps } (M,M) \\ & r & \mapsto & \varphi(r) \quad \text{with} \quad \varphi(r)m = rm \end{array}$$

defines a ring homomorphism with values in $\mathrm{End}(M)$. It is called the structure map of the module M.

For a given abelian group M, there exists by Examples 1.1.2.6 a unique (unital) ring homomorphism $\mathbb{Z} \to \mathrm{End}(M)$, so an abelian group carries a unique $\mathbb{Z}$-module structure, namely the one from Examples 1.1.9.1.

Other important examples of rings are polynomial rings and power series rings. We recall:

Definition 1.1.11 Let R be a commutative ring with unit. A pair (A, X), consisting of a unital R-algebra A and an element $X \in A$ is called a polynomial ring (or, more accurately: polynomial algebra) in the indeterminate X over R, if every element $f \in A$ can be written *uniquely* in the form

$$f = r_0 X^0 + r_1 X^1 + \ldots + r_n X^n$$

with $r_0, r_1, \ldots, r_n \in R$. Here we set $X^0 = 1 \in A$ and interpret uniqueness as follows: if we have an equality

$$r_0 + r_1 X^1 + \ldots + r_n X^n = b_0 + b_1 X^1 + \ldots + b_m X^m$$

in A with $m \geq n$, then $r_i = b_i$ for $0 \leq i \leq n$ and $b_i = 0$ for $i > n$.

Note that polynomial algebras are always commutative. Their elements are called polynomials.

A polynomial algebra over R is thus a pair, consisting of an R-algebra and an element in this algebra, called the "indeterminate".

Theorem 1.1.12 [Universal propery of the polynomial algebra] Let A be a polynomial ring in the indeterminate X over R. For every R-algebra S and every choice of element $s \in S$ there exists a unique homomorphism of R-algebras $\varphi_s : A \to S$ such that $\varphi_s(X) = s$.

(Just like for algebras over a field, a morphism of algebras over R is an R-linear map that intertwines the ring multiplications.)

Proof.

- Uniqueness: Since every element $f \in A$ admits a unique expression

$$f = \sum_{i=0}^{n} r_i X^i$$

the value of φ_s on f is determined as:

$$\varphi_s(f) = \sum_{i=0}^{n} r_i \varphi_s(X)^i = \sum_{i=0}^{n} r_i s^i \qquad (*)$$

- Existence: we may define φ_s using $(*)$. Well-definedness is a consequence of the uniqueness of the presentation of f. Clearly we have $\varphi_s(X) = s$ and a straightforward check shows that φ_s is indeed a morphism of R-algebras.

□

Remarks 1.1.13

1. Because of $(*)$, the map φ_s is called the evaluation homomorphism associated to $s \in S$. For a polynomial $f \in A$ we also use the notation

$$f(s) := \varphi_s(f) \in S \ .$$

2. In the special case of the polynomial ring, $(S, s) = (A, X)$, the map φ_X is the identity and our convention above is compatible with the familiar notation

$$f(X) := \varphi_X(f) = f \ .$$

3. For $S = R$ we get for every $\lambda \in R$

$$\varphi_\lambda(f) = f(\lambda) \in R \ .$$

A polynomial thus defines a function $R \to R$ and this assignment constitutes a ring homomorphism

$$\begin{array}{rcl} A & \to & \mathrm{Abb}(R, R) \ , \\ f & \mapsto & \tilde{f} \ . \end{array}$$

In general this does *not* have to be injective, i.e. a polynomial cannot be identified with its induced polynomial function:
for example, over the field $R = \mathbb{F}_2$ there are only 4 distinct functions $R \to R$, but infinitely many distinct polynomials. We only see them by evaluating polynomials on more general R-algebras.

4. Any two polynomial rings A, A' over R in indeterminates X resp. X' are isomorphic:
By Theorem 1.1.12 there are algebra morphisms

$$\begin{array}{rl} \Phi\colon\ A \to A' & \text{and}\ \ \Psi:\ A' \to A \\ \text{with}\ \ \Phi(X) = X' & \text{and}\ \ \Psi(X') = X \ . \end{array}$$

Then

$$\Psi \circ \Phi:\ A \to A \ \text{ and } \ \Phi \circ \Psi:\ A' \to A'$$

are algebra morphisms satisfying

$$\Psi \circ \Phi(X) = X \ \text{ and } \ \Phi \circ \Psi(X') = X'.$$

From the uniqueness part of Theorem 1.1.12 we deduce

$$\Psi \circ \Phi = \mathrm{id}_A \ \text{ and } \ \Phi \circ \Psi = \mathrm{id}_{A'} \ .$$

Indeed, we have shown more: any two polynomial rings over the same ring R are unique up to a *unique* isomorphism. This type of argument is a standard argument to show that a mathematical object that is defined by a universal property up to unique isomorphism.

5. One also has to show that polynomial rings actually exist. An explicit construction in terms of sequences of elements of R is typically covered in lecture courses on linear algebra.

Example 1.1.14 Sometimes one also considers the commutative ring $R[[X]]$ of formal power series, whose elements are the power series $\sum_{i=0}^{\infty} r_i X^i$ with $r_i \in R$. The multiplication is defined as in the case of polynomials: note that every one of the infinitely many coefficients of the product are expressed in terms of a *finite* sum. In general there is no notion of convergence of such power series. Neither do we have general evaluation homomorphisms: a formal powers series can typically only be evaluated at $0 \in R$, yielding the coefficient $r_0 \in R$.

Lemma 1.1.15 [Polynomial rings and endomorphisms] Let K be a field.

1. If M is a $K[X]$-module, then M also carries the structure of a K-vector space, by restricting to the constant polynomials, i.e. by pullback along the embedding $K \hookrightarrow K[X]$. The multiplication with $X \in K[X]$ is a K-linear map $M \to M$.

2. If M is a K-vector space and $A\colon M \to M$ a K-linear map, then the assignment

$$f.m := f(A)m \quad \text{for all} \quad m \in M, f \in K[X]$$

with $f(A)$ as in (1.1.13) equips the K-vector space M with the structure of a $K[X]$-module.

Modules over the polynomial ring $K[X]$ over a field are thus the same as K-vector spaces with a K-linear endomorphism. This can be generalized by replacing K by a commutative ring.

The theory of endomorphisms of vector spaces thus reduces to the theory of modules over a polynomial ring. This is the conceptual home of important polynomials such as the characteristic polynomial and the minimal polynomial (or, more generally, invariant divisors and determinant divisors) associated to endomorphisms.

We also see that the notion of a module over a ring provides a unified framework for the notion of an abelian group and of a vector space with an endomorphism: both are modules over principal ideal domains (PIDs).

Another important class of examples of rings and modules are the following.

Definition 1.1.16 Let K be a commutative ring and G a group (or, more generally, a monoid). The group ring $K[G]$ (or monoid ring) is defined to have as underlying abelian group the set of all maps

$$f\colon G \to K\,,$$

that vanish on all but finitely many $g \in G$. Elements of $K[G]$ are can thus be expressed uniquely as linear combinations

$$f = \sum f(g)\delta_g \quad \text{with } f(g) \in K$$

where δ_g denotes the map that sends $g \in G$ to $1 \in K$ and that vanishes on all other group elements. Wherever confusion seems unlikely, we may also write g in place of δ_g, such that we get expressions of the form

$$f = \sum f(g)g \quad \text{with } f(g) \in K\,.$$

The multiplication in the group ring is the convolution:

$$\left(\sum_{g\in G} a_g g\right) \star \left(\sum_{h\in G} b_h h\right) \quad = \quad \sum_{x\in G} \left(\sum_{g,h\in G, gh=x} a_g b_h\right) x\,.$$

It is important to distinguish the multiplication by convolution from the pointwise multiplication, which is commutative. For the pointwise multiplication G only needs to be a set, while the convolution uses the group multiplication in an essential way: e.g. we have $\delta_g \star \delta_h = \delta_{gh}$.

There is a ring homomorphism

$$\begin{array}{rcl} K & \hookrightarrow & K[G] \\ a & \mapsto & a\delta_e \ , \end{array}$$

where e denotes the neutral element of G, and a group homomorphism

$$\begin{array}{rcl} G & \to & K[G]^\times \\ g & \mapsto & 1g \equiv 1_K \delta_g \ , \end{array}$$

along which we may consider the underlying set of G as a basis of the group ring $K[G]$. This notion of basis will be introduced in Definition 1.3.1. Group rings are thus rings equipped with a distinguished basis. Observe that the group ring $K[G]$ is commutative if and only if the group G is abelian.

We will see that modules over a group ring over a field K are nothing but K-linear group representations. We now recall this alternative language.

Definition 1.1.17 A representation of a group G over a field K is a pair (V, ρ), consisting of a K-vector space V and a group homomorphism ρ into the invertible K-linear endomorphisms of V,

$$\rho : G \to \mathrm{GL}(V) := \{\varphi \in \ \mathrm{End}_K(V), \varphi \text{ invertible } \}\,.$$

In typical applications the vector space V may e.g. arise as space of solutions to a linear differential equation or as state space of a quantum-mechanical system. The action of the group then describes the action of symmetries. One goal of the lecture is to give an overview of group actions for given groups G on finite-dimensional vector spaces V.

Remark 1.1.18

1. Given a representation (V, ρ), we also sometimes write ρ_V for ρ.

2. If (V, ρ) is a representation of G over K, then the map

$$\begin{array}{rcl} G \times V & \to & V \\ (g, v) & \mapsto & \rho(g)v \end{array}$$

   defines an action of the group G on the underlying set of the vector space V. The group acts by linear maps.

3. If $G \times V \to V$ is an action of the group G on the set underlying a K-vector space V, such that

$$g(v + w) = gv + gw \qquad g(\lambda v) = \lambda g v$$

   holds for all $v, w \in V, g \in G$ and $\lambda \in K$, then

$$\rho(g)v = g(v)$$

   defines a representation $\rho\colon G \to \mathrm{GL}(V)$.

   In summary, a representation is an "action on a vector space by linear maps".

4. Every vector space V carries an action by its automorphism group $\mathrm{GL}(V)$, namely by $\rho = \mathrm{id}_{\mathrm{GL}(V)}$.

5. Every vector space V may be considered as a representation of any given group G with the trivial action $\rho(g) = \mathrm{id}_V$ for all $g \in G$.

6. For a field extension L/K, the K-vector space L is a representation of the Galois group $\mathrm{Gal}(L/K)$ over K.

7. A representation (V, ρ) of the group $\mathbb{Z}$ is equivalent to the data of an automorphism $A \in \mathrm{GL}(V)$, namely $A = \rho(1)$. Then one also has $\rho(n) = A^n$.

8. Representations of $\mathbb{Z}/2\mathbb{Z}$ are equivalent to the data of a vector space V with an automorphism $A : V \to V$, such that $A^2 = \mathrm{id}_V$. If the characteristic of K is not two, then V is the direct sum of the eigenspaces of A for the eigenvalues ± 1,

$$V = V^+ \oplus V^- .$$

This is because every vector $v \in V$ can be decomposed as

$$v = \frac{1}{2}(v + Av) + \frac{1}{2}(v - Av) \ ;$$

which are eigenvectors of A for the eigenvalues ± 1 as the following check shows:

$$A\frac{1}{2}(v \pm Av) = \frac{1}{2}(Av \pm A^2 v) = \pm\frac{1}{2}(v \pm Av)$$

For a field of characteristic two, only the eigenvalue 1 appears. By $A^2 = \mathrm{id}_V$ the minimal polynomial of A divides $X^2 - 1 = (X-1)^2$. The Jordan blocks of A thus have size 1 or 2. Jordan blocks of size 2 may indeed appear:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} .$$

Lemma 1.1.19 Let G be a group and K a field. There is a bijection

$$\{ \text{ representations of } G \text{ over } K \} \xleftrightarrow{\sim} \{ K[G] - \text{modules } \} \ .$$

Proof. Given a K-linear G-representation (V, ρ), we can define on the underlying abelian group $(V, +)$ of the vector space the structure of a $K[G]$-module by specifying the scalar multiplication $(\sum_{g\in G} \lambda_g \delta_g).v := \sum_{g\in G} \lambda_g \rho(g)(v)$ for $v \in V$ and $\lambda_g \in K$. It is straightforward to check that this indeed defines a $K[G]$-module.

Conversely, a $K[G]$-module M has an underlying abelian group, which is a K-vector space with respect to the scalar multiplication $\lambda m := (\lambda \delta_e).m$ for $m \in M$ and $\lambda \in K$. For $g \in G$ we then define $\rho(g) \in \mathrm{End}_K(V)$ by $\rho(g)(v) := \delta_g.v$ for $v \in M$. This defines a G-representation over K and the two assignments constructed here are manifestly mutually inverse to each other. □

More generally, for a monoid G a $\mathbb{Z}[G]$-module is equivalent to the data of an abelian group with a G-action by group homomorphisms. We leave this as an exercise to the reader.

The module homomorphisms of modules over the group ring $K[G]$ are also studied under a different name in the language of representations.

Definition 1.1.20 Given representations V, W of a group G over the same field K, a morphism of representations or intertwiner is a K-linear map $f \colon V \to W$, satisfying

$$f(\rho_V(g)v) = \rho_W(g) f(v) \quad \text{for all } \ g \in G \, .$$

An isomorphism is a bijective morphism. Two representations are called isomorphic, if an isomorphism exists between them.

One checks that the inverse of an intertwiner is itself an intertwiner.
We continue in the theory of modules:

Definition 1.1.21 Let M be an R-left module and $U \subseteq M$ a subgroup. Then U is called a submodule of M, if U is closed under the scalar multiplication on M, i.e. if $m \in U$ and $r \in R$ implies $r.m \in U$.

Remark 1.1.22

1. The subgroups of an abelian group are precisely the $\mathbb{Z}$-submodules.

2. Considering the ring R as a module over itself, the R-submodules of R are exactly the ideals of R. More precisely, the R-left-submodules are the left ideals, the right R-submodules are the right ideals and the R-bi-submodules are the two-sided ideals.

3. A subset $W \subset V$ of a representation V is called a subrepresentation if it is vector subspace that is stable under G; i.e. if $g \in G$ and $w \in W$ imply $gw \in W$. Under the bijection from Lemma 1.1.19 the subrepresentation correspond to the $K[G]$-submodules.

4. The image and the preimage of a submodule under a module homomorphism are again submodules. In particular, the image and the kernel of a module homomorphism are submodules.

5. If U is a submodule of M, then on the level of underlying abelian groups, U is normal in M and M/U is again an abelian group.

   The quotient group M/U inherits the structure of an R-module, called the quotient module or factor module of M by U, with the scalar multiplication:

   $$\begin{aligned} R \times M/U &\to M/U \\ (\alpha, x+U) &\mapsto \alpha x + U \end{aligned}$$

   In verifying this, it is important to check that the scalar multiplication is well-defined.

6. We illustrate this in an example: Let $\mathfrak{a}$ be a left ideal of R and M an R-module, then

   $$\mathfrak{a}M = \left\{ \sum_{\text{finite}} \alpha_i x_i \;\middle|\; \alpha_i \in \mathfrak{a}, x_i \in M \right\}$$

   is a submodule of M: for $r \in R, \alpha \in \mathfrak{a}$ and $x \in M$ we have $r\alpha \in \mathfrak{a}$ since $\mathfrak{a}$ is a left ideal, and thus $r(\alpha m) = (r\alpha)m \in \mathfrak{a}M$. By remark (5) the quotient $M/\mathfrak{a}M$ is an R-module.

   If $\mathfrak{a}$ is actually a two-sided ideal, then $R/\mathfrak{a}$ is a ring with respect to the multiplication $(a+\mathfrak{a}) \cdot (a'+\mathfrak{a}) := a \cdot a' + \mathfrak{a}$. Then the scalar multiplication

   $$(\alpha + \mathfrak{a})(x + \mathfrak{a}M) = \alpha x + \mathfrak{a}M$$

   is well-defined and thus the R-module structure on $M/\mathfrak{a}M$ descends to an $R/\mathfrak{a}$-module structure.

   We consider a concrete example: the ring $\mathbb{Z}$ of integers is a module over itself, i.e. a $\mathbb{Z}$-module; $n\mathbb{Z}$ is a two-sided ideal for every $n \in \mathbb{Z}$ and the cyclic group $\mathbb{Z}/n\mathbb{Z}$ is a $\mathbb{Z}$-module with scalar multiplication

   $$n.\overline{m} = \overline{nm}$$

   and also a $\mathbb{Z}/n\mathbb{Z}$-module with $\overline{n}.\overline{m} = \overline{nm}$.

Lemma 1.1.23 [restriction of scalars/pullback] If $\varphi\colon R \to S$ is a ring homomorphism, then every S-module (M, μ) (in particular S itself) becomes an R-module via $\mu \circ (\varphi \times \mathrm{id}_M)$, i.e. by setting

$$r.m := \varphi(r).m\,.$$

This operation is called restriction of scalars, even when R is not a subring of S, i.e. φ need not be injective. The resulting R-module is also called the pullback of the S-module M along the ring homomorphism φ.

In other words: the S-module structure on M can be expressed as a ring homomorphism $S \to \mathrm{End}(M)$ and the R-module structure of the pullback is then expressed by the composite ring homomorphism

$$R \xrightarrow{\varphi} S \to \mathrm{End}(M).$$

For example, let $\mathfrak{a} \subset R$ be a two-sided ideal of R and $\mathrm{can}\colon R \to R/\mathfrak{a}$, the canonical surjection, then the quotient ring $R/\mathfrak{a}$ is a module over itself and by pullback also naturally an R-module.

Example 1.1.24 Restriction of scalars provides an alternative explanation of why the quotient ring $\mathbb{Z}/n\mathbb{Z}$ of the ring of integers is a module over the ring of integers.

Definition 1.1.25

1. Let $A \subseteq M$ be a subset of an R-module M. Then

$$\langle A\rangle = \left\{ \sum_{\text{finite}} \alpha_i a_i \;\middle|\; \alpha_i \in R, a_i \in A \right\}$$

   denotes the submodule of M generated by A. We have

$$\langle A\rangle = \bigcap_{\substack{U \subset M \text{ submodule} \\ A \subseteq U}} U$$

   i.e. $\langle A\rangle$ is the smallest submodule of M that contains A.

   To see this, note that $\langle A\rangle$ is a submodule containing A and thus one of the modules being intersected, and thus contained in the intersection. Conversely, every submodule being intersected must also contain the elements of $\langle A\rangle$.

2. If $\langle A\rangle = M$, then the set A is called a generating set of the module M. M is called finitely generated, if a finite generating set exists.

3. A module is called a cyclic module, if it admits a generating set consisting of a single element.

Note that not every element of a cyclic module needs to be a generator. We leave it as an exercise to check that the cyclic groups are exactly the cyclic $\mathbb{Z}$-modules.

Theorem 1.1.26 (Homomorphism theorems for modules)

1. Let M, N be R-modules and $f\colon M \to N$ a module homomorphism, then there exists a canonical isomorphism

$$\begin{array}{ccc} M/\ker f & \xrightarrow{\sim} & f(M) \\ x + \ker f & \mapsto & f(x) \end{array}$$

2. If U and V are submodules of a module M, then

$$(U+V)/V \quad \xrightarrow{\sim} \quad U/(U\cap V)$$

with $U+V=\{u+v, u\in U \text{ and } v\in V\}$. To see this, check that the map

$$\begin{array}{ccc} U+V & \to & U/\ U\cap V \\ u+v & \mapsto & u+(U\cap V) \end{array}$$

is well-defined compute its kernel.

3. For every chain $U\subseteq V\subseteq M$ of submodules, V/U is a submodule of M/U and

$$(M/U)\,/\,(V/U) \quad \xrightarrow{\sim} \quad M/V\,.$$

The proof of this theorem is completely analogous to that in the case of vector spaces.

Definition 1.1.27

1. Let U be a subset of an R-module M. Then

$$\text{Ann}\ (U)=\{\alpha\in R \mid \alpha u=0 \quad \text{for all } u\in U\}$$

is called the annihilator of the subset U. In the case of a left module, this is a left ideal of R. The annihilator of an element $x\in M$ is denoted by

$$\text{Ann}(x)=\{\alpha\in R\,|\,\alpha x=0\}\,.$$

By Theorem 1.1.26 (1) there is an isomorphism of left modules

$$\begin{array}{ccc} R/\text{Ann}(x) & \xrightarrow{\sim} & Rx \\ \overline{\alpha} & \mapsto & \alpha x\ . \end{array}$$

If U is a submodule, then the annihilator is even a two-sided ideal.

2. A module M is called faithful, if Ann $M=(0)$. We remark that a representation on a K-vector space V is faithful if the group homomorphism $\rho\colon\ G\to \mathrm{GL}(V)$ is injective. If V is faithful as $K[G]$-module then the corresponding representation is also faithful. Suppose $\rho(g)=\rho(g')$ for $g\neq g'$, then $g-g'$ would be contained in the annihilator of V. The converse is not true, however: the one-dimensional representation of the cyclic group $\mathbb{Z}/2\mathbb{Z}=\{e,g\}$ with $\rho(g)=-1$ is faithful as group representation, but the associated $K[G]$-module is not faithful, since the element $e+g\in K[G]$ is contained in the annihilator.

3. An element $x\in M$ is called a torsion element, if Ann $(x)\neq 0$. We denote the set of all torsion elements in M by Tor M; in general it is not a submodule.

4. A module M is called torsion-free, if Tor $M=(0)$.

In a torsion-free module the annihilators of all nonzero elements are zero, in particular $\text{Ann}(M)=(0)$, and so torsion-free modules are automatically faithful. The converse is false: for example the ring $R=\mathbb{Z}/6\mathbb{Z}$ is faithful as module over itself (because it is unital). But the element $\overline{2}$ is contained in the annihilator of $\overline{3}$, and so $\overline{3}$ is a torsion element.

Example 1.1.28 The ring of integers $\mathbb{Z}$ is torsion-free over itself; the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ consists exclusively of torsion elements.

A commutative ring R is called integral or an integral domain if it has no zero divisors, i.e. if for $\alpha, \beta \in R$ the equation $\alpha \cdot \beta = 0$ implies $\alpha = 0$ or $\beta = 0$.

Theorem 1.1.29 If M is a module over an integral domain R, then Tor M is a submodule of M and the quotient module $M/\text{Tor } M$ is a torsion-free R-module.

Proof.

- If $x \in \text{Tor}(M)$ is a torsion element, $\beta \in R$, then we can find a nonzero $\alpha \in \text{Ann}(x)$. Then $\alpha(\beta x) = (\alpha\beta)x = \beta(\alpha x) = 0$ and thus $\beta x \in \text{Tor } M$.
- Given two torsion elements $x, y \in \text{Tor } M$, we can find $\alpha, \alpha' \in R \setminus \{0\}$, such that $\alpha x = \alpha' y = 0$. Then $\alpha\alpha' \neq 0$ since R is integral by assumption, and we have $\alpha\alpha'(x+y) = 0 + 0 = 0$, which implies $x + y \in \text{Tor } M$. Thus $\text{Tor}(M)$ is a submodule.
- Finally let $x + \text{Tor } M \in M/\text{Tor } M$ be a torsion element. We find $\alpha \in R\setminus\{0\}$, such that $\alpha(x + \text{Tor } M) = 0$. Since $\alpha x \in \text{Tor } M$ there exists a $\beta \in R \setminus \{0\}$ with $\beta\alpha x = 0$. As R is integral, we have $\beta\alpha \neq 0$ and hence $x \in \text{Tor } M$. Thus the quotient $M/\text{Tor } M$ is torsion-free. □

1.2 Operations on modules, the tensor product

Definition 1.2.1 Let $(M_\lambda)_{\lambda\in\Lambda}$ be a family of modules over a ring R. We form two new R-modules:
the product

$$\prod_{\lambda\in\Lambda} M_\lambda = \{(m_\lambda)_{\lambda\in\Lambda} \mid m_\lambda \in M_\lambda\}$$

and the direct sum

$$\bigoplus_{\lambda\in\Lambda} M_\lambda = \{(m_\lambda)_{\lambda\in\Lambda} \mid m_\lambda \in M_\lambda, \text{ only finitely many } m_\lambda \text{ are nonzero}\}.$$

The R-module structures on these sets are given by the componentwise addition and componentwise scalar multiplication with scalars from R.

Remarks 1.2.2

1. For every natural number n we have the R-module $R^n = \underbrace{R \oplus \ldots \oplus R}_{n- \text{ times}}$.
2. For finite families, $|\Lambda| < \infty$, the notions of direct sum and product coincide. We then do not distinguish between $\prod_{i=1}^s M_i = M_1 \times M_2 \times \ldots \times M_s$ and $M_1 \oplus M_2 \oplus \ldots \oplus M_s$.
3. Both notions can be characterized by universal properties. For this we consider the canonical

   injection bzw. surjection

   $$i_\lambda : M_\lambda \hookrightarrow \bigoplus_{\mu\in\Lambda} M_\mu \qquad pr_\lambda : \prod_{\mu\in\Lambda} M_\mu \twoheadrightarrow M_\lambda \ .$$

   Here ι_λ maps the element $m \in M_\lambda$ to the element of the direct sum, whose entries are all zero except for the component λ. The map pr_λ projects onto the component λ. Both maps are homomorphisms of R-modules.

The two universal properties are: if M is an arbitrary R-module, then the two maps

$$\begin{aligned} \mathrm{Hom}_R(\oplus_{\mu\in\Lambda} M_\mu, M) &\longrightarrow \prod_{\mu\in\Lambda} \mathrm{Hom}_R(M_\mu, M) \\ f &\mapsto (f\circ i_\mu)_{\mu\in\Lambda} \end{aligned}$$

$$\begin{aligned} \mathrm{Hom}_R\Big(M, \prod_{\mu\in\Lambda} M_\mu\Big) &\longrightarrow \prod_{\mu\in\Lambda} \mathrm{Hom}_R(M, M_\mu) \\ f &\mapsto (pr_\mu \circ f)_{\mu\in\Lambda} \end{aligned}$$

are isomorphisms of abelian groups.

In other words: A family of maps from some modules *into* one module M can be described *uniquely* by a single map from the direct sum of the modules into M. In the case of the direct product a family of maps *out of* one module M into some modules can be described uniquely as a single map out of M into the direct product.

The direct sum and the product should not be considered as just a module (with some properties), but as a module with this properties *together* with a family of injections resp. surjections. This module with its family of morphisms is determined by the corresponding universal property up to unique isomorphism.

4. Given a family $(U_\lambda)_{\lambda\in\Lambda}$ of submodules of a module M, then the submodule of M generated by their union

$$\sum_{\lambda\in\Lambda} U_\lambda := \langle\ \cup_{\lambda\in\Lambda} U_\lambda\ \rangle$$

is called the (inner) sum of the family.

Every submodule is equipped with an injection $s_\lambda\colon U_\lambda \to M$; by the universal property of the direct sum we may collect this family of morphisms into a natural morphism

$$s: \quad \oplus_{\lambda\in\Lambda} U_\lambda \to M$$

The sum $\sum_{\lambda\in\Lambda} U_\lambda$ is the image of the morphism s. If s is injective, then we say the sum of submodules is direct and sometimes write $\oplus_{\lambda\in\Lambda} U_\lambda$ instead of $\sum_{\lambda\in\Lambda} U_\lambda$, which we may call an inner direct sum. The injectivity of s means that we can write every element of the inner direct sum in a *unique* way as a sum of elements of the submodules U_λ.

5. Given two representations (V,ρ_V) and (W,ρ_W) of a group G over a field K then their direct sum is defines as the K-vector space $V\oplus W$ with the action $g(v,w) = (\rho_V(g)v, \rho_W(g)w)$. Analogously one defines direct sums and products of infinitely many representations, corresponding to the parallel notions for modules over the group ring $K[G]$.

We will also need the notion of the tensor product, which may be familiar from linear algebra in the case of vector spaces.

Definition 1.2.3 Let M be an R^{opp}-module and N an R-module. The tensor product $M\otimes_R N$ is defined as the abelian group generated by pairs $m\otimes n$ with $m\in M$ and $n\in N$, modulo the relations

$$\begin{aligned} 0\otimes n = \ m\otimes 0 = 0 &\quad \text{for all} \quad m, n \\ (m_1+m_2)\otimes n = \ m_1\otimes n + m_2\otimes n &\quad \text{for all} \quad m_1, m_2, n \\ m\otimes(n_1+n_2) = \ m\otimes n_1 + m\otimes n_2 &\quad \text{for all} \quad m, n_1, n_2 \\ (m.r)\otimes n = \ m\otimes(r.n) &\quad \text{for all} \quad m\in M, n\in N, r\in R \end{aligned}$$

Remarks 1.2.4

1. Note that M is required to be a right module, so that the final relation is consistent with the relations defining the module structures: indeed we must have

$$m.(r_1 r_2) \otimes n = (m.r_1).r_2 \otimes n = m.r_1 \otimes r_2.n = m \otimes r_1.(r_2.n) = m \otimes (r_1 \cdot r_2).n \ .$$

2. A typical element of $M \otimes_R N$ is not of the form $m \otimes n$ with $m \in M$ and $n \in N$; such special elements are called elementary tensors. A typical element is actually a sum of elementary tensors, i.e. $\sum_i m_i \otimes n_i$ with $m_i \in M$ and $n_i \in N$.

Lemma 1.2.5 Let R be a ring and suppose M, M_i are R^{opp}-modules and N an R-module. Then there are distinguished isomorphisms:

1. Let 0 be the zero module. Then we have: $0 \otimes_R N \cong M \otimes_R 0 \cong 0$.
2. $R \otimes_R N \cong N$ and $M \otimes_R R \cong M$ as abelian groups.
3. $\oplus_{\lambda \in \Lambda} (M_\lambda \otimes_R N) \cong (\oplus_{\lambda \in \Lambda} M_\lambda) \otimes_R N$ and analogously in the second argument.
4. Let S be another ring, Q an S-module and P an R-S-bimodule. Then $M \otimes_R P$ is naturally an S^{opp}-module and $P \otimes_S Q$ an R-module and we have an isomorphism of abelian groups:

$$(M \otimes_R P) \otimes_S Q \cong M \otimes_R (P \otimes_S Q) \ .$$

Proof. The first identity follows directly from the first defining relation of the tensor product.

For the second identity consider the morphism of abelian groups

$$\begin{array}{ccc} M & \to & M \otimes_R R \\ m & \mapsto & m \otimes 1 \ , \end{array}$$

which has the inverse

$$\begin{array}{ccc} M \otimes_R R & \to & M \\ m \otimes r & \mapsto & m.r \end{array}$$

and is thus an isomorphism of abelian groups.

The distributivity for direct sums can be seen as follows: by the universal property of the direct sum a morphism

$$\Phi \colon \ \oplus_{\lambda \in \Lambda} (M_\lambda \otimes_R N) \to (\oplus_{\lambda \in \Lambda} M_\lambda) \otimes_R N$$

is determined by its restrictions to $M_\lambda \otimes N$ for all $\lambda \in \Lambda$. There we set on generators $\Phi(m_\lambda \otimes n) = \iota_\lambda(m_\lambda) \otimes n$. To specify the inverse map we note that in $(\oplus_{\lambda \in \Lambda} M_\lambda) \otimes_R N$ every element is of the form $x = \sum_\lambda \iota_\lambda(m_\lambda) \otimes n_\lambda$. The inverse map Ψ is now given by $\Psi(\iota_\lambda(m_\lambda) \otimes n_\lambda) = \iota_\lambda(m_\lambda \otimes n_\lambda)$.

The S^{opp}-module structure on $M \otimes_R P$ is defined by $(m \otimes p).s = m \otimes p.s$. The R-module structure on $P \otimes_S Q$ is defined analogously. The isomorphism is defined on generators by

$$(m \otimes p) \otimes s \mapsto m \otimes (p \otimes s) \ . \qquad \square$$

Examples 1.2.6

1. Let R be a ring and $R^n := R \oplus R \oplus \ldots \oplus R$ the n-fold direct sum of R. Then

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

This is a consequence of the distributivity law 1.2.5.3.

2. If R is a commutative ring, then the polynomial rings satisfy

$$R[X] \otimes_R R[Y] \cong R[X,Y]$$

where $R[X,Y]$ is the ring of polynomials in two variables, considered here at first as an abelian group. (Exercise)

3. Let $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ be the $\mathbb{Z}$-module of integers modulo n which we may also consider bimodule as over $\mathbb{Z}$. Then

$$\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m \cong \mathbb{Z}_g$$

where g is the greatest common divisor of m and n.

To see this note that every element in the tensor product can be written as finite sum

$$x = \overline{a_1} \otimes \overline{b_1} + \ldots + \overline{a_k} \otimes \overline{b_k}$$

with $a_i, b_i \in \mathbb{Z}$. By $\mathbb{Z}$-bilinearity of the tensor product we have

$$x = (a_1 b_1 + \ldots + a_k b_k)\ (1_{\mathbb{Z}/n\mathbb{Z}} \otimes 1_{\mathbb{Z}/m\mathbb{Z}})\ ;$$

and so the tensor product is also a cyclic group. The group homomorphism

$$\begin{array}{rccc} \Phi\colon & \mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m & \to & \mathbb{Z}_g \\ & \overline{k} \otimes \overline{l} & \mapsto & \overline{k \cdot l} \end{array}$$

is well-defined as $g = \gcd(m,n)$ divides n and m, and clearly surjective. If $\Phi(a(1\otimes 1)) = 0$, then a is a multiple of the gcd g. Bézout's lemma yields $\alpha, \beta \in \mathbb{Z}$ such that $\alpha n + \beta m = a$. Thus we have

$$a(1 \otimes 1) = \alpha(\overline{n} \otimes 1) + \beta(1 \otimes \overline{m}) = 0$$

in $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m$, and so Φ is also injective.

4. Tensoring with $\mathbb{Q}$ over $\mathbb{Z}$ kills the torsion elements of abelian groups. Indeed, $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Q}$ is zero for every $n \in \mathbb{Z}_{>0}$ since for all $i \in \mathbb{Z}$ and $q \in \mathbb{Q}$

$$[i] \otimes q = [(in)] \otimes \frac{q}{n} = [0] \otimes \frac{q}{n} = 0\ .$$

If, conversely, an element of an abelian group is not torsion, then it generates a subgroup isomorphic to $\mathbb{Z}$. Since tensoring with $\mathbb{Q}$ sends subgroups to subgroups (proof later in Example 1.4.12) and $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$ by Lemma 1.2.5.2, such an element does not vanish upon tensoring with $\mathbb{Q}$.

5. The tensor product is *not* distributive with respect to *infinite* direct products: Let $M := \prod_{n\geq 1} \mathbb{Z}_n$. One the one hand, by (4) $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Q} = 0$ and so $\prod_{n\geq 1}(\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Q}) = 0$. On the other hand, let $e \in M$ denote the element, with entry 1 in every component. Then $e \otimes 1 \neq 0$, since e has infinite order in the abelian group M, i.e. generates a subgroup isomorphic to $\mathbb{Z}$. Then by Lemma 1.2.5.2 we have $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$. Thus the tensor product $M \otimes_{\mathbb{Z}} \mathbb{Q}$ is nonzero.

If R is a *commutative* ring, then one can define the tensor product of two (left) R-modules M, N, by first considering N via $m.r := r.m$ as an R-right module and in fact even a bimodule. rIn this case the tensor product carries not only the structure of an abelian group, but that of an R-module:

Theorem 1.2.7 If R is a *commutative* ring and M, N are two R-modules, then

$$\mu(r, m \otimes n) := (r.m) \otimes n = m \otimes r.n$$

defines an R-module structure on $M \otimes_R N$.

In this case, for three R-modules M, N, P one has canonical isomorphisms

$$\begin{array}{rcl} a_{M.N.P} : M \otimes (N \otimes P) & \to & (M \otimes N) \otimes P \\ m \otimes (n \otimes p) & \mapsto & (m \otimes n) \otimes p \end{array}$$

along which the R-modules $M \otimes (N \otimes P)$ and $(M \otimes N) \otimes P$ can be identified. In this sense the tensor product is associative.

The proof is left to the reader. Also note the formal similarity to the Hom between modules, which yields abelian groups over general rings, but R-modules in the case of a commutative ring.

We now discuss the universal property of the tensor product. As in the case of vector spaces, it involves bilinear maps.

Definition 1.2.8 Let R be a ring, M an R^{opp}-module, N an R-module, and T an abelian group. A map $f\colon M \times N \to T$ is called R-bilinear, if it satisfies the following properties:

$$\begin{array}{rcll} f(m, 0) = f(0, n) = 0 & \text{for all} & m \in M, n \in N \\ f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n) & \text{for all} & m_1, m_2 \in M, n \in N \\ f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2) & \text{for all} & m \in M, n_1, n_2 \in N \\ f(m.r, n) = f(m, r.n) & \text{for all} & m \in M, n \in N, r \in R \end{array}$$

We denote by $\text{Bil}_R(M, N, T)$ the abelian group of such maps.

The map

$$\begin{array}{rcl} M \times N & \to & M \otimes_R N \\ (m, n) & \mapsto & m \otimes n \end{array}$$

is R-bilinear by definition.

Theorem 1.2.9 [Universal property of the tensor product] Let R be a ring, M an R^{opp}-module, N an R-module, and T an abelian group.

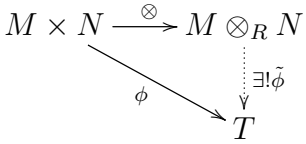
1. The R-bilinear map

$$\begin{array}{rccl} \otimes\colon & M \times N & \to & M \otimes N \\ & (m, n) & \mapsto & m \otimes n \end{array}$$

induces an isomorphism of abelian groups

$$\begin{array}{rcl} \text{Hom}_{\mathbb{Z}}(M \otimes_R N, T) & \to & \text{Bil}_R(M, N, T) \\ \tilde{\phi} & \mapsto & \tilde{\phi} \circ \otimes \ . \end{array}$$

In other words, every R-bilinear map $\phi\colon M \times N \to T$ can be described *uniquely* by a morphism of abelian groups $\tilde{\phi}\colon M \otimes_R N \to T$. As commutative diagram:



2. The abelian group $\mathrm{Hom}_{\mathbb{Z}}(N,T)$ carries a natural R^{opp}-module structure defined by $(f.r)(n) := f(r.n)$ for $f\colon N \to T$, $r \in R$, and $n \in N$. Indeed

$$f.(r_1 \cdot r_2)(n) = f((r_1 \cdot r_2).n) = f(r_1.(r_2.n)) = (f.r_1)(r_2.n) = ((f.r_1).r_2))(n)$$

for all $n \in N$.

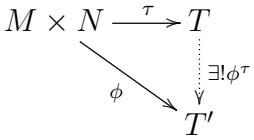
Analogously the abelian group $\mathrm{Hom}_{\mathbb{Z}}(M,T)$ carries a natural R-left module structure defined by $(r.g)(m) := g(m.r)$ for $g\colon M \to T$, $r \in R$, and $m \in M$.

With respect to these R-module structures we have the isomorphisms of abelian groups

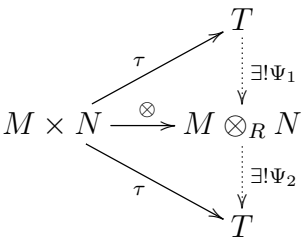
$$\mathrm{Hom}_R(N, \mathrm{Hom}_{\mathbb{Z}}(M,T)) \cong \mathrm{Hom}_{\mathbb{Z}}(M \otimes_R N, T) \cong \mathrm{Hom}_{R^{\mathrm{opp}}}(M, \mathrm{Hom}_{\mathbb{Z}}(N,T))\,.$$

Proof. The first part follows directly from the definition of the tensor product. The second part requires a straightforward calculation. The final statement follows from the observation that all three spaces describe R-bilinear maps $M \times N \to T$. (Exercise). □

Remark 1.2.10 The universal property of the tensor product implies the following uniqueness statement. Let T be an abelian group and $\tau\colon M \times N \to T$ an R-bilinear map, such that every bilinear map $\phi\colon M \times N \to T'$ can be expressed as a homomorphism of abelian groups $\Phi^\tau\colon T \to T'$ precomposed with τ:



Then we claim that T is already isomorphic to $M \otimes N$ with τ playing the role of $\otimes$. To see this, we consider the above diagram for $\phi = \otimes$, as well as the diagram obtained by switching the roles of τ and $\otimes$. Composing the two diagrams we get the commutative diagram:

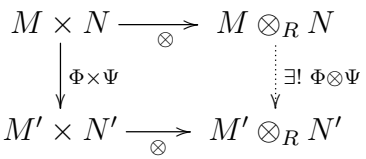


The vertical map $T \to T$ on the right is the unique Φ^τ for $\Phi = \tau$ from the universal property of (T,τ); it must be the identity and so $\Psi_2 \circ \Psi_1 = \mathrm{id}_T$. By exchanging the roles of $\otimes$ and τ in the argument, one gets $\Psi_1 \circ \Psi_2 = \mathrm{id}_{M \otimes_R N}$, and so Ψ_1 and Ψ_2 are isomorphisms that intertwine $\otimes$ and τ.

An important application of the universal property of the tensor product is the definition of the tensor product of morphisms of modules.

Observation 1.2.11 Let R be a ring and let $\Phi\colon M \to M'$ be a morphism of R^{opp}-modules and $\Psi\colon N \to N'$ a morphism of R-modules.

We consider the following diagram:



Since the map $\otimes \circ (\Phi \times \Psi)$ is clearly R-bilinear, the universal property of the tensor product guarantees the existence of a unique homomorphism of abelian groups $\Phi \otimes \Psi$ making the diagram commute, i.e.

$$(\Phi \otimes \Psi)(m \otimes n) = \Phi(m) \otimes \Psi(n) \ .$$

By bilinearity of $\otimes$, the tensor product of morphisms is also $\mathbb{Z}$-bilinear:

$$\begin{array}{rcl} (\Phi_1 + \Phi_2) \otimes \Psi & = & \Phi_1 \otimes \Psi + \Phi_2 \otimes \Psi \\ \Phi \otimes (\Psi_1 + \Psi_2) & = & \Phi \otimes \Psi_1 + \Phi \otimes \Psi_2 \end{array}$$

Remarks 1.2.12

1. If R, S are unital rings then, in particular, they are abelian groups, i.e. $\mathbb{Z}$-modules. The tensor product over $\mathbb{Z}$ thus defines an abelian group $R \otimes_{\mathbb{Z}} S$. Another, distinct abelian group is the Cartesian product $R \times S$. We equip both groups with unital ring structures:

$$\begin{array}{rcl} \text{on } R \times S & (r,s)(r',s') & := \ (rr', ss') \\ \text{on } R \otimes_{\mathbb{Z}} S & (r \otimes s)(r' \otimes s') & := \ (rr') \otimes (ss') \, . \end{array}$$

2. If M is an R-module and N an S-module, then $M \times N$ becomes an $R \times S$-module via $(r,s).(m,n) := (r.m, s.n)$ and $M \otimes_{\mathbb{Z}} N$ becomes an $R \otimes_{\mathbb{Z}} S$-module by $r \otimes s.m \otimes n := r.m \otimes s.n$.

3. Similarly one can define the product of infinitely many rings. Question: Why is the infinite direct sum of unital ring not a unital ring anymore?

4. The universal properties of this construction is as follows:
The product $\prod_{\lambda \in \Lambda} R_\lambda$ of an arbitrary family of rings together with the usual projections

$$pr_\lambda \colon \prod_{\mu \in \Lambda} R_\mu \to R_\lambda$$

satisfies the universal property of a product: for every ring S we have an isomorphism of sets

$$\begin{array}{rcl} \mathrm{Hom}(S, \prod_{\lambda \in \Lambda} R_\lambda) & \to & \prod_{\lambda \in \Lambda} \mathrm{Hom}(S, R_\lambda) \\ f & \mapsto & (pr_\mu \circ f)_{\mu \in \Lambda} \, . \end{array}$$

5. If R_1 and R_2 are commutative rings, then the tensor product $R_1 \otimes_{\mathbb{Z}} R_2$ together with the maps

$$\begin{array}{rcccccc} \iota_1 : & R_1 & \to & R_1 \otimes_{\mathbb{Z}} & R_2 & \qquad \iota_2 : & R_2 & \to & R_1 \otimes_{\mathbb{Z}} & R_2 \\ & r_1 & \mapsto & r_1 \otimes 1 & & & r_2 & \mapsto & 1 \otimes r_2 & \end{array}$$

satisfies a universal property of the same typ as the direct sum of modules: for every commutative ring S the map

$$\begin{array}{rcl} \mathrm{Hom}(R_1 \otimes_{\mathbb{Z}} R_2, S) & \to & \mathrm{Hom}(R_1, S) \times \mathrm{Hom}(R_2, S) \\ f & \mapsto & (f \circ \iota_1, f \circ \iota_2) \end{array}$$

is an isomorphism of sets. One says that the tensor product is a coproduct for commutative unital rings. Both properties will be discussed in the exercises.

1.3 Free modules

Definition 1.3.1

1. A family $(m_\lambda)_{\lambda\in\Lambda}$ of elements of an R-module is called linearly independent or free, if the following condition is satisfied: whenever

$$\sum_{\lambda\in\Lambda} r_\lambda m_\lambda = 0\,,$$

for a family $(r_\lambda)_{\lambda\in\Lambda}$ of elements in R, in which only finitely many members are nonzero, then one must have $r_\lambda = 0$ for all $\lambda \in \Lambda$.

2. A (not necessarily finite) subset $S \subset M$ is called basis of the module M, if S is linearly independent and S is a generating set of M, $\langle S\rangle = M$.

3. A module is called free, if it has a basis.

Obviously, any subfamily of a free family is again free. Note that here we are explicitly considering a module along with its underlying set.

Remark 1.3.2

1. If R is a field and M an R-vector space, then M is free over R because every vector space has a basis. There are, however, rings which admit non-free modules: let $R = \mathbb{Z}$ and $M = \mathbb{Z}/2\mathbb{Z}$. Since $2\cdot\overline{1} = \overline{0}$ we see that $\{\overline{1}\}$ is not linearly independent for any subset of M containing $\overline{1}$. On the other hand, $\{\overline{0}\}$ is not a generating set since $n.\overline{0} = \overline{0}$ for all $n \in \mathbb{Z}$. So there is no basis.

2. Similarly $\mathbb{Z}/5\mathbb{Z}$ is not a free $\mathbb{Z}$-module, but it is a free $\mathbb{Z}/5\mathbb{Z}$-module. In general, the left regular module ${}_RR$ is free with basis (1_R); the same applies to the right regular module.

3. For every set Λ the module

$$R\Lambda := \{f : \Lambda \to R \,|\, f(\lambda) = 0 \text{ for almost all } \lambda \in \Lambda\}$$

is free. The indicator functions taking value 1 at some element of Λ and 0 elsewhere form a distinguished basis, that we identify with Λ. In this way we may consider Λ as a subset of $R\Lambda$.

We call $R\Lambda$ the free R-module generated by Λ. Conversely, our definitions imply that a family $(m_\lambda)_{\lambda\in\Lambda}$ in an R-module module is a basis if and only if the map $R\Lambda \to M$ sending $(r_\lambda) \mapsto \sum r_\lambda m_\lambda$ is an isomorphism of R-modules.

4. An R-module M is free over a subset $S \subset M$ if and only if

$$M \cong \bigoplus_{s\in S} Rs\,.$$

In this case S is a basis of the module. Also note $Rs \cong R$ as R-modules for all $s \in S$.

Proof. Let $(s)_{s\in S}$ be a basis. The inclusions of submodules $Rs \to M$ define a morphism

$$\begin{array}{ccc} \bigoplus_{s\in S} Rs & \longrightarrow & M \\ (r_s)_{s\in S} & \mapsto & \sum r_s.s \end{array}$$

of R-modules by the universal property of the direct sum from Remarks 1.2.2.3. This is surjective since $\langle S\rangle = M$ and injective since S is linearly independent. The converse is immediate. □

5. If M is free and finitely generated, then there exists an $n \in \mathbb{N}$ such that

$$M \cong R^n = \underbrace{R \oplus \ldots \oplus R}_{n-\text{times}}$$

Suppose that $M = \langle x_1, \ldots, x_m \rangle$, i.e. that $\{x_1, \ldots, x_m\}$ is a finite generating set, and S a basis. Then each of the finitely many generators x_i can be uniquely written as

$$x_i = \sum_{\text{finite}} \alpha_{ij} s_j \qquad \text{with } \alpha_{ij} \in R, s_j \in S\,.$$

Thus there is a finite subset of S, which generates M and is still free as a subset of a free set.

6. Given finitely many modules $M_1, \ldots, M_m$ and $N_1, \ldots N_n$ over a ring R, then the universal property of the direct sum resp. the direct product imply the natural identification

$$\mathrm{Hom}_R(M_1 \oplus \cdots \oplus M_m, N_1 \oplus \cdots \oplus N_n) \xrightarrow{\sim} \prod_{i=1}^{m} \mathrm{Hom}_R(M_i, \prod_{j=1}^{n} N_j) \xrightarrow{\sim} \prod_{i,j} \mathrm{Hom}_R(M_i, N_j)\,.$$

Writing the elements of the direct sum $M_1 \oplus \cdots \oplus M_m$ as column vectors, where the entry of the ith row lives in M_i, then every homomorphism between the direct sums can be described as a matrix, whose entries are homomorphisms in $\mathrm{Hom}_R(M_i, N_j)$. The composition of homomorphisms between the direct sums is then described by the familiar matrix multiplication.

Finitely generated free modules can be decomposed into copies of R as in (5), and morphisms between them are thus modelled by matrices with entries in $\mathrm{Hom}_R(R, R) \cong R$. The latter isomorphism is given by $\phi \mapsto \phi(1)$ with inverse $R \ni r \mapsto (\phi(s) := sr)$, cf. Examples 1.1.9.

Theorem 1.3.3 If R is a non-zero *commutative* ring with 1 and M a free R-module, then any two bases of M have the same cardinality. This cardinality is called the rank of the module M. It can be, but need not be, finite. In case of finite rank

$$\mathrm{rank}_R M = n \iff M \cong R^n\,.$$

Proof. Let $\mathfrak{m}$ be a maximal ideal in R which exists by Zorn's lemma, see appendix. As R is commutative, the quotient $K := R/\mathfrak{m}$ is a field, and by Remark 1.1.22.5 the quotient $M/\mathfrak{m}M$ is a vector space over K.

Let S be a basis of the free module M, i.e. $M \cong \bigoplus_{s \in S} Rs$. Then $\mathfrak{m}M \cong \bigoplus_{s \in S} \mathfrak{m}s$, and for the quotient we get

$$M/\mathfrak{m}M \cong \bigoplus_{s \in S} Ks.$$

Thus we have $\dim_K(M/\mathfrak{m}M) = |S|$ and the assertion follows from the linear algebra fact that all bases of a given K-vector space have the same cardinality. □

Remark 1.3.4 For arbitrary rings R an isomorphism $R^n \cong R^m$ as R-left modules does not generally imply $n = m$. The simplest counterexample is the null ring (it is also the only commutative counterexample).

Here is a more interesting counterexample over a non-commutative ring R. Let K be a field and V the free K-vector space over the set $\mathbb{N}$ of natural numbers. Every isomorphism of sets $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$ induces an isomorphism of vector spaces $V \xrightarrow{\sim} V \oplus V$. Let $R := \mathrm{End}_K(V)$. Then we get an isomorphism of R-modules

$$R \;=\; \mathrm{End}_K(V) \xrightarrow{\sim} \mathrm{Hom}_K(V \oplus V, V) \;\cong R \oplus R\;.$$

The next results concerns a relationship between free modules and arbitrary modules.

Theorem 1.3.5 Let R be a unital ring. Every R-module M is a homomorphic image of a free R-module.

Proof. We define a (very large) free module with basis M:

$$F := \bigoplus_{m \in M} R_m \qquad \text{with } R_m \cong R \quad \text{for all } m \in M \ .$$

The map

$$\begin{array}{rcl} F & \to & M \\ (\alpha_m)_{m \in M} & \mapsto & \displaystyle\sum_{m \in M} \alpha_m m \end{array}$$

is a surjective R-module homomorphism since R is unital. □

For the $\mathbb{Z}$-module $\mathbb{Z}/5\mathbb{Z}$ the proof constructs a surjective homomorphism $\mathbb{Z}^5 \to \mathbb{Z}/5\mathbb{Z}$. However, the usual quotient morphism $\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ sending $l \mapsto l \bmod 5$ would already be sufficient to show the statement in Theorem 1.3.5

Theorem 1.3.6 Let F and M be R-modules with F free. Let $f\colon M \twoheadrightarrow F$ be a surjective homomorphism. Then there exists an R-module homomorphism

$$g\colon F \to M$$

such that $f \circ g = \mathrm{id}_F$, and we have $M \cong \ker f \oplus \operatorname{Im} g$. One says that g splits the epimorphism f.

We remark that the module homomorphism g is typically not uniquely determined — already in the case of vector spaces choices of complement are not unique. The surjective $\mathbb{Z}$-module morphism $\mathbb{Z} \to \mathbb{Z}_5$ does not split: the only morphism $\mathbb{Z}_5 \to \mathbb{Z}$ is the zero morphism, since the abelian group $\mathbb{Z}$ does not contain elements of order 5.

Proof.

- Let S be a basis of F. Choose a preimage $m_s \in f^{-1}(s) \subset M$ for every $s \in S$ and define

  $$g\colon F \to M$$

  by $s \mapsto m_s$ on the basis vectors $s \in S$, i.e.

  $$\sum_{s \in S} \alpha_s s \mapsto \sum_{s \in S} \alpha_s m_s \qquad \alpha_s \in R.$$

  This is a well-defined R-module homomorphism since the representation of elements of F in terms of linear combinations of the $s \in S$ is unique, because F is free. Then we have

  $$f \circ g(s) = f(m_s) = s \quad \text{for all } s \in S$$

  and so $f \circ g = \mathrm{id}_F$.

- Now we use g to decompose every $x \in M$ as follows:

  $$x = gf(x) + (x - gf(x)) \, .$$

Clearly $gf(x) \in \operatorname{Im} g$, and furthermore

$$f(x - gf(x)) = f(x) - f(x) = 0 \ .$$

Thus we have written M as sum of submodules, $M = \ker f + \operatorname{Im} g$. This sum is direct: If $x \in \ker f \cap \operatorname{Im} g$, then $x = g(y)$ for a $y \in F$ and $0 = f(x) = fg(y) = y$, and so $y = 0$, which implies $x = 0$. □

Corollary 1.3.7 If N is a submodule of M, such that the quotient module M/N is free, then there exists a submodule N' of M, such that

$$M = N \oplus N' \quad \text{and} \quad N' \cong M/N.$$

In other words, the submodule N has a complement N' in M.

Proof. Applying Theorem 1.3.6 to the canonical surjection $M \twoheadrightarrow N$, we find a morphism $g : M/N \to M$ and a direct sum decomposition $M = \ker f \oplus \operatorname{Im} g$. The kernel of the canonical surjection is N. Since g has a left inverse, g is injective, and we can identify $\operatorname{Im} g \cong M/N =: N'$. □

The $\mathbb{Z}$-submodule $5\mathbb{Z} \subset \mathbb{Z}$ is an example of a submodule for which there is no complement.

One might be tempted to think that free modules can be characterized by the property expressed in Theorem 1.3.6. However, there are modules that satisfy this property without being free. Instead the property from Theorem 1.3.6 is characterizing for the class of projective modules, the subject of the next subsection. Their importance stems from the fact that their characterizing property can be formulated purely in terms of morphisms: it is "categorical". The correct universal property that characterizes free modules will be discussed in the exercises.

1.4 Projective, flat, divisible and injective modules

Can we hope to describe arbitrary modules by free modules? We know from Remark 1.3.2 that the $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ is not free. But it is a quotient of the free module $\mathbb{Z}$ under $\pi\colon \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ with $l \mapsto \bar{l}$. The kernel of π is the submodule $2\mathbb{Z} \subset \mathbb{Z}$, itself another free module. So, $\mathbb{Z}/2\mathbb{Z}$ can be described as a quotient of free modules. Actually we need a more general framework:

Definition 1.4.1 Let R be a ring. We consider sequences of R-modules and module homomorphisms:

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

Such a sequence is called an R-chain complex if $f_i \circ f_{i+1} = 0$ holds for all i. A sequence is called exact, if $\ker(f_i) = \operatorname{Im}(f_{i+1})$ holds for all i.

Remarks 1.4.2

1. The condition on consecutive maps in a chain complex can also be expressed as $\operatorname{Im}(f_{i+1}) \subseteq \ker(f_i)$.

2. Analogously one can define finite or half-infinite sequences define; exactness is only called for, where it makes sense. For example, every 2-step sequence $M \to N$ is exact, since it contains no conditions.

3. The morphisms f_n in a chain complex (M_n, f_n) are usually collectively called the differential and one uses the letter d for it. The notation for the chain complex is often abbreviated $M_\bullet$, where the black dot indicates that one is working with a $\mathbb{Z}$-graded chain complex.

4. Of special interest in homological algebra are the short exact sequences. These are of the form
$$0 \to M' \xrightarrow{\iota} M \xrightarrow{p} M'' \to 0 \ .$$
The exactness at M' means that ι is injective. The exactness are M'' means that p is surjective. The exactness at M can be expressed equivalently by the following two isomorphisms:
$$M' \cong \operatorname{Im}\iota = \ker p \quad \text{resp.} \quad M'' \cong M/\ker p = M/\operatorname{Im}\iota = \operatorname{coker}\iota \ .$$

5. For every $n \in \mathbb{N}$ the map $\mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}$ that sends $x \mapsto nx$ is an injective homomorphism of abelian groups. This fits into the short exact sequence of abelian groups
$$0 \to \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0.$$

6. Chain complexes appear in (almost) all areas of mathematics. In differential geometry for each smooth manifolds X one considers the de Rham complex $\Omega^\bullet(X)$, a chain complex of smooth differential forms on X. The smooth p-forms $\Omega^p(X)$ form a module over the ring $C^\infty(X)$ of smooth functions on X. The differential is in this case the exterior derivative. Exactness of the de Rham complexes would mean that all closed differential forms indeed exact. In algebraic topology there are several invariants of (certain kinds of) topological spaces that take values in chain complexes of abelian groups. Some of these are even used in data science and computer graphics. Another example in pure mathematics is the Khovanov chain complex of a knot, which is a knot invariant that categorifies the Jones polynomial.

Theorem 1.4.3 Let $0 \to M' \xrightarrow{\iota} M \xrightarrow{p} M'' \to 0$ be an exact sequence. Then the following are equivalent:

1. The injection ι admits a retraction, i.e. there exists an R-module homomorphism $\pi\colon M \to M'$ with the property $\pi \circ \iota = \mathrm{id}_{M'}$.
2. The surjection p admits a section, i.e. there exists an R-module homomorphism $s\colon M'' \to M$ with the property $p \circ s = \mathrm{id}_{M''}$.
3. There exists an isomorphism $\phi\colon M \to M' \oplus M''$ of R-modules, such that $\phi \circ \iota = \iota_1$ and $pr_2 \circ \phi = p$.

The proof will be an exercise. To understand the last condition better, we consider the commutative diagram
$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{\iota} & M & \xrightarrow{p} & M'' & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \phi} & & \| & & \\ 0 & \longrightarrow & M' & \xrightarrow{\iota_1} & M' \oplus M'' & \xrightarrow{pr_2} & M'' & \longrightarrow & 0 \end{array}$$
where the lower row contains the injection ι_1 of M' into the direct sum and the surjection pr_2 onto M'' out of the direct product. Here we have an instance of "isomorphic (short) exact sequences" in a sense that will be made precise in Section 6.7.

Definition 1.4.4 A short exact sequence, that satisfies one (and thus all) of the three equivalent conditions in Theorem 1.4.3, is said to split.

Examples 1.4.5

1. Short exact sequences of vector spaces always split, as every vector subspace has a complement, see Corollary 1.3.7.

2. The short exact sequence of $\mathbb{Z}$-modules $0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}_4 \to \mathbb{Z}/2\mathbb{Z} \to 0$ does not split, for otherwise we would have $\mathbb{Z}_4 \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Free modules are too special for the purposes of many constructions in homological algebra. Moreover, they are defined using the set underlying a module. To single out a better class of modules, we first note the following general property of modules:

Lemma 1.4.6 Let M be an R-module and

$$0 \to T' \xrightarrow{\iota} T \xrightarrow{\pi} T'' \to 0$$

a short exact sequence of R-modules. Then the sequence of abelian groups

$$0 \to \mathrm{Hom}_R(M, T') \xrightarrow{\iota_*} \mathrm{Hom}_R(M, T) \xrightarrow{\pi_*} \mathrm{Hom}_R(M, T'')$$

is also exact. Here, the morphisms of abelian groups are induced by postcomposition with the map from the short exact sequence, e.g.

$$\begin{array}{rccc} \iota_* : & \mathrm{Hom}_R(M, T') & \to & \mathrm{Hom}_R(M, T) \\ & \phi & \mapsto & \iota \circ \phi \end{array}$$

Proof. Since $\iota \colon T' \to T$ is injective, an equality $\iota_*(\phi) \overset{\text{def}}{=} \iota \circ \phi = \iota \circ \phi' \overset{\text{def}}{=} \iota_*(\phi')$ implies $\phi = \phi'$. So, ι_* is also injective.

If $\phi \in \mathrm{Hom}(M, T)$ is in the image of ι_*, then there exists $\phi' \in \mathrm{Hom}(M, T')$ with $\phi = \iota_*\phi' = \iota \circ \phi'$. In this case $\pi_*(\phi) = \pi \circ \phi = \pi \circ \iota \circ \phi' = 0$, and so $\phi \in \ker \pi_*$.

Conversely, let $f \in \ker \pi_*$, i.e. $\pi_* f(m) = \pi \circ f(m) = 0$ for all $m \in M$. Then for every $m \in M$ we also have $f(m) \in \ker \pi = \mathrm{Im}\, \iota$. For every $m \in M$ we now find a $\phi'(m) \in T'$ with $\iota \circ \phi'(m) = f(m)$. As ι is injective, such $\phi'(m)$ are uniquely determined and ϕ' is a module homomorphism. By construction $\iota_*\phi' = f$, and so $f \in \mathrm{Im}\, \iota_*$. □

In the conclusion of the lemma we omitted "$\to 0$" for a reason. Indeed, if $\pi \colon T \to T''$ is a surjective morphism of modules is, then $\pi_* \colon \mathrm{Hom}_R(M, T) \to \mathrm{Hom}_R(M, T'')$ need not be a surjective morphism of abelian groups. For example, the morphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ of $\mathbb{Z}$-modukes is surjective, but the induced morphism

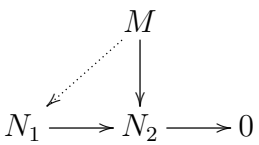
$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = 0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$$

is clearly not surjective. One says that $\mathrm{Hom}(M, -)$ is left-exact, but not exact, see Definition 3.1.13.

Next we generalize free modules to projective modules, which are characterized by the following theorem.

Theorem 1.4.7 Let R be a unital ring. The following statements about an R-module M are equivalent:

1. For every diagram



with exact row there exists a lift (dotted), making the diagram commute. (The lift need not be unique.)

2. There exists an R-module N, such that the R-module $M \oplus N$ is free.

3. Every short exact sequence of the form $0 \to N' \to N \to M \to 0$ splits.

4. For every short exact sequence of R-modules $0 \to T' \to T \to T'' \to 0$ the induced sequence of abelian groups

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

is also exact.

The formulation of this theorem illustrates that in homological algebra one often tends to avoid giving morphisms names. Note that the properties from the theorem are satisfied by every vector space over a field, but not by every every module. For example, the $\mathbb{Z}$-module $M = \mathbb{Z}/2\mathbb{Z}$:

1. The identity on M does not admit a lift

$$\begin{array}{ccccc} & & \mathbb{Z}/2\mathbb{Z} & & \\ & \swarrow & \downarrow{\scriptstyle \mathrm{id}} & & \\ \mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0\ , \end{array}$$

because the only group homomorphism $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$ is the trivial morphism.

2. There is no $\mathbb{Z}$-module of the form $M \oplus \mathbb{Z}/2\mathbb{Z}$ that is free. Already the elements of $\mathbb{Z}/2\mathbb{Z} \subset M \oplus \mathbb{Z}/2\mathbb{Z}$ have torsion. But a free $\mathbb{Z}$-module is of the form $\oplus_{i \in I}\mathbb{Z}$ and thus has no torsion elements.

3. The exact sequence

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

with its unique non-zero group homomorphisms does not split.

4. Applying $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, -)$ transforms the short exact sequence

$$0 \to \mathbb{Z} \xrightarrow{2\cdot} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0 \quad \text{into} \quad 0 \to 0 \to 0 \to \mathbb{Z}/2\mathbb{Z} \to 0,$$

which is not exact. Here we used $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) = 0$ and $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

Proof.

(1)⇒(3) The splitting of the sequence $0 \to N' \to N \to M \to 0$ is given by the lift of the identity in the diagram:

$$\begin{array}{ccccc} & & M & & \\ & \swarrow & \downarrow{\scriptstyle \mathrm{id}_M} & & \\ N & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

(3)⇒(2) By Theorem 1.3.5 every R-module M is the codomain of a surjective R-module homomorphism from a free module F, for example $F := \oplus_{m \in M} R$. Let $F \to M$ be such a surjection with kernel N'. Since the exact sequence $0 \to N' \to F \to M \to 0$ splits, Theorem 1.4.3 implies $F \cong M \oplus N'$ for the free module F.

(2)⇒(4) First we observe that (4) holds for every free module $M \cong \oplus_{i\in I} R$, where I is an indexing set for a basis of the free module M. In this case, $\mathrm{Hom}_R(M,N) \cong \mathrm{Hom}_R(\oplus_{i\in I} R, N) \cong \prod_{i\in I} N$ for every module N. The maps are simply the given maps, applied in every component.

If M is a direct summand of a free module, say $M \oplus N$, then the sequence

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

is exact. By the universal property of the direct sum from Remark 1.2.2(3) this exact sequence is termwise isomorphic to:

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

Note that the kernel of a product of maps is the product of the kernels of the individual maps, and the image of a product of maps is the product of the images; this we deduce the exactness of the sequence from (4).

(4)⇒(1) As $N_1 \to N_2$ is surjective, we get a short exact sequence

$$0 \to \ker((N_1 \to N_2)) \to N_1 \to N_2 \to 0$$

and (4) yields the exact sequence

$$0 \to \mathrm{Hom}_R(M, \ker(N_1 \to N_2)) \to \mathrm{Hom}_R(M, N_1) \to \mathrm{Hom}_R(M, N_2) \to 0$$

and the surjectivity of the second to last map is exactly the statement of (1). □

Definition 1.4.8 An R-module, that satisfies one (and thus all) of the four equivalent properties from Theorem 1.4.7 is called a projective module.

Examples 1.4.9

1. Free modules are projective by Theorem 1.4.7 (2). For $R = \mathbb{Z}$ every projective module is free since, as we will see later in Theorem 4.1.1, submodules of submodules of free $\mathbb{Z}$-modules are free, in particular, all direct summands of free modules are free. The same holds, as we will also see later, for every PID R. The Quillen–Suslin theorem says that every finitely generated projective module over the polynomial ring $F[x_1, \ldots, x_n]$ over a PID (thus in particular over a field F) is free. We refer to [K80, IV.3.15] and [L02, Theorem XX1.3.7] for proofs.

2. For $R = R_1 \times R_2$ with $R_2 \neq 0$, the R-module $M = R_1$ with $(r_1, r_2).m = r_1 \cdot m$ is a direct summand in $R_1 \oplus R_2 = R$ and thus projective, but not free: in fact, every element of $m \in M$ is linearly dependent since $(0, r_2).m = 0$ for all $r_2 \in R_2$. Thus there are no (nontrivial) linearly independent families. Note that the ring $R = R_1 \times R_2$ has zero divisors.

3. Examples of non-free projective modules over integral domains (i.e. rings without zero divisors) R need some number theory or algebraic geometry:

   Let $\tau := \sqrt{-5}$; consider the commutative ring $R = \mathbb{Z}[\tau]$. Let $M = \langle 2, 1+\tau \rangle$ be the ideal generated by 2 and $1+\tau$; as an ideal, it is an R-module.

   We first show that M is not free as an R-module. Suppose M were free. As for vector spaces, the rank of a free module is a lower bound for the cardinality of a generating set. (To see this one can argue as in Theorem 1.3.3 modulo a maximal ideal.) Thus the

rank of M is at most two. It actually cannot be two, because this would require two R-linearly independent generators, which themselves are R-linear combinations of 2 and $1+\tau$. But 2 and $1+\tau$ are linearly dependent over R, which is witnessed bythe relation $3 \cdot 2 + (\tau - 1)(1+\tau) = 0$.

Thus the module M is free if and only if it is of rank one, i.e. a principal ideal of R, i.e. $M = (a)$ for some $a \in R$. We then necesarily have $a|2$ and $a|1+\tau$. Now we show that 2 is irreducible in R, i.e. is not multiplicatively invertible and cannot be written as the product of two non-invertible elements. To show this, we define the norm map $N\colon R \to \mathbb{Z}$ by $N(x+\tau y) := x^2 + 5y^2$. The norm is multiplicative, $N(a \cdot b) = N(a) \cdot N(b)$, and so $N(b) = 1$ if and only if b is a unit, i.e. is multiplicatively invertible in R.

Since $N(2) = 4$ and $N(1+\tau) = 6$ neither 2 nor $1+\tau$ are units. A common non-unit factor a of 2 and $1+\tau$ must have $N(a) = 2$. But for $a = x+\tau y$ the equation $N(a) = x^2+5y^2 = 2$ does not have any solutions for $x, y \in \mathbb{Z}$. Thus M is not free. This also implies that M is a proper submodule of R, since the regular module is free.

To show that M is projective, we consider the surjective morphism provided by the generating set $2, 1+\tau$

$$\begin{array}{rccl} p\colon & R \oplus R & \to & M \\ & (r_1, r_2) & \mapsto & r_1 2 + r_2(1+\tau)\ . \end{array}$$

This epimorphism has a section:

$$s(2x + (1+\tau)y) = (-2x - (1+\tau)y, (1-\tau)x + 3y).$$

Thus, by Theorem 1.4.3, the module M is a direct summand in free module $R \oplus R$, and hence projective by Theorem 1.4.7.

4. Let X be a connected smooth manifold and $E \to X$ a smooth vector bundle of finite rank. The space of smooth sections $\Gamma(X, E)$ is a module over the ring $C^\infty(X)$ of smooth functions on X. If the manifold X is compact, then the module $\Gamma(X, E)$ is projective. The Serre–Sw ann theorem says that finitely generated projective $C^\infty(X)$-modules are in bijection with vector bundles of finite rank. For details, see e.g. [N03, Theorem 11.32].

Theorem 1.4.10 Let M be an R^{opp}-module and $0 \to N' \xrightarrow{\iota} N \xrightarrow{p} N'' \to 0$ a short exact sequence of R-modules.

1. Then for every R-module the sequence of abelian groups

$$M \otimes_R N' \xrightarrow{\mathrm{id}_M \otimes \iota} M \otimes_R N \xrightarrow{\mathrm{id}_M \otimes p} M \otimes_R N'' \to 0$$

is exact.

2. If M is projective, then even the sequence

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

is exact.

Compare the first statement with the statement for Hom in Lemma 1.4.6. One says that tensoring is right exact, see Definition 3.1.13.

To see how exactness on the left may fail in 1.4.10, note that for every abelian group A we have $A \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong A/nA$. Indeed, the morphism

$$\begin{array}{ccc} A & \to & A \otimes_{\mathbb{Z}} \mathbb{Z}_n \\ a & \mapsto & a \otimes 1 \end{array}$$

has kernel nA. In particular $\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Q}/2\mathbb{Q} \cong 0$. Now tensoring with $\mathbb{Z}/2\mathbb{Z}$ transforms the short exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0 \quad \text{into} \quad 0 \to \mathbb{Z}/2\mathbb{Z} \to 0 \to 0 \to 0,$$

which is clearly not exact.

Proof. • For the first part we have to show exactness at $M \otimes_R N''$ and at $M \otimes_R N$. Let $x = \sum m_i \otimes n_i'' \in M \otimes_R N''$. As $N \to N''$ is surjective, we can find preimages $n_i \in N$ of the $n_i'' \in N''$. Then $M \otimes_R N \to M \otimes_R N'$ maps $\sum m_i \otimes n_i \mapsto x$, which establishes the required surjectivity.

For exactness at $M \otimes_R N$ we consider the quotient

$$Q := \operatorname{coker}(M \otimes_R N' \xrightarrow{\mathrm{id}_M \otimes \iota} M \otimes_R N) \equiv (M \otimes_R N)/\mathrm{Im}\,(M \otimes_R N' \to M \otimes_R N)$$

as well as the map $M \otimes_R N \xrightarrow{\mathrm{id}_M \otimes p} M \otimes_R N''$ of abelian groups. The image of $\mathrm{id}_M \otimes \iota$ is in the kernel of $\mathrm{id}_M \otimes p$, so the latter factors through a map

$$\begin{array}{ccc} Q & \to & M \otimes_R N'' \\ [m \otimes n] & \mapsto & m \otimes p(n) \end{array}$$

by

$$\begin{array}{ccc} M \otimes_R N & & \\ {\scriptstyle \mathrm{can}}\downarrow & \searrow^{\mathrm{id}_M \otimes p} & \\ Q & \dashrightarrow & M \otimes_R N'' \end{array}$$

We claim that this is an isomorphism. Once the claim is proved, the isomorphism theorem implies $\mathrm{Im}\,(M \otimes_R N' \to M \otimes_R N) = \ker(M \otimes_R N \to M \otimes_R N'')$, i.e. exactness.

To prove the claim, we construct the inverse map $M \otimes_R N'' \to Q$: to find its image on $m \otimes n''$ we choose a preimage $n \in N$ of n'' and set $m \otimes n'' \mapsto [m \otimes n]$. This is well-defined: every other choice of preimage is of the form $n + k$ with $k \in \ker(p) = \mathrm{Im}\,(\iota)$ and thus defines the same class in the cokernel Q.

The map thus defined is an isomorphism with inverse $[m \otimes n] \mapsto m \otimes p(n)$.

• For the second part of the theorem we have to show that injective maps stay injective upon tensoring $M \otimes_R -$ with a projective right module M.

We first consider the case when M is not just projective, but actually free, $M = \oplus_{i \in I} R$. By distributivity of $\otimes_R$ for direct sums, this case yields

$$\begin{array}{ccc} M \otimes_R N' & \xrightarrow{\mathrm{id}_M \otimes \iota} & M \otimes_R N \\ \downarrow \cong & & \downarrow \cong \\ \oplus_{i \in I} N' & \xrightarrow{\oplus \iota} & \oplus_{i \in I} N \end{array}$$

where the map on every component (indexed by $i \in I$) is given by ι. Here we have used $R \otimes_R N \cong N$ for every N. The lower row is injective if and only if $\iota\colon N' \to N$ is injective.

A projective module M is a direct summand of a free module F by Theorem 1.4.7, say $M \oplus \tilde{M} \cong F$. Again by distributivity of $\otimes_R$ we have a commuting diagram

$$\begin{array}{ccc} F \otimes_R N' & \longrightarrow & F \otimes_R N \\ \downarrow \cong & & \downarrow \\ M \otimes_R N' \oplus \tilde{M} \otimes_R N' & \longrightarrow & M \otimes_R N \oplus \tilde{M} \otimes_R N \end{array}$$

with the map given as direct sum. Thus it is injective on every summand.

□

We define two additional notions for modules over a ring:

Definition 1.4.11

1. An R-module M is called <u>flat</u>, if tensoring $- \otimes_R M$ preserves short exact sequences, or equivalently, if tensoring with M preserves the injectivity of maps.

2. A module is called <u>divisible</u>, if for every $0 \neq r \in R$ the map $M \xrightarrow{r.} M$, given by scalar multiplication with r, is surjective.

Example 1.4.12 Exchanging the two sides of the tensor product in Theorem 1.4.10 shows that all projective modules are flat. There are, however, flat modules that are not projective:

The $\mathbb{Z}$-module $\mathbb{Q}$ is flat. Indded, consider an injective morphism of $\mathbb{Z}$-modules $M' \hookrightarrow M$. Then the kernel of the composite map $M' \to M \to M \otimes_{\mathbb{Z}} \mathbb{Q}$ where $M \to M \otimes_{\mathbb{Z}} \mathbb{Q}$ is given by $m \mapsto m \otimes 1$, is by Example 1.2.6.4 exactly the set of those $m' \in M'$, whose image in M is a torsion element. By injectivity of the morphism $M' \to M$ this can only happen if m' is torsion already in M, but then already $m' \otimes 1 = 0 \in M' \otimes_Z \mathbb{Q}$.

However, $\mathbb{Q}$ is not projective over $\mathbb{Z}$; for otherwise it would admit an embedding into a free $\mathbb{Z}$-module (even as direct summand), which is impossible as $\mathbb{Q}$ is a divisible $\mathbb{Z}$-module, but free $\mathbb{Z}$-modules are never divisible.

Dual to the definition of projective modules is the notion of injective modules. For a morphism $f\colon T_1 \to T_2$ of R-modules we consider the morphism of algebras induced by precomposition:

$$\begin{array}{rccc} f^*\colon & \mathrm{Hom}(T_2, N) & \to & \mathrm{Hom}(T_1, N) \\ & \varphi & \mapsto & \varphi \circ f \end{array}$$

Note the order of T_1 and T_2 in the Hom-spaces! The proof of the following proposition will be completed in Section 3.3.

Theorem 1.4.13 The following statements about an R-module M are equivalent:

1. For every diagram

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

with exact row there exists a lift (dotted), making the diagram commute.

2. Every short exact sequence $0 \to M \to N_1 \to N_2 \to 0$ splits.

3. For every short exact sequence of R-modules $0 \to T' \to T \to T'' \to 0$, the induced sequence of abelian groups

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

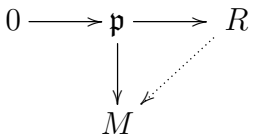
is also exact.

Proof. The implication (1) ⇒(2) is proved analogously to (1)⇒(2) in Theorem 1.4.7 for projective modules, by reversing the arrows. Similarly, (3)⇒(1) here is analogous to (4)⇒(1) in Theorem 1.4.7.

We are still missing an analogue of the characterization of projective modules as direct summands of free modules. This will be considered in 3.3, after which we will complete the proof here in analogy to Theorem 1.4.7. □

Definition 1.4.14 An R-module that satisfies one (and thus all) of the three equivalent properties from Theorem 1.4.13 is called an injective module.

Theorem 1.4.15 [Baer's criterion] An R-module M is injective if and only if for every ideal $\mathfrak{p}$ in R and every morphism $\mathfrak{p} \to M$ of R-left modules, the lifting property from Theorem 1.4.13 holds:

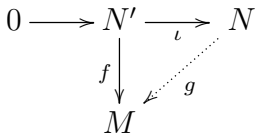


Proof.

- If M injective the lifting property follows from 1.4.13.1 in the special case of R-modules $N_1 = \mathfrak{p}$ and $N = R$.

- The converse for modules that are not finitely generated is an application of Zorn's lemma (see Appendix A):

  Let $0 \to N' \xrightarrow{\iota} N$ be an injective morphism of R-modules and $f\colon N' \to M$ an arbitrary morphism of R-modules. In the diagram



  we have to find a morphism g defined on all of N, such that the diagram commutes. We say that g extends f from the submodule N' to N. To this end we consider the set of all extensions,

$$X := \{(K, g) \,|\, N' \subseteq K \subseteq N, g\colon K \to M \text{ is an extension of } f\} \,.$$

  The set X contains the trivial extension (N', f), and is thus non-empty. We define a partial order on X by

$$(K, g) \leq (K', g') \overset{\text{def}}{\iff} K \subseteq K' \text{ and } g'|_K = g \,.$$

  It is straightforward to see that every totally-ordered subset of X has the union as an upper bound. By Zorn's lemma X has a maximal element $g_0\colon K_0 \to M$, and we have to show that $K_0 = N$.

  Suppose $K_0 \neq N$, then we could find $n \in N \setminus K_0$ and set $\mathfrak{p} := \{r \in R | r.n \in K_0\}$. This ideal is not the zero ideal, for otherwise the inner sum $K' := K_0 + Rn$ would be direct.

In that case we could extend g_0 to K' by specifying some value of M as image of n, in contradiction to the maximality of K_0.

Now consider the module homomorphism $g_0 \circ n \colon \mathfrak{p} \xrightarrow{\cdot n} K_0 \xrightarrow{g_0} M$. By assumption it can be extended to a module homomorphism $\tilde{g} \colon R \to M$. Consider on $K' := K_0 + Rn \subset N$ the extension $g'(k + rn) = g_0(k) + \tilde{g}(r)$. This g' is well-defined because $\tilde{g}$ is an extension of $g \circ n$, i.e. agrees with g_0 on the intersection $\mathfrak{p} \cong Rn \cap K_0$. But then $(K', g') > (K_0, g_0)$, a contradiction to the maximality of (K_0, g_0). □

Corollary 1.4.16 A module M over a PID R is injective if and only if it is divisible, i.e. if the multiplication by any ring element $r \in R \setminus \{0\}$ is surjective.

Proof. • We show that an R-module is divisible if and only if it satisfies Baer's lifting criterion from Theorem 1.4.15. In the PID R all ideals are of the form $\mathfrak{p} = (\alpha)$ for some $\alpha \in R$. Consider the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & (\alpha) & \longrightarrow & R \\ & & \downarrow{\scriptstyle \phi} & \swarrow{\scriptstyle \tilde{\phi}} & \\ & & M & & \end{array}$$

Then ϕ is determined by its value $\phi(\alpha)$ on the generator α of the principal ideal and $\tilde{\phi}$ by its value on the generator $1 \in R$.

- If M is divisible, then we can find $\tilde{m} \in M$ with $\alpha.\tilde{m} = \phi(\alpha)$. We define the morphism $\tilde{\phi}$ by prescribing the value $\tilde{\phi}(1) := \tilde{m}$ on the generator $1 \in R$. For α we then have the equation $\tilde{\phi}(\alpha) = \alpha\tilde{\phi}(1) = \alpha\tilde{m} = \phi(\alpha)$, i.e. $\tilde{\phi}|_{(\alpha)} = \phi$. Hence, divisible R-modules have the lifting property for ideals and are, thus, injective by Baer's criterion from Theorem 1.4.15.

- Conversely, let M be injective and satisfy the lifting property from 1.4.13. To see that M is divisible, let $\alpha \in R \setminus \{0\}$ and $m \in M$ be given and we have to find an $\tilde{m} \in M$ with $\alpha\tilde{m} = m$. To this end we consider the previous diagram with ϕ defined by $\phi(\alpha) = m$, find $\tilde{\phi}$ using lifting property, and set $\tilde{m} := \tilde{\phi}(1) \in M$. Then we have

$$m = \phi(\alpha) = \tilde{\phi}(\alpha) = \alpha\tilde{\phi}(1) = \alpha\tilde{m} \ .$$

□

In particular, an abelian group considered as a $\mathbb{Z}$-module is injective if and only if it is divisible, i.e. if the multiplication with any $n \in \mathbb{Z} \setminus \{0\}$ is surjective. Examples of injective abelian groups are the divisible groups $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$; examples of non-injective modules are given by free $\mathbb{Z}$-modules, which are never divisible.

1.5 Simple modules and composition series

We have already met several important classes of modules, such as free, projective, injective, and flat modules. Finally, we will also consider simple modules; despite the name, their structure is actually not so "simple".

Definition 1.5.1

1. A module M over a ring is called simple, if it is nonzero has no submodules except the zero module and M itself.

2. Similarly, a representation V of a group G is called irreducible or simple, if $V \neq 0$ and 0 and V are the only subrepresentations of V.

3. A module M over a ring is called indecomposable, if it is nonzero and there are no two nonzero submodules N_1 and N_2, such that $M = N_1 \oplus N_2$.

4. Similarly, a representation V of G is indecomposable, if V is nonzero and the are no two nonzero subrepresentations $W_1, W_2 \subset V$, such that V is the inner direct sum $V = W_1 \oplus W_2$.

Lemma 1.5.2

1. Let R be a ring and M an R-module. Then M is simple if and only if every $x \in M$ with $x \neq 0$ is a generator of M. Simple modules are thus, in particular, cyclic.

2. Every generator m of a cyclic module M defines a surjection:

$$\begin{array}{rccc} \phi_m : & R & \to & M \\ & r & \mapsto & r.m \end{array}$$

   Its kernel is a *maximal* left ideal of R if and only if M is simple.

Proof. 1. Let M be a simple module. Consider for $x \in M$, $x \neq 0$ the submodule $\langle x \rangle$ generated by x. Since $1.x = x \in \langle x \rangle$, this submodule is nonzero. Since M has no non-trivial proper submodules, we must have $\langle x \rangle = M$.

   Conversely, let us assume that every nonzero $x \in M$ is a generator. Suppose $U \subset M$ is an arbitrary nonzero submodule. Choose $x \in U$ with $x \neq 0$; this is a generator of M and thus $M = \langle x \rangle \subset U \subset M$. This shows $U = M$ hence M has no nonzero proper submodules.

2. Let M be simple; suppose the kernel were not a maximal left ideal, but rather strictly contained in a maximal ideal $\mathfrak{m}$, i.e. $\ker \phi_m \subsetneq \mathfrak{m} \subsetneq R$. Then $\phi_m(\mathfrak{m}) \subsetneq M$ would be a nonzero proper submodule of M, in contradiction to simplicity.

   Conversely, let $\ker \phi_m$ be maximal, but suppose there exists a submodule U with $0 \subsetneq U \subsetneq M$. Then $\ker \phi_m \subsetneq \phi_m^{-1}(U) \subsetneq R$, in contradiction to maximality of the ideal $\ker \phi_m \subset R$. □

Warning: not every cyclic module is simple. For example the $\mathbb{Z}$-module $\mathbb{Z}/6\mathbb{Z}$ is cyclic, but by the Chinese remainder theorem $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ not simple. For another counterexample consider the polynomial ring $R = K[X]$ over a field K and the R-module given by a K-vector space with an endomorphism consisting of a single Jordan block of size at least two. Finally, the regular module ${}_R R$ is cyclic, but typically not simple.

Examples 1.5.3

1. Representations of groups on a K-vector space of dimension 1 are irreducible.

2. If char $K \neq 2$ then the group $\mathbb{Z}/2\mathbb{Z}$ two irreducible one-dimensional representations $K_\pm$. By Example 1.1.18 (8), every finite-dimensional $\mathbb{Z}/2\mathbb{Z}$-representation over K is completely reducible, i.e. isomorphic to a unique representation of the form

$$K_+^m \oplus K_-^n \quad \text{with } m, n \in \mathbb{N}\,.$$

3. If char $K = 2$, then the trivial one-dimensional representation K is irreducible and there exists a two-dimensional representation P that is indecomposable, but not irreducible, see Example 1.1.18 (8). Every finite-dimensional representation is isomorphic to

$$K^n \oplus P^m \quad \text{with } \; n, m \in \mathbb{N}\,.$$

   The representation P is actually a free module of rank 1 and, thus, projective and cyclic.

4. Consider the quotient $K[X]/(X^2)$ of the polynomial ring. It has, up to isomorphism, a single indecomposable projective module and a single, one-dimensional simple module which is free.

Lemma 1.5.4 Let R be a ring, E a simple R-module, and M an arbitrary R-module.

1. Every homomorphism $E \to M$ is injective or zero because the kernel is a submodule of E.

2. Every homomorphism $M \to E$ is surjective or zero because the image is a submodule of E.

3. The endomorphism ring $\mathrm{End}_R(E)$ is a division ring, i.e. all nonzero endomorphisms are invertible.

Theorem 1.5.5 [Schur's lemma]
Let K be an algebraically closed field and A a K-algebra. Let M be a simple A-module, that is finite-dimensional as K-vector space, $\dim_K M < \infty$.

Then M has no endomorphisms except scalar multiples of the identity:

$$\begin{array}{ccc} K & \xrightarrow{\sim} & \mathrm{End}_A(M) \\ \lambda & \mapsto & \lambda \mathrm{id}_M \end{array} .$$

Proof. As M is simple by assumption, we have $M \neq 0$. Every endomorphism $\varphi \in \mathrm{End}_A(M)$ has at least one eigenvalue λ since $\dim_K M < \infty$ and K is algebraically closed. The corresponding eigenspace the kernel of the module homomorphism $\varphi - \lambda \,\mathrm{id}_M$ and thus a submodule of M. As M is simple, the kernel must be equal to M, i.e. $\varphi = \lambda \,\mathrm{id}_M$. □

Remarks 1.5.6

1. For a finite group G, the group algebra $K[G]$ is finite-dimensional over K and so is every irreducible representation V, since it appears as a quotient of $K[G]$ by Lemma 1.5.2. For such V we can drop the separate assumption on finite-dimensionality in Schur's lemma.

2. Every finite-dimensional irreducible representation of an *abelian* group over an algebraically closed field is one-dimensional. This is because every group element $g \in G$ acts on a finite-dimensional representation by an endomorphism $\rho(g)$ of the representation:

   $$\rho(g)\rho(h) = \rho(gh) = \rho(hg) = \rho(h)\rho(g) \quad \text{for all} \quad h \in G \ .$$

   Schur's lemma 1.5.5 now implies that all group elements act by multiples of the identity, and so the representation can be decomposed into a direct sum of one-dimensional subrepresentations.

3. We consider an example over the field of real numbers. The group of fourth roots of unity in the complex numbers, $G = \{\pm 1 \pm \mathrm{i}\} \cong \mathbb{Z}_4$ acts by multiplication on the two-dimensional $\mathbb{R}$-vector space $V = \dot{\mathbb{C}}$. They act by rotations, thus there are no invariant one-dimensional subvector spaces. We thus obtain an irreducible real representation of G on $\dot{\mathbb{C}}$, but we also have

   $$K = \mathbb{R} \subsetneqq \mathrm{End}_G(V) \cong \mathbb{C}$$

   as $\mathbb{R}$-algebra. Indeed, the field $\mathbb{R}$ is not algebraically closed, so that we cannot apply Schur's lemma 1.5.5. Note, however, that the endomorphism ring $\mathbb{C}$ is a division ring over the field $\mathbb{R}$, compatible with Lemma 1.5.4.

4. Let $K \subset L$ be a proper field extension. Then the K-vector space $V = L$ carries a representation of the group $G = L^\times$ over K. Every element of $L \setminus \{0\}$ is a generator for the $L^\times$-action, so the representation is irreducible by Lemma 1.5.2. In this example

$$\mathrm{End}_G V = L \ ,$$

which is not equal to K, even when K is algebraically closed. But for algebraically closed K a proper field extension L/K is not finite-dimensional!

A natural question is, how to build modules from simple modules. This leads to the following definition:

Definition 1.5.7 Let R be a ring and M an R-module. M is said to be of finite length if and only if there exists a *finite* chain of submodules

$$M = M_r \supset M_{r-1} \supset \ldots \supset M_0 = 0,$$

such that all quotient modules M_i/M_{i-1} are simple. Such a chain is called composition series of M, the modules M_i/M_{i-1} are called subquotients of the composition series. The minimal possible length r of a composition series is called the length of the module M.

We will see that a version of the theorem of Jordan-Hölder holds for modules. The subquotients are unique up to ordering and are called the composition factors of the module M.

For this we will need the following important lemma.

Lemma 1.5.8 [Nine lemma] Consider a diagram of modules with short exact rows:

$$\begin{array}{ccccc}
A' & \xrightarrow{\iota_1} & A & \xrightarrow{\pi_1} & A'' \\
\downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} \\
B' & \xrightarrow{\iota_2} & B & \xrightarrow{\pi_2} & B'' \\
\downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_2} & & \downarrow{\scriptstyle \psi_3} \\
C' & \xrightarrow{\iota_3} & C & \xrightarrow{\pi_3} & C''
\end{array}$$

such that the vertical composites are zero, i.e. $\psi_i \circ \varphi_i = 0$ for $i = 1, 2, 3$. Suppose the diagram is commutative in the sense, that all 4 squares commute. Now if two of the columns are short exact sequences, then also the third column is a short exact sequence.

Proof. We only consider the case, in which the left middle column are assumed to be short exact sequences.

- The surjectivity of ψ_3 follows from the commutativity of the lower right square, $\psi_3 \circ \pi_2 = \pi_3 \circ \psi_2$. This implies

$$\mathrm{Im}\,(\psi_3) \supseteq \mathrm{Im}\,(\psi_3 \circ \pi_2) = \mathrm{Im}\,(\pi_3 \circ \psi_2) = C'' \,,$$

since π_3 and ψ_2 are surjective by assumption.

- To show the injectivity of φ_3 we consider $a'' \in A''$, such that $\varphi_3(a'') = 0$. By surjectivity of π_1 we find a preimage $a \in A$ under π_1:

$$\pi_1(a) = a'' \,.$$

Define $b := \varphi_2(a) \in B$. This element has two properties:

$$\begin{aligned} \psi_2(b) &= \psi_2 \circ \varphi_2(a) = 0 \quad \text{because } \psi_2 \circ \varphi_2 = 0 \\ \pi_2(b) &= \pi_2 \circ \varphi_2(a) = \varphi_3 \circ \pi_1(a) = \varphi_3(a'') = 0\ . \end{aligned}$$

The last property and the exactness of the second row let us find a $b' \in B'$, such that

$$b = \iota_2(b')$$

and the first property then implies

$$\iota_3 \circ \psi_1(b') = \psi_2 \circ \iota_2(b') = \psi_2(b) = 0\,.$$

As ι_3 is injective, we deduce $\psi_1(b') = 0$. Now we use the exactness of the first column to find a preimage of b' in A', i.e.

$$b' = \varphi_1(a') \quad \text{with} \quad a' \in A'.$$

We now compute $\varphi_2 \circ \iota_1(a') = \iota_2\varphi_1(a') = \iota_2(b') = b = \varphi_2(a)$. Now φ_2 was assumed to be injective, so we have $i_1(a') = a$. Then we get $a'' = \pi_1(a) = \pi_1 i_1(a') = 0$ by exactness of the first row, which shows that φ_3 is injective.

- $\operatorname{Im}\varphi_3 \subset \ker\ \psi_3$ was already part of our assumptions, so we have to show the reverse inclusion. Let $b'' \in \ker\psi_3$. As π_2 is surjective we find a preimage $b \in B$, such that $\pi_2(b) = b''$. We compute

$$0 = \psi_3(b'') = \psi_3 \circ \pi_2(b) = \pi_3 \circ \psi_2(b)\,,$$

which, by exactness of the third row, implies that $c := \psi_2(b)$ can be written as $i_3(c') = c$. As ψ_1 is surjective we find a preimage $b' \in B'$, such that $\psi_1(b') = c'$. We consider the difference $x_b := -\iota_2(b') + b \in B$:

$$\begin{aligned} \pi_2(x_b) &= -\pi_2 \circ \iota_2(b') + \pi_2(b) = \pi_2(b) = b'' \\ \psi_2(x_b) &= -\psi_2\iota_2(b') + \psi_2(b) = -\iota_3\psi_1(b') + c \\ &= -\iota_3(c') + c = -c + c = 0. \end{aligned}$$

By the last equation and exactness of the second column there exists $a \in A$, such that $\varphi_2(a) = x_b$. Set $a'' := \pi_1(a)$ and compute

$$\varphi_3(a'') = \varphi_3 \circ \pi_1(a) = \pi_2 \circ \varphi_2(a) = \pi_2(x_b) = b''\,.$$

Thus we have $b'' \in \operatorname{Im}\varphi_3$; and so the right column is exact. □

The technique used in this proof is called a diagram chase.

Theorem 1.5.9 [Jordan-Hölder theorem]

1. If a module M has finite length, then so does every submodule $N \subset M$ and every quotient M/N of M, and
$$\ell(M) = \ell(M/N) + \ell(N).$$
2. Any two composition series of a module of finite length have equal length and subquotients that are isomorphic, up to reordering. I.e. if
$$M = M_r \supset M_{r-1} \supset \ldots \supset M_0 = 0, \quad \text{and} \quad M = \tilde{M}_s \supset \tilde{M}_{s-1} \supset \ldots \supset \tilde{M}_0 = 0$$
are two composition series of a module M, then $r = s$ and there exists a permutation $\sigma \in S_r$ with
$$\tilde{M}_i/\tilde{M}_{i-1} \cong M_{\sigma(i)}/M_{\sigma(i)-1} \quad \text{for all } i\,.$$

Proof. Let M be an R-module with composition series

$$M = M_r \supset \ldots \supset M_0 = 0$$

and $N \subset M$ a submodule. We consider the canonical surjection

$$\mathrm{can}\colon M \twoheadrightarrow \overline{M} := M/N$$

and the submodules

$$N_i := M_i \cap N \subset N \quad \text{and} \quad \overline{M}_i := \mathrm{can}\,(M_i) \subset \overline{M}$$

In the commutative diagram

$$\begin{array}{ccccc} N_{i-1} & \hookrightarrow & N_i & \twoheadrightarrow & N_i/N_{i-1} \\ \downarrow & & \downarrow & & \downarrow \\ M_{i-1} & \hookrightarrow & M_i & \twoheadrightarrow & M_i/M_{i-1} \\ \downarrow & & \downarrow & & \downarrow \\ \overline{M}_{i-1} & \hookrightarrow & \overline{M}_i & \twoheadrightarrow & \overline{M}_i/\overline{M}_{i-1} \end{array}$$

the rows are exact and the first two columns are exact. By the Nine Lemma 1.5.8 we get for every $i = 1, \ldots r$ a short exact sequence

$$N_i/N_{i-1} \hookrightarrow M_i/M_{i-1} \twoheadrightarrow \overline{M}_i/\overline{M}_{i-1}\,. \qquad (*)$$

The quotient module M_i/M_{i-1} in the middle is a composition factor of M and thus simple. Then the quotient modules N_i/N_{i-1} and $\overline{M}_i/\overline{M}_{i-1}$ have to be zero or simple too. More specifically, N_i/N_{i-1} is zero if and only if $\overline{M}_i/\overline{M}_{i-1}$ is a simple module. After omitting those modules N_i, for which the quotient is zero is, the remaining N_i form a composition series for the submodule N. Conversely, the nonzero $\overline{M}_i/\overline{M}_{i-1}$ form a composition series for the quotient M/N. We deduce that all submodules and all quotients of M have finite length. From the short exact sequence $(*)$ we also deduce

$$\ell(N) + \ell(M/N) = \ell(M)\,.$$

2. is proved by induction in the length of the module. The induction start $\ell(M) = 1$ is immediate. Now consider two composition series for the module M:

$$M \supset X \supset \cdots \supset (0) \quad \text{and} \quad M \supset Y \supset \cdots \supset (0)$$

If $X = Y$, then we may use the induction hypothesis. Otherwise we consider the canonical surjection

$$\pi\colon M \to M/Y\,.$$

The module M/Y is simple, and so $\pi(X) = M/Y$. To see this, note that otherwise we would have $\pi(X) = 0$, and so $X \subset Y$. But by Lemma 1.5.2.2 X is maximal as it is the kernel of a surjection onto a simple module; i.e. $X = Y$.

Thus π induces an isomorphism of modules

$$X/(X \cap Y) \cong M/Y\,. \qquad (**)$$

By exchanging X and Y we analogously get

$$Y/(X \cap Y) \cong M/X\,. \qquad (***)$$

Now we choose a composition series of the intersection $X \cap Y$ and compare the following four composition series of M:

$$\begin{aligned} M &\supset X \supset \cdots \supset (0) \\ M &\supset X \supset (X \cap Y) \supset \cdots \supset (0) \\ M &\supset Y \supset (X \cap Y) \supset \cdots \supset (0) \\ M &\supset Y \supset \cdots \supset (0) \ . \end{aligned}$$

The first and the second composition series are equivalent by the induction hypothesis applied to the module X. By an analogous argument the third and fourth composition series are equivalent. Finally, the second and the third composition series are equivalent by the isomorphisms $(**)$ and $(***)$. □

Corollary 1.5.10 Let R be a ring that has finite length as left module over itself. Then every simple R-module M is a quotient of R, considered as left module over itself, and thus appears in every composition series of R as subquotient.

Proof. By Lemma 1.5.2 every generator of M yields a surjection $\varphi\colon R \twoheadrightarrow M$. Thus there exists a composition series of the form $R \supsetneq \ker\varphi \supsetneq \ldots$, in which $R/\ker\varphi \cong M$ appears as composition factor. By the Jordan-Hölder Theorem 1.5.9 M appears in all composition series of R as subquotient. □

Corollary 1.5.11 Let R be a ring that has a field K as subring. If R is finite-dimensional over K, then there exist at most $\dim_K R$ distinct simple R-modules up to isomorphism.

Proof. Every R-module M is also a K-vector space by restriction of scalars. If M is simple, and thus nonzero, we have $\dim_K M \geq 1$. For general M we have $\ell(M) \leq \dim_K(M)$. By Corollary 1.5.10 every simple module appears in all composition series of R as subquotient, so there are at most $\ell(R) \leq \dim_K(R)$ distinct simple R-modules. □

The statement holds, in particular, for finite-dimensional K-algebras and thus for the group algebras of finite groups from Definition 1.1.16.

Theorem 1.5.12 Let G be a finite group and K a field. Then there exist at most $|G|$ distinct isomorphism classes of irreducible representations of G over K.

Proof. By Lemma 1.1.19 we can consider representations of G as modules over the group ring $K[G]$. The claim then follows directly from Corollary 1.5.11, since $\dim_K K[G] = |G|$. □

2 Categories, functors and natural transformations

In this chapter we introduce categorical language that allows a very efficient description of constructions for modules over rings (and similar constructions in many other areas of mathematics). The essential feature here is that one simultaneously considers mathematical structures and their structure-preserving maps. As references for category theory, we recommend the classical work [McL71] as well as [R16] and, for the German reading audience [B16].

2.1 Categories

Definition 2.1.1 A category $\mathcal{C}$ consists of a class $\operatorname{ob}\mathcal{C}$ of objects and a class $\operatorname{mor}\mathcal{C}$ of morphisms, together with the following maps:

1. The identity map $\mathrm{id}\colon \operatorname{ob}\mathcal{C} \to \operatorname{mor}\mathcal{C}$
2. The source and target maps $s, t\colon \operatorname{mor}\mathcal{C} \to \operatorname{ob}\mathcal{C}$
3. The composition map $\circ\colon \operatorname{mor}\mathcal{C} \times_{\operatorname{ob}\mathcal{C}} \operatorname{mor}\mathcal{C} \to \operatorname{mor}\mathcal{C}$. Its preimage consists of those pairs $(x, y) \in \operatorname{mor}\mathcal{C} \times \operatorname{mor}\mathcal{C}$, for which $s(x) = t(y)$.

These maps are required to satisfy the following axioms:

1. $\operatorname{Hom}_{\mathcal{C}}(a, b) := \{f \in \operatorname{mor}\mathcal{C} \mid s(f) = a, t(f) = b\}$ is a *set* and not a proper class.
2. $s \circ \mathrm{id} = t \circ \mathrm{id} = \mathrm{id}_{\operatorname{ob}\mathcal{C}}$
   ("source and target of the identity on an object X is X itself.")
3. $s(f \circ g) = s(g)$, $t(f \circ g) = t(f)$
   ("target of a composite is the target of the map applied last, source of a composite is the source of the map applied first.")
4. $\mathrm{id}_{t(f)} \circ f = f$, $f \circ \mathrm{id}_{s(f)} = f$.
   ("composition with identity morphisms is the identity.")
5. $f \circ (g \circ h) = (f \circ g) \circ h$, whenever the composition is defined (associativity).

We immediately define

Definition 2.1.2 Two objects c, c' in a category are isomorphic, if there are morphisms $f \in \operatorname{Hom}_{\mathcal{C}}(c.c')$ and $g \in \operatorname{Hom}_{\mathcal{C}}(c', c)$ such that $g \circ f = \mathrm{id}_c$ and $f \circ g = \mathrm{id}_{c'}$. We then write $c \cong c'$. Isomorphism is an equivalence relation. The equivalence classes are called isomorphism classes.

Examples 2.1.3

1. The category Set of sets, whose objects sets and whose morphisms are maps of sets.
2. Similarly one defines the categories Grp of groups and Ab of abelian groups. For a commutative ring R one also defines the category Alg_R of R-algebras and the category Alg_R^1 of unital R-algebras.

   For rings R and S one defines the categories $R-$Mod of R-left modules, $\mathrm{Mod}-R$ of R-right modules, and R-$S-$Bimod of R-S-bimodules. We use the notation vect_K for the category of vector spaces over a field K.
3. Top: the objects are topological spaces and the morphisms are continuous maps.

4. If the objects form a set rather than a proper class, then the category is called small.

   We explain why in the definition of a category we talk about *sets* and *classes*: for applying category in practice one would like to have a notion of a "category of all sets" and, for constructing interesting categories, for a given a property $\varphi(x)$ of a set x, also a category "$\{x \mid \varphi(x)\}$" of all sets having the property φ. Famously, this leads to contradictions, such as the one of the category of all sets that are not elements of themselves.

   A solution to this problem is to restrict the application of φ to be allowed only for sets that are elements in some specific set $\mathfrak{U}$ (where it is supposed that the notion of a set is defined, e.g. by working with Zermelo-Fraenkel axioms.) Further, such a set $\mathfrak{U}$ must be sufficiently nice – technically speaking, it must be a *universe* (for details see [McL71, Sect. I.6]). All mathematical constructions are then carried out inside the universe $\mathfrak{U}$. A set that is an element of $\mathfrak{U}$ is called *small* (relative to $\mathfrak{U}$). It should be appreciated that, with this definition, sets that are small in terms of cardinality are not necessarily $\mathfrak{U}$-small; for example, the one-element set $\{\mathfrak{U}\}$ is *not* $\mathfrak{U}$-small. Functions between small sets relative to $\mathfrak{U}$ can be constructed inside $\mathfrak{U}$. This yields for each universe $\mathfrak{U}$ a category of $\mathfrak{U}$-small sets.

   A category $\mathcal{C}$ is now called $\mathfrak{U}$-small if the set $\mathrm{ob}(\mathcal{C})$ of objects is in $\mathfrak{U}$. The category of $\mathfrak{U}$-small categories is *not* $\mathfrak{U}$-small, because this would imply $\mathfrak{U} \in \mathfrak{U}$, thus violating the axioms of a universe. A *class* C (relative to a universe $\mathfrak{U}$) can then be defined as an arbitrary subset $C \subseteq \mathfrak{U}$. It follows that every $\mathfrak{U}$-small set is a $\mathfrak{U}$-class, but the converse is not true. Using classes, we can now talk about the category of $\mathfrak{U}$-small categories.

   The choice of $\mathfrak{U}$ is usually supressed in the notation. It is common to enlarge the axioms of set theory by requiring that for any set X there is a universe $\mathfrak{U}$ such that $X \in \mathfrak{U}$, which in particular ensures the existence of universes.

5. The empty category and the category with exactly one object with its identity morphisms are the two smallest categories. More generally, for every object a of a category, $\mathrm{Hom}(a, a)$ is a unital associative monoid. Categories with one object are in fact in bijection with unital monoids. If G is an associative unital monoid, we write BG or $*//G$ for the corresponding one-object category.

6. If R is even a ring, the hom-set of the one-object category BR has the structure of an abelian group and composition is bilinear. If A is even an R-algebra over a commutative ring R, the hom-set of the one-object category BA has the structure of an R module and composition is bilinear and thus induces a map $\mathrm{Hom}(*,*) \otimes_R \mathrm{Hom}(*,*) \to \mathrm{Hom}(*,*)$.

7. Groups are in bijection to categories with a single object, in which all morphisms are isomorphisms. For a group G we denote the associated category with one object with $*//G$. Categories, in which all morphisms are isomorphisms, are called groupoids.

8. Partially-ordered sets: Let $(X, \leq)$ be a partially-ordered set, considered as a category $\underline{X}$, whose objects are the elements of X and $\mathrm{Hom}_{\underline{X}}(x, y)$ is a one-element set if $x \leq y$ and empty otherwise. The composition is thus uniquely determined, since there is at most one map between any two objects.

9. The identity is a particular example of a partial order that can be considered on any set X. Any set X thus gives rise to a category $\underline{X}$ whose objects are the elements of the set and that has only identity morphisms. Such a category is called a discrete category.

10. The category of finite ordinals Δ has as objects the totally ordered sets $[n] := \{0, 1, 2, \dots n\}$ and as morphisms order preserving maps.

    We discuss some examples of morphisms in the category Δ: The coface maps

    $$d^i : \quad [n-1] \ \to \ [n] \quad \text{for } 0 \le i \le n$$

    with $d^i(j) = j$ for $0 \le j \le i-1$ and $d^i(j) = j+1$ for $i \le j \le n$ are strictly monotonously increasing and omit the value i. The codegeneracy maps

    $$s^i : \quad [n+1] \ \to \ [n] \quad \text{for } 0 \le i \le n$$

    with $s^i(j) = j$ for $j = 0, \dots i$, $s^i(i) = s^i(i+1) = i$ and $s^i(j+1) = j-1$ for $j = i+1, \dots n+1$ are strictly monotonously increasing, except for taking twice the value i. We find the relations

    $$\begin{array}{ll} d^j d^i = d^i d^{j-1} & \text{if } i < j \\ s^j s^i = s^i s^{j+1} & \text{if } i \le j \\ s^j d^i = d^i s^{j-1} & \text{if } i < j \\ s^i d^i = \mathrm{id} = s^i d^{i+1} & \\ s^j d^i = d^{i-1} s^j & \text{if } i > j+1. \end{array}$$

    These maps can be seen as a set of generators for the morphisms of Δ in the sense that any morphism in Δ is a composition of these morphisms. The relations given can be seen to be the only relations in Δ.

Definition 2.1.4 Let $\mathcal{C}, \mathcal{D}$ categories.

1. The category $\mathcal{C}^{\mathrm{opp}}$ is the category with the same objects as $\mathcal{C}$, but with morphisms $\mathrm{Hom}_{\mathcal{C}^{\mathrm{opp}}}(a, b) := \mathrm{Hom}_{\mathcal{C}}(b, a)$ and the composition $f \circ_{\mathrm{opp}} g := g \circ_{\mathcal{C}} f$.

2. The category $\mathcal{C} \coprod \mathcal{D}$ is the category, whose objects and morphisms are the disjoint unions of the objects resp. morphisms of $\mathcal{C}$ and of $\mathcal{D}$.

3. Similarly one define $\mathcal{C} \times \mathcal{D}$, the Cartesian product category. One can also construct infinite disjoint unions resp. products.

4. A subcategory of a category $\mathcal{C}$ is a category $\mathcal{S}$ whose objects are objects in $\mathcal{C}$ and whose morphisms are morphisms in $\mathcal{C}$ with the same identities and composition of morphisms. A subcategory $\mathcal{S}$ is called a full subcategory of $\mathcal{C}$ if for each pair of objects $X, Y \in \mathcal{S}$, we have $\mathrm{Hom}_{\mathcal{S}}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(X, Y)$.

Next we have to introduce "maps" between categories. They have to act on objects and morphisms.

Definition 2.1.5 Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A functor $F \colon \mathcal{C} \to \mathcal{D}$ assigns to each object c of $\mathcal{C}$ an object $F(c)$ of $\mathcal{D}$, and to every morphism $f \in \mathrm{Hom}_{\mathcal{C}}(c, c')$ a morphism $F(f) \in \mathrm{Hom}_{\mathcal{D}}(F(c), F(c'))$. These assignments have to satisfy:

1. $F(\mathrm{id}_c) = \mathrm{id}_{F(c)}$.

2. $F(f \circ g) = F(f) \circ F(g)$.

A functor $F \colon \mathcal{C} \to \mathcal{D}^{\mathrm{opp}}$ is also called contravariant functor from $\mathcal{C}$ to $\mathcal{D}$. If we wish to emphasize the difference, we call functors $\mathcal{C} \to \mathcal{D}$ covariant.

This is clearly the same data as a functor $F\colon \mathcal{C}^{\mathrm{opp}} \to \mathcal{D}$; a contravariant functor "switches the direction of arrows".

Examples 2.1.6

1. For an any category $\mathcal{C}$, there exists an identity functor $\mathrm{id}\colon \mathcal{C} \to \mathcal{C}$, defined as the identity on objects and morphisms.

2. The functor $U\colon R\text{−Mod} \to \mathrm{Ab}$, that sends R-modules to their underlying abelian groups. Functors of this kind are called forgetful functors. Another important forgetful functor $\mathrm{Grp} \to \mathrm{Set}$ sends a group to the underlying set.

3. For G a group, a functor $F_\rho\colon BG \to \mathrm{vect}_K$ is the same as a K-linear representation of the group G. For a ring R, a functor $BR \to \mathrm{Ab}$, where Ab is the category of abelian groups, is an R-module. Similarly, a functor $BR^{\mathrm{opp}} \to \mathrm{Ab}$ is a right R-module and $B(R \otimes R^{\mathrm{opp}}) \to \mathrm{Ab}$ an R-bimodule.

4. Every ring homomorphism $\Phi\colon R \to S$ defines a functor that performs restriction of scalars $S\text{−Mod} \to R\text{−Mod}$, see Lemma 1.1.23. For example, by restriction of scalars along the inclusion $\mathbb{R} \hookrightarrow \mathbb{C}$ we may view every complex vector space as a real vector space.

5. The functor $F = -^*\colon \mathrm{vect}_K \to \mathrm{vect}_K^{\mathrm{opp}}$, that sends vector space to their dual spaces, $F(V) = V^*$, and linear maps to their dual maps, $F(f) = f^*$.

6. The functor $F = -^{**}\colon \mathrm{vect}_K \to \mathrm{vect}_K$ that sends vector space to their double dual spaces, $F(V) = V^{**}$ and linear maps to their double dual maps, $F(f) = f^{**}$.

7. The functor $\coprod\colon \mathrm{Set} \times \mathrm{Set} \to \mathrm{Set}$, that sends two sets X, Y to their disjoint union $X \coprod Y$, and the functor $\prod$, that sends pairs of sets to their Cartesian product.

8. The functor $\otimes_R\colon R^{\mathrm{opp}}\text{−Mod} \times R\text{−Mod} \to \mathrm{Ab}$. If the ring R is even commutative, then one obtains functors into the category of R-modules.

9. Let $\mathcal{C}$ be an arbitrary category. For every object W in $\mathcal{C}$ we define as in Lemma 1.4.6 a covariant functor
$$\mathrm{Hom}(W, -)\colon \mathcal{C} \to \mathrm{Set}$$
on objects by
$$\mathrm{Hom}(W, -)\colon \quad X \mapsto \mathrm{Hom}_{\mathcal{C}}(W, X) \ .$$
A morphism $X \xrightarrow{\varphi} Y$ is sent to the map of sets given by precomposition
$$\begin{array}{rccc} \varphi_*\colon & \mathrm{Hom}_{\mathcal{C}}(W, X) & \to & \mathrm{Hom}_{\mathcal{C}}(W, Y) \\ & f & \mapsto & \varphi \circ f \ . \end{array}$$
It is straightforward to check that this defines a functor. with values in the category of sets.

10. Let $\mathcal{C}$ again be an arbitrary category. For every object W in $\mathcal{C}$ we define as we did after Example 1.4.12 a contravariant functor, i.e. a functor
$$\mathrm{Hom}(-, W)\colon \mathcal{C} \to \mathrm{Set}^{\mathrm{opp}}$$
on objects by
$$\mathrm{Hom}(-, W)\colon X \to \mathrm{Hom}_{\mathcal{C}}(X, W) \ .$$

A morphism $X \xrightarrow{\varphi} Y$ is sent to the map of sets given by postcomposition

$$\begin{array}{rccc} \varphi^*\colon & \mathrm{Hom}_{\mathcal{C}}(Y,W) & \to & \mathrm{Hom}_{\mathcal{C}}(X,W) \\ & f & \mapsto & f\circ\varphi \quad . \end{array}$$

It is straightforward to check that this defines a contravariant functor. with values in the category of sets.

11. The morphism sets $\mathrm{Hom}_{\mathcal{C}}(\cdot,\cdot)$ of the category $\mathcal{C} = R-\mathrm{Mod}$ of modules over a ring R, the morphism sets carry the structure of abelian groups. One says that the category $R-\mathrm{Mod}$ is enriched over the category Ab. In this case, we have a functor

$$\mathrm{Hom}_R\colon R^{\mathrm{opp}}-\mathrm{Mod}\times R-\mathrm{Mod}\to \mathrm{Ab}$$

If the ring R is even commutative, then one obtains functors into the category of R-modules.

12. Let $\mathcal{C}$ be the category with two objects $0,1$ and only two morphisms $0 \xrightarrow{s} 1$ and $0 \xrightarrow{t} 1$ different from identities. A functor $\mathcal{C}^{\mathrm{opp}} \to \mathrm{Set}$ is an oriented graph.

13. A <u>simplicial set</u> is a presheaf on the simplex category Δ introduced in Examples 2.1.3, that is, a functor $X : \Delta^{\mathrm{opp}} \to \mathrm{Set}$ from the opposite category of the simplex category to the categorySet of sets. More generally, a <u>simplicial object</u> in a category $\mathcal{C}$ is a functor $X : \Delta^{\mathrm{opp}} \to \mathcal{C}$.

Let X be a topological space. Consider the functor $|\cdot| : \Delta \to Top$ that assigns to an object $[n] \in \Delta$ the standard n-simplex in $\mathbb{R}^{n+1}$. The functor

$$\mathrm{Hom}_{Top}|(|-|, X) : \qquad \Delta^{\mathrm{opp}} \to \mathrm{Set}$$

is a simplicial set. Composing it with the functor that assigns to a set the corresponding freely generated R-module gives a simplicial object in $R-\mathrm{Mod}$ which is central in algebraic topology.

Definition 2.1.7 Two categories $\mathcal{C}, \mathcal{D}$ are <u>isomorphic</u>, if there are two functors $F\colon \mathcal{C} \to \mathcal{D}$ and $G\colon \mathcal{D} \to \mathcal{C}$, such that $G \circ F$ is the identity functor on $\mathcal{C}$ and $F \circ G$ is the identity functor on $\mathcal{D}$.

Remarks 2.1.8

1. We already know examples of isomorphic categories:
   - For every ring R the categories of R-right modules and the category of R^{opp}-left modules are isomorphic, see Remarks 1.1.6.
   - For every field K the category of $K[X]$-modules and the category of K-vector spaces with a K-linear endomorphism are isomorphic, see Lemma 1.1.15.
   - For every field K and every group G the category of K-linear G-representations and the category of $K[G]$-modules are isomorphic, see Lemma 1.1.19.
2. Isomorphism of categories is, as we will see, a too narrow notion.

To compare categories in an adequate way it is important to have structures that relate functors. For example, recall that a functor $F_\rho\colon *//G \to \mathrm{vect}_K$ is the same data as a K-linear representation of G, but we have not yet seen the categorical concept that would correspond to a morphism of representations.

As another example, we consider the category vect_K of K-vector spaces for a field K. Both the identity and the double dual functor $-^{**}$ are endofunctors

$$\mathrm{id}, -^{**}: \qquad \mathrm{vect}_K \to \mathrm{vect}_K \ .$$

For every object in the category, i.e. every K-vector space V, we have a linear map

$$\begin{array}{rccc} \iota_V: & V & \mapsto & V^{**} \\ & v & \mapsto & (\varphi \mapsto \varphi(v)) \end{array}$$

that is an isomorphism whenever V is finite-dimensional. Via this map one often identifies a finite-dimensional vector space with its double dual space. Here we relate the two functors id and $-^{**}$, by assigning to every object of the source category a morphism in the target category between the two images of the object under the two functors. These maps satisfy certain relations and this leads to the following definition.

Definition 2.1.9

1. If F, G are functors from a category $\mathcal{C}$ to a category $\mathcal{D}$, then a natural transformation $N: F \to G$, sometimes denoted $F \Rightarrow G$, is an assignment that sends an object c in the category $\mathcal{C}$ to morphism $N_c: F(c) \to G(c)$ in the category $\mathcal{D}$, such that for every morphism $f \in \mathrm{Hom}_{\mathcal{C}}(c, c')$ in the category $\mathcal{C}$ the following diagram in the category $\mathcal{D}$ commutes:

$$\begin{array}{ccc} F(c) & \xrightarrow{N_c} & G(c) \\ \Big\downarrow{\scriptstyle F(f)} & & \Big\downarrow{\scriptstyle G(f)} \\ F(c') & \xrightarrow{N_{c'}} & G(c') \end{array}$$

2. If all components N_c of a natural transformation are isomorphisms in the category $\mathcal{D}$, then we call it a natural isomorphism.

Examples 2.1.10

1. For the restriction of the two endofunctors

$$\mathrm{id}, -^{**}: \mathrm{vect}_K^f \to \mathrm{vect}_K^f$$

onto the subcategory vect_K^f of finite-dimensional K-vector spaces the isomorphisms recalled above define a natural isomorphism $\mathrm{id} \to -^{**}$.

2. For a small category $\mathcal{C}$ and an arbitrary category $\mathcal{D}$, one can define the functor category $[\mathcal{C}, \mathcal{D}]$, whose objects are the functors $F: \mathcal{C} \to \mathcal{D}$ and whose morphisms are the natural transformations between the functors. The readers are encouraged to check that all axioms of a category are satisfied. We have, for example, $R\text{−Mod} = [BR, \mathrm{Ab}]$.

3. Let $\mathcal{C}$ be the totally-ordered set $[n] := \{0, \ldots, n\}$, that we consider as a small category as in Example 2.1.3.6. A functor $[n] \to R\text{−Mod}$ is the same as a sequence $R_0 \to R_1 \to \ldots \to R_n$ of R-modules and maps between them. A natural transformation between two such functors R and S is a commutative diagram of the form

$$\begin{array}{ccccccc} R_0 & \to & R_1 & \to & \ldots & \to & R_n \\ \downarrow & & \downarrow & & & & \downarrow \\ S_0 & \to & S_1 & \to & \ldots & \to & S_n \end{array}$$

This gives us a notion of morphisms for when two sequences of modules and morphisms, and by restriction, also for complexes. Since simplicial sets have been introduced in Examples 2.1.6 as functors, we obtain a category of simplicial sets and, more generally, of simplicial objects in a category.

4. In the same way, we get a category Graph of directed graphs. Considering categories with functos as morphisms as a category Cat, we obtain a forgetful functor $U : Cat \to \text{Graph}$.

Natural transformations allow us to weaken the notion of isomorphism of categories. It is often problematic to require two objects of a category to be equal, the more natural requirement is isomorphism. For a small category $\mathcal{C}$ the functors $\mathcal{C} \to \mathcal{D}$ form the functor category from Examples 2.1.10. Correspondingly, it appears unnatural to require the two composites $F \circ G$ and $G \circ F$ of two functors to be equal to identity functors.

Definition 2.1.11 Let $F\colon \mathcal{C} \to \mathcal{D}$ be a functor between two categories $\mathcal{C}$ and $\mathcal{D}$. Then F is called an equivalence of categories, if there exists a functor $G\colon \mathcal{D} \to \mathcal{C}$ and natural isomorphisms

$$\epsilon\colon G \circ F \to \mathrm{id}_{\mathcal{C}} \quad \text{and} \quad \eta\colon \mathrm{id}_{\mathcal{D}} \to F \circ G \ .$$

In words, a functor F is an equivalence if there exists an "inverse" functor G, such that the composites $F \circ G$ and $G \circ F$ are, not necessarily equal, but at least naturally isomorphic to the appropriate identity functors.

We give another characterization of the notion of equivalence.

Definition 2.1.12

1. A functor $F\colon \mathcal{C} \to \mathcal{D}$ is called full/faithful/fully faithful, if all maps $F\colon \mathrm{Hom}_{\mathcal{C}}(c,d) \to \mathrm{Hom}_{\mathcal{D}}(F(c),F(d))$ on Hom-spaces are surjective/injective/bijective.

2. A functor $F\colon \mathcal{C} \to \mathcal{D}$ is called essentially surjective, if for every object d of $\mathcal{D}$ there exists an object c in $\mathcal{C}$, such that $F(c)$ and d are isomorphic, $F(c) \cong d$.

Theorem 2.1.13 A functor $F\colon \mathcal{C} \to \mathcal{D}$ is an equivalence of categories if and only if it is fully faithful and essentially surjective.

Proof.

- Let F be a equivalence of categories with functor $G\colon \mathcal{D} \to \mathcal{C}$ and natural isomorphisms $\eta\colon \mathrm{id}_{\mathcal{D}} \xrightarrow{\sim} FG$ and $\epsilon\colon GF \xrightarrow{\sim} \mathrm{id}_{\mathcal{C}}$. Then for every object $W \in \mathcal{D}$ there exists an isomorphism $\eta_W\colon W \xrightarrow{\sim} FG(W)$, which implies that the functor F is essentially surjective.

- For every morphism $V \xrightarrow{f} V'$ in $\mathcal{C}$ the naturality of $\epsilon : G \circ F \to \mathrm{id}_{\mathcal{C}}$ yields a commuting diagram

$$\begin{array}{ccc} GF(V) & \xrightarrow[\epsilon_V]{\sim} & V \\ {\scriptstyle GF(f)}\downarrow & & \downarrow{\scriptstyle f} \\ GF(V') & \xrightarrow[\epsilon_{V'}]{\sim} & V' \ . \end{array} \qquad (*)$$

  Now the assumption $F(f_1) = F(f_2)$ implies $G(F(f_1)) = G(F(f_2))$ and thus $f_1 = f_2$ using $(*)$, so is F is faithful. Using the natural isomorphism η we also get that the functor G is faithful.

- To show that the functor F is full, consider a morphism $g\colon F(V) \to F(V')$ in $\mathcal{D}$. Set $f := \epsilon_{V'} \circ G(g)\epsilon_V^{-1}\colon V \to V'$, then the commuting diagram $(*)$ implies the identity

$$\epsilon_{V'} \circ G(F(f))\epsilon_V^{-1} \overset{(*)}{=} f = \epsilon_{V'} \circ G(g)\epsilon_V^{-1}$$

  and so $GF(f) = G(g)$. As G is faithful, i.e. injective on morphisms, this implies $F(f) = g$, and so the functor F is full. Analogously one shows that G is full.

- Conversely, suppose that $F\colon \mathcal{C} \to \mathcal{D}$ is an essentially surjective and fully faithful functor. Using essential surjectivity of F we can find for every given object $W \in \mathcal{D}$ an object $G(W)$ in $\mathcal{C}$ and an isomorphism $\eta_W\colon W \xrightarrow{\sim} F(G(W))$. (Here we may need to use the axiom of choice.)

  For a morphism $g\colon W \to W'$ in $\mathcal{D}$ we consider

  $$\eta_{W'} \circ g \circ \eta_W^{-1}\colon FG(W) \to W \to W' \to FG(W') \ .$$

  Since the functor F was assumed to be fully faithful, there exists a unique morphism $G(g)\colon G(W) \to G(W')$ that maps to $\eta_{W'} \circ g \circ \eta_W^{-1}$ under F. It is straightforward to check that this defines a functor G and that $\eta\colon \mathrm{id}_{\mathcal{D}} \to FG$ is a natural transformation.

- We still have to define a natural isomorphism $\epsilon_G\colon GF \to \mathrm{id}_{\mathcal{C}}$. For an object V in $\mathcal{C}$ we have an isomorphism

  $$\eta_{F(V)}\colon \quad F(V) \to FGF(V)$$

  and thus $\eta_{F(V)}^{-1}\colon FGF(V) \to F(V)$. Since F was assumed to be fully faithful, we can define $\epsilon_V\colon GF(V) \xrightarrow{\sim} V$ as the unique preimage of the morphism $\eta_{F(V)}^{-1}$ under F. It is straightforward to check that this defines a natural isomorphism.

□

Examples 2.1.14

1. We give an example for two equivalent categories: the category vect_K^f of finite-dimensional K-vector spaces is equivalent to the category with an object $[n]$ for every $n \in \mathbb{N}$ – we think of this as the vector spaces K^n – and with matrices as morphisms $\mathrm{Hom}([n],[m]) := M(n \times m, K)$. composition is matrix multiplication. Note that the category vect_K^f has the property that morphisms spaces are themselves objects in the category, i.e. vector spaces. But the second category does not have this property! This makes, for example, the definition of the dual vector space less straightforward. For practical purposes, the second category is still very useful, though.

2. A generator of a category $\mathcal{C}$ is an object X, such that the functor $\mathrm{Hom}(X,-) : \mathcal{C} \to \mathrm{Set}$ is faithful. Let A and B be rings. Then the following statements are equivalent:

   (a) The categories A-mod and B-mod of left modules are equivalent.

   (b) The categories A^{opp} -mod and B^{opp}-mod are equivalent.

   (c) There exists a finitely generated projective generator P of A-mod and a ring-isomorphism $B \cong \mathrm{End}_A(P)$.

   For the proof of this statement, known as Morita's theorem, we refer to the literature, e.g. [P97, Chapter 4].

We are working towards an important category-theoretical lemma, for which we need to consider functors into the category Set of sets. Recall from Examples 2.1.6.9 that for every object c of a category $\mathcal{C}$ we have the functor:

$$y_c := \mathrm{Hom}_{\mathcal{C}}(c,-)\colon \mathcal{C} \to \mathrm{Set}$$

This gives rise to a special class of functors $\mathcal{C} \to \mathrm{Set}$.

Definition 2.1.15 Let $\mathcal{C}$ be a category. A functor $F\colon \mathcal{C} \to \mathrm{Set}$ is called representable, if it is naturally isomorphic to a functor y_c for an object c. In this case we say that the object c represents the functor F and call c a representing object.

Examples 2.1.16

1. Let $F\colon \mathrm{Ring} \to \mathrm{Set}$ be the forgetful functor that sends every ring to its underlying set. Then we have by Theorem 1.1.12 for every ring R the isomorphism of sets

$$\begin{array}{rcl} \mathrm{Hom}_{\mathrm{Ring}}(\mathbb{Z}[X], R) & \to & F(R) \\ \varphi & \mapsto & \varphi(X) \ , \end{array}$$

   These morphisms are compatible with ring morphisms and thus define a natural isomorphism. Thus, the polynomial ring $\mathbb{Z}[X]$ represents the forgetful functor from rings to sets.

2. Let $F\colon \mathrm{Ring} \to \mathrm{Set}$ be the functor that sends ring every R to its set of units $R^\times$. This functor is represented by the quotient ring $\mathbb{Z}[X,Y]/(XY-1)$. Indeed we have an isomorphism of sets

$$\begin{array}{rcl} \mathrm{Hom}_{\mathrm{Ring}}(\mathbb{Z}[X,Y]/(XY-1), R) & \to & R^\times \\ \varphi & \mapsto & \varphi(X) \ , \end{array}$$

   where the inverse sends $r \in R^\times$ to the ring morphism defined by $X \mapsto r, Y \mapsto r^{-1}$.

Here we have examples of an important technique of constructing objects in categories, namely by first constructing a functor to Set and then checking that it is representable. One would then also like to know that the representing object is unique. This is a consequence of the following lemma on functors into the category Set, which plays a central role in category theory:

Theorem 2.1.17 [Yoneda lemma]

1. Let $\mathcal{C}$ be a category, $F\colon \mathcal{C} \to \mathrm{Set}$ a functor, and $c \in \mathcal{C}$ an object. Then the natural transformations $\mathrm{Hom}(y_c, F)$ form a set.

2. Consider the map

$$\begin{array}{lcllcl} \mathrm{Hom}(y_c, F) & \to & \mathrm{Hom}_{\mathrm{Set}}(y_c(c), F(c)) \stackrel{\mathrm{def}}{=} \mathrm{Hom}_{\mathrm{Set}}(\mathrm{Hom}_{\mathcal{C}}(c,c), F(c)) & \to & F(c) \\ N & \mapsto & N_c & \mapsto & N_c(\mathrm{id}_c) \ , \end{array}$$

   where the first arrow is the projection of the natural transformation onto its component at c and the last arrow is given by evaluation at id_c. This map is a bijection of sets.

Proof. If $N\colon y_c \to F$ is a natural transformation, then by definition we have a commutative diagram for every morphism $f\colon c \to c'$ in $\mathcal{C}$, namely:

$$\begin{array}{ccc} y_c(c) & \xrightarrow{y_c(f)} & y_c(c') \\ \downarrow{\scriptstyle N_c} & & \downarrow{\scriptstyle N_{c'}} \\ F(c) & \xrightarrow{F(f)} & F(c') \end{array}$$

If we track the image of $\mathrm{id}_c \in y_c(c) = \mathrm{Hom}_{\mathcal{C}}(c,c)$ through the diagram and use for the path that first goes horizontally and then vertically that

$$N_{c'}(y_c(f)(\mathrm{id}_c)) = \ N_{c'}(f_*\mathrm{id}_c) = N_{c'}(f)$$

we obtain the equation

$$N_{c'}(f) = F(f)(N_c(\mathrm{id}_c))$$

for every $f \in \mathrm{Hom}(c, c') = y_c(c')$. Thus the natural transformation N depends only on element $N_c(\mathrm{id}_c) \in F(c)$, which proves the injectivity of the Yoneda map.

Conversely, every element $x \in F(c)$ for a fixed object c of the category $\mathcal{C}$ determines a map of sets

$$\begin{array}{rcl} \mathrm{Hom}_{\mathcal{C}}(c, c') = y_c(c') & \to & F(c') \\ f & \mapsto & {}^xN(f) := F(f)(x) \quad , \end{array}$$

which assembles to a natural transformation ${}^xN \colon y_c \to F$ of functors $\mathcal{C} \to \mathrm{Set}$. □

The Yoneda lemma has many consequences. First we use it in the following observation:

Observation 2.1.18

1. Suppose the functor F is also of the form $F = y_{c'} = \mathrm{Hom}(c', -)$. Then we find bijections

   $$\mathrm{Hom}(c', c) \cong F(c) \cong \mathrm{Hom}(y_c, y_{c'})$$

   The morphism $f \in \mathrm{Hom}(c', c)$ is sent to the natural transformation $y_c \to y_{c'}$, which acts on the object d by

   $$\begin{array}{rcl} f^* \colon \mathrm{Hom}(c, d) & \to & \mathrm{Hom}(c', d) \\ \varphi & \mapsto & \varphi \circ f \end{array}$$

   We have thus found a functor

   $$\mathcal{C}^{\mathrm{opp}} \to [\mathcal{C}, \mathrm{Set}]$$

   with $c \mapsto y_c$. This functor is fully faithful; it is called the Yoneda embedding. Its image are the representable functors.

2. Thus the functors $\mathrm{Hom}(c', -)$ and $\mathrm{Hom}(c, -)$ are isomorphic, if and only if the objects c and c' are isomorphic. In particular: if a functor $F \colon \mathcal{C} \to \mathrm{Set}$ is representable, then the representing object is unique up to isomorphism.

3. Applying the same observation to the functor

   $$\mathrm{Hom}(-, d) \colon \mathcal{C}^{\mathrm{opp}} \to \mathrm{Set}$$

   we find that the functors $\mathrm{Hom}(-, d)$ and $\mathrm{Hom}(-, d')$ are isomorphic if and only if the objects d and d' are isomorphic. We obtain a second Yoneda embedding

   $$\mathcal{C} \to [\mathcal{C}^{\mathrm{opp}}, \mathrm{Set}]$$

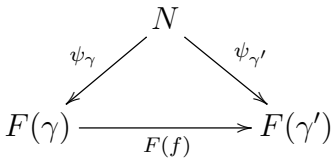
   that sends $c \mapsto \mathrm{Hom}_{\mathcal{C}}(-, d)$. It maps objects on $\mathcal{C}$ to presheaves on $\mathcal{C}$.

2.2 Limits and colimits

Definition 2.2.1
Let Γ be an (essentially) small category and $\mathcal{C}$ be a category.

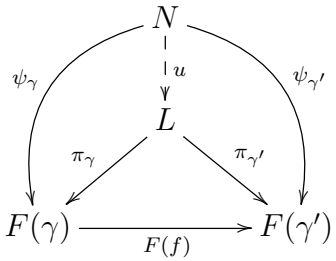
1. A functor $F : \Gamma \to \mathcal{C}$ is called a diagram of shape Γ with values in $\mathcal{C}$. The functor category $[\Gamma, \mathcal{C}]$ is called the category of diagrams of shape Γ with values in $\mathcal{C}$. Its morphisms are just natural transformations.

2. A cone to a diagram F is a pair (N, ψ), consisting of an object $N \in \mathcal{C}$, together with a family $(\psi_\gamma : N \to F(\gamma))_{\gamma\in\Gamma}$ of morphisms indexed by the objects $\gamma \in \Gamma$, such that for every morphism $f : \gamma \to \gamma'$ in Γ, we have $F(f) \circ \psi_\gamma = \psi_{\gamma'}$.



The object $N \in \mathcal{C}$ is called the summit or the apex of the cone.

3. A limit of the diagram $F : \Gamma \to \mathcal{C}$ is a cone (L, π) to a diagram F with the universal property that for any other cone (N, ψ) to F there exists a unique morphism $u : N \to L$ such that $\pi_\gamma \circ u = \psi_\gamma$ for all $\gamma \in \Gamma$.



We write $L = \lim_\Gamma F$.

4. The definition of a cocone and a colimit is dual, i.e. obtained by reversing arrows. The object in a cocone is also called the nadir. We write $\operatorname{colim}_\Gamma X$ for the colimit.

Categorical language generally follows the design principle that an X in $\mathcal{C}$ corresponds to a co-X in $\mathcal{C}^{\mathrm{opp}}$.

Examples 2.2.2 1. Let Γ be a discrete category, i.e. a category with only identity arrows, cf. Examples 2.1.3.9. A diagram of shape Γ is then simply a family of objects $(V_\gamma)_{\gamma\in\Gamma}$ indexed by Γ. A cone with apex N is then a family of morphisms $(\psi_\gamma : N \to X_\gamma)_{\gamma\in\Gamma}$. Assume that the limit (L, π) of this diagram exists. By definition, given any object N and family of maps $(\psi_\gamma : N \to X_\gamma)_{\gamma\in\Gamma}$, there is a unique morphism $u : N \to L$ such that $\pi_\gamma \circ u = \psi_\gamma$. Denoting the limit by $L = \prod_\gamma X_\gamma$, this amounts to an isomorphism

$$\begin{array}{ccc} \operatorname{Hom}_{\mathcal{C}}(Y, \prod_\gamma X_\gamma) & \xrightarrow{\cong} & \prod_\gamma \operatorname{Hom}_{\mathcal{C}}(Y, X_\gamma) \\ u & \mapsto & (\pi_\gamma \circ u)_{\gamma\in\Gamma} \end{array}$$

which is just the universal property we encountered for products of modules.

2. Dually, the colomit C is a cocone, i.e. comes with structure morphisms $(\iota_\gamma : X_\gamma \to C)_{\gamma\in\Gamma}$ such that we get an isomorphism isomorphism

$$\begin{array}{ccc} \operatorname{Hom}_{\mathcal{C}}(\coprod_\gamma X_\gamma, Y) & \xrightarrow{\cong} & \prod_\gamma \operatorname{Hom}_{\mathcal{C}}(X_\gamma, Y) \\ u & \mapsto & (u \circ \iota_\gamma)_{\gamma\in\Gamma} \end{array}$$

This leads to the following definition:

Definition 2.2.3 Let Γ be a discrete category and $X : \Gamma \to \mathcal{C}$ a diagram of shape Γ. This is the same as a family of objects indexed by the set of objects of Γ. We write for diagrams of shape Γ

$$\coprod_{\gamma} X_\gamma := \mathrm{colim}_\Gamma X \quad \text{and} \quad \prod_{\gamma} X_\gamma := \lim_{\Gamma} X$$

and call the limit a product and the colimit a coproduct of the family $(X_\gamma)_{\gamma\in\Gamma}$ of objects in $\mathcal{C}$.

Remarks 2.2.4

1. There are categories, in which not all products and coproducts exist. But if they exist, then their universal properties imply that they are unique up to unique isomorphism. This justifies giving a (co)product a definite notation.

2. The coproduct in the category Set of sets is disjoint union. The product in the category Set of sets is the Cartesian product.

3. In the category of R-modules the direct sum and the direct product from Definition 1.2.1 are exactly the categorical coproduct resp. product, see Remark 1.2.2 (2).

4. The Cartesian product of rings is also a categorical product in the category of rings. The tensor product is the coproduct in the category of *commutative* rings, although not in the category of all rings, cf. Remarks 1.2.12.5.

Examples 2.2.5 1. Consider the empty family and assume that the corresponding coproduct $\coprod_\emptyset$ exists in a category $\mathcal{C}$. Given any object $M \in \mathcal{C}$, there is a single cocone over the diagram indexed by $\emptyset$ with nadir M, namely the empty family. By the universal property of the coproduct, there exists a uniquely determined morphism $\coprod_\emptyset \to M$. This shows that $\coprod_\emptyset$ is an initial object in $\mathcal{C}$. This is an object $0 \in \mathcal{C}$, from which there exists a unique morphism to every object of $\mathcal{C}$.

2. Dually, a product $\prod_\emptyset$ with values in $\mathcal{C}$ is a terminal object of $\mathcal{C}$.

3. The terminal object in the category Set of sets is any singleton set $\{*\}$ with one element. The empty set is an initial object. In the category $R-$Mod, the zero module is both an initial and terminal object.

Definition 2.2.6 Consider a diagram of the shape

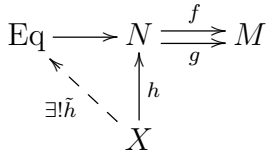
$$N \underset{g}{\overset{f}{\rightrightarrows}} M$$

with values in any category $\mathcal{C}$, i.e. $M, N \in \mathcal{C}$. We say that f, g is a pair of parallel morphisms.

1. We call the limit of this diagram, if it exists, the equaliser or difference kernel of the parallel pair of morphisms f and g.

2. We call the colimit of this diagram, if it exists, the coequaliser or difference cokernel of the parallel pair of morphisms f and g.

Remarks 2.2.7 1. Spelling out the definition of a limit explicitly, we see that the difference kernel is a morphism $\mathrm{Eq} \to N$, such that for any diagram



with a morphism $h : X \to N$ such that $f \circ h = g \circ h$, there exists a unique morphism $\tilde{h}\colon X \to \mathrm{Eq}$ such that the left triangle commutes. If $\mathrm{Hom}(x, y)$ is even an abelian group for all objects $x, y \in \mathcal{C}$, then the difference kernel is just the kernel of the difference $f - g$ of the morphisms.

2. Dually, the coequalizer is a morphism $M \to \mathrm{Coeq}$, such that for any diagram

$$\begin{array}{ccccc} N & \overset{f}{\underset{g}{\rightrightarrows}} & M & \longrightarrow & \mathrm{Coq} \\ & & {\scriptstyle h}\downarrow & \swarrow_{\exists! \tilde{h}} & \\ & & X & & \end{array}$$

with a morphism h such that $h \circ f = h \circ g$, there exists a unique morphism $\tilde{h}\colon \mathrm{Coeq} \to X$. If $\mathrm{Hom}(x, y)$ is even an abelian group for all objects x, y, then the difference kernel is just the cokernel of the difference $f - g$ of the morphisms.

3. The tensor product of a right R-module (M, ρ) and a left R-module (N, λ) is the coequalizer of the two morphisms

$$\rho \otimes_{\mathbb{Z}} \mathrm{id}_N, \mathrm{id}_M \otimes_{\mathbb{Z}} \lambda : \quad M \otimes_{\mathbb{Z}} R \otimes_{\mathbb{Z}} N \to M \otimes_{\mathbb{Z}} N$$

of abelian groups.

4. Dual to the notion of a ring is the notion of a coring. A ring is a monoid in $\mathbb{Z}$-Mod. A coring is a monoid in the dual category, or, more explicitly, an abelian group C with comultiplication $\Delta : C \to C \otimes C$ that is coassociative and counital. Dual to left modules is the notion of a left comodule, i.e. an abelian group M with a coaction $\delta : M \to C \otimes M$. The cotensor product of a right and left comodule is then defined as an equalizer of the coactions,

$$\rho \otimes_{\mathbb{Z}} \mathrm{id}_N, \mathrm{id}_M \otimes_{\mathbb{Z}} \lambda : \quad M \otimes_{\mathbb{Z}} N \to M \otimes_{\mathbb{Z}} \otimes C \otimes_{\mathbb{Z}} N$$

We now discuss an important class of limits and colimits that we will later: pullbacks and pushouts.

Examples 2.2.8

1. Consider the partially ordered set $\Omega = \{0, 1, 2\}$ with $0 < 1, 0 < 2$. It gives rise to a category Γ with non-identity arrows

$$\begin{array}{ccc} \gamma_0 & \longrightarrow & \gamma_1 \\ \downarrow & & \\ \gamma_2 & & \end{array}$$

A Γ-shaped diagram in a category $\mathcal{C}$ is called a <u>span</u> in $\mathcal{C}$:

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

Here, we have $A, B, N \in \mathcal{C}$. The category $[\Gamma, \mathcal{C}]$ is the category of spans in $\mathcal{C}$.

2. The category of cospans in a category $\mathcal{C}$ is defined as $[\Gamma^{\mathrm{opp}}, \mathcal{C}]$. A cospan thus is a diagram of the form

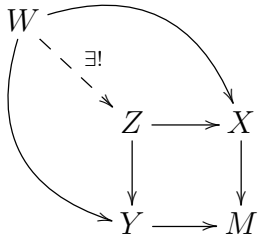
$$\hat{\Gamma} := \qquad \begin{array}{ccc} & & X \\ & & \downarrow{\scriptstyle f} \\ Y & \xrightarrow[g]{} & M \end{array} \quad . \qquad (*)$$

with $X, Y, M \in \mathcal{C}$.

Definition 2.2.9 1. We call the limit of a cospan in $\mathcal{C}$ the pullback of the cospan.

2. We call the colimit of a span in $\mathcal{C}$ the pushout of the span.

Remarks 2.2.10 1. We describe the universal property of the pullback Z of the cospan $\hat{\Gamma}$ in $(*)$ that characterizes it up to unique isomorphisms (provided it exists). For every object W together with morphisms $W \to X$ and $W \to Y$ such that the diagram of solid arrows commutes, there exists a unique morphism $W \to Z$ in $\mathcal{C}$, such that the diagram



For a pullback, we also write $Z = X \times_M Y = X \,{}_f\!\times_g Y$ or

$$\begin{array}{ccc} Z_{\rfloor} & \longrightarrow & X \\ \downarrow & & \downarrow{\scriptstyle f} \\ Y & \xrightarrow[g]{} & M \end{array}$$

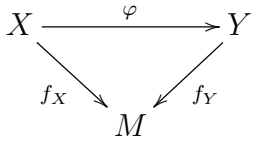
2. Dually we write for the pushout of a span

$$\begin{array}{ccc} N & \xrightarrow{f} & A \\ {\scriptstyle g}\downarrow & & \downarrow \\ B & \longrightarrow & W \end{array}$$

denoted $W = A \sqcup_N B$. It has the dual universal property.

Remarks 2.2.11

1. Let M be an object in a category $\mathcal{C}$. The over category $\mathcal{C} \downarrow M$ of objects over M is defined as the category, whose objects are pairs (X, f_X), with X an object in $\mathcal{C}$ and a morphism $f_X \colon X \to M$, and whose morphisms are commuting diagrams



The pullbacks $\cdot \times_M \cdot$ are precisely the products in over category over M. They are also called fibre products over M.

2. In the categories Set, Top, Ab, $R-$Mod the pullback is given by

$$X \times_M Y = X \,{}_f\!\times_g Y = \{(x,y) \,|\, x \in X,\ y \in Y, \quad f(x) = g(y)\} \ . \qquad (*)$$

The structure morphism $X \times_M Y \to X$ of the pullback is the (restriction of the) projection $(x,y) \mapsto x$ onto the first component, the structure morphism $X \times_M Y \to Y$ is the (restriction of the) projection $(x,y) \mapsto y$. The morphism $Z \to X \times_M Y$, induced by two suitable morphisms $\varphi\colon Z \to X$ and $\psi\colon Z \to Y$ is given by $z \mapsto (\varphi(z), \psi(z))$.

The pullback $(*)$ is realized as the equalizer of a product. In the categories Set, Top, Ab, $R-$Mod the pullback is thus the difference kernel

$$X \times_M Y = X \,{}_f\!\times_g Y = \mathrm{Eq}(\ X \times Y \underset{g\circ pr_2}{\overset{f\circ pr_1}{\rightrightarrows}} M\ ) \ .$$

3. One defines the category $N \downarrow \mathcal{C}$ of objects under N as the category, whose objects are pairs (X, f) with $f\colon N \to X$. The pushouts are exactly the coproducts in the under category. They are also called amalgamated sums.

4. Dually, the pushout can be realized as the coequaliser of the maps

$$A \sqcup_N B := \mathrm{CoEq}(\ N \underset{\iota_2\circ g}{\overset{\iota_1\circ f}{\rightrightarrows}} A \coprod B\ )$$

into the coproduct, if it exists.

In the category $R-$Mod, the pushout is thus given by the quotient module

$$A \sqcup_N B = A \oplus B / (f(n), 0) \sim (0, g(n)) \ .$$

The structure morphism $A \to A \sqcup_N B$ is the injection $a \mapsto [a, b]$ into the first component. The morphism $A \sqcup_N B \to Z$, induced by two suitable morphisms $f\colon A \to Z$ and $g\colon B \to Z$, is given by $[a, b] \mapsto f(a) + g(b)$. It is instructive to consider why it is well-defined on the quotient.

It should now be clear that it is important to be able to check the existence of limits and colimits. We start with the definition:

Definition 2.2.12

1. A category is called (finitely) cocomplete, if every (essentially finite) diagram in $\mathcal{C}$ has a colimit.

2. A category $\mathcal{C}$ is called (finitely) complete, if every (essentially finite) diagram in $\mathcal{C}$ has a limit.

We can now explain a result which ensures the existence of colimits, generalizing the construction in Remarks 2.2.11.2 and for pullbacks and pushouts:

Proposition 2.2.13
Let $\mathcal{C}$ be a category and $X : \Gamma \to \mathcal{C}$ a diagram in $\mathcal{C}$ of the shape Γ. If in $\mathcal{C}$ difference cokernels and coproducts for the sets of objects and morphisms of Γ exist, then X has a colimit which can be expressed as a difference cokernel.

A dual statement holds for limits.

Proof. By assumption, the two coproducts

$$\coprod_{\gamma_1 \xrightarrow{f} \gamma_2} X(\gamma_1) \quad \text{and} \quad \coprod_{\gamma \in \Gamma} X(\gamma)$$

indexed by morphisms and objects of Γ exist. By the universal property of the first coproduct, indexed by morphisms in Γ, there exist a unique morphism α such that for any $\gamma_1 \xrightarrow{f} \gamma_2$ the diagram

$$\begin{array}{ccc} X(\gamma_1) & \xrightarrow{X(f)} & X(\gamma_2) \\ \downarrow{\scriptstyle \iota(f)} & & \downarrow{\scriptstyle \iota(\gamma_2)} \\ \coprod_{\gamma_1 \to \gamma_2} X(\gamma_1) & \xrightarrow[\alpha]{} & \coprod_{\gamma \in \Gamma} X(\gamma) \end{array}$$

commutes. Similarly, there exists a unique morphism β such that for all $\gamma_1 \xrightarrow{f} \gamma_2$ the diagram

$$\begin{array}{ccc} & X(\gamma_1) & \\ {\scriptstyle \iota(f)} \swarrow & & \searrow {\scriptstyle \iota(\gamma_1)} \\ \coprod_{\gamma_1 \to \gamma_2} X(\gamma_1) & \xrightarrow[\beta]{} & \coprod_{\gamma \in \Gamma_0} X(\gamma) \end{array}$$

The difference cokernel C of

$$\coprod_{\gamma_1 \to \gamma_2} X(\gamma_1) \underset{\beta}{\overset{\alpha}{\rightrightarrows}} \coprod_{\gamma} X(\gamma)$$

comes with maps

$$X(\gamma) \xrightarrow{\iota(\gamma)} \coprod_{\gamma_1 \to \gamma_2} X(\gamma_1) \underset{\beta}{\overset{\alpha}{\rightrightarrows}} \coprod_{\gamma \in \Gamma} X(\gamma) \longrightarrow C$$

which turn C into a colimit for the diagram X. Indeed, a morphism $C \to T$ is the same as a morphism $\varphi : \coprod_\gamma X(\gamma) \to T$ such that $\varphi \circ \alpha = \varphi \circ \beta$. This is the same as a family of morphisms $(\varphi_\gamma : X(\gamma) \to T)_{\gamma \in \Gamma}$ such that

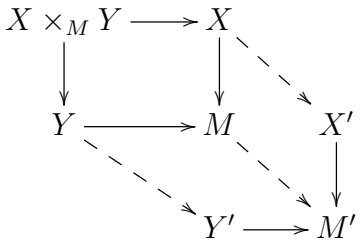
$$\varphi_{\gamma_1} = \varphi_{\gamma_2} \circ X(\gamma_1 \xrightarrow{f} \gamma_2)$$

for all morphisms $\gamma_1 \xrightarrow{f} \gamma_2$ in Γ. The latter is just a cocone of the diagram X. □

Examples 2.2.14 The following categories are complete and cocomplete: Set, Ab, Grp, R-mod and Top, since they have difference (co-)kernels and (co-)products. The categories of finite sets, finite abelian groups and finite-dimensional vector spaces are finitely complete and finitely cocomplete, but neither complete nor cocomplete.

We will need more properties of pullbacks later in the lecture. Hence we work a bit more with them:

Remarks 2.2.15 1. If pullbacks exist, they yield a functor from the category of cospans in $\mathcal{C}$ to $\mathcal{C}$. On objects, this functor is just a choice of pullback. To define this functor on morphisms, we oberseve that a morphisms of cospans is a commuting diagram



given by the dashed morphisms. The outer arrows compose to equal morphisms $X \times_M X \to Y \to Y' \to M'$ and $X \times_M X \to X \to X' \to M$ and thus, by the universal property of the pullbacks $X' \times_{M'} Y'$, determine a unique morphism $X \times_M Y \to X' \times_{M'} Y'$ between the pullbacks.

2. If pullbacks exist, then any morphism $M \xrightarrow{g} M'$ yields a functor of over categories

$$g^*: \quad \mathcal{C} \downarrow M' \;\to\; \mathcal{C} \downarrow M$$

that sends the object $X \to M'$ to the object $X \times_{M'} M \to M$ in the category $\mathcal{C} \downarrow M$:

$$\begin{array}{ccc} g^*(X) = X \times_{M'} M & \longrightarrow & X \\ \downarrow & & \downarrow \\ M & \xrightarrow{\quad g \quad} & M' \end{array}$$

We then call g^* the pullback functor associated with the morphism g.

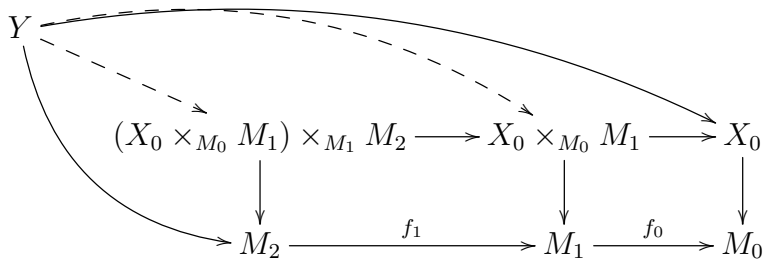
3. If both small squares in the diagram

$$\begin{array}{ccccc} X_2 & \longrightarrow & X_1 & \longrightarrow & X_0 \\ \downarrow & & \downarrow & & \downarrow \\ M_2 & \longrightarrow & M_1 & \longrightarrow & M_0 \end{array}$$

are pullback diagrams, then so is the big one. This is called pasting of pullback diagrams: we have

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

To see this we consider the diagram



for an arbitrary object Y and let morphisms $Y \to X_0$ and $Y \to M_2$ be given, such that the outer pentagon commutes. The pullback property of the right square, applied to the morphisms $Y \to X_0$ and $Y \to M_2 \xrightarrow{f_1} M_1$ yields a unique morphism $Y \to X_0 \times_{M_0} M_1$. To this and to $Y \to M_2$ we now apply the pullback property of the left square and obtain a unique morphism $Y \to (X_0 \times_{M_0} M_1) \times_{M_1} M_2$, which shows that also the big rectangle is a pullback diagram.

4. This result has an important reinterpretation in terms of pullback functors: given morphisms $M_2 \xrightarrow{f_1} M_1 \xrightarrow{f_0} M_0$, there exists a distinguished natural isomorphisms of pullback functors:

$$(f_0 \circ f_1)^* \Rightarrow f_1^* \circ f_0^* \ .$$

Note that here one typically does not have an equality of functors. One can show, however, that a certain coherence condition holds, namely that the following diagram of natural transformations commutes

$$\begin{array}{ccc} (f_0 \circ f_1 \circ f_2)^* & \Longrightarrow & f_2^* \circ (f_0 \circ f_1)^* \\ \Downarrow & & \Downarrow \\ (f_1 \circ f_2)^* \circ f_0^* & \Longrightarrow & f_2^* \circ f_1^* \circ f_0^* \ . \end{array}$$

5. All statements about pullback have dual analogs for the pushout.

More generally, we have

Proposition 2.2.16 Suppose that a category $\mathcal{C}$ has all Γ-shaped limits. Then a choice of limit for each diagramm defines a functor

$$\lim_{\Gamma} : \quad [\Gamma, \mathcal{C}] \to \mathcal{C} \, .$$

Proof. On objects, the functor is defined by the choice of limits. Given two diagrams $F, G : \Gamma \to \mathcal{C}$ and a natural transformation $\alpha : F \to G$, which is just a morphism of diagrams, the limit cone $\lambda : \lim_\Gamma F \to F$ defines a cone

$$\lim_{\Gamma} F \to F \xrightarrow{\alpha} F'$$

with summit $\lim_\Gamma F$ over the diagram F'. It factorizes by the universal property of $\lim_\Gamma F'$ uniquely to a morphism $\lim_\Gamma F \to \lim_\Gamma F'$ which we call $\lim_\Gamma(\alpha)$. □

We finally discuss the interaction of functors with limits and colimits:

Definition 2.2.17

1. A functor $F : \mathcal{C} \to \mathcal{D}$ is called <u>cocontinuous</u> (or preserves colimits), if for any universal cocone $X \to \Delta_\Gamma$ over a diagram Δ_Γ in $\mathcal{C}$ the induced cocone $F(X) \to F(\Delta_\Gamma)$ is universal as well.

2. The notion of a <u>continuous functor</u> is dual.

Remarks 2.2.18

1. A cocontinous functor can be characterized equivalently by the condition that for any diagram X in $\mathcal{C}$ with a colimit $\mathrm{colim}(X)$, also the diagram $F(X)$ in $\mathcal{D}$ has a colimit and the canonical morphism
$$\mathrm{colim}(F(X)) \ \to F(\mathrm{colim}(X))$$
is an isomorphism.

2. The forgetful functor $U : \mathrm{Ab} \to \mathrm{Set}$ is not cocontinous. Indeed, the initial object, i.e. the colimit of the empty diagram as explained in Examples 2.2.2.1, is the trivial group for Ab and the empty set for Set and thus not preserved. Alternatively, we can also look at a coproduct of two elements: the map
$$U(A_1) \sqcup U(A_2) \to U(A_1 \sqcup A_2) = U(A_1 \oplus A_2) = U(A_1) \times U(A_2)$$
is not surjective in general and hence not an isomorphism.

   Forgetful functors can not be expected to be cocontinuous in general. (The forgetful functor $\mathrm{Top} \to \mathrm{Set}$ is continuous, though.)

3. If Γ is a small category, then the functor category $\hat{\Gamma} := [\Gamma^{\mathrm{opp}}, \mathrm{Set}]$ is cocomplete [B16, Satz 9.4.13]. The Yoneda embedding $\Gamma \to \hat{\Gamma}$ induces [B16, Proposition 9.4.13] for any cocomplete category $\mathcal{D}$ an equivalence of categories
$$\mathrm{Fun}_c(\hat{\Gamma}, \mathcal{D}) \cong [\Gamma, \mathcal{D}] \quad .$$
   Here Fun_c denotes the full subcategory of cocontinuous functors.

4. Any representable functor $\mathcal{C}^{\mathrm{opp}} \to \mathrm{Set}$ is continuous. For any diagram $X \in [\Gamma, \mathcal{C}]$ with colimit $\mathrm{colim}_\Gamma X \in \mathcal{C}$, the canonical map

$$\mathrm{Hom}(\mathrm{colim}_\Gamma X, c) \ \to \lim_\Gamma \mathrm{Hom}(X, c)$$

is an isomorphism for any $c \in \mathcal{C}$. (Note that a colimit in $\mathcal{C}$ is a limit in $\mathcal{C}^{\mathrm{opp}}$.) Indeed, the limit in the category Set is a subset of the product $\prod_{i\in I} X(i)$ consisting of tuples (x_i) such that $X(i \to j)x_i = x_j$.

Similarly, the canonical map

$$\mathrm{Hom}_{\mathcal{C}}(c, \lim_\Gamma X) \ \to \lim_\Gamma \mathrm{Hom}(c, X)$$

is an isomorphism for any $c \in \mathcal{C}$.

We finally mention a specific type of limit and colimit and one application to the theory of finite-dimensional algebras.

Remark 2.2.19 1. We first introduce the notion of an end and of a coend of a functor

$$F\colon \qquad \mathcal{C}^{\mathrm{opp}} \times \mathcal{C} \to \mathcal{D}\ ,$$

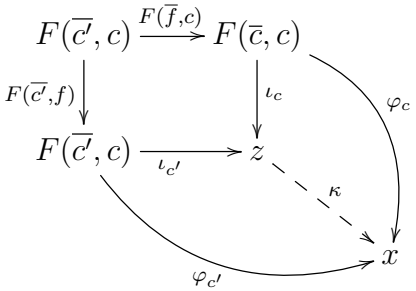
see [McL71, Ch. IX.4].

A <u>dinatural transformation</u> $F \Rightarrow x$ from functor F to an object $x \in \mathcal{D}$ is a family $\varphi = \{\varphi_c\colon F(\overline{c}, c) \to x\}_{c\in\mathcal{C}}$ of morphisms satisfying

$$\begin{array}{ccc} F(\overline{c'}, c) & \xrightarrow{F(\overline{f},c)} & F(\overline{c}, c) \\ {\scriptstyle F(\overline{c'},f)}\downarrow & & \downarrow{\scriptstyle \varphi_c} \\ F(\overline{c'}, c') & \xrightarrow[\varphi_{c'}]{} & x \end{array}$$

for all $f \in \mathrm{Hom}_{\mathcal{C}}(c, c')$.

2. A coend (z, ι) for a functor $F\colon \mathcal{C}^{\mathrm{opp}} \times \mathcal{C} \to \mathcal{D}$ is an object $z \in \mathcal{D}$ together with a dinatural transformation ι from F to z having the universal property that for any dinatural transformation $\varphi\colon F \Rightarrow x$ to some $x \in \mathcal{D}$ there is a unique morphism $\kappa = \kappa(\varphi) \in \mathrm{Hom}_{\mathcal{D}}(z, x)$ such that $\varphi_c = \kappa \circ \iota_c$ for all $c \in \mathcal{C}$.



3. The notion of an end for a functor $F\colon \mathcal{C}^{\mathrm{opp}} \times \mathcal{C} \to \mathcal{D}$ is defined dually. We often suppress the universal dinatural transformation and denote the coend and end of a functor $F\colon \mathcal{C}^{\mathrm{opp}} \times \mathcal{C} \to \mathcal{D}$, as well as the underlying objects, by $\int^{c\in\mathcal{C}} F(\overline{c}, c)$ and by $\int_{c\in\mathcal{C}} F(\overline{c}, c)$, respectively.

4. Let K be a field and A and B be finite-dimensional K-algebras and $G\colon A\text{-mod} \to B\text{-mod}$ a linear functor, i.e. a functor that consists of K-lienar maps on the Hom-spaces, cf. Definition 3.1.8. Consider the functor

$$\begin{aligned} \widetilde{G}: \qquad A\text{-mod}_{fd} \times A\text{-mod}_{fd}^{\text{opp}} &\longrightarrow B - \text{bimod} - A \\ m \times \overline{n} &\longmapsto G(m) \otimes_K n^* \end{aligned}$$

where we use the vector space dual to turn a left module m into a right module m^*. Its end is given as a B-A-bimodule by

$$\int_{m \in A\text{-mod}} G(m) \otimes_K m^* = G(A)$$

with the natural B-A-bimodule structure on $G(A)$. Note that $G(A)$ is a B left module as the image of the regular left A module ${}_AA$ under the functor $G: A-\text{Mod} \to B\text{-Mod}$. For each $a \in A$, the endomorphism $r_a : A \to A$ with $a' \mapsto a' \cdot a$ of the regular left module gives morphisms $G(r_a) : G(A) \to G(A)$ which endow $G(A)$ with the structure of a right A module and even an B-A-bimodule. For the dinatural family, we refer to [FSS20, Proposition 2.8] where also a proof is given. Specializing G to the identity functor, we find the following Peter-Weyl theorem:

$$\int_{m \in A\text{-mod}} m \otimes_K m^* \;\cong\; {}_AA_A$$

The bimodule A is also characterized categorically by the fact that $A \otimes_A B \cong B \cong B \otimes_A A$ for any A-bimodule B. Here, we have constructed it in a purely categorical way from the category of all finite-dimensional A-modules.

5. Similarly, the coend of the functor $\widetilde{G}$ is

$$\int^{m \in A\text{-mod}} G(m) \otimes_K m^* = G(A^*) \tag{1}$$

In particular, we have

$$\int^{m \in A\text{-mod}} m \otimes_K m^* \;\cong\; {}_AA^*_A$$

of A-bimodules. The categorical characterization of the bimodule A^* is more subtle [**?**].

2.3 Universal properties and adjoint functors

We now consider universal properties in an abstract setting. To access a good example, we once again use the notion of a product which is characterized by the isomorphisms

$$\text{Hom}_{\mathcal{C}}(Y, \prod_{\gamma} X_\gamma) \xrightarrow{\cong} \prod_{\gamma} \text{Hom}_{\mathcal{C}}(Y, X_\gamma)$$

We consider the direct sum and the direct product of a family $(X_\lambda)_{\lambda \in \Lambda}$ of modules over a given ring R, i.e. $X \in \mathcal{D} = R\text{-mod}$, in a more formal context. Let

$$\mathcal{C} := \prod_{\lambda \in \Lambda} \mathcal{D} = [\Lambda, \mathcal{D}]$$

denote the product category from Definition 2.1.4, whose objects are Λ-tuples of modules. A morphism $(X_\lambda)_{\lambda \in \Lambda} \to (Y_\lambda)_{\lambda \in \Lambda}$ is a Λ-tuple of R-module homomorphisms $f_\lambda\colon\ X_\lambda \to Y_\lambda$.

In the universal properties of the direct sum and the product a arbitrary fixed object appears in all factors of a product of Hom-sets. We thus introduce the diagonal functor

$$\begin{array}{rcl} \Delta\colon \mathcal{D} & \to & \mathcal{C} \\ X & \mapsto & (X, X, \ldots, X) = (X)_{\lambda\in\Lambda} \end{array}$$

that sends an object X to the constant family and a morphism $X \xrightarrow{f} Y$ to the constant family of morphisms, $\Delta(f) = (f)_{\lambda\in\Lambda}$.

Suppose that *all* direct sums and *all* products are defined in the category $\mathcal{D}$. For example, this is the case for $\mathcal{D} = R-\mathrm{Mod}$ for a ring R. The direct sum resp. the direct product of modules and module homomorphisms yields functors

$$\prod, \coprod \colon \mathcal{C} \to \mathcal{D} \ .$$

The universal property of the coproduct says that for every object $c \in \mathcal{C}$ — i.e. for every family of objects in $\mathcal{D}$ — and for every object $d \in \mathcal{D}$ there exist isomorphisms of Hom-sets:

$$\mathrm{Hom}_{\mathcal{D}}(\coprod c, d) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(c, \Delta d) \ \ ;$$

in the case of the product, on the other hand, we have isomorphisms

$$\mathrm{Hom}_{\mathcal{D}}(d, \prod c) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(\Delta d, c) \ \ .$$

This leads to the following definition:

Definition 2.3.1

1. Let $\mathcal{C}$ and $\mathcal{D}$ be arbitrary categories. A functor $F\colon \mathcal{C} \to \mathcal{D}$ is called left adjoint to a functor $G\colon \mathcal{D} \to \mathcal{C}$ if for any two objects c in $\mathcal{C}$ and d in $\mathcal{D}$ there exists an isomorphism of sets

$$\Phi_{c,d}\colon \ \mathrm{Hom}_{\mathcal{C}}(c, Gd) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{D}}(Fc, d)$$

with the following natural property:

For every morphism $c' \xrightarrow{f} c$ in $\mathcal{C}$ and $d \xrightarrow{g} d'$ in $\mathcal{D}$ consider for $\varphi \in \mathrm{Hom}_{\mathcal{D}}(Fc, d)$ the morphism

$$\mathrm{Hom}(Ff, g)(\varphi) := Fc' \xrightarrow{Ff} Fc \xrightarrow{\varphi} d \xrightarrow{g} d' \in \mathrm{Hom}_{\mathcal{D}}(Fc', d')$$

and for $\varphi \in \mathrm{Hom}_{\mathcal{C}}(c, Gd)$ the morphism

$$\mathrm{Hom}(f, Gg)(\varphi) := c' \xrightarrow{f} c \xrightarrow{\varphi} Gd \xrightarrow{Gg} Gd' \in \mathrm{Hom}_{\mathcal{C}}(c', Gd') \ \ .$$

The natural property is then the compatibility requirement on morphisms, namely that the diagram

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(c, Gd) & \xrightarrow{\mathrm{Hom}(f,Gg)} & \mathrm{Hom}_{\mathcal{C}}(c', Gd') \\ \Big\downarrow{\scriptstyle \Phi_{c,d}} & & \Big\downarrow{\scriptstyle \Phi_{c',d'}} \\ \mathrm{Hom}_{\mathcal{D}}(Fc, d) & \xrightarrow[\mathrm{Hom}(Ff,g)]{} & \mathrm{Hom}_{\mathcal{D}}(Fc', d') \end{array}$$

commutes for all morphisms f, g.

2. In the case we write $F \dashv G$ and say that the functor G is right adjoint to F.

Examples 2.3.2

1. We have seen that the coproduct is a left adjoint functor to the diagonal functor, i.e. $\coprod \dashv \Delta$, and that the product is a right adjoint functor to the diagonal functor, i.e. $\Delta \dashv \prod$.

2. We consider the forgetful functor

$$U\colon R\text{−Mod} \to \text{Set}\ ,$$

that sends every vector space to its underlying set. Its left adjoint functor is the the functor that assigns to a set the free module on the set

$$F:\ \text{Set} \to R\text{−Mod}\,,$$

that sends a set M to the free R-module $R(M)$ that was introduced in Remark 1.3.2. It has a canonical basis labelled by the elements of M. A map $f\colon M \to N$ of sets is sent by F to the linear map $F(M) \to F(N)$ that maps the basis element δ_m with $m \in M$ of the canonical basis of $F(M)$ to the basis element $\delta_{f(m)}$ of the canonical basis of $F(N)$.

For every set M and every R-module V we then have an isomorphism of sets

$$\begin{array}{rccc} \Phi_{M,V}: & \mathrm{Hom}_{\mathrm{Set}}(M, U(V)) & \to & \mathrm{Hom}_R(F(M), V) \\ & \varphi & \mapsto & \Phi_{M,V}(\varphi) \end{array}$$

with

$$\Phi_{M,V}(\varphi)(\sum_{m\in M} \lambda_m m) := \sum_{m\in M} \lambda_m \varphi(m)\ .$$

In particular, we find that for every K-vector space V, the one-element set $\mathrm{Hom}_{\mathrm{Set}}(\emptyset, G(V))$ has to be isomorphic to the space of R-module morphisms $\mathrm{Hom}_R(F(\emptyset), V)$. The only R-module that admits only a single linear map into any K-vector space V is the zero vector space, $F(\emptyset) = \{0\}$. In this sense, the zero vector space is spanned by the empty set.

3. A similar example is the forgetful functor $U\colon Gr \to \text{Set}$, that sends groups to their underlying sets. Here a left adjoint functor exists, namely the functor F that sends a set to the free group generated by it.

   The category Ab of abelian groups is a subcategory of the category Gr of all groups. We can thus restrict the forgetful functor to Ab. The left adjoint functor is then a functor $F'\colon \text{Set} \to \text{Ab}$ that sends a set to the free *abelian* group generated by it. It is different from from the left adjoint functor described before. For example, the free abelian group on two elements is just $\mathbb{Z}^2$ while the free group on two elements x, y consists of all word in the letters $\{x, y, x^{-1}, y^{-1}\}$ modulo the relations $xx^{-1} = x^{-1}x = e = yy^{-1} = y^{-1}y$.

   We have thus learnt that freely generated objects may be defined as images of the left adjoint to a forgetful functor.

4. There are also forgetful functors that have no left adjoint functor. An example is the forgetful functor U from the category of fields into the category of sets. If there were a left adjoint functor, then it would assign a field $K(M)$ to each set M. In particular we could choose $M = \emptyset$, for which we would have to find a field $K = K(\emptyset)$, such that for every field L there exists a bijection of sets

$$\mathrm{Hom}_{\mathrm{Field}}(K, L) \cong \mathrm{Hom}_{\mathrm{Set}}(\emptyset, U(L)) \cong \star.$$

Since non-trivial field homomorphisms are injective, the sought-after field would be a subfield of every field. But such a field does not exist: the prime field depends on the characteristic of L. (In other words: the category of sets has an initial object, the empty set. In the category of all field there does not exist an initial object.) Thus there is no notion of "freely generated field".

5. The inclusion functor $I\colon \mathrm{Ab} \to Grp$ of abelian groups into all groups has a left adjoint functor, namely $(-)_{\mathrm{ab}}\colon Grp \to \mathrm{Ab}$, that sends a group G to its abelianization $G_{ab} := G/[G,G]$. This is because we have:

$$\mathrm{Hom}_{Grp}(G, I(A)) \cong \mathrm{Hom}_{\mathrm{Ab}}(G_{ab}, A) \ .$$

(This will be an exercise.)

6. There is a forgetful functor U from categories (with functors as isomorphisms) to the category of oriented graphs. The vertices of the graph $U(\mathcal{C})$ are the objects of $\mathcal{C}$; the edges are the morphisms, except for identity morphisms. We thus forget identities and composition. Its left adjoint assigns to a graph Γ the free category $F(\Gamma)$. Its objects are the vertices of graphs, the morphisms are paths, i.e. finitely many composable edges. For details, see [McL71, Chapter II.7].

If a functor admits an adjoint, then it enjoys additional properties, as we will see for example in Corollary 2.3.6.

We consider another example relating modules over different rings:

Example 2.3.3 Let R, S be (unital) rings and $\phi\colon R \to S$ a ring homomorphism. (If ϕ injective, then R is a subring of S.) Then pullback resp. restriction of scalars as in example 2.1.6.2 defines a forgetful functor

$$U\colon S\text{−Mod} \to R\text{−Mod} \ .$$

We will study its adjoint functors.

1. To get a left adjoint functor $F\colon R\text{−Mod} \to S\text{−Mod}$ to U, we define it on objects by $F(M) = S \otimes_R M$, where S is considered as a right module over R via pullback along ϕ and the left action of S on $S \otimes_R M$ is defined by the multiplication in S, i.e. $s'.(s \otimes m) := (s' \cdot s) \otimes m$. On morphisms we set $F(f) = \mathrm{id}_S \otimes_R f$. This functor is called <u>extension of scalars</u> or <u>induction</u>.

   To see that F is in fact a left adjoint functor of U, we consider for $M \in R\text{−Mod}$ and $N \in S\text{−Mod}$ the following two morphisms of abelian groups:

$$\begin{array}{rcl} \mathrm{Hom}_R(M, U(N)) & \xrightarrow{\sim} & \mathrm{Hom}_S(S \otimes_R M, N) \\ f & \mapsto & (s \otimes m \mapsto s.f(m)) \end{array}$$

   and

$$\begin{array}{rcl} \mathrm{Hom}_S(S \otimes_R M, N) & \xrightarrow{\sim} & \mathrm{Hom}_R(M, U(N)) \\ g & \mapsto & (m \mapsto g(1_S \otimes m)) \ . \end{array}$$

   It is straightforward to check that they are mutually inverse and satisfy the naturality property from Definition 2.3.1.

2. To find the right adjoint functor $G\colon R-\mathrm{Mod} \to S-\mathrm{Mod}$ for the pullback functor $U : S-\mathrm{Mod} \to R-\mathrm{Mod}$, we define on objects

$$G(M) = \mathrm{Hom}_R(S, M).$$

Here S is considered as a left R-module by pullback along ϕ; $G(M)$ is an S-left module via the right action of S on itself, $(s.\varphi)(s') := \varphi(s' \cdot s)$ for $\varphi \in \mathrm{Hom}_R(S, M)$. The functor G is called coinduction.

To see that G is in fact a right adjoint functor of U, we consider for $M \in R-\mathrm{Mod}$ and $N \in S-\mathrm{Mod}$ the following two morphisms of abelian groups

$$\begin{array}{rcl} \mathrm{Hom}_R(U(N), M) & \tilde{\to} & \mathrm{Hom}_S(N, \mathrm{Hom}_R(S, M)) \\ f & \mapsto & (\ n \mapsto (s \mapsto f(sn))) \end{array}$$

and

$$\begin{array}{rcl} \mathrm{Hom}_S(N, \mathrm{Hom}_R(S, M)) & \tilde{\to} & \mathrm{Hom}_R(U(N), M) \\ g & \mapsto & (n \mapsto g(n)(1_S)) \ . \end{array}$$

Again it is straightforward to check that they are mutually inverse and satisfy the naturality property from Definition 2.3.1.

3. Let R, S be rings and B a $S - R$-bimodule. Then we have a functor

$$\begin{array}{rcl} \tilde{B}\colon R-\mathrm{Mod} & \to & S-\mathrm{Mod} \\ N & \mapsto & B \otimes_R N \end{array}$$

that is left adjoint to the functor

$$\begin{array}{rcl} S-\mathrm{Mod} & \to & R-\mathrm{Mod} \\ Q & \mapsto & \mathrm{Hom}_S(B, Q) \end{array} .$$

Tensor products and Hom-functors are again adjoint.

Sometimes it is useful to have a different formulation of the definition of adjoint functors:

Observation 2.3.4

1. Let $F \dashv G$ be adjoint functors with $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$. From the definition we deduce the existence of isomorphisms

$$\mathrm{Hom}_{\mathcal{C}}(G(d), G(d)) \cong \mathrm{Hom}_{\mathcal{D}}(F(G(d)), d)$$

and

$$\mathrm{Hom}_{\mathcal{D}}(F(c), F(c)) \cong \mathrm{Hom}_{\mathcal{C}}(c, G(F(c))).$$

The image of the identity on $G(d)$ resp. $F(c)$ under these isomorphisms assemble to natural transformations

$$\epsilon\colon F \circ G \to \mathrm{id}_{\mathcal{D}} \quad \text{and} \quad \eta\colon \mathrm{id}_{\mathcal{C}} \to G \circ F \ .$$

(Note the distinct ordering of the functors G and F.) These have the property, that for all objects c in $\mathcal{C}$ and d in $\mathcal{D}$ the morphisms

$$G(d) \xrightarrow{\eta_{G(d)}} (GF)\,G(d) = G(FG)(d) \xrightarrow{G(\epsilon_d)} G(d)$$

and

$$F(c) \xrightarrow{F(\eta_c)} F(GF)(c) = (FG)F(c) \xrightarrow{\epsilon_{F(c)}} F(c)$$

are identity morphisms. These identities are called triangle identities. For a proof of these statements we refer to [McL71, Chapter IV]. We mention that η is called the unit and ϵ the unit of the adjunction.

2. Conversely, the natural transformations ϵ and η determine the adjunction isomorphisms via
$$\mathrm{Hom}_{\mathcal{C}}(c, G(d)) \xrightarrow{F} \mathrm{Hom}_{\mathcal{D}}(F(c), F(G(d)) \xrightarrow{(\epsilon_d)_*} \mathrm{Hom}_{\mathcal{D}}(F(c), d)$$
and the inverse by
$$\mathrm{Hom}_{\mathcal{D}}(F(c), d) \xrightarrow{G} \mathrm{Hom}_{\mathcal{C}}(G(F(c)), G(d)) \xrightarrow{\eta_c^*} \mathrm{Hom}_{\mathcal{C}}(c, G(d)) .$$

3. Consider a pair of adjoint functors $F \dashv G$; it yields an equivalence of categories if and only if ϵ an η are natural *iso*morphisms. This is even an adjoint equivalence.

4. One can show that any equivalence $F : \mathcal{C} \to \mathcal{D}$ with quasi-inverse $G : \mathcal{D} \to \mathcal{C}$ and isomorphisms
$$\eta : \quad \mathrm{id}_{\mathcal{C}} \xrightarrow{\sim} G \circ F \quad \text{and} \quad \epsilon : \quad F \circ G \xrightarrow{\sim} \mathrm{id}_{\mathcal{D}}$$
can be promoted to an adjoint equivalence, in which the natural isomorphisms satisfy the triangle identities, by replacing either one of the originally specified natural isomorphisms by a new unit or counit. For a proof, we refer to [R16, Proposition 4.4.5].

5. Consider the adjunction $I \dashv U$ between the forgetful functor $U : R-\mathrm{Mod} \to \mathrm{Set}$ and the free functor $F : \mathrm{Set} \to R-\mathrm{Mod}$. Then the component of the counit at a set M is a morphism $\eta_M : M \to U(F(M))$ of sets into the set undeflying the free module $F(M)$. It exhibts the elements of M as a basis of $F(M)$. Notice that the morphism η_M is far from being an isomorphism of sets.

We are now ready to prove the following theorem.

Proposition 2.3.5
Any left adjoint functor is cocontinous, i.e. preserves colimits. Any right adjoint functor is continuous, i.e. preserves limits.

Proof. Given an adjunction $F \dashv G$, with $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$, we have a natural isomorphism
$$\Phi : \quad \mathrm{Hom}_{\mathcal{D}}(F-, -) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(-, G-) .$$
Let X be a diagram of shape Γ in $\mathcal{C}$ with universal cocone $(X_\gamma \to C)_{\gamma\in\Gamma}$. Now let $(F(X_\gamma) \to Y)_{\gamma\in\Gamma}$ be any cocone of the diagram $F \circ X$ of shape Γ in $\mathcal{D}$. Since Φ is natural, we obtain a cocone $(X_\gamma \to G(Y))_{\gamma\in\Gamma}$ over the original diagram in $\mathcal{C}$.

The universal property of the universal cocone gives us a unique morphism $C \to G(Y)$ such that $X_\gamma \to C \to G(Y)$ equals $X_\gamma \to G(Y)$ for all $\gamma \in \Gamma$. Via Φ^{-1}, this gives a unique morphism $F(C) \to Y$ such that $F(X_\gamma) \to F(C) \to Y$ equals $F(X_\gamma) \to Y$. Thus $F(X_\gamma) \to F(C)$ is a universal cocone. By Remarks 2.2.18.1, F is cocontinuous □

Note that this proposition allows us to deduce from Example 2.3.3 again that the functor $B \otimes_R -$ is cocontinuous and that the functor $\mathrm{Hom}_R(B, -)$ is continuous

Corollary 2.3.6 Let $F\colon \mathcal{C} \to \mathcal{D}$ be a functor that admits a left adjoint functor G. Then F commutes with products. If $G\colon \mathcal{D} \to \mathcal{C}$ is a functor that admits a right adjoint functor F, then G commutes with coproducts.

Proof. This follows from the fact that products are specific limits. We go through the argument in more detail: For every object d of $\mathcal{D}$, there are distinguished isomorphisms

$$\begin{array}{rcll} \mathrm{Hom}_{\mathcal{D}}(d, F(\prod_i c_i)) & \cong & \mathrm{Hom}_{\mathcal{C}}(G(d), \prod_i c_i) & \text{since } G \dashv F \\ & \cong & \prod_i \mathrm{Hom}_{\mathcal{C}}(G(d), c_i) & \text{univ. prop. of direct product} \\ & \cong & \prod_i \mathrm{Hom}_{\mathcal{D}}(d, F(c_i)) & \text{since } G \dashv F \\ & \cong & \mathrm{Hom}_{\mathcal{D}}(d, \prod_i F(c_i)) & \text{univ. prop. of direct product.} \end{array}$$

It is straightforward to check that these distinguished isomorphisms assemble to a natural transformation from the functor

$$\mathrm{Hom}_{\mathcal{D}}(-, F(\prod_i c_i))\colon \mathcal{D}^{\mathrm{opp}} \to \mathrm{Set}$$

to the functor

$$\mathrm{Hom}_{\mathcal{D}}(-, \prod_i F(c_i))\colon \mathcal{D}^{\mathrm{opp}} \to \mathrm{Set}.$$

Thus we have an isomorphism of the functors $\mathrm{Hom}_{\mathcal{D}}(-, F(\prod_i c_i))$ and $\mathrm{Hom}_{\mathcal{D}}(-, \prod_i F(c_i))$ and thus, by Observation 2.1.18.1 that is based on the Yoneda lemma, that $F(\prod_i c_i) \cong \prod_i F(c_i)$ holds. The proof for coproducts is analogous. □

Here is another consequence of the Yoneda lemma 2.1.17:

Theorem 2.3.7 If a functor $G\colon \mathcal{D} \to \mathcal{C}$ admits a left adjoint functor, then this left adjoint functor is uniquely determined up to natural isomorphism. Analogously, right adjoint functors are determined uniquely up to natural isomorphisms, if they exist.

Proof. Let $F, F'\colon \mathcal{C} \to \mathcal{D}$ be two left adjoints to $G : \mathcal{D} \to \mathcal{C}$. Then for all objects $c \in \mathcal{C}$ and $d \in \mathcal{D}$ there exist distinguished isomorphisms

$$\mathrm{Hom}_{\mathcal{D}}(F(c), d) \cong \mathrm{Hom}_{\mathcal{C}}(c, G(d)) \cong \mathrm{Hom}_{\mathcal{D}}(F'(c), d)\,.$$

These isomorphisms again satisfy the naturality property, and so we obtain a natural isomorphism $y_{F(c)} \to y_{F'(c)}$, which comes from an isomorphism $F'(c) \to F(c)$ by Observation 2.1.18. □

We finally relate the existence of limits and colimits of diagrams of shape Γ to adjoints of the diagonal functor for Γ:

Proposition 2.3.8 A category $\mathcal{C}$ admits all limits of all diagrams indexed by a small category Γ, if and only if the constant diagram functor $\Delta : \mathcal{C} \to [\Gamma, \mathcal{C}]$ admits a right adjoint. Dually, a category admits all colimits of all Γ-shaped diagrams if and only if Δ admits a left adjoint.

Proof. These statements follow directly from the definition of a limit: $\mathrm{Hom}(\Delta(c), F)$ is the set of natural transformations from the constant diagram to the diagram $F : \Gamma \to \mathcal{C}$. This is the set of cones with summit c. The limit $\lim_\Gamma F$ has the property

$$\mathrm{Hom}(\Delta(c), F) \cong \mathrm{Hom}_{\mathcal{C}}(c, \lim_{\Gamma} F)$$

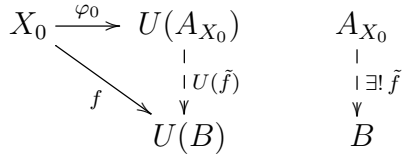
which is natural in c if the limit exists. One then checks that this allows to extend lim to a limit functor. For details, see [R16, Proposition 4.5.1]. □

Next we will discuss universal properties in the language of categories and functors and the connection to adjoint functors. We consider the following situation: we start with a functor $U\colon \mathcal{D} \to \mathcal{C}$. Here the category $\mathcal{D}$ is often the "better" or "more interesting" category, e.g. when U is a forgetful functor. An example would be to take for $\mathcal{D}$ the category of vector spaces and for $\mathcal{C}$ the category of sets. We would now like to "improve" an object $X \in \mathcal{C}$ by creating an object $A_X \in \mathcal{D}$, e.g. to linearize a set X by creating the vector space A_X freely spanned by X. Note that the vector space A_X comes with a distinguished morphism $\varphi\colon X \to U(A_X)$ of sets. The universal property says that for every vector space B, every morphism $f\colon X \to U(B)$ of *sets* can be extended uniquely to an "improved" morphism $\tilde{f} : A_X \to B$ of vector spaces.

Definition 2.3.9 Let $\mathcal{C}, \mathcal{D}$ be categories and $U\colon \mathcal{D} \to \mathcal{C}$ a functor. Let X_0 be an object in $\mathcal{C}$.

1. An initial universal morphism from X_0 to U is a pair (A_{X_0}, φ_0), consisting of an ("improved") object A_{X_0} in $\mathcal{D}$ and a morphism $\varphi_0\colon X_0 \to U(A_{X_0})$ in $\mathcal{C}$ (in the original category), such that the following universal property holds:

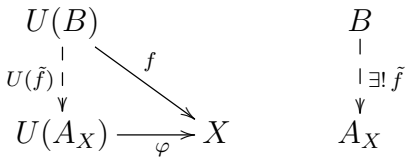
   For every object B of $\mathcal{D}$ and every morphism $f\colon X_0 \to U(B)$ in $\mathcal{C}$ there exists a *unique* ("improved") morphism $\tilde{f}\colon A_{X_0} \to B$ in $\mathcal{D}$, such that the following diagram in $\mathcal{C}$ commutes:



   in $\mathcal{C}$ in $\mathcal{D}$

2. A terminal universal morphism from U to an object X in $\mathcal{C}$ is a pair (A_X, φ), consisting of an object A_X in $\mathcal{D}$ and a morphism $\varphi\colon U(A_X) \to X$ in $\mathcal{C}$, such that the following universal property holds:

   For every object B of $\mathcal{D}$ and every morphism $f\colon U(B) \to X$ in $\mathcal{C}$ there exists a *unique* morphism $\tilde{f}\colon B \to A_X$ in $\mathcal{D}$, such that the following diagram in $\mathcal{C}$ commutes:



   in $\mathcal{C}$ in $\mathcal{D}$

To see the connection to adjoint functors, note that e.g. for an initial universal morphism we have a bijection $\mathrm{Hom}_{\mathcal{C}}(X_0, U(B)) \cong \mathrm{Hom}_{\mathcal{D}}(A_{X_0}, B)$. Conversely, a left adjoint functor for U yields an initial universal morphism for every X_0.

Example 2.3.10
To understand the universal property of the polynomial ring, we consider the forgetful functor

$$U\colon \ K\text{-Alg} \to \mathrm{Set}$$

and initial universal morphisms for the one-element set $\bullet$. This consists of an object in K-Alg, i.e. a K-algebra R, with a morphism of sets $\bullet \to U(R)$, i.e. an element $X \in R$.

The universal property for an initial universal morphism is the requirement, that for every K-algebra S and a morphism of sets $\bullet \to U(S)$, i.e. for every pair of a K-algebra S and an element $a \in S$, there exists a unique morphism $f\colon R \to S$ of K-algebras, such that $\bullet \to U(R) \overset{U(f)}{\to} U(S)$ equals $\bullet \to S$ is, i.e. that $f(X) = a$ holds.

Remarks 2.3.11

1. As usual, universal properties define objects up to unique isomorphism. If one shows that two distinct objects satisfy the same universal property, then they have to be isomorphic.

2. Universal constructions are functorial: let (A_{X_1}, φ_1) be a universal morphism from X_1 to U and (A_{X_2}, φ_2) a universal morphism from X_2 to U. To define a functor $X \mapsto A_X$ also on morphisms, consider a morphism $h\colon X_1 \to X_2$ in $\mathcal{C}$.

   Let $h\colon X_1 \to X_2$ be any morphism in $\mathcal{C}$ Consider the morphism $\varphi_2 \circ h : X_1 \to X_2 \to U(A_{X_2})$ in $\mathcal{C}$. Applying Definition 2.3.9 to this morphism, we find a uniquely determined morphism $\widetilde{\varphi_2 \circ h}\colon A_{X_1} \to A_{X_2}$, such that the following diagram in $\mathcal{C}$ commutes:

$$\begin{array}{ccc} X_1 & \xrightarrow{\varphi_1} & U(A_{X_1}) \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle U(\widetilde{\varphi_2 \circ h})} \\ X_2 & \xrightarrow{\varphi_2} & U(A_{X_2}) \end{array}$$

   If there exists a universal morphism for *every* object X of $\mathcal{C}$, then $X_i \mapsto A_{X_i}$ and $h \mapsto \widetilde{\varphi_2 \circ h}$ defines a functor V from $\mathcal{C}$ to $\mathcal{D}$ and the morphisms φ_i yield a natural transformation from the identity functor to $U \circ V$. As a straightforward consequence we get that the functors are adjoint, namely $V \dashv U$.

   We have already seen that every pair of adjoint functors yields universal morphisms for *all* objects. Conversely, universal constructions assemble into adjoint functors if *every* object in $\mathcal{C}$ admits a universal morphism.

3. This implies the following uniqueness statement which is stronger than the statement in Theorem 2.3.7:

   Adjoint functors are not only unique up to isomorphism, they are unique up to unique isomorphism; that is, if F is left adjoint to G and also to G', then there is a unique isomorphism $G \overset{\cong}{\to} G'$ compatible with the data of the two adjunctions.

2.4 A brief look at quivers

Quivers are a source of examples for algebras whose representation categories can be controlled to a certain extent.

Definition 2.4.1 1. A (finite) quiver is a (finite) directed graph, i.e. a pair (Q_0, Q_1) of (finite) sets, together with a pair of maps $t, h : Q_1 \to Q_0$, called tail and head, indicating the vertex that is a source and a target of an arrow.

2. A representation of a quiver over a field K assigns to each vertex $v \in Q_0$ a vector space V_v and to an arrow $a \in Q_1$ a linear map $V_a : V_{t(a)} \to V_{h(a)}$.

3. A morphism $\phi : V \to W$ of representations of a quiver is a collection of maps $\{\phi_x : V_x \to W_x\}_{x \in Q_0}$ such that all diagrams

$$\begin{array}{ccc} V_{t(a)} & \xrightarrow{V_a} & V_{h(a)} \\ \downarrow{\scriptstyle \phi_{t(a)}} & & \downarrow{\scriptstyle \phi_{h(a)}} \\ W_{t(a)} & \xrightarrow[W_a]{} & W_{h(a)} \end{array}$$

commute for all arrows $a \in Q_1$.

Remarks 2.4.2 1. Representations of quivers form a category. Finite-dimensional representations of quivers form a subcategory; to each object in this subcategory, one can associate a dimension vector $(\dim_K V_v)_{v \in Q_0}$.

2. Consider the category $\mathcal{F}(Q_0, Q_1)$ that is freely generated by the quiver, cf. Examples 2.3.2.6. The category of representations of the quiver is then just the functor category $[\mathcal{F}(Q_0, Q_1), \mathrm{vect}]$.

3. To a quiver, one associates its path algebra $K[Q]$: it is defined on the vector space freely generated by the set of morphisms of $\mathcal{F}(Q_0, Q_1)$, which is the set of paths on the quiver. Multiplication is induced from concatenation of paths, if this is possible, and defined to be zero otherwise. The K-linear representations of the quiver are $K[Q]$ modules.

Quivers unify problems from linear algebra.

Examples 2.4.3 1. Let Γ_1 be the quiver with one vertex and no edge. A representation of this quiver is just a K-vector space. The only indecomposable module up to isomorphism is the one-dimensional vector space which is also simple. The quiver algebra is just the ground field.

2. Let Γ_2 be the quiver with one vertex and one edge from the vertex to itself. A representation is a pair (V, f), consisting of a vector space V and an endomorphism of V. This problem was treated in linear algebra. If K is algebraically closed, indecomposable modules are described by a Jordan block, simple modules by an eigenvalue. There are infinitely many isomorphism classes of simple module. The quiver algebra is the polynomial ring $K[X]$.

3. Let Γ_3 be the quiver with two vertices $1, 2$ and a single edge from 1 to 2. A representation is a triple $V_1 \xrightarrow{f} V_2$. We can find complements such that

$$V_1 = U \oplus \ker f \qquad \text{and} \qquad V_2 = W \oplus \operatorname{Im} f$$

and $f|_U : U \to \operatorname{Im} f$ is bijective. We can thus decompose as a direct sum

$$(V_1 \xrightarrow{f} V_2) \cong (\ker f \xrightarrow{0} 0) \oplus (U \xrightarrow{f|_U} \operatorname{Im} f) \oplus (0 \xrightarrow{0} W)$$

Writing each direct summand as a direct sum involving vector spaces of dimension at most 1, we find three indecomposable modules up to isomorphism:

$$(K \xrightarrow{0} 0)\,, \quad (K \xrightarrow{\mathrm{id}} K) \quad \text{and} \quad (0 \xrightarrow{0} K)\,.$$

Any finite-dimensional representation is a direct sum of these indecomposable representations. Only the indecomposables $(K \xrightarrow{0} 0)$ and $(0 \xrightarrow{0} K)$ are simple. The representation $(0 \to K)$ is a subrepresentation of $(K \xrightarrow{\mathrm{id}} K)$ and $(K \to 0)$ is a quotient:

$$0 \to (0 \to K) \to (K \to K) \to (K \to 0) \to 0$$

so that $(K \to K)$ is not simple.

The quiver algebra consists of upper triangular matrices of the form

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

with $a, b, d \in K$.

4. Let Γ_4 be the quiver with one vertex and two edges joining it. To classify all finite-dimensional representations, one has to classify all pairs of matrices up to simulteneous conjugation. This is a very hard problem.

Remarks 2.4.4

1. The examples shows that the representation categories of quivers can be rather different.

2. The finite quiver Γ_2 contains oriented cycles. In fact, the quiver algebra $K[Q]$ of a finite quiver is infinite-dimensional, if and only if Q contains oriented cycles.

3. For each vertex $v \in Q_0$, we obtain a representation of Q by assigning K to this vertex and the zero vector space to all other vertices. These representations are simple. If Q does not contain oriented cycles, these are, up to isomorphism, all simple representations. For the (simple) proof, we refer to [JS06, Satz J.6]. In the example of Γ_3, we obtain the 2 simples $(K \to 0)$ and $(0 \to K)$. The example of the quiver Γ_2 shows that the statement does not have to hold for quivers with oriented cycles.

4. For each vertex v, the identity id_v in the category $\mathcal{F}(Q_0, Q_1)$ is an idempotent ϵ_i in the quiver algebra. Suppose that the quiver is finite and does not have oriented cycles. Then $1 = \sum_{v \in Q_0} \epsilon_v$ and we have a direct sum decomposition

$$K[Q] \cong \oplus_{v \in Q_0} K[Q]\epsilon_v$$

of the regular module as the direct sum of indecomposable projective modules. We obtain in the example Γ_1 that the one-dimensional vector space K is projective. In the example of Γ_3, we obtain the indecomposable projectives

$$(K \to K) \quad \text{and} \quad (0 \to K)\ .$$

5. Quivers come in three different types:

   - A quiver is said to be *of finite type*, if it has only finitely many indecomposable representations, up to isomorphism. The equivers Γ_1 and Γ_3 are of finite type. A famous theorem of Gabriel states that a quiver is of finite type, if and only if its underlying undirected graph is the finite union of Dynkin graphs of type A,D and E. This is a surprising link to Lie theory which goes even further: the indecomposable representations are in bijection to the positive roots of the corresponding root system.
   - If it has infinitely many indecomposable representations, but they appear in families of dimension at most 1, the quiver is said to be *of tame type*. The quiver Γ_2 is of tame type.
   - Otherwise, it is called wild. The quiver Γ_4 is wild.

3 Additive, abelian and linear categories

3.1 Abelian categories

We start by requiring additional algebraic structure on the morphisms sets of categories. For example, in the category $R-$Mod the morphisms sets were abelian groups. It is then natural to study the class of functors that respect these structures.

Definition 3.1.1

1. A category $\mathcal{C}$ is called additive, if
   (a) All Hom-sets are abelian groups and the composition $\circ$ is bilinear.
   (b) All finite products and coproducts exist in $\mathcal{C}$.
2. Let $\mathcal{C}$ and $\mathcal{D}$ be additive categories. A functor $F\colon \mathcal{C} \to \mathcal{D}$ is called additive, if for every pair X, Y of objects of $\mathcal{C}$ the map $F\colon \mathrm{Hom}_{\mathcal{C}}(X,Y) \to \mathrm{Hom}_{\mathcal{D}}(F(X),F(Y))$ is a group homomorphism.

We know that 1.(b) means that the diagonal functor $\Delta\colon \mathcal{C} \to \prod_{i\in I}\mathcal{C}$ for a finite indexing set I has the coproduct functor $\coprod_{i\in I}$ as left adjoint and the product functor $\prod_{i\in I}$ as right adjoint.

The category $R-$Mod of modules over a ring is additive. Its full subcategory of projective objects is additive as well.

Remark 3.1.2 Note that for an additive category we also require the existence of the empty product and coproduct.

- We already know from Examples 2.2.5 that the empty coproduct $\coprod_{\emptyset}$ is an initial object in $\mathcal{C}$. Dually, the empty product $\prod_{\emptyset}$ is a terminal object $\star \in \mathcal{C}$.
- The initial object $0 \in \mathcal{C}$ has a unique endomorphism, namely the identity id_0. On the other hand, id_0 is the neutral element 0_0 for the abelian group structure on $\mathrm{Hom}_{\mathcal{C}}(0,0)$. Thus we have $\mathrm{id}_0 = 0_0$.

  For an arbitrary morphism $c \xrightarrow{f} 0$ the bilinearity of the composition implies $f = \mathrm{id}_0 \circ f = 0_0 \circ f = 0 \in \mathrm{Hom}_{\mathcal{C}}(c,0)$ for all objects $c \in \mathcal{C}$. Thus there exists only a single morphisms to 0, i.e. $\mathrm{Hom}_{\mathcal{C}}(c,0) = \{0\}$. The initial object 0 in an additive category is thus also terminal, $0 \cong \star$. Categories with isomorphic terminal and initial object are called pointed categories. Additive categories are thus pointed.
- In every pointed category we find for every pair of objects X, Y a morphism $X \xrightarrow{0} 0 \xrightarrow{0} Y \in \mathrm{Hom}(X,Y)$. We leave it as an exercise to check that such a morphism in an additive category gives the neutral element of the abelian group $\mathrm{Hom}(X,Y)$.

Remark 3.1.3 We now consider whether being additive is a property of a category or an additional structure on a category.

- Being pointed is a property of a category.
- In every pointed category there exists a canonical morphism

$$\coprod_{i\in I} X_i \to \prod_{i\in I} X_i$$

from the coproduct to the product. For this we provide a family of morphisms:

$$f_{ij}\colon X_i \to X_j$$

this is $0\colon X_i \to X_j$ for $i \neq j$ and id_{X_i} for $i = j$.

If this morphism has the property of being an isomorphism for every finite family I, then for two morphisms $f, g\colon A \to B$

$$A \xrightarrow{(\mathrm{id}_A, \mathrm{id}_A)} A \prod A \cong A \coprod A \xrightarrow{(f,g)} B$$

defines a structure of an abelian monoid on $\mathrm{Hom}(A, B)$, such that the composition is bilinear. Now it is again a property of an abelian monoid to be a group. The additive structure thus exhibited is actually the only possible one, see e.g. [B94, Proposition 1.2.7].

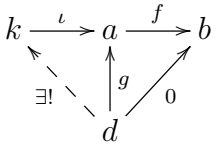
For a given category it is thus a *property* to be an additive category, and this does not require choosing any additional structure.

- Conversely, if the Hom-sets of a category carry the structure of abelian monoids and all finite coproducts (resp. products) exist, then the category is pointed and the coproducts are also products (resp. the products are coproducts).

We next adapt the notions of an equalizer and coequalizer from Definition 2.2.6 to the setting of abelian categories:

Definition 3.1.4

1. Let $f\colon a \to b$ be a morphism in an additive category $\mathcal{C}$. The <u>kernel</u> of f consists of a pair (k, ι), consisting of and object k and a morphism $\iota\colon k \to a$ such that $f \circ \iota = 0$ and such that for every morphism $d \xrightarrow{g} a$ with $f \circ g = 0$ there exists a unique morphism $d \to k$, such that the diagram



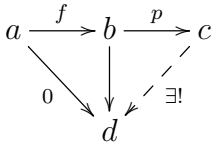
commutes. Equivalently, one requires that for all objects d the following sequence of abelian groups is exact:

$$0 \to \mathrm{Hom}_{\mathcal{C}}(d, k) \xrightarrow{\iota_*} \mathrm{Hom}_{\mathcal{C}}(d, a) \xrightarrow{f_*} \mathrm{Hom}_{\mathcal{C}}(d, b)$$

2. Analogously, the <u>cokernel</u> of f is a pair (c, p) consisting of an object c and a morphism $p\colon b \to c$ such that for all objects d the following sequence of abelian groups is exact:

$$0 \to \mathrm{Hom}_{\mathcal{C}}(c, d) \xrightarrow{p^*} \mathrm{Hom}_{\mathcal{C}}(b, d) \xrightarrow{f^*} \mathrm{Hom}_{\mathcal{C}}(a, d)\ .$$

As diagram:



In a general category, not every morphism has to have a kernel resp. cokernel.

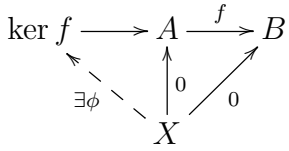
Definition 3.1.5 Let $\mathcal{C}$ be a category.

1. A morphism $\iota\colon a \to b$ is called a monomorphism, if $\iota \circ f = \iota \circ f'$ implies $f = f'$ for all morphism f and f' with target a and equal source. (In an additive category it is sufficient to require this for $f' = 0$.)

2. A morphism $p\colon a \to b$ is called an epimorphism, if $f \circ p = f' \circ p$ implies $f = f'$ for all morphisms f, f' with source b and equal target.

Lemma 3.1.6 Let $\mathcal{C}$ be an additive category. Let $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ be a morphism that has a kernel $K \xrightarrow{\iota} A$. Then the kernel ι is a monomorphism. Dually, if f has a cokernel, then the cokernel is an epimorphism.

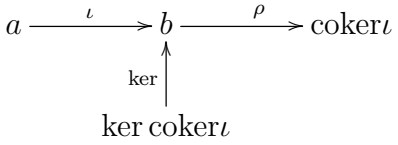
Proof. For an arbitrary object X we consider the zero morphism $X \xrightarrow{0} A$. By the universal property of the kernel there exists a unique morphism ϕ, such that the diagram



commutes. The choice 0 for ϕ also makes the diagram commutes, so we must have $\phi = 0$. Given $X \xrightarrow{g} \ker f$ with $\ker f \circ g = 0$, then we must have $g = 0$, so $\ker f$ is a monomorphism. The argument for the cokernel is dual. □

Definition 3.1.7 Let $\mathcal{C}$ be a category. An additive category is called an abelian category, if every morphism has a kernel and a cokernel, and the following compatibility condition holds:

– For every monomorphism $\iota\colon a \to b$ one has $\iota = \ker(\mathrm{coker}(\iota))$. Explicitly, in the diagram for the monomorphism



the left horizontal arrow and the vertical arrow have the same universal property.

– For every epimorphism $p\colon a \to b$ one has $p = \mathrm{coker}(\ker(p))$.

For a given category it is again a property to be an abelian category, without choice of an additional structure. Before we continue the study of abelian categories, we define

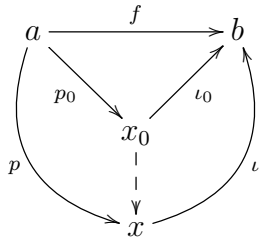
Definition 3.1.8 Let R be a commutative ring (possibly even a field).

1. A R-linear category is a category for which all Hom-sets have been endowed with the structure of an R-module and for which the composition is R-bilinear.

2. A linear functor is an additive functor that consists of R-linear maps on the Hom-spaces.

Examples 3.1.9 The category $R-$Mod of modules over a ring is $\mathbb{Z}$-linear. The category $R-$Mod is also abelian. The full subcategory $\mathrm{Proj}(R)$ of projective R-modules is $\mathbb{Z}$-linear, but not abelian. For example, the morphism $\mathbb{Z} \xrightarrow{2} \mathbb{Z}$ is a monomorphism. It is, however, not the kernel of its cokernel which is zero.

Definition 3.1.10 Suppose, a morphism $f\colon a \to b$ in an arbitrary category $f\colon a \to b$ can be decomposed as $f = \iota \circ p$, where $p\colon a \to x$ is an epimorphism and $\iota\colon x \to b$ a monomorphism. Consider an initial such decomposition $f = \iota_0 \circ p_0$. This means that for any such decompsosition $f = \iota \circ p$, there exists a unique morphism



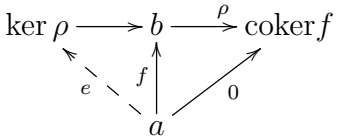
Then $x_0 = \mathrm{Im}\,(f)$ is called an image of f. Since it is defined by a universal property, it is unique up to unique isomorphism.

Remarks 3.1.11

1. As usual for object defined via universal properties, one can show that kernels, cokernels and images are unique up to unique isomorphism, if they exist.

2. In abelian categories every morphism f can be written as $f = \iota \circ p$ with ι a monomorphism and p an epimorphism, and so all images exist.

   To see this, we consider the kernel of the cokernel $\rho : b \to \mathrm{coker} f$ of $a \xrightarrow{f} b$:

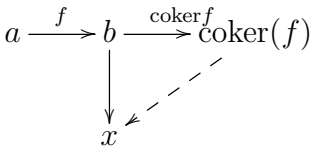
   As $\rho \circ f = 0$, there exists a unique morphism e by the universal property of the kernel.

   One still has to show that e is an epimorphism. This technical proof can be found in [K07, pp. 239] or [McL71, Chapter VIII.3]. There it is also shown that $e = \mathrm{coker}(\ker f)$ and that the factorization (and thus the image) is functorial.

Examples 3.1.12

1. We consider the category Ab_{fr} of finitely generated *free* abelian groups with group homomorphisms as morphisms.

   - Subgroups of finitely generated free abelian groups are, as we will see, again finitely generated and free. Thus the kernels in Ab_{fr} are the kernels in the category Ab of abelian groups.
   - The image of the torsion elements into a free abelian group is always zero. Consider the diagram in the category Ab of abelian groups:

     In our case x is always a free abelian group. Thus the dashed morphism factors through the torsion-free group $\mathrm{coker}(f)/\mathrm{Tor}$. The cokernel of a map $f\colon M' \to M$ in Ab_{fr} is thus given by the free group $\mathrm{coker}(f)/\mathrm{Tor}$, i.e. by the quotient group by the subgroup of all torsion elements.

- The category Ab_{fr} thus has all kernels and cokernels, but the cokernels may be different from the cokernels in Ab. We have to be careful: consider for $0 \neq n \in \mathbb{Z}$ the multiplication map $\iota_n \colon \mathbb{Z} \to \mathbb{Z}$; it has trivial kernel and cokernel in Ab_{fr}. Thus the image of this map in Ab_{fr} is the identity map $\mathbb{Z} \to \mathbb{Z}$. As ι_n is an injective map of the underlying sets, it is also a monomorphism, but $\ker(\mathrm{coker}(\iota_n)) = \mathrm{id}_{\mathbb{Z}} \neq \iota_n$. Thus Ab_{fr} is *not* an abelian category.

2. For every ring R the category of R-modules is abelian, because kernels and cokernels are defined on the level of the underlying abelian groups.

   The converse also holds and is known as the full embedding theorem: every small abelian category can be fully faithfully embedded by an exact funcgtor in the category of modules over a suitable ring, such that exactness properties are preserved, See e.g. [Mi65, p. 151].

3. If $\mathcal{C}$ is an abelian category, then so is the opposite category $\mathcal{C}^{opp}$. The kernels in $\mathcal{C}^{opp}$ are the cokernels in $\mathcal{C}$ and vice versa.

We now have all required notions to make sense of exact sequences in abelian categories, which are defined in complete analogy to Definition 1.4.1. Abelian categories are thus a natural framework for homological algebra.

Definition 3.1.13 Let $F \colon \mathcal{C} \to \mathcal{D}$ be an additive functor between abelian categories. We consider all short exact sequences $0 \to a' \to a \to a'' \to 0$ in $\mathcal{C}$. Now F is called

half exact,	if $F(a') \to F(a) \to F(a'')$ is exact for all short exact sequences in $\mathcal{C}$;
left exact,	if $0 = F(0) \to F(a') \to F(a) \to F(a'')$ is exact for all short exact sequences in $\mathcal{C}$;
right exact,	if $F(a') \to F(a) \to F(a'') \to 0$ is exact for all short exact sequences in $\mathcal{C}$;
exact,	if $0 \to F(a') \to F(a) \to F(a'') \to 0$ is exact for all short exact sequences in $\mathcal{C}$.

Examples 3.1.14

1. The functors $\coprod$ and $\prod \colon \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ are exact whenever they exist, cf. the proof of 1.4.7, step (2)⇒(4). By Remark 3.1.2 product and coproduct then coincide.

2. Let M be an R-right module. The functor $M \otimes_R - \colon R\text{−Mod} \to \mathrm{Ab}$ is right exact by Theorem 1.4.10. It is exact if and only if the module M is flat, cf. Definition 1.4.11.

3. Let M be an R-module. The functor $\mathrm{Hom}_R(M, -) \colon R\text{−Mod} \to \mathrm{Ab}$ is left exact. It is exact if and only if the module M is projective, cf. Theorem 1.4.7.

4. Let M be an R-module. The functor $\mathrm{Hom}_R(-, M) \colon (R\text{−Mod})^{opp} \to \mathrm{Ab}$ is left exact. It is exact if and only if the module M is injective, cf. Theorem 1.4.13.

Let R,S be rings. We have seen in Theorem 1.4.10 that for any S-R-bimodule B the functor

$$\begin{array}{rcl} R\text{-mod} & \to & S\text{-mod} \\ M & \mapsto & B \otimes_{A'} M \end{array}$$

is right exact. We next show that any right exact functor that commutes with direct sums is of this form:

Theorem 3.1.15 [Eilenberg-Watts] Let $F : R\text{−Mod} \to S\text{−Mod}$ be a right exact functor that commutes with direct sums. Then there exists an S-R-bimodule B and a natural isomorphism $F \cong B \otimes_R$ of functors.

Proof. For any $r \in R$, the map

$$\begin{array}{rccc} \rho_r : & R & \to & R \\ & r' & \mapsto & r' \cdot r \end{array}$$

is an R-module endomorphism of the left regular R-module. Therefore $F(\rho_r) : F({}_RR) \to F({}_RR)$ gives for each $r \in R$ a module endomorphisms of $F(R)$ which is by definition a left S-module. We indeed obtain an S-R-bimodule $B := F(R)$ in this way.

Given an R-module M, for each $m \in M$, the R-module morphism

$$\begin{array}{rccc} \phi_m : & R & \to & M \\ & r & \mapsto & r.m \end{array}$$

gives a morphism

$$F\phi_m : \quad B = F(R) \to F(M)$$

of S-modules. The map

$$\begin{array}{rccc} \hat{\psi}_M : & F(R) \times M & \to & F(M) \\ & (b, m) & \mapsto & F(\phi_m)(b) \end{array}$$

is R-balanced. To see this, note that $\phi_m \circ \rho_r$ is the R-module morphism ${}_RR \to M$ mapping

$$r' \mapsto r'r \mapsto r'rm$$

so that we get $\phi_m \circ \rho_r = \phi_{rm}$. Therefore, we have

$$\begin{array}{rcl} \tilde{\psi}_M(br, m) & = & F(\phi_m)(br) = F(\phi_m)F(\rho_r)(b) \\ & = & F(\phi_m \circ \rho_r)(b) = F(\phi_{rm})(b) = \tilde{\psi}_M(b, rm) \end{array}$$

The map $\tilde{\psi}_M$ thus gives rise to a map

$$\psi_M : \quad B \otimes_R M \to F(M)$$

for each $M \in R{-}\mathrm{Mod}$. These maps are natural and for the regular module ${}_RR$

$$\psi_R : \quad B \otimes_R R \to B$$

is the canonical isomorphism. Since the two functors F and $B \otimes_R -$ both commute with direct sums, ψ_F is an isomorphism, if F is a free module.

For an arbitrary R-module M, find an exact sequence

$$0 \to K \to L \to M \to 0$$

where L is a free R-module. We get a diagram with exact rows

$$\begin{array}{ccccccc} B \otimes_R K & \longrightarrow & B \otimes_R L & \longrightarrow & B \otimes_R M & \longrightarrow & 0 \\ \downarrow{\scriptstyle \psi_K} & & \downarrow{\scriptstyle \psi_L} & & \downarrow{\scriptstyle \psi_M} & & \\ F(K) & \longrightarrow & F(L) & \longrightarrow & F(M) & \longrightarrow & 0 \end{array}$$

where ψ_L is an isomorphism. This implies at once that ψ_M is surjective. This applies to any module, hence also to the module K and we learn that ψ_K is surjetive as well. An easy diagram chase in the spirit of the proof of the nine Lemma 1.5.8 now implies that ψ_M is also injective. □

Remark 3.1.16 • There is a corresponding statement for a left exact functor $F : R{-}\mathrm{Mod} \to S{-}\mathrm{Mod}$. Then there exists a R-S-bimodule C and a natural equivalence of functors $\mathrm{Hom}_R(C, -) \cong F$. For details, see [W60].

- Consider the pullback functor $\phi^* : S-\mathrm{Mod} \to R-\mathrm{Mod}$ for a ring homomorphism $\phi : R \to S$ that was studied in Example 2.3.3. It is exact, which can be shown to imply the existence of adjoints. The Eilenberg-Watts theorem then implies immediately that the induction functor can be expressed as a tensor product with a bimodule and the coinduction functor in terms of a Hom functor.

We now come to the more general definitions for abelian categories:

Definition 3.1.17

1. An object U of an abelian category is called projective, if the functor $\mathrm{Hom}(U, -)\colon \mathcal{C} \to \mathrm{Ab}$ is exact.

2. An abelian category $\mathcal{C}$ is called semisimple , if every object U of $\mathcal{C}$ is projective, i.e. if all functors $\mathrm{Hom}(U, -)$ are exact.

3. An object U of an abelian category is called injective, if the functor $\mathrm{Hom}(-, U)\colon \mathcal{C}^{\mathrm{opp}} \to \mathrm{Ab}$ is exact.

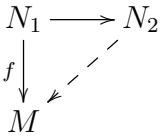
4. If an abelian category $\mathcal{C}$ has a tensor product $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ with similar properties as tensor product of A-bimodules over rings, [1] then an object U is called flat, if the functor $U \otimes -\colon \mathcal{C} \to \mathcal{C}$ is exact.

In this abstract language we will later access the area of homological algebra, which concerns the study of half exact functors. The focus will be on the functors $\otimes$ and Hom. Using the full embedding theorem from Examples 3.1.12.2 it is clear, that statements such as the Nine Lemma 1.5.8 hold in arbitrary abelian categories.

Remark 3.1.18

1. One can define projective and injective objects in arbitrary categories, not just abelian categories. Let $\mathcal{C}$ be an arbitrary category. An object $P \in \mathcal{C}$ is called projective, if for every epimorphism $e\colon M \to N$ and every morphism $f\colon P \to N$ there exists a lift $\tilde{f}\colon P \to M$ with $e \circ \tilde{f} = f$. Injective objects are defined dually.

2. In the category of sets every object M is injective: consider for a subset $N_1 \subset N_2$ and a morphism $f\colon N_1 \to M$ the diagram



   Then the map f can indeed be extended to the superset. In other mathematical contexts the existence of extensions can be a nontrivial problem or just fail!

3. The statement, that every object in the category of sets is projective, is equivalent to the axiom of choice.

   Assuming the axiom of choice, we may choose for a given epimorphism $e\colon M \to N$ a section $s\colon N \to M$, i.e. $e \circ s = \mathrm{id}_N$. For an arbitrary morphism $f\colon P \to N$ we then set $\tilde{f} := s \circ f$. Then we have $e \circ \tilde{f} = e \circ s \circ f = f$, which shows that every object P is projective.

[1] More precisely, it is a monoidal category as defined e.g. in the lecture *Hopf algebras, quantum groups and topological field theory*.

Conversely, if every set is projective, we consider for a given epimorphism $e\colon M \to N$ the morphism $f = \mathrm{id}_N$ and find by the lifting property for the identity a section of e, as diagram:

$$\begin{array}{ccccc} & & N & & \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \\ M & \xrightarrow{e} & N & \longrightarrow & 0 \end{array}$$

3.2 Finite linear categories and categories of finite-dimensional modules

We fix a field K. In this section, we follow [DSPS19]:

Definition 3.2.1 A K-linear abelian category $\mathcal{C}$ is *finite* if

1. $\mathcal{C}$ has finite-dimensional spaces of morphisms;
2. The composition series of every object of $\mathcal{C}$ has finite length;
3. $\mathcal{C}$ has enough projectives, i.e. for every object X, there is a projective object P with an epimorphism $P \twoheadrightarrow X$.
4. There are finitely many isomorphism classes of simple objects.

Example 3.2.2 The category of finite dimensional vector spaces is a finite linear category.

The following proposition justifies the name *finite category*:

Proposition 3.2.3 A K-linear abelian category is finite, if and only if it is equivalent to the category $A-$Mod of finite-dimensional modules over a finite-dimensional K-algebra A.

We will first prove two lemmas.

Lemma 3.2.4 Let $F : \mathcal{C} \leftrightarrows \mathcal{D} : U$ be an adjunction between abelian categories.

1. The right adjoint U is faithful, if and only if the counit $FU(X) \to X$ is an epimorphism for every object $X \in \mathcal{D}$.
2. If U is faithful, then U reflects isomorphisms, i.e. if $U(f)$ is an isomorphism in $\mathcal{C}$, then f is already an isomorphism in $\mathcal{D}$.

Proof. • The functor U is faithful precisely when $U(f) = 0$ implies $f = 0$ for all morphisms $f : X \to Y$ in $\mathcal{D}$. Suppose that the counit $\varepsilon_X : FU(X) \to X$ is a surjection for every object $X \in \mathcal{D}$ and let $f : X \to Y$ be a morphism such that $U(f) : U(X) \to U(Y)$ is the zero morphism. Then the composite $FU(X) \to FU(Y) \to Y$ is the zero morphism as well. Since the counit is natural, this composite is the same as the composite $FU(X) \to X \to Y$,

$$\begin{array}{ccc} FU(X) & \xrightarrow{F(f)} & FU(Y) \\ \downarrow{\scriptstyle \varepsilon_X} & & \downarrow{\scriptstyle \varepsilon_Y} \\ X & \xrightarrow{f} & Y \end{array}$$

hence this composite is also the zero morphism. Now since the counit $\epsilon_X : FU(X) \to X$ is surjective, the original map $f : X \to Y$ must be the zero morphism. Hence the functor U is faithful.

- In the other direction, suppose that U is faithful, and fix an object $X \in \mathcal{D}$. Let $f : X \to C$ be the cokernel of the counit map $\varepsilon_X : FU(X) \to X$. We wish to show that the cokernel is zero. Since the composite $f \circ \varepsilon_X = 0$ by definition of the cokernel, we have $U(f) \circ U(\varepsilon_X) = 0$. However $U(\varepsilon_X) : UFU(X) \to U(X)$ is split (by the unit $\eta_{UX} : UX \to UFUX$ of the adjunction) and hence is surjective, which implies that $U(f) = 0$. Since U is by assumption faithful, we have that $f = 0$ and so the cokernel has to be, in fact, zero as desired.

- For the last statement, notice that a faithful functor $U : \mathcal{D} \to \mathcal{C}$ reflects monomorphisms: let $g : z \to x$ and $h : z \to x$ be morphisms in $\mathcal{D}$ such that $f \circ g = f \circ h$. Since U is a functor, we have

$$U(f) \circ U(g) = U(f \circ g) = U(f \circ h) = U(f) \circ U(h) \ .$$

  Since $U(f)$ is by assumption a monomorphism, we have $U(g) = U(h)$. Since U is faithful, it follows that $g = h$. Hence f is a monomorphism in $\mathcal{D}$. A similar argument shows that U reflects epimorphisms. In an abelian category, a morphism is an isomorphism if and only if it is a monomorphism and an epimorphism.

□

Lemma 3.2.5 Let $F : \mathcal{C} \leftrightarrows \mathcal{D} : U$ be an adjunction between linear categories in which U and F are linear functors, and where U is exact and faithful. Suppose that $\mathcal{C}$ is finite, then $\mathcal{D}$ is also finite.

Proof. • Since U is faithful, the morphism spaces in $\mathcal{D}$ are subspaces of the morphism spaces of $\mathcal{C}$, hence finite dimensional.

- Since U is a right adjoint, it preserves subobjects. Thus U sends a decreasing chain of subobjects to a decreasing chain of subobjects. Since U is exact and faithful, by Lemma 3.2.4 it reflects isomorphisms, and hence U also preserves *strictly* decreasing chains of subobjects. Since every such chain in $\mathcal{C}$ has finite length, the same is true in $\mathcal{D}$.

- Let $X \in \mathcal{D}$ be an object, and let $P \twoheadrightarrow U(X)$ be a surjection in $\mathcal{C}$ from a projective object P. Since F is a left adjoint, it preserves surjections. Since U is faithful, by Lemma 3.2.4, $FU(X) \to X$ is a surjection. Thus the composite

$$F(P) \to FU(X) \to X$$

  is surjective. Moreover, the functor $\mathrm{Hom}_{\mathcal{D}}(F(P), -) \cong \mathrm{Hom}_{\mathcal{C}}(P, U(-)) = \mathrm{Hom}_{\mathcal{C}}(P, -) \circ U$ is exact, and hence $F(P)$ is projective. Thus $\mathcal{D}$ also has enough projectives.

- Now suppose that $X \in \mathcal{D}$ is a non-zero object. We claim that then the object $U(X) \in \mathcal{C}$ is also non-zero. Note that U as a right adjoint preserves the zero object. Hence the unique morphism $f : 0 \to X$ is mapped to the unique morphism $0 \to U(X)$. If $U(X)$ were a zero object, then this morphism and thus $U(f)$ would be an isomorphism. Since U reflects isomorphisms by Lemma 3.2.4.2, the isomorphism $0 \cong U(X)$ in $\mathcal{D}$ would come from an isomorphism $0 \cong X$ in $\mathcal{C}$ and X would be also a zero object.

  Moreover, $U(X)$ has finite length, hence there exists a non-zero morphism $f : S \to U(X)$ where S is some simple object of $\mathcal{C}$. The adjoint of this morphism is the unique morphism $\overline{f} : F(S) \to X$ such that f factors as

$$S \overset{\eta_S}{\to} UF(S) \overset{U(\overline{f})}{\to} U(X) \ .$$

Hence, since f is non-zero, $\overline{f}$ must also be non-zero.

Now let $W = \oplus S_i$ be the direct sum of representatives from each of the finitely many isomorphism classes of simple objects of $\mathcal{C}$. We have shown that for every object $X \in \mathcal{D}$, there exists a non-zero morphism $F(W) \to X$. If X is simple, then a non-zero morphism is necessarily a surjection. In particular, it follows that every simple object of $\mathcal{D}$ occurs as a simple factor in some composition series for the object $F(W) \in \mathcal{D}$. Since $F(W)$ is finite length and by the Jordan-Hölder theorem, any two composition series have the same simple factors up to permutation and isomorphism, and hence there are finitely many isomorphism classes of simple objects in $\mathcal{D}$.

□

Proof of Prop. 3.2.3. • Let A be a finite-dimensional K-algebra and consider the linear category $A-$Mod of finite-dimensional left A-modules. The linear category vect_k is finite and the free-forgetful adjunction $A \otimes (-) : \mathrm{vect}_K \leftrightarrows A-\mathrm{Mod} : U$ satisfies the conditions of Lemma 3.2.5. Hence the linear category $A-$Mod is finite.

- Now assume that $\mathcal{C}$ is a finite linear abelian category. Let $\{X_i\}$ be a set of representatives for the (finitely many) isomorphism classes of simples. Let $P_i \to X_i$ be a surjection, with P_i projective, let $P = \oplus P_i$. This is a finite direct sum, hence $P \in \mathcal{C}$. Let $A = \mathrm{Hom}_{\mathcal{C}}(P, P)$. As the morphism spaces of $\mathcal{C}$ are finite-dimensional, A is a finite-dimensional algebra, where the algebra structure on A is defined by composition, $a \cdot b := b \circ a$. We will see in an exercise that P is a generator, so that by Examples 2.1.14.2 $\mathrm{Hom}_{\mathcal{C}}(P, -)$ is faithful.

- Given a finite-dimensional vector space W and an object $c \in \mathcal{C}$, the functor

$$\begin{array}{ccc} \mathcal{C} & \to & \mathrm{vect}_K \\ c' & \mapsto & \mathrm{Hom}_{\mathcal{C}}(c, c') \otimes W^* \end{array}$$

  is left exact. By Remark 3.1.16, this functor is representable. Thus there exists an object in $\mathcal{C}$ that we denote by $c \otimes W$ such that

$$\mathrm{Hom}_{\mathcal{C}}(c \otimes W, c') \cong \mathrm{Hom}_{\mathcal{C}}(c, c') \otimes W^* \qquad (*) \ .$$

  For morphisms $V \xrightarrow{f} W$ in vect_K, this implies

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(c \otimes W, c') & \xrightarrow{\sim} & \mathrm{Hom}_{\mathcal{C}}(c, c') \otimes W^* \\ {\scriptstyle (\mathrm{id}_c \otimes f)^*}\downarrow & & \downarrow{\scriptstyle \mathrm{id} \otimes f^*} \\ \mathrm{Hom}_{\mathcal{C}}(c \otimes V, c') & \longrightarrow & \mathrm{Hom}_{\mathcal{C}}(c, c') \otimes V^* \end{array}$$

  One checks that since we have finite direct sums $c \otimes W \cong c^{\oplus \dim W}$, we also have

$$\mathrm{Hom}_{\mathcal{C}}(c', c \otimes W) \cong \mathrm{Hom}_{\mathcal{C}}(c', c) \otimes W \qquad (**) \ .$$

- Applying $(*)$ to $c = P$ and $W = \mathrm{Hom}_{\mathcal{C}}(P, P) = A$, we find

$$\mathrm{Hom}_{\mathcal{C}}(P \otimes A, P) \cong \mathrm{Hom}_{\mathcal{C}}(P, P) \otimes \mathrm{Hom}_{\mathcal{C}}(P, P)^* \ .$$

  The right hand side contains a canonical element corresponding to the identity linear endomorphism of the vector space $\mathrm{Hom}_{\mathcal{C}}(P, P)$. We thus get a canonical morphism in $\mathcal{C}$

$$\lambda : P \otimes A \to P \ .$$

We define a functor $P \otimes_A (-) : A\text{−Mod} \to \mathcal{C}$ by

$$P \otimes_A M := \mathrm{coeq}\{P \otimes A \otimes M \rightrightarrows P \otimes M\} \ .$$

Here, the arrows are $\lambda \otimes \mathrm{id}_M$ and $\mathrm{id}_P \otimes \rho_M$.

We claim that we have an adjunction, which we will show is an equivalence:

$$P \otimes_A (-) : A\text{−Mod} \leftrightarrows \mathcal{C} : \mathrm{Hom}_{\mathcal{C}}(P, -).$$

We have to find isomorphisms

$$\mathrm{Hom}_{\mathcal{C}}(P \otimes_A M, c) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_{\mathcal{C}}(P, c))$$

for any $M \in A\text{−Mod}$ and $c \in \mathcal{C}$. Indeed, a morphism $\overline{\varphi} \in \mathrm{Hom}_{\mathcal{C}}(P \otimes_A M, c)$ is described by a morphism in $\varphi \in \mathrm{Hom}_{\mathcal{C}}(P \otimes M, c)$ such that

$$\varphi \circ (\lambda \otimes \mathrm{id}_M) = \varphi \circ (\mathrm{id}_P \otimes \rho_M) \ .$$

We translate this to $\hat{\varphi} \in \mathrm{Hom}_{\mathcal{C}}(P, c) \otimes M^* \cong \mathrm{Hom}_K(M, \mathrm{Hom}_{\mathcal{C}}(P, c))$. Consider the diagram:

$$\begin{array}{ccccc}
\mathrm{Hom}_{\mathcal{C}}(P \otimes M, c) & \xrightarrow{\sim} & \mathrm{Hom}_{\mathcal{C}}(P, c) \otimes M^* & \xrightarrow{\sim} & \mathrm{Hom}_K(M, \mathrm{Hom}_{\mathcal{C}}(P, c)) \\
\downarrow & & \downarrow{\scriptstyle \mathrm{id} \otimes \rho^*} & & \downarrow \\
\mathrm{Hom}_{\mathcal{C}}(P \otimes A \otimes M, c) & \xrightarrow{\sim} & \mathrm{Hom}_{\mathcal{C}}(P, c) \otimes (A \otimes M)^* & \xrightarrow{\sim} & \mathrm{Hom}_K(M \otimes A, \mathrm{Hom}_{\mathcal{C}}(P, c))
\end{array}$$

φ in the top left corner is mapped under the left vertical arrow to $\varphi \circ (\mathrm{id}_P \otimes \rho_M)$. On the right vertical arrow, $\hat{\varphi}$ is mapped to $\hat{\varphi} \circ \rho_M$. Noticing that $A = \mathrm{Hom}_{\mathcal{C}}(P, P)$ we now consider λ^* at the left vertical arrow which gives the same element in the bottom left corner. The middle vertical arrow is now precomposition by the composition $\mathrm{Hom}_{\mathcal{C}}(P, c) \otimes A \cong \mathrm{Hom}_{\mathcal{C}}(P, c) \otimes \mathrm{Hom}_{\mathcal{C}}(P, P) \to \mathrm{Hom}_{\mathcal{C}}(P, c)$. The identity of the two right vertical arrows then shows that $\hat{\varphi}$ is a morphism of A-modulkes.

- In order to show that this adjunction is an equivalence, we need only show that the unit and counit maps are isomorphisms. Because P projective, the functor $\mathrm{Hom}_{\mathcal{C}}(P, -)$ is exact and preserves coequalizers. Thus

$$\begin{array}{rcl}
\mathrm{Hom}_{\mathcal{C}}(P, P \otimes_A M) & = & \mathrm{coeq}\,(\mathrm{Hom}_{\mathcal{C}}(P, P \otimes A \otimes M) \rightrightarrows \mathrm{Hom}_{\mathcal{C}}(P, P \otimes M)) \\
& = & \mathrm{coeq}\,(\mathrm{Hom}_{\mathcal{C}}(P, P) \otimes A \otimes M \rightrightarrows \mathrm{Hom}_{\mathcal{C}}(P, P) \otimes M) \\
& = & A \otimes_A M \cong M
\end{array}$$

  The composition of the unit map $M \to \mathrm{Hom}_{\mathcal{C}}(P, P \otimes_A M)$ of the adjunction with this isomorphism is the identity, hence the unit map is an isomorphism.

- It only remains to show that the counit

$$ev : P \otimes_A \mathrm{Hom}_{\mathcal{C}}(P, c) \to c$$

  of the adjunction is an isomorphism for every $c \in \mathcal{C}$. The counit becomes an isomorphism after applying $\mathrm{Hom}_{\mathcal{C}}(P, -)$, and so the desired result follows, if we show that the functor $\mathrm{Hom}_{\mathcal{C}}(P, -)$ reflects isomorphisms. This would follow immediately from Lemma 3.2.4.2, if we had already proven that P is a generator, since then $\mathrm{Hom}_{\mathcal{C}}(P, -)$ is faithful.

As P is projective, the functor $\mathrm{Hom}_{\mathcal{C}}(P,-)$ is exact. Hence, the fact that it reflects isomorphisms is equivalent to that statement that for all $c \in \mathcal{C}$,

$$\mathrm{Hom}_{\mathcal{C}}(P,c) \cong 0 \quad \text{ if and only if } \quad c \cong 0\ .$$

By construction this holds for all objects c of length at most 1, i.e. for all simple objects. We prove that it holds for all objects by induction on the length. Suppose that c is an object of $\mathcal{C}$ and, by induction, that for all objects c' with length strictly less than the length of c, we know $\mathrm{Hom}_{\mathcal{C}}(P,c') \cong 0$ if and only if $c' \cong 0$. By assumption there exists an exact sequence in $\mathcal{C}$

$$0 \to c' \to c \to c'' \to 0$$

with c'' simple, and with the length of c' strictly less than the length of c. We obtain an exact sequence:

$$0 \to \mathrm{Hom}_{\mathcal{C}}(P,c') \to \mathrm{Hom}_{\mathcal{C}}(P,c) \to \mathrm{Hom}_{\mathcal{C}}(P,c'') \to 0.$$

If the middle term is zero, then all terms vanish. By the induction hypothesis, we conclude that $c'' \cong c' \cong 0$, and hence c itself was zero. Thus $\mathrm{Hom}_{\mathcal{C}}(P,-)$ reflects isomorphisms, as required.

□

3.3 Free and cofree modules

We now have the tools available that will allow to give a characterization of injective modules that is dual to the characterization of projective modules as direct summands of free modules.

For this we need the following lemma:

Lemma 3.3.1 Let $(M_i)_{i\in I}$ be a family of objects of an abelian category $\mathcal{C}$.

1. The coproduct $\coprod_{i\in I} M_i$ of the family is projective if and only if every summand M_i is projective.
2. The product $\prod_{i\in I} M_i$ of the family is injective if and only if every factor M_i is injective.

Proof. We only show the second statement about injective objects. The first statement uses the universal property of the direct sum instead.

We show that the functor $\mathrm{Hom}(-, \prod_{i\in I} M_i)$ is exact, if and only if all M_i are injective. For this we apply the functor to an arbitrary short exact sequence

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

and obtain, by the universal property of the product, the sequence of abelian groups:

$$0 \to \prod_{i\in I} \mathrm{Hom}_R(C,M_i) \to \prod_{i\in I} \mathrm{Hom}_R(B,M_i) \to \prod_{i\in I} \mathrm{Hom}_R(A,M_i) \to 0$$

This apparently is exact if and only if the individual sequences

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

for all i are exact, i.e. when all objects M_i are injective. □

Definition 3.3.2 Let R be a ring.

1. An R-module $\tilde{R}$ is called regular if it is projective and for every R-module M there exists an exact sequence
$$\oplus_{i\in I}\tilde{R} \to M \ \to 0$$
for a suitable family I. Every module of the form $\oplus_{i\in I}\tilde{R}$ is called a free module relative to $\tilde{R}$.

2. An R-module R^* is called coregular, if it is injective and for every R-module M there exists an exact sequence
$$0 \to M \to \prod_{i\in I} R^*$$
for a suitable family I. Every module of the form $\prod_{i\in I} R^*$ is called a cofree module relative to R^*.

By Lemma 3.3.1.2 free modules are projective and cofree modules are injective.

Examples 3.3.3

1. R itself is regular, and so are direct sums of copies of R.

2. The abelian group $R^* := \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$ is an R-module via the right action of R on itself, cf. Theorem 1.2.9.2.

   - Consider a divisible abelian group D and the coinduced R-module $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ (coinduced with respect to the unique morphism $\mathbb{Z} \to R$). We claim that $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ is injective. Theorem 1.2.9.3 implies the isomorphism of functors: $R-\mathrm{Mod} \to \mathrm{Ab}$
   $$\mathrm{Hom}_R(-, \mathrm{Hom}_{\mathbb{Z}}(R, D)) \cong \mathrm{Hom}_{\mathbb{Z}}(R \otimes_R -, D) \cong \mathrm{Hom}_{\mathbb{Z}}(-, D)\,.$$
   Note that in the last functor one has to apply the forgetful functor from R-modules to abelian groups in the first argument which is exact. We can summarize our finding in the statement that the coinduction functor is right adjoint to the forgetful functor $R-\mathrm{Mod} \to \mathrm{Ab}$.
   As D is divisible, it is injective in the category of $\mathbb{Z}$-modules by Corollary 1.4.16. Thus the functor on the right-hand side is exact, and so is the functor on the left, but this implies that the R-module $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ is injective.
   - Second, we argue that every R-module M can be mapped injectively into a product of copies of the module R^*. To this end we use again that coinduction is right adjoint to the forgetful functor, so we have an isomorphism of abelian groups:
   $$(*) \qquad \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})) \cong \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$$
   The abelian group $\mathbb{Q}/\mathbb{Z}$ has torsion elements of arbitrary order, and so every every (non-trivial) abelian group M admits a nonzero group homomorphism to $\mathbb{Q}/\mathbb{Z}$.
   The adjunctions isomorphism $(*)$ implies that every nonzero R-module M admits a nonzero morphism of R-modules $M \to \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z}) \equiv R^*$.
   - Next we construct a morphism of R-modules $M \to R^*$ that takes a nonzero value on a given element $0 \neq m \in M$. Let $\langle m\rangle$ denote the submodule generated by m. By the previous argument, there exists a nonzero morphism $\alpha_m \colon \langle m\rangle \to R^*$. Since the module R^* is injective, there exists an extension β_m to M, such that the diagram
   $$\begin{array}{ccccc} 0 & \longrightarrow & \langle m\rangle & \longrightarrow & M \\ & & {\scriptstyle\alpha_m}\downarrow & \swarrow_{\beta_m} & \\ & & R^* & & \end{array}$$

commutes. Then we have $\beta_m(m) = \alpha_m(m) \neq 0$.

- In the final step we use the universal property of the product to collect all homomorphisms β_m into a single one:

$$\beta \colon M \to \prod_{m \in M \setminus \{0\}} R^* \ .$$

For every $m \neq 0$ we have $\beta(m) \neq 0$ because the morphism β_m in the m-th component takes a nonzero value on m. Thus β is injective and hence a monomorphism.

Theorem 3.3.4

1. Let $\tilde{R}$ be regular. Then an R-module M is projective if and only if it is a direct summand in a direct sum $\oplus_{i \in I} \tilde{R}$.

2. Let R^* be coregular. Then M is injective if and only if it is a direct factor in a product $\prod_{i \in I} R^*$.

Proof. We only prove the second statement, the first statement is dual (and known in the special case $\tilde{R} = R$ as one of the characterizations of a projective object in Theorem 1.4.7). If M is injective, then the exact sequence $0 \to M \to \prod_{i \in I} R^*$ splits, and so M is a direct factor of the product. Conversely, $\prod_{i \in I} R^*$ is a product of injective modules and thus injective by Lemma 3.3.1. If $M \times M' \cong \prod_{i \in I} R^*$, then by the same lemma the injectivity of the right-hand side implies the injectivity of M. □

We now invite the reader to complete Theorem 1.4.13 by adding the characterizations of injective modules that we have just obtained.

4 Representation theory

In this section, we invstige the representation categories of concrete algebraic structures: principal ideal domains and group algebras.

Our goal in the first two subsections is to give a complete description of finitely generated modules over principal ideal domains (PIDs). PIDs are arguably the next simple class of rings beyond fields. (Recall that PIDs are always commutative and have no zero divisors. Moreover, any element in a PID can be decomposed uniquely into prime elements.) Examples are the ring $\mathbb{Z}$ of integers and the polynomial ring $K[X]$ over a field.

4.1 Submodules and morphisms of modules over principal ideal domains

Theorem 4.1.1 Let M be a free module over a PID R. Then also every submodule U of M is free. If M has finite rank, then $\mathrm{rank}(U) \leq \mathrm{rank}(M)$.

The example $n\mathbb{Z} \subsetneq \mathbb{Z}$ of $\mathbb{Z}$-modules shows that also *proper* submodules may have equal rank.

Proof. We give the proof only in the case when M has finite rank, namely by induction in $\mathrm{rank}M =: n$. In the general case one uses Zorn's lemma.

- For $n = 0$ we have $M = 0$ and there is nothing to show.
- For $n = 1$ we consider a (nonzero) submodule $I \subset_R R$, i.e, an ideal of R. This is a principal ideal, $I = (a)$, and thus is generated by a single element. Since R has no zero divisors, the family (a) is free and thus a basis of I when $a \neq 0$. So, every nonzero submodule of R is free of rank 1.
- Let $\{x_1, \ldots, x_n\}$ be a basis of M. Then the family $(x_1, \ldots, x_{n-1})$ is free and the submodule $M' = \langle x_1, \ldots, x_{n-1}\rangle$ of M generated by it is free of rank $n-1$. The linear form

$$\begin{array}{rccc} f: & M & \to & R \\ & \sum_{i=1}^n \lambda_i x_i & \mapsto & \lambda_n \end{array}$$

  gives an exact sequence

$$0 \to M' \to M \xrightarrow{f} R \to 0 \ .$$

  For every submodule $U \subset M$ we then get a short exact sequence

$$0 \to M' \cap U \to U \to f(U) \to 0 \ .$$

  The submodule $f(U) \subset R$ is free of rank 1 by the induction start, and so Theorem 1.3.6 implies that the sequence splits:

$$U \cong (M' \cap U) \oplus f(U) \ .$$

  The submodule $M' \cap U$ of M' is free by induction hypothesis and of rank $\leq n-1$. □

Corollary 4.1.2 Every projective module over a PID is free.

Proof. Every projective module is a direct summand of a free module and thus, in particular, a submodule of a free module. For PIDs, these are again free by Theorem 4.1.1. □

Observation 4.1.3

- Let M be a finitely generated module over a PID R. As for every finitely generated module over an arbitrary ring we can find a surjection

$$p\colon R^m \twoheadrightarrow M$$

for a suitable $m \in \mathbb{N}$. Since R is a PID, the ideal $\ker p$ is finitely generated and free by Theorem 4.1.1, i.e. $\ker p \cong R^n$. Consider the map $\ker p\colon R^n \to R^m$ of free modules. We find an isomorphism

$$M \cong R^m / \ker p \cong \operatorname{coker} \ker p \ .$$

Thus we can understand the finitely generated module M via the morphism $\ker p$ between two finitely generated *free* modules. This will allow us to described morphisms in terms of matrices.

- Note that it is essential that we can work with free modules rather than projective modules. There are significantly more rings with the property that every submodule of a projective module is projective. Such rings are called hereditary. A finitely generated module over a hereditary ring is always the cokernel of a morphism of finitely generated projective modules. Such morphisms are typically not as easy to describe as morphisms between free modules.

Next we study morphisms of free modules, and generalize some well-known results from linear algebra along the way.

Let R be a unital ring. As for fields we also have for rings bijections between Hom-spaces of free modules and matrices with entries in R, cf. Remark 1.3.2.6:

$$M\colon \quad \operatorname{Hom}_R(R^n, R^m) \to M(m \times n, R) \ .$$

The columns of the matrix $M(f) = (a_{ij})$ are the images under f of the vectors $e_1, \ldots, e_n$ of the standard basis of the module R^n. In formulas:

$$f(e_j) \ = \ \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix} \ .$$

For an arbitrary ring R we consider the matrices with entries in R as an abelian group with respect to matrix addition. Then M is an isomorphism of abelian groups. Matrix multiplication corresponds to the composition of maps and is a ring isomorphism. An R-module homomorphism φ is an isomorphism if and only if the matrix $M(\varphi)$ is invertible.

If the ring R is commutative, then we equip the matrices with the structure of an R-module by multiplying all entries by an element from R. Then M is an isomorphism of (free) R-modules.

Definition 4.1.4 If the ring R is *commutative*, then for square matrices $A = (a_{ij}) \in M(n \times n, R)$ with $n \neq 0$ we define the determinant by setting

$$\det A = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{1\sigma(1)} \ldots a_{n\sigma(n)} \ .$$

One can also consider the same formula for matrices with entries in a non-commutative ring. But then the formula $\det A \cdot \det B = \det AB$ fails to hold and the notion is less useful.

Theorem 4.1.5 Let R be a commutative ring.

1. For any two square matrices $A, B \in M(n \times n, R)$ we have
$$\det A \cdot \det B = \det AB$$
2. A square matrix A is invertible in $M(n \times n, R)$ if and only if its determinant is invertible in R, i.e. $\det A \in R^\times$.

Proof. 1. The proof of the multiplicativity of the determinant for matrices with entries in a field is familiar from linear algebra. Now we may consider the integral domain
$$\mathbb{Z}[X_{ij}, Y_{ij}]_{1 \le i,j \le n}$$
as a subring of its fraction field, and thus the determinant with entries in a domain is multiplicative. Into this abstract identity we can substitute elements of an arbitrary commutative ring for X_{ij} and Y_{ij}, and the claim follows.

2. If A is invertible, then by multiplicativity $\det A \cdot \det A^{-1} = 1$, so the determinant is invertible in R. Conversely, consider the adjoint matrix with entries
$$A^{\#}_{ij} := (-1)^{i+j} \det A^{ji}$$
where A^{ji} denotes the $(n-1) \times (n-1)$-matrix, obtained from A by deleting the jth row and the ith column. For matrices with entries in a field on shows in linear algebra that
$$A^{\#} A = (\det A) I \,.$$
As in the first part of the proof, this argument extends to arbitrary commutative rings R. □

We can now generalize the following theorem from linear algebra to finitely generated *free* modules over principal ideal domains:

Theorem 4.1.6 [Smith normal form] Let R be a PID and $f\colon M \to N$ a homomorphism between two *free* R-modules of finite rank m resp. n.

1. There exists a diagonal matrix $D \in M(n \times m, R)$ whose entries satisfy the divisibility conditions
$$d_{11} \,|\, d_{22} \,|\, d_{33} \ldots \,|\, d_{rr} \ ,$$
where $r = \min(n, m)$, and isomorphisms $M \cong R^m$, $N \cong R^n$, such that the following diagram commutes
$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \wr & & \wr \\ R^m & \xrightarrow{D} & R^n \end{array}$$
2. The diagonal entries d_{ii} are unique up to multiplication by invertible elements of R, and are called elementary divisors.

Proof.

- We may assume $M = R^m$ and $N = R^n$, such that f is represented by a matrix $A \in M(n \times m, R)$. We are looking for invertible square matrices
$$X \in M(n \times n, R)\,, \quad Y \in M(m \times m, R) \ ,$$
such that the product XAY has the desired diagonal form with divisibility properties.

- For a matrix A we let $\langle A\rangle \subset R$ denote the ideal generated by the entries of A. For every matrix X, the equation
$$(XA)_{ij} = \sum_k x_{ik}a_{kj}$$
implies the inclusion
$$\langle XA\rangle \subseteq \langle A\rangle$$
of ideals. If X is invertible, then one also gets the reverse inclusion and hence
$$\langle XA\rangle = \langle A\rangle\,.$$

- In the main part of the proof, we will describe a procedure to find invertible matrices $\tilde{X}$ and $\tilde{Y}$, such that
$$\langle(\tilde{X}A\tilde{Y})_{11}\rangle = \langle A\rangle\,,$$
i.e. such that the upper left entry of the modified matrix generates the entire ideal $\langle A\rangle$. This will be done in steps. If $\langle a_{11}\rangle = \langle A\rangle$ then the invertible matrices can be chosen to be identity matrices and we are done. On the other hand, if $\langle a_{11}\rangle \subsetneqq \langle A\rangle$, then we will describe a subroutine to find invertible matrices X and Y, such that the smaller ideal gets enlarged: $\langle(XAY)_{11}\rangle \supsetneqq \langle a_{11}\rangle$. Using this subroutine, we enlarge the principal ideal generated by the upper left entry. In every PID there exist only finite many distinct ideals $\mathfrak{a}$ between two given ideals, $\mathfrak{a}_0 \subseteq \mathfrak{a} \subseteq \mathfrak{a}_1$ (this is a consequence of the uniqueness of the prime decomposition). Thus our subroutine reaches after finitely many steps the ideal $\langle A\rangle$, and thus we get the invertible matrices $\tilde{X}$ and $\tilde{Y}$ as desired.

  Now one can perform row and column operations to eliminate all but the first entry in the first row and the first column, without changing the upper left entry: here we use that a_{11} divides all entries, which allows us to subtract suitable multiples of the first row resp. column from every other row resp. column. This corresponds to finding invertible matrices $\hat{X}$ and $\hat{Y}$ such that $\hat{X}\ A\ \hat{Y}$ has only zeros in the first column and row, except the one entry in the upper left, now called d_{11}. Here we also record $\langle d_{11}\rangle = \langle A\rangle$, i.e. d_{11} divides all other entries.

  By induction one now proceeds on the submatrices obtained by omitting the first row and column.

- We still have to describe the subroutine to enlarge the principal ideal generated by the upper left entry. To this end we distinguish three cases:

  (a) a_{11} does not divide all elements in the first row, without loss of generality it does not divide a_{12}. Then we write the ideal $\langle a_{11}, a_{12}\rangle$ in the PID R as principal ideal:
  $$\langle a_{11}, a_{12}\rangle = \langle d\rangle \quad \text{with} \quad d \neq 0\,.$$
  Thus we can find $x, y, \lambda, \mu \in R$ such that:
  $$\begin{aligned} d &= xa_{11} + ya_{12} \\ a_{11} &= d\lambda \\ a_{12} &= d\mu\,. \end{aligned}$$
  As PIDs have, by definition, no zero divisors, this implies $1 = x\lambda + y\mu$. We now consider the product of the following two matrices:
  $$\left(\begin{array}{cc|c} a_{11} & a_{12} & \\ & & * \\ * & * & \\ \hline & * & * \end{array}\right) \quad \left(\begin{array}{cc|c} x & -\mu & \\ & & 0 \\ y & \lambda & \\ \hline & 0 & I \end{array}\right) = \left(\begin{array}{cc|c} d & * & \\ & & * \\ * & * & \\ \hline & * & * \end{array}\right)$$

The second matrix Y on the left-hand side has determinant one and is thus invertible by Theorem 4.1.5. Since $\langle d \rangle$ contains the ideal $\langle a_{11} \rangle$ properly, we have found a pair of matrices $X = I$ and Y as desired.

(b) An analogous argument works if a_{11} does not divide all elements in the first column.

(c) If a_{11} divides all elements the first row and column, then we can eliminate all these elements by elementary row and column operations. But since $\langle a_{11} \rangle \neq \langle A \rangle$, the entry a_{11} cannot be divisor of all entries of A. To proceed, we add a suitable row to the first row and thus put ourselves into case (a) and continue from there.

- We still have to prove the uniqueness of the resulting diagonal matrix. Let $J_i(A)$ for $i \geq 1$ be the ideal in R that is generated by the determinants of $i \times i$-submatrices of A. Again we have

$$J_i(XA) \subseteq J_i(A)$$

for every matrix X, thus also equality of ideals for an invertible matrix X. We deduce

$$J_i(A) = \langle d_{11} d_{22} \cdots d_{ii} \rangle$$

and thus the uniqueness of the diagonal elements d_{ii} up to multiplication by units of R. □

4.2 Classification of modules over principal ideal domains

We will now see a simple, explicit description of finitely generated modules over a PID. We start with an existence result:

Lemma 4.2.1 Let M be a finitely generated module over a PID R. Then there exists an ascending chain $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_r \subsetneq R$ of ideals of R, such that

$$M \cong R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_r \,.$$

Here we allow $\mathfrak{a}_i = 0$ and have $R/0 \cong R$ as R-module.

Proof. We had already seen in Observation 4.1.3 that there exists a morphism $f\colon R^n \to R^m$ of finitely generated free modules, such that M is isomorphic to the cokernel of f.

Theorem 4.1.6 on the Smith normal form lets us find invertible maps X, Y, such that the diagram

$$\begin{array}{ccc} R^n & \xrightarrow{f} & R^m \\ {\scriptstyle X}\uparrow & & \downarrow{\scriptstyle Y} \\ R^n & \xrightarrow{D} & R^m \end{array}$$

commutes and D is a diagonal matrix, whose elements satisfy the divisibility conditions $d_{11} | d_{22} | \ldots | d_{rr}$ with $r = \min(m, n)$. We thus have an isomorphism of R-modules:

$$M \cong R^m/\mathrm{Im}\ \ D \cong R/d_{11}R \times \cdots \times R/d_{rr}R \times R^{m-r}$$

The factors with $d_{ii} \in R^\times$ with units may be omitted. This implies the existence of the stated decomposition. □

The following theorem summarizes our considerations and notes that the description is unique. We give two equivalent versions.

Theorem 4.2.2 Let M be a finitely generated module over a PID R.

1. Then there exists exactly one ascending chain $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_r$ of ideals in R, such that
$$M \cong R/\mathfrak{a}_1 \times R/\mathfrak{a}_2 \times \cdots \times R/\mathfrak{a}_r \ .$$
2. Then there exist prime powers $q_1, \ldots, q_t$ in R such that
$$M \cong R^s \times R/q_1R \times \cdots \times R/q_tR\,. \qquad (*)$$
Here $s \in \mathbb{N}_0$ is uniquely determined, i.e. it does not depend on the choice of decomposition (*), and the prime powers q_i are determined up to units and ordering.

Proof. • The existence of a decomposition as in 1. has already been established in Lemma 4.2.1. The existence statement in 2, follows from the other one by choosing for $\mathfrak{a}_i \neq 0$ a generator α_i, $\mathfrak{a}_i = (\alpha_i)$, and writing them as products of pairwise relatively prime prime powers:
$$\alpha_i = \prod_j q_j^{(i)} \ .$$
Then we use the Chinese remainder theorem for each i and find
$$R/\mathfrak{a}_i \cong R/(q_1^{(i)}) \times R/(q_2^{(i)}) \times \cdots \times R/(q_s^{(i)})\,.$$

- Conversely we can deduce the uniqueness statement in 1. from the uniqueness statement in 2. by again using the Chinese remainder theorem. It thus remains to show the uniqueness statement in 2. The key idea is to deduce the uniqueness statement from the uniqueness of the dimension of vector spaces, over various fields related to the PID R.

- We start with the uniqueness of the rank of the free part. Let $Q := \mathrm{Quot}(R)$ the fraction field of R. Then $\mathrm{Hom}_R(M, Q)$ is a Q-vector space. By the universal property 1.2.2.1 of the direct sum we have
$$\mathrm{Hom}_R(M, Q) \cong \mathrm{Hom}_R(R/q_1R, Q) \times \cdots \times \mathrm{Hom}_R(R/q_tR, Q) \times \mathrm{Hom}_R(R, Q)^s\,.$$
By Examples 1.1.9 (4) we have $\mathrm{Hom}_R(R, Q) \cong Q$. Let $\mathfrak{a}$ be a nonzero ideal of R. Then by the universal property of the quotient module
$$\mathrm{Hom}_R(R/\mathfrak{a}, Q) \cong \{f \in \mathrm{Hom}_R(R, Q) \mid f|_{\mathfrak{a}} = 0\} \ .$$
Every nonzero module homomorphism $f\colon R \to Q$ is injective: let $f(1) \neq 0$. Then for all $m \neq 0$ in the ring R we have $f(m) = mf(1)$ and thus $f(m) \neq 0$ since there are no zero divisors in the fraction field Q. Thus the right-hand side contains only the zero morphism, i.e. for $\mathfrak{a} \neq 0$ we have
$$\mathrm{Hom}_R(R/\mathfrak{a}, Q) = 0\,.$$
This implies
$$s = \dim_Q \mathrm{Hom}_R(M, Q)\,,$$
and so the rank s of the free part does not depend on the decomposition (*) in 2.

- We use a similar strategy to verify the independence of the prime powers. For this we consider for every fixed irreducible $p \in R$ the residue field R/pR.

  Let M be an R-module. For every $n \geq 1$ the quotient $p^{n-1}M/p^nM$ is a (R/pR)-vector space. Define
  $$d_p^n(M) := \dim_{R/pR}(p^{n-1}M/p^nM)\,.$$
  Then we have
  $$d_p^n(M \oplus N) = d_p^n(M) + d_p^n(N)\,.$$

  We compute $d_p^n(M)$ in three different cases:

  1. We first compute $d_p^n(R)$.
     The multiplication with p^{n-1} yields a surjection to $p^{n-1}R$ that we compose with a canonical surjection:
     $$R \overset{\cdot p^{n-1}}{\twoheadrightarrow} p^{n-1}R \twoheadrightarrow p^{n-1}R/p^nR\,.$$
     Thus we get an isomorphism of R/pR-vector spaces
     $$R/pR \xrightarrow{\sim} p^{n-1}R/p^nR\,.$$
     From this we deduce for all $n \in \mathbb{N}$ that for R as left module over itself one has
     $$d_p^n(R) = \dim_{R/pR}(p^{n-1}R/p^nR) = 1\,.$$

  2. Next we consider modules of the form R/p^mR.
     For $n > m$ we have $p^{n-1}(R/p^mR) = 0$. For $n \leq m$ we find a surjection
     $$\begin{aligned} R \twoheadrightarrow R/p^mR \overset{\cdot p^{n-1}}{\twoheadrightarrow} \quad & p^{n-1}(R/p^mR) \twoheadrightarrow \\ & p^{n-1}(R/p^mR)/p^n(R/p^mR) \end{aligned}$$
     with kernel pR. Thus we have
     $$d_p^n(R/p^mR) = \begin{cases} 0 & \text{for} \quad n > m \\ 1 & \text{for} \quad n \leq m\,. \end{cases}$$

  3. Finally, we consider modules of the form $R/\tilde{p}^mR$, where $\tilde{p}$ is prime and not a unit multiple of p.
     Then the class of p in the quotient ring
     $$\tilde{R} := R/\tilde{p}^mR$$
     is invertible. Thus multiplication with p^n is an isomorphism on $\tilde{R}$ and
     $$d_p^n(R/\tilde{p}^mR) = \dim_{R/pR}(\tilde{R}/\tilde{R}) = 0\,.$$

  From these three computations we get
  $$d_p^n(M) = s + |\{i \,|\, p^n \quad \text{divides} \quad q_i\}|\,,$$
  and so the uniqueness of the q_i up to unit multiples and ordering follows form the uniqueness of the dimensions $d_p^n(M)$.

  □

Corollary 4.2.3

1. Every finitely generated module M over a PID R is isomorphic to the direct sum of its torsion submodule and a free module,

$$M \cong \text{Tor } (M) \oplus R^s \, .$$

2. A finitely generated torsion-free module over a PID is free. (Conversely, the free modules for every domain are torsion-free.)

Note that the decomposition into a direct sum is *not* canonical: the torsion elements form a well-defined submodule, but the free part is not uniquely determined as submodule. For example, in the $\mathbb{Z}$-module $\mathbb{Z} \times \mathbb{Z}_2$ both $(\pm 1, 0)$ and $(\pm 1, 1)$ generate a free subgroup of rank 1.

We now consider this structural result in two important special cases: for abelian groups, i.e. $\mathbb{Z}$-modules, and for K-vector spaces with endomorphisms, i.e. $K[X]$-modules.

Corollary 4.2.4 Let G be a finitely generated abelian group, considered as finitely generated module over the PID $\mathbb{Z}$.

1. Then there exists a unique sequence of natural numbers $d_1, d_2, \ldots, d_s \in \{0, 2, 3, 4, \ldots\}$ with $d_i | d_{i+1}$ for $i = 1, \ldots, s-1$, such that

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_s}$$

   Here we allow $\mathbb{Z}_0 = \mathbb{Z}/0\mathbb{Z} \;\cong\; \mathbb{Z}$.

2. Then there exist prime powers $q_1, \ldots, q_t$ and a natural number $r \in \mathbb{N}$ with

$$G \cong \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_t} \times \mathbb{Z}^r$$

   The natural number r is uniquely determined by G and it is called the rank of G. The prime powers are unique up to ordering.

The free factors in the decompositions here are also not uniquely determined as subgroups of G. The displayed isomorphisms are *not* canonical, i.e. not distinguished in a unique way.

Observation 4.2.5

- Let V be a finite-dimensional K-vector space and $A \in \text{End}_K(V)$ an endomorphism. Then by Lemma 1.1.15 we may consider V as a $K[X]$-module, that is finitely generated because the vector space dimension is already finite. Also for dimension reasons, the free parts as a $K[X]$-module vanishes. Thus we can find principal ideals $\mathfrak{a}_i = (f_i)$ as in Theorem 4.2.2, where we specify the generators $f_i \in K[X]$ uniquely by requiring that they are monic polynomials.

- Thus we have assigned to every endomorphism a sequence of monic polynomials $f_1, \ldots, f_r$, which satisfy the divisibility condition $f_i | f_{i-1} | \ldots | f_1$. These polynomials are called the invariant factors of the endomorphism A.

- For every class $\overline{v} \in K[X]/\,\mathfrak{a}_i$ we get

$$f_1 . \overline{v} = \overline{f_1 \cdot v} = 0 \; ,$$

  since $f_1 = 0 \bmod f_i$ for all i. Hence $f_1(A) = 0$. Conversely, on the summand $K[X]/(f_1)$ it is exactly the multiples of f_1 that act by zero. Thus f_1 is the monic polynomial of least degree, for which $f(A) = 0$ holds, i.e. the minimal polynomial of A.

- For every summand of the form $K[X]/(f)$ we now discuss the action of the endomorphism given by multiplication by X. For this let

$$f = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \,.$$

Choose as K-basis of $K[X]/(f)$ the classes $b_i := \overline{X^i}$ with $i = 0, \ldots n-1$. Then we have $X.b_i = b_{i+1}$ for $i = 0, \ldots n-2$ and $X.b_{n-1} = -\sum_{i=0}^{n-1} a_i b_i$. We thus find that the endomorphism is described with respect to this basis by the matrix

$$B_f := \begin{pmatrix} 0 & 0 & & & -a_0 \\ 1 & 0 & & & \vdots \\ & 1 & \ddots & & \\ & & \ddots & 0 & -a_{n-2} \\ & & & 1 & -a_{n-1} \end{pmatrix} \in M(n \times n, K)$$

which is called the companion matrix of the polynomial f. The resulting normal form of the endomorphism – blockdiagonal with blocks given by companion matrices for polynomials obeying the divisibility condition – is also called the Frobenius normal form of the endomorphism.

The special case over algebraically closed fields is especially important.

Corollary 4.2.6 [Jordan normal form] Let K be an algebraically closed field, V a finite-dimensional K-vector space and $A\colon V \to V$ an endomorphism of V. Then there exists a basis of V, in which A is block diagonal, where in each block the diagonal entries are constant, only 1s appear directly above the diagonal, and zeros elsewhere.

Proof. As K is algebraically closed is, the prime elements are given (up to unit multiples) by linear polynomials. By Theorem 4.2.2.2 we find an isomorphism of $K[X]$-modules

$$V \cong K[X]/(X-\lambda_1)^{n_1} \times \cdots \times K[X]/(X-\lambda_t)^{n_t}$$

with $n_i \in \mathbb{N}$ and $\lambda_i \in K$ for $i = 1, \ldots, n$. In each summand on the right-hand side we choose as basis the classes of the polynomials

$$1, (X-\lambda), (X-\lambda)^2, \ldots, (X-\lambda)^{n-1} \,.$$

Then the multiplication by X, and thus the action of A in the above basis, is given by the Jordan block since:

$$X(X-\lambda)^i = \lambda(X-\lambda)^i + (X-\lambda)^{i+1}$$ □

Similarly one obtains normal forms for fields that are not algebraically closed, e.g. $\mathbb{R}$ (see e.g. [K61, Satz 35.8]).

4.3 Semisimple rings and categories

Here we start into a more thorough discussion of modules over the group rings of finite groups. Throughout this section we let K be a field of arbitrary characteristic, G a finite group, and by $R := K[G]$ we denote the group ring of G over K, unless explicitly stated otherwise.

We begin with a general definition:

Definition 4.3.1 A ring R is called self-injective, if R as left module over itself is coregular in the sense of Definition 3.3.2.

Recall that an R-module M is finitely generated, if there exists $n \in \mathbb{N}$ and a surjective morphism of R-modules $R^n \to M$. Let us assume that the ring R is self-injective. We call an R-module finitely co-generated, if there exists $n \in \mathbb{N}$ and an injective morphism of R-modules $M \hookrightarrow R^n$. For finitely generated modules over self-injective rings the following statement holds:

Theorem 4.3.2 Let R be a self-injective ring. Then an R-module that is finitely generated and finitely cogenerated is projective if and only if it is injective.

Proof. We consider the following chain of implications:

$$\begin{aligned} M \text{ projective} &\Leftrightarrow M \text{ direct summand in } \bigoplus_{\text{finite}} R \\ &\Leftrightarrow M \text{ direct factor in } \prod_{\text{finite}} R \\ &\Leftrightarrow M \text{ injective} \end{aligned}$$

The first and last implications follow from Theorem 3.3.4. The finiteness follows because in the proof of Theorem 1.3.5 for a finitely generated module M, we can choose a free module of finite rank. □

Let K be a field. In case one considers finite-dimensional modules over a finite-dimensional self-injective K-algebra A, one can show [F05, Lemma 1] that a module is projective if and only if it is injective.

Our goal is the following theorem:

Theorem 4.3.3 Let K be an arbitrary field and G a finite group. Then the group ring $R = K[G]$ is self-injective. As a consequence, a finite-dimensional G-representation on a K-vector space is projective if and only if it is injective.

In this theorem it is essential that K is a field and also that the group G is finite. We first proof the following

Lemma 4.3.4 Let R be a K-algebra. We denote by R^* the R-module $R^* := \mathrm{Hom}_K(R, K)$, induced by the right action of R on itself. Then the R-module R^* is injective.

Proof. The proof proceeds as in Example 3.3.3.2: We aim to establish an isomorphism between the functors $\mathrm{Hom}_R(-, R^*)$ and $\mathrm{Hom}_K(-, K)$. For an arbitrary R-module M we have:

$$\mathrm{Hom}_R(M, R^*) \stackrel{\text{def}}{=} \mathrm{Hom}_R(M, \mathrm{Hom}_K(R, K)) \cong \mathrm{Hom}_K(R \otimes_R M, K) \cong \mathrm{Hom}_K(M, K)\,.$$

The second isomorphism holds because both spaces describe the K-bilinear maps $M \times R \to K$. In the last expression we implicitly apply the forgetful functor from R-modules to K-vector spaces. Thus we have an isomorphism of the functors $\mathrm{Hom}_R(-, R^*)$ and $\mathrm{Hom}_K(-, K)$. The functor $\mathrm{Hom}_K(-, K)$ is exact, since the field K as module over itself is injective. In this step we use that we consider the group ring over a field. By the isomorphism of functors, $\mathrm{Hom}_R(-, R^*)$ is also exact, so R^* is injective. □

The other arguments in Example 3.3.3 can also be generalized, showing e.g. that R^* is coregular. The proof Theorem 4.3.3 will follow from the next lemma.

Lemma 4.3.5 Let G be a finite group and $R = K[G]$. Then the K-linear map

$$\begin{array}{rccc} \Phi\colon & R^* & \to & R \\ & f & \mapsto & \sum_{g \in G} f(g) g^{-1}\,, \end{array}$$

is an isomorphism of R-modules. Here $(g)_{g \in G}$ is the distinguished basis of $K[G]$.

For the group ring of a finite group the modules R and R^* are thus isomorphic. Motivated by the terminology from the theory of Hopf algebras, we call Φ the Frobenius map.

Proof. The map is obviously bijective, since the preimage of the standard basis element $g \in R$ given by $\delta_{g^{-1}} \in R^*$ with $\delta_g(g') = \delta_{g,g'}$. We compute that Φ is a morphism of R-modules: for $g_0 \in G$ we have

$$\Phi(g_0.f) = \sum_{g \in G} f(gg_0)g^{-1} = \sum_{\tilde{g} \in G} f(\tilde{g})g_0\tilde{g}^{-1} = g_0\Phi(f) \ .$$

Note that the sum is well-defined because the group is finite. □

One can now ask whether it is possible that *all* K-linear representations of a given finite group are projective, i.e. that the category of representations is semisimple in the sense of Definition 3.1.17. We will first study categories of modules over a ring, in which all objects are projective, in a more abstract setting.

Definition 4.3.6

1. A module M is called semisimple, if every submodule U of M has a *complement* D, i.e. if for every submodule U there exists a submodule D with $D \oplus U = M$.

2. A ring is called semisimple if it is semisimple as left module over itself.

Every vector space — so every module over a field — admits by extension of bases complements and thus is semisimple. Over any ring, the zero module $M = 0$ is semisimple.

As we have only used left modules to define, when a ring is semisimple, we should actually call this notion left-semisimple. In Corollary 4.4.5 we will see, however, that every left-semisimple ring is also right-semisimple.

Theorem 4.3.7 Let R be a ring and M an R-module. Then the following are equivalent:

1. M is an (inner) direct sum of simple submodules.

2. M is a (not necessarily direct) sum of simple submodules.

3. M is semisimple, i.e. every submodule U of M has a complement D.

Proof.

- 1. $\Rightarrow$ 2. is clear by definition.

- 2. $\Rightarrow$ 3. we start by considering $M = \sum_{i \in I} M_i$, a sum of simple submodules M_i. For every subset $J \subset I$ we denote the corresponding inner sum of submodules as

$$M_J := \sum_{i \in J} M_i \, .$$

  Let U be the submodule for which we want to find a complement. By Zorn's lemma, we can find among the subsets $J \subset I$ with $M_J \cap U = 0$ a maximal subset J (with respect to inclusion). By the requirement $M_J \cap U = 0$ on the index set J, the sum $M_J + U$ is direct. It thus suffices to prove that

$$M_J + U = M.$$

  Suppose, on the contrary, that $M_J + U$ is a proper submodule of M, then there would be at least one $M_i \not\subset M_J + U$. This excludes the option $M_i \cap (M_J + U) = M_i$, so since M_i is simple, we must have $M_i \cap (M_J + U) = 0$. But then we also have $(M_i + M_J) \cap U = 0$, in contradiction to the maximality of J.

- 3. $\Rightarrow$ 2. starts by noting that property 3. is inherited by submodules. Let $U \subset N \subset M$ be submodules, V a complement of U in M, then $V \cap N$ is a complement of U in N.

  Let S be the sum of all simple submodules of M. (If M has no simple submodules, this would mean $S = 0$.) Now suppose $S \neq M$, then by 3. we find a nonzero complement D of S.

  Continuing with the assumption $D \neq 0$ we can find $D \ni d \neq 0$ and consider Rd, the submodule of D generated by d. The proper submodules of a module form a partially ordered set under inclusion, in which every chain has an upper bound. As upper bound of such a chain of submodules we can take their union. Using Zorn's lemma we find a maximal proper submodule U' in Rd. Since the submodule Rd also satisfies (3), we find a complement $Rd = U' \oplus E$. Then $E \cong Rd/U'$ is simple by maximality of U' in Rd, see Lemma 1.5.2.2. By definition of S we have $E \subset S$, in contradiction to $E \subset Rd \subset D$ and $D \cap S = 0$.

- 2. $\Rightarrow$ 1. here we start with $M = \sum_{i \in I} M_i$ for simple modules M_i. Let X be the set of all subsets $J \subset I$, such that the sum $M_J = \sum_{j \in J} M_j$ is direct. By $\emptyset \in X$ this set is non-empty.

  We show that every chain in X has an upper bound in X. Let Y be a totally ordered non-empty subset of X. Our candidate for an upper bound for Y is $I_0 := \cup_{I' \in Y} I'$, so our next goal is to show $I_0 \in X$.

  The sum M_{I_0} is direct if and only if for every finite subset $I_1 \subset I_0$ the sum is direct. As Y is totally ordered, there exists for every *finite* I_1 an $I' \in Y$ with $I_1 \subset I'$. By $Y \subset X$, the sum $M_{I'}$ is direct, and then the smaller sum M_{I_1} is also direct. Thus the sum M_{I_0} is direct, and so $I_0 \in X$.

  By Zorn's lemma we find a maximal element $J \in X$ and claim $M_J = M$. For this it suffices to show $M_i \subset M_J$ for all $i \in I$. Suppose this would fail for i_0, then $M_{i_0} \cap M_J$ is a proper submodule of M_{i_0}. As M_{i_0} is simple, we must have $M_{i_0} \cap M_J = 0$, and so the sum $M_{i_0} \oplus M_J$ is direct, in contradiction to the maximality of J. $\square$

Corollary 4.3.8 Every quotient and every submodule of a semisimple module is semisimple.

Proof. For a given submodule $U \subset M$, consider the canonical surjection $M \to M/U$. The image of a simple submodule of M is either zero or isomorphic to the simple submodule. Thus the quotient M/U is a sum of simple submodules, by Theorem 4.3.7 thus semisimple.

Again by Theorem 4.3.7 we find a complement D for U. Thus the submodule U is isomorphic to a quotient, $U \cong M/D$, and hence semisimple by the previous argument. $\square$

Corollary 4.3.9 Let R be a ring. Then the following statements are equivalent.

1. The ring R is semisimple, i.e. as a left module over itself, R is a direct sum of simple submodules.

2. Every R-module is semisimple, i.e. every R-module is a direct sum of simple submodules.

3. The category $R-$Mod is semisimple in the sense of Definition 3.1.17, i.e. all R-modules are projective.

Proof.

3.⇒2. Let the category $R-$Mod be semisimple and M an R-module. For every submodule $U \subset M$ we have a short exact sequence

$$0 \to U \to M \to M/U \to 0 \ ,$$

that splits by Theorem 1.4.7 since M/U is projective. By Theorem 1.4.3 the submodule U then has a complement in M.

2.⇒1. This implication is trivial since 1. is a special case of 2.

1.⇒3. We need to show that every R-module M is projective, i.e. a direct summand of a free R-module F. By Theorem 1.3.5, M is a homomorphic image of a free module F, so we may consider the exact sequence

$$0 \to \ker \pi \to F \xrightarrow{\pi} M \to 0$$

The ring R is semisimple by assumption, and thus also F, as it is a direct sum of copies of R. By Theorem 4.3.7 $\ker \pi$ has a complement, which is isomorphic to M, i.e. $F \cong M \oplus \ker \pi$. Thus M is projective.

□

Theorem 4.3.10 Let R be a semisimple ring. Then as R-module R has finite length and every simple R-module is isomorphic to a simple submodule of R. In particular, there exist only finitely many simple R-modules up to isomorphism.

Proof. We find a decomposition of R as a direct sum simple R-modules, $R = \oplus M_i$ with M_i simple. As unital ring, R cyclic as module over itself with generator $1 \in R = \oplus M_i$. The generator can only have nonzero components in finitely many summands, so R has finite length. For an arbitrary simple module M we consider a generator $x \in M$ to get a surjection

$$\begin{array}{rcl} R \cong \oplus M_i & \to & M \\ r & \mapsto & rx \end{array}$$

This corresponds to a family $(M_i \to M)$ of module homomorphisms. Since the map is surjective at least one of the maps out of M_i must be nonzero. By Schur's lemma 1.5.5 this must be an isomorphism, along which we can identify M with a submodule of R. □

Definition 4.3.11

1. Let R be a ring and M an R-module. Given a simple R-module E, we denote by $M_E \subset M$ the sum of all submodules of M that are isomorphic to E and call this the isotypic component of M of type E.

2. The submodule generated by all simple submodules of M is called the socle of M and it is denoted by $\mathrm{soc}(M)$.

Theorem 4.3.12 [Decomposition into isotypic components]

1. The socle is the largest semisimple submodule of M. In particular, a module is semisimple if and only if it is equal to its socle.

2. Let R be a ring and $\mathrm{irr}(R)$ system of representatives for the isomorphism classes of simple R-modules. Then the socle $\mathrm{soc}(M)$ decomposes into the direct sum of isotypic components:

$$\mathrm{soc}(M) = \bigoplus_{E \in \mathrm{irr}(R)} M_E \, .$$

Proof.

- The socle is a sum of simple modules and, thus, semisimple by Theorem 4.3.7.
- As $\mathrm{soc}(M)$ is semisimple, we only have to show that the sum of isotypic components is direct, i.e. that we have
$$M_E \cap \sum_{F \neq E} M_F = 0$$
for all E. For this it suffices to show that every simple submodule in a sum of simple submodules is isomorphic to one of the summands. Then every simple submodule of M_E is isomorphic to E, but no simple submodule of $\sum_{F \neq E} M_F$ can be isomorphic to E. Thus the intersection is trivial.

  So we let E be a simple submodule in a sum $M := \sum_{j \in J} M_j$ of simple modules. Since the sum $\sum_{j \in J} M_j$ is semisimple, the simple submodule E is also a quotient of this sum. As in the proof of Theorem 4.3.10 we deduce that E is also isomorphic to a simple direct summand in M.

□

We can now provide a condition under which the category of representations of a finite group G on K-vector spaces is semisimple.

Theorem 4.3.13 [Maschke] Let G be a finite group and K a field, whose characteristic does not divide the order of the group $|G|$. Then the category of representations of G on K-vector spaces is semisimple.

There exists a simple method of proof in the cases $K = \mathbb{R}$ or $K = \mathbb{C}$; since this method admits many generalizations in other contexts we first consider these special cases. It is based on the following lemma.

Lemma 4.3.14 If V is a representation of a finite group G over $K = \mathbb{R}$ or $K = \mathbb{C}$, then there exists a G-invariant inner product on V, i.e. $(gv, gw) = (v, w)$ for all elements $g \in G$ and $v, w \in V$.

Proof. We choose on V an arbitrary sesquilinear inner product $b\colon V \times V \to K$, for example by declaring an arbitrary basis to be orthonormal. Then the finite sum
$$(v, w) := \sum_{g \in G} b(gv, gw)$$
defines a G-invariant inner product. This is clearly sesquilinear and positively definite since $(v, v) = \sum_{g \in G}(gv, gv)$ is a finite sum positive real numbers and thus positive. The G-invariance follows from
$$(gv, gw) = \sum_{\tilde{g} \in G} b(\tilde{g}gv, \tilde{g}gw) = (v, w) \quad . \qquad \square$$

Proof of Maschke's Theorem 4.3.13 for $K = \mathbb{R}$ or $K = \mathbb{C}$ and finite-dimensional representations.. If $W \subset V$ is a subrepresentation, then there exists an orthogonal complement $W^\perp \subset V$ since V is finite-dimensional. With respect to an invariant inner product, the complement $W^\perp$ is a subrepresentation: if $(v, w) = 0$ for all $w \in W$ then, by invariance, we also have $(gv, w) = (v, g^{-1}w) = 0$, for all $g \in G$ and $w \in W$. We thus have the following orthogonal decomposition into subrepresentations:
$$V = W \oplus W^\perp .$$
Now that we know that complements exist, semisimplicity follows from Theorem 4.3.7. □

This technique is also called "Weyl's unitarian trick". In case of infinite-dimensional inner product spaces, one additionally has to assume the completeness of the subspace W, to conclude that an orthogonal complement exists. The general case, i.e. for general fields and representations of infinite dimension, needs more work.

Proof of Maschke's Theorem 4.3.13, general case. By Theorem 4.3.7 it suffices to show that every submodule W of V has a complement.

- If $i\colon W \hookrightarrow V$ is a subrepresentation, then we can find a retraction in the category of K-vector spaces, i.e. we pick a K-linear map

  $$\pi\colon V \to W$$

  such that $\pi \circ i = \mathrm{id}_W$. The problem is that π is in general only a map of vector spaces, but not of G-representations. We intend to improve the map by averaging over the group G so that it intertwines the action of G. We thus consider the map $\psi\colon V \to W$:

  $$\psi := \frac{1}{|G|} \sum_{g \in G} g \circ \pi \circ g^{-1}$$

  This only makes sense when the characteristic of K does not divide the order of the group. (Compare this expression with the proof of Theorem 4.3.3, where we also saw a sum over group elements, in which g and g^{-1} appear in pairs.

- For arbitrary $h \in G$ we now compute:

  $$h \circ \psi = \frac{1}{|G|} \sum_{g \in G} hg \circ \pi \circ g^{-1} = \frac{1}{|G|} \sum_{\tilde{g} \in G} \tilde{g} \circ \pi \circ \tilde{g}^{-1} h = \psi \circ h \ ,$$

  where we have substituted $\tilde{g} := hg$. Thus we see $\psi \in \mathrm{Hom}_G(V, W)$. Furthermore we have

  $$\psi \circ i = \frac{1}{|G|} \sum_{g \in G} g \circ \pi \circ g^{-1} \circ i = \sum_{g \in G} \frac{1}{|G|} g \circ \pi \circ i \circ g^{-1} = \mathrm{id}_W \ ,$$

  where in the second equation we use that i is a G-morphism and in the third equation $\pi \circ \iota = \mathrm{id}_W$. Here it becomes clear, why one has to divide by the group order $|G|$, which imposes the stated restriction on the characteristic of the field.

- By Theorem 1.4.3 V is the inner direct sum of $\iota(W)$ and $\ker \psi$. □

For any group G and field K, such that $\mathrm{char}(K)$ does not divide the group order $|G|$, the K-linear representation theory of G can thus be reduced to understanding simple representations and, by Theorem 4.3.10, understanding the decomposition of the group ring into simple left modules.

4.4 Structure theory of semisimple rings

Semisimple rings resp. semisimple algebras over a field can be described very explicitly. These descriptions will be used in the next section to study semisimple group rings.

We recall Schur's lemma 1.5.5: every homomorphism $\Phi\colon M_1 \to M_2$ is injective or zero, whenever M_1 is a simple module, and is surjective or zero, whenever M_2 is a simple module.

Corollary 4.4.1

1. For every simple R-module M, the endomorphism ring $\mathrm{End}_R(M)$ is a division ring, i.e. a ring, in which every nonzero element has a multiplicative inverse.

2. Homomorphisms between semisimple modules preserve isotypic components.

3. If R is commutative, then for every ideal $I \subset R$ the quotient R/I is a ring and we have ring isomorphisms
$$\mathrm{End}_R(R/I) \cong \mathrm{End}_{R/I}(R/I) \cong R/I \ .$$
It follows that the module R/I is simple if and only if the left ideal I is maximal, cf. Lemma 1.5.2. The endomorphism ring of a simple module over a *commutative* ring is thus a field.

A finitely generated semisimple module M always has finite length: Let $e_1, \ldots, e_n$ be a finite generating set of M. Each of the finitely many generators has nonzero components in only finitely many summands in the decomposition $M = \bigoplus_i M_i$ into simple modules. Thus only finitely many components $M_1, \ldots, M_r$ can be hit, and we can deduce $M \cong M_1 \oplus \cdots \oplus M_r$.

Theorem 4.4.2 Let R be a ring and M a finitely generated semisimple R-module. Then the endomorphism ring $\mathrm{End}_R(M)$ is isomorphic to a finite product of matrix rings over division rings.

Proof. The module M is semisimple and decomposes into isotypic components $M \cong \oplus_{i=1}^k M_i^{n_i}$ with $n_i \in \mathbb{N}$ and M_i pairwise non-isomorphic simple R-modules, see Theorem 4.3.12. As M is finitely generated, the decomposition is a finite direct sum. Then we have
$$\mathrm{End}_R(M) = \oplus_{ij} \mathrm{Hom}(M_i^{n_i}, M_j^{n_j}) \cong \oplus_i M(n_i \times n_i, \mathrm{End}_R(M_i)) \ .$$
By the Corollary 4.4.1.1 of Schur's lemma, $\mathrm{End}_R(M_i)$ is a division ring. □

Theorem 4.4.3 [Artin–Wedderburn theorem] Every semisimple ring R is isomorphic to a finite product of matrix rings over division rings. Any commutative semisimple ring R is isomorphic to a finite product of fields.

Proof. As R is semisimple, it has finite length as a left module over itself, see Theorem 4.3.10. By Theorem 4.4.2 we have
$$\mathrm{End}_R(R) \cong \prod_i M(n_i \times n_i, D_i)$$
for some $n_i \in \mathbb{N}$ and certain division rings D_i. For every ring R there exists an isomorphism by right multiplication,
$$\begin{array}{rcl} R^{\mathrm{opp}} & \xrightarrow{\sim} & \mathrm{End}_R(R) \\ r & \mapsto & (\varphi_r \colon x \mapsto xr) \end{array}$$
The inverse associates to a module morphism $\varphi_0 :_R \to_R R$ the elements $\varphi_0(1) \in R$. Note that
$$\varphi_0(r) = \varphi_0(r \cdot 1) = r\varphi_0(1)$$
so that $\varphi_0(1)$ indeed characterizes φ_0 uniquely. Thus
$$R \cong (R^{\mathrm{opp}})^{\mathrm{opp}} \cong \prod_i M(n_i \times n_i, D_i)^{\mathrm{opp}} \cong \prod_i M(n_i \times n_i, D_i^{\mathrm{opp}}) \ ,$$
where the last isomorphism is given by transposition of the $n_i \times n_i$-matrices. □

Remark 4.4.4 The decomposition of a semisimple ring R

$$R \cong \prod_i M(n_i \times n_i, D_i)$$

is unique up to reordering.

Corollary 4.4.5 A ring is right-semisimple if and only if it is left-semisimple.

If instead of arbitrary rings we work with algebras over fields, then for an algebraically closed field K, the semisimple K-algebras can be explicitly described. For this we need the following lemma:

Lemma 4.4.6 Let F be an algebraically closed field. If D is a finite-dimensional division algebra over F, then $D = F$.

Proof. For every element $x \in D$, the family $(1, x, \ldots, x^m)$ with $m := \dim_F D$ is linearly dependent over the field F. Thus there exists a monic polynomial $f \in F[X]$ with $f(x) = 0$. Choose such a polynomial f of minimal degree. If f were reducible, $f = f_1 \cdot f_2$, then $0 = f_1(x) \cdot f_2(x)$ for non-constant polynomials of strictly lower degree than f. Since D is a division algebra, we must have $f_1(x) = 0$ or $f_2(x) = 0$, in contradiction to the minimality of f.

Since F is algebraically closed, the irreducible polynomial f is of the form $f(X) = X - a$ with $a \in F$. Thus $x = a$ and $D = F$. □

Over the field $\mathbb{R}$, which is not algebraically closed, there are different division algebras: the fields $\mathbb{R}$ and $\mathbb{C}$ and the quaternions $\mathbb{H}$, a non-commutative division algebra.

From Theorem 4.4.3 we now get:

Corollary 4.4.7 Let K be an algebraically closed field. Every finite-dimensional semisimple K-algebra is isomorphic to a finite product of matrix rings with entries in K.

We can also combine Lemma 4.4.6 with Schur's lemma 4.4.1.1 to get:

Corollary 4.4.8 Let K be an algebraically closed field and R a K-algebra. Let M be a simple R-module of finite dimension. Then we have an isomorphism of rings:

$$\begin{array}{ccc} K & \xrightarrow{\sim} & \mathrm{End}_R(M) \\ \lambda & \mapsto & \lambda \mathrm{id}_M\,. \end{array}$$

Such a module is also called absolutely simple.

Proof. As K is a field, we know that the map is injective. On the other hand, $\mathrm{End}_R(M)$ is a division algebra over the algebraically closed field K and thus isomorphic to K by Lemma 4.4.6. Thus the K-linear map is also surjective. □

We also use the Artin–Wedderburn Theorem 4.4.3 to read off the representation theory of semisimple rings.

Corollary 4.4.9 The isomorphism classes of simple representations of a semisimple ring are in bijection to the individual factors of the ring; only the corresponding factor acts non-trivially on the simple representation. Associated to the factor $M(n_i \times n_i, D_i)$ is a simple representation given by acting with matrices on column vectors in $(D_i)^n$.

4.5 Fourier transform for groups

We would like to avoid assuming that the group algebra of a finite group G over a field K is semisimple, and thus need an additional tool. Let M be an R-module. Then M is also a module over the ring $\mathrm{End}_R(M)$:

$$\begin{array}{rcl} \mathrm{End}_R(M) \times M & \to & M \\ (\varphi, m) & \mapsto & \varphi(m)\ . \end{array}$$

Every ring element $x \in R$ defines by scalar multiplication

$$\begin{array}{rccl} \lambda_x \colon & M & \to & M \\ & m & \mapsto & x.m \end{array}$$

an element of $\mathrm{End}(M)$ that commutes with any $\varphi \in \mathrm{End}_R(M)$, i.e. that is contained in $\mathrm{End}_{\mathrm{End}_R(M)}(M)$. In particular, we have a ring homomorphism

$$\varphi_{\mathrm{Jac}} \colon R \to \mathrm{End}_{\mathrm{End}_R(M)}(M)\,.$$

Theorem 4.5.1 (Jacobson density theorem) Let R be a ring and M a *semisimple* R-module. Let $f \in \mathrm{End}_{\mathrm{End}_R(M)}(M)$ and finitely many elements $m_1, \ldots, m_r \in M$ be given. Then there exists an $x \in R$ with $f(m_i) = xm_i$ for all i.

This statement is often expressed by saying that the image $\varphi_{\mathrm{Jac}}(R)$ in $\mathrm{End}_{\mathrm{End}_R(M)}(M)$ is dense: We can encode the action of every morphism $f \in \mathrm{End}_{\mathrm{End}_R(M)}(M)$ on finitely many elements of the module as multiplication with a scalar $x \in R$.

Proof. We first consider the case $r = 1$, i.e. with a single element $m_1 \in M$. As M is semisimple, the submodule $Rm_1 \subset M$ has a complement D by Theorem 4.3.7. We now consider the direct sum decomposition

$$M = Rm_1 \oplus D\ .$$

The idempotent map

$$\pi \colon M \twoheadrightarrow Rm_1 \hookrightarrow M,$$

defined as the composite of the canonical surjection and injection, is an element of the endomorphism ring $\mathrm{End}_R(M)$. As $f \in \mathrm{End}_{\mathrm{End}_R(M)}(M)$, we must have

$$f \circ \pi = \pi \circ f\,,$$

and so

$$f(m_1) = f \circ \pi(m_1) = \pi \circ f(m_1)\,.$$

This implies $f(m_1) \in Rm_1$ and so there exists an element $x \in R$, such that

$$f(m_1) = xm_1\,.$$

For the general case $r > 1$ we consider the finite direct sum of copies of M

$$(m_1, \ldots, m_r) \in M \oplus \cdots \oplus M\ ,$$

which is a semisimple R-module, and the map

$$f \times f \times \cdots \times f\,,$$

which indeed commutes with all elements of

$$\mathrm{End}_R(M \oplus \ldots \oplus M) \cong M(r \times r, \mathrm{End}_R M),$$

and then we use the case $r = 1$. □

Remark 4.5.2 We explain the name *density* theorem, using some elementary topology. [2] We endow the set underlying the module M with the discrete topology and $\mathrm{End}_{\mathrm{End}_R(M)}(M)$ with the *compact-open topology* which has by deifnition the subbasis

$$\{W(K,U) \mid K \subset M \text{ compact and } U \subset M \text{ open } \} ,$$

where

$$W(K,U) := \{g \in \mathrm{End}_{\mathrm{End}_R(M)}(M) \,|\, g(K) \subset U\} \ .$$

We now claim:

The image of the ring homomorphism

$$\varphi_{\mathrm{Jac}} \colon R \to \mathrm{End}_{\mathrm{End}_R(M)}(M) .$$

is dense in $\mathrm{End}_{\mathrm{End}_R(M)}(M)$ if and only if for every morphism $f \in \mathrm{End}_{\mathrm{End}_R(M)}(M)$ and and any finite set $F \subseteq M$ there exists a ring element $x \in R$ such that $f(m) = xm_i$ for all $m \in F$.

Suppose that the image of φ_{Jac} is dense. Then any open neighborhood U of f has non-empty intersection with $\mathrm{Im}\,(\varphi_{\mathrm{Jac}})$. Given a finite subset $F \subset M$, the finite intersection of open sets

$$U := \cap_{m \in F} W(\{m\}, \{f(m)\})$$

is an open neighbourhood of f. Thus, there exists $x \in R$ such that $\varphi_{\mathrm{Jac}}(x) \in U$. By definition of U, this implies for x that $f(m) = x.m$.

Conversely, suppose that for any $f \in \mathrm{End}_{\mathrm{End}_R(M)}(M)$ and any finite subset $F \subset M$, there exists $x \in R$ such that $f(m) = x.m$ for all $m \in M$. Now let $U \in \mathrm{End}_{\mathrm{End}_R(M)}(M)$ be an open neighbourhood of f. By definition of the compact-open topology, we can write U in the form

$$U = \cup_{i \in I} \left(\cap_{j \in J_i} W(K_{ij}, V_{ij})\right)$$

where all index sets J_i are finite, each $K_{ij} \subset M$ is compact and thus finite and $V_{ij} \subset M$ is open. There is at least one $k \in I$ such that $f \in \cap_{j \in J_k} W(K_{kj}, V_{kj})$. Then $K := \cup_{j \in J_k} K_{kj}$ is, as a finite union of finite sets, a finite subset of M. By assumption, we find $x \in R$ such that $f(m) = x.m$ for all $m \in M$. For this x, we have $\varphi_{\mathrm{Jac}}(x) \in \cap_{j \in J_k} W(K_{kj}, V_{kj}) \subset U$. Thus the image of φ_{Jac} is dense in $\mathrm{End}_{\mathrm{End}_R(M)}(M)$.

Corollary 4.5.3 [Wedderburn] If K is an *algebraically closed* field and A a subring of $M(n \times n, K)$, such that K^n is simple as an A-module, then A is the entire matrix ring,

$$A = M(n \times n, K) .$$

Proof. As K is algebraically closed and K^n is a simple A-module, by Corollary 4.4.8 of Schur's lemma $\mathrm{End}_A(K^n) \cong K$. As a simple A-module, K^n is also semisimple; by the density theorem 4.5.1 A is dense in $\mathrm{End}_{\mathrm{End}_A(K^n)}(K^n) = \mathrm{End}_K(K^n)$. Since K^n is generated by finitely many $m_i \in K^n$ as K-vector space, linear maps can be determined on finitely many values. This implies the surjectivity of $\varphi_{\mathrm{Jac}} \colon A \to \mathrm{End}_K(K^n)$. □

Remark 4.5.4 One can also give a coordinate-free description of this theorem: If K is an algebraically closed field and V a finite-dimensional K-vector space and $A \subset \mathrm{End}_K(V)$ a subring, such that V is simple is as ab A-module, then $A = \mathrm{End}_K(V)$. This version is especially helpful for seeing why the condition "algebraically closed" is necessary: is $K \subset L$ is a finite field extension and we consider the subring $L \subset \mathrm{End}_K(L)$, where an element of L acts by left multiplication on L. Then L is a simple L-module over itself, but if $K \neq L$ then dimension reasons already imply $L \neq \mathrm{End}_K(L)$.

[2] I am grateful to Max Demirdilek for bringing up this argument.

Corollary 4.5.5 Let K be an algebraically closed field and V an irreducible finite-dimensional representation of the group G over K. Then the action of G on V defines a surjection

$$K[G] \twoheadrightarrow \operatorname{End}_K(V)$$

Proof. Apply Corollary 4.5.3, to the image of $K[G]$ in $\operatorname{End}_K(V)$. □

Theorem 4.5.6 [Fourier transform] Let K be an algebraically closed field of arbitrary characteristic and G a finite group. Let $L_1, \dots, L_r$ be a system of representatives of the isomorphism classes of irreducible representations of G.

1. The action of G defines a surjection of rings

$$F\colon K[G] \twoheadrightarrow (\operatorname{End}_K L_1) \times \cdots \times (\operatorname{End}_K L_r)\,. \tag{2}$$

2. If the characteristic of the field K does not divide the order $|G|$ of the group, then this is a ring isomorphism.

Proof. 1. As K is algebraically closed, the semisimple $K[G]$-module $M := L_1 \oplus \cdots \oplus L_r$ has endomorphism ring

$$\operatorname{End}_{K[G]}(L_1 \oplus \cdots \oplus L_r) = K \times K \times \cdots \times K\,.$$

Thus we have

$$\operatorname{End}_{\operatorname{End}_{K[G]}}(M) = \operatorname{End}_{K\times\cdots\times K}(M) = \operatorname{End}_K(L_1) \times \dots \operatorname{End}_K(L_r)$$

and the surjectivity follows from the density theorem 4.5.1.

2. If the characteristic of K does not divide the order of the group, then by Maschke's Theorem 4.3.13 the group ring $K[G]$ is semisimple, i.e. a direct sum of simple subrepresentations. Then the isomorphism follows from Theorem 4.4.3. Alternatively, one can consider $a \in K[G]$ in the kernel of the surjection. Then left multiplication with a induces the zero map on every simple module, and thus on every semisimple module, and thus also on the regular module $K[G]$. Writing $a = \sum \lambda_g g$ we get $ae = 0$, and so $\lambda_g = 0$ for all group elements $g \in G$, hence $a = 0$. □

It is an important goal to describe for every pair of field K and group G all irreducible K-linear representations of G. (Ideally, one would then also like to describe tensor products of representations.) This information is not sufficient to describe the group ring as a ring, when it is not semisimple. However, when it is semisimple, e.g. in characteristic zero, then this information is indeed sufficient. We now collect facts about irreducible representations in the semisimple case.

From Theorem 4.5.6 we immediately get:

Corollary 4.5.7 Let K be an algebraically closed field and G a finite group, whose order is not divisible by the the characteristic of K. Let $L_1, \dots, L_r$ be a system of representatives of the isomorphism classes of simple representations. Then we have

$$|G| = (\dim_K L_1)^2 + (\dim_K L_2)^2 + \cdots + (\dim_K L_r)^2$$

Corollary 4.5.8 Under the same assumptions we have: There exist as many isomorphism classes of simple representations of G as conjugacy classes in G.

Proof. The centre $Z(R)$ of a ring is

$$Z(R) := \{z \in R \,|\, za = az \quad \text{for all } a \in R\}\,.$$

It is a commutative subring of R. Warning: in general the centre $Z(K[G])$ of the group ring $K[G]$ of a group G is distinct from the group ring of the centre $Z(G)$ of the group; but we have $K[Z(G)] \subseteq Z(K[G])$.

By Theorem 4.5.6, the dimension $\dim_K Z(K[G])$ of the group ring of a finite group equals the number of inequivalent irreducible representations,

$$\dim_K Z(K[G]) = \ |\text{iso classes of simple representations}|\ .$$

For an element in the centre $Z(K[G])$ of the group ring we make the ansatz $z = \sum_h \lambda_h \delta_h$ with $\lambda_h \in K$. By comparing

$$\begin{aligned} zg &= \sum_{h\in G} \lambda_h h \cdot g = \sum_{h\in G} \lambda_{hg^{-1}} h \\ gz &= \sum_{h\in G} \lambda_{g^{-1}h} h\,. \end{aligned}$$

we find $\lambda_{ghg^{-1}} = \lambda_h$ for all $g, h \in G$. Here one has to choose one coefficient for each conjugacy class of G, and so

$$\dim_K Z(K[G]) = \ |\text{conjugacy classes}|\ .$$

By comparing the two formulas for $\dim_K Z(K[G])$ we conclude the desired statement. □

Remark 4.5.9 Here we explain the relation to the usual Fourier transform. Consider all complex numbers of unit norm as an abelian group with respect to multiplication,

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\}\,.$$

One can show that all irreducible, continuous, finite-dimensional representations are one-dimensional. A representative for all isomorphism classes can be described by the group homomorphism

$$\begin{array}{rccll} L_n\colon & S^1 & \to & \mathrm{GL}(1,\mathbb{C}) \cong \mathbb{C}^\times & \text{for } n \in \mathbb{Z}\,. \\ & z & \mapsto & z^n & \end{array}$$

As analogue of the group ring we consider continuous complex-valued functions on S^1, $C^0(S^1)$, that we may identify with periodic functions on $\mathbb{R}$. The product is given by the convolution

$$(f * g)(h) = \int_{S^1} f(hx) g(x^{-1}) \mathrm{d}x,$$

cf. Definition 1.1.16. The continuous function $f \in C^0(S^1)$ acts on a continuous finite-dimensional representation V by

$$fv = \int_{S^1} f(z) \rho_V(z)(v)\, dz \quad \text{for} \quad v \in V$$

and, in particular, on the irreducible representation L_n by multiplication with

$$\int_{S^1} f(z) z^n \,\mathrm{d}z \in \mathbb{C}\ ,$$

which are exactly the Fourier coefficients of f. The map in Theorem 4.5.6

$$C^0(S^1) \xrightarrow{\sim} \prod_{n\in\mathbb{Z}} \mathrm{End}_{\mathbb{C}} L_n \cong \prod_{n\in\mathbb{Z}} \mathbb{C}$$

sends a function $f \in C^0(S^1)$ to its sequence of Fourier coefficients.

4.6 Characters

In this section we let K be an algebraically closed field and G a finite group, such that char K does not divide the the order $|G|$ of the group. Then we have by Theorem 4.5.6 an isomorphism of rings

$$F\colon K[G] \xrightarrow{\sim} (\mathrm{End}_K L_1) \times \cdots \times (\mathrm{End}_K L_r)\,.$$

Definition 4.6.1 Let L be a simple representation of G. By the isomorphism from Theorem 4.5.6 there exists a unique element $e_L \in K[G]$, that acts as the identity on L and by zero on any simple representation M of G, that is not isomorphic to L:

$$e_L : M \to M = \begin{cases} \mathrm{id}_M & \text{if} \quad M \cong L \\ 0 & \text{if} \quad M \text{ simple},\ M \ncong L \end{cases}$$

This element

$$e_L = F^{-1}\Big(\mathrm{id}_{\mathrm{End}_K L}\Big) \in K[G]$$

is called the (central) projector or idempotent associated with the simple representation L.

Lemma 4.6.2 Let $(L_i)_{i=1\ldots r}$ be representatives of the isomorphism classes of irreducible representations of G and $e_i \in K[G]$ the associated central idempotents of the group ring. Then we have

$$e_i \cdot e_j = \delta_{ij} e_i$$
$$1 = e_1 + \cdots + e_r$$

and the family $(e_i)_{i=1,\ldots r}$ of idempotents forms a basis of the centre of $K[G]$.

Proof. A direct consequence of Theorem 4.5.6 on the Fourier transform. □

We aim to express the idempotents (e_L) explicitly and need the following definition:

Definition 4.6.3 For a finite-dimensional representation of a group G on a K-vector space V the character

$$\chi_V\colon G \to K$$

is defined by $\chi_V(g) = \mathrm{Tr}_V\, g \equiv \mathrm{Tr}_V\, \rho(g)$. This function on the group G can be extended to a linear form on the group algebra $K[G]$, which we also denote by $\chi_V \in K[G]^*$:

$$\chi_V\colon \quad K[G] \to K$$

By linearity of the trace we have $\chi_V(h) = \mathrm{Tr}_V h$ for every $h \in K[G]$.

Example 4.6.4 The group algebra $K[G]$ is, like every ring, a module over itself, the so-called regular module. This left action is given by

$$\begin{aligned} \rho(g) : K[G] &\to K[G] \\ \rho(g)\Big(\sum_{h\in G} \lambda_h h\Big) &= \sum_{h\in G} \lambda_h\, gh\,. \end{aligned}$$

We can thus compute the character of the regular module:

$$\chi_{K[G]}(g) = \mathrm{Tr}_{K[G]}\rho(g) = \begin{cases} |G| & \text{for } g = e \\ 0 & \text{otherwise.} \end{cases}$$

We recall the isomorphism of $K[G]$-modules from Lemma 4.3.5, the Frobenius map:

$$\begin{array}{rccc} \Phi\colon & K[G]^* & \to & K[G] \\ & f & \mapsto & \sum_{g\in G} f(g)g^{-1}\,. \end{array}$$

Theorem 4.6.5 [character projector formula] The Frobenius map Φ relates the character $\chi_L \in K[G]^*$ and the projector $e_L \in K[G]$ for a simple representation L:

$$e_L = \frac{\dim_K L}{|G|}\ \Phi(\chi_L)\ .$$

Proof. For every $K[G]$-module M we have a ring homomorphism $K[G] \stackrel{\rho_M}{\to} \mathrm{End}_K(M)$ and thus consider the map

$$\tau_M\colon \quad K[G]^* \stackrel{\Phi}{\to} K[G] \stackrel{\rho_M}{\to} \mathrm{End}_K(M).$$

Using the character of the regular module from Example 4.6.4 we find for an arbitrary function $f \in K[G]^*$:

$$(*) \qquad \mathrm{Tr}_{K[G]}\left(\rho(g)\tau_{K[G]}(f)\right) = \sum_{h\in G} f(h)\mathrm{Tr}_{K[G]}\ gh^{-1} = |G|f(g)\ .$$

We are looking for the function $f_i \in K[G]^*$ that is the preimage of the ith projector under the Frobenius map, $\Phi(f_i) = e_i$. For this function and every $K[G]$-module L we have the equation $\tau_L(f_i) = \rho_L(e_i)$.

Now we compute

$$\begin{array}{rcll} f_i(g) & = & \frac{1}{|G|}\mathrm{Tr}_{K[G]}\rho(g)\tau_{K[G]}(f_i) & \\ & = & \frac{1}{|G|}\sum_{j=1}^{r}\mathrm{Tr}_{\mathrm{End}_K(L_j)}(\rho_{L_j}(g))_*\circ\rho_{L_j}(e_i)_*\ . & (*) \end{array}$$

where we have first used $(*)$ and then the isomorphism from Theorem 4.5.6. To evaluate the result we will use the following linear algebra lemma. □

Lemma 4.6.6 If L is a finite-dimensional K-vector space and $A\colon L \to L$ a K-linear map, then the linear map given by postcomposing with A

$$\begin{array}{rccc} A_*\colon & \mathrm{End}_K L & \to & \mathrm{End}_K L \\ & \varphi & \mapsto & A\circ\varphi \end{array}$$

has trace

$$\mathrm{Tr}_{\mathrm{End}_K L} A_* = \dim_K L \cdot \mathrm{Tr}_L A$$

Proof. Without loss of generality let $L = K^n$. Then $\mathrm{End}_K(K^n) \cong M(n\times n, K)$. The map multiplies the matrix associated with A on the left onto an arbitrary $n\times n$ matrix. Here one multiplies every column vector of this matrix by A. Thus A_* acts on every column of the $n\times n$-matrix like A on K^n. Thus the matrix of A_* is block diagonal with n blocks of type A. □

Proof. Proof of Theorem 4.6.5, continued Equation $(*)$ implies

$$f_i(g) = \sum_{j=1}^{r}\frac{\dim_K L_j}{|G|}\mathrm{Tr}_{L_j}(\rho(g))_{L_j}\circ\rho_{L_j}(e_i) = \frac{\dim_K L_i}{|G|}\chi_i(g)\ .$$ □

Remarks 4.6.7 The familiar properties of the trace immediately imply:

1. The character is constant on conjugacy classes, i.e. it is a class function:

$$\chi_L(ghg^{-1}) = \chi_L(h) \quad \text{for all} \quad g, h \in G$$

   By linear extension we consider the space of class functions as a vector subspace of the dual space $K[G]^*$.

2. If V and W are representations of G, then for the direct sum we have $\chi_{V\oplus W} = \chi_V + \chi_W$.

3. If V and W are G-representations, then the tensor product of vector spaces $V \otimes_K W$ has the structure of a G-representation by

$$g(v \otimes w) := (gv) \otimes (gw)\,.$$

   Then we have

$$\chi_{V\otimes W} = \chi_V \cdot \chi_W\,.$$

   Warning: this tensor product should not be confused with the tensor product $V \otimes_{K[G]} W$ of a right and a left module, which carries only the structure of a K-vector space; here it is actually a quotient of $V \otimes_K W$.

4. For a G-representation V the dual space $V^* = \mathrm{Hom}_K(V, K)$ with the action

$$(g\lambda)(v) = \lambda(g^{-1}v) \quad \text{for } \lambda \in V^*, g \in G\,, v \in V$$

   is called the contragradient representation. Then we have

$$\chi_{V^*}(g) = \chi_V(g^{-1})\,.$$

To learn more about characters we define another product on $K[G]^*$ (the first was the pointwise product), by declaring the Frobenius map to be an algebra isomorphism

$$K[G]^* \to K[G]^{\mathrm{opp}}.$$

The resulting product need not be commutative.

Definition 4.6.8 For two functions $f_1, f_2 \in K[G]^*$ we define the convolution product by

$$\begin{aligned} f_1 \star f_2(h) &:= \Phi^{-1}(\Phi(f_1) \cdot \Phi(f_2))(h) \\ &= \Phi^{-1}(\textstyle\sum_{h_1,h_2\in G} f_1(h_1)f_2(h_2)h_1^{-1}h_2^{-1})(h) = \sum_{h_1\cdot h_2=h} f_1(h_1)\cdot f_2(h_2)\ . \end{aligned}$$

Lemma 4.6.9 Let (L_i) be a system of representatives for the isomorphism classes of simple K-linear representations of a finite group G. Then for the convolution product of the characters we have

$$\chi_{L_i} \star \chi_{L_j} = \delta_{ij}\ \frac{|G|}{\dim_K L_i} \quad \chi_{L_i}$$

Proof. In the group algebra $K[G]$ we have

$$e_{L_i} \cdot e_{L_j} = \delta_{ij} e_{L_i}$$

and using $\chi_L = \frac{|G|}{\dim_K L}\Phi^{-1}(e_L)$ we compute

$$\chi_{L_i} \star \chi_{L_j} = \frac{|G|^2}{\dim_K L_i \dim_K L_j}\Phi^{-1}(e_{L_i} \cdot e_{L_j}) \ = \frac{|G|^2}{\dim_K L_i \dim_K L_j}\delta_{ij}\Phi^{-1}(e_{L_i}) = \delta_{ij}\frac{|G|}{\dim_K L_i}\ \chi_{L_i}\ .$$

□

Theorem 4.6.10 Let G be a finite group and K a field of characteristic zero. Then the dimension of any simple G-representation divides the order $|G|$ of the group.

Proof. Let L be a simple representation. Let $n = |G|$ be the order of the group. Then we have $g^n = 1$ for all $g \in G$. The value $\chi_L(g)$ of the character is the trace, i.e. the sum of eigenvalues, of $\rho(g)$. Thus $\chi_L(g)$ is an element of the ring $\mathbb{Z}[\zeta]$, with ζ a primitive nth root of unity.

Let $I \subset \mathbb{Z}[\zeta]$ be the ideal generated by the values of the character. Lemma 4.6.9 implies the inclusion

$$I \supset \frac{|G|}{\dim_K L}\, I\,.$$

From number theory we know that $\mathbb{Z}[\zeta]$ is a finitely generated free abelian group. By Theorem 4.1.1 the subgroup I is also finitely generated and free, and thus torsion-free. Hence we have $I \cong \mathbb{Z}^r$ for some $r \in \mathbb{N}$ and we must have

$$\frac{|G|}{\dim_K L} \in \mathbb{Z}\ ,$$

because only scaling by an integer maps $\mathbb{Z}^r$ to itself. □

Theorem 4.6.11 On the vector space $K[G]^*$ we consider the symmetric bilinear form

$$(\varphi, \psi) := \frac{1}{|G|} \sum_{g \in G} \varphi(g)\psi(g^{-1})$$

Then the characters form an orthonormal basis for the space of class functions with respect to this bilinear form.

Proof. By Definition 4.6.8 of the convolution product we have

$$(\varphi, \psi) = \frac{1}{|G|}(\varphi * \psi)(e)$$

with $e \in G$ the neutral element. Let (L_i) be a system of representatives for for the isomorphism classes of simple representations. Evaluating the equality in Lemma 4.6.9 on the neutral element e and noting

$$\chi_L(e) = \mathrm{Tr}\ {}_L\rho(e) = \mathrm{Tr}\ {}_L\mathrm{id}_L = \dim_K L\,,$$

we get

$$(\chi_{L_i}, \chi_{L_j}) = \delta_{ij}\ \frac{1}{|G|}\ \frac{|G|}{\dim_K L_j}\quad \chi_{L_j}(e) = \delta_{ij}\ .$$

In particular, the characters of simple representations are linearly independent in the space of class functions. By Corollary 4.5.7 they also span the space of class functions, and thus form a basis. □

If the group algebra $K[G]$ is not semisimple, then the characters only span a proper subspace of the space of class functions.

Corollary 4.6.12 Two finite-dimensional representations of a finite group over an algebraically closed field of characteristic zero are isomorphic if and only if they have the same character.

Proof. Since the group algebra is semisimple by Maschke's Theorem 4.3.13, Corollary 4.3.9 implies that every finite-dimensional representation is a finite direct sum of simple representations. We can compute the multiplicity of a given simple representation L in a direct sum

decomposition of the representation V into simples as follows: if $V = \oplus_{i=1}^r n_i L_i$ then for the character we get $\chi_V = \sum_{i=1}^r n_i \chi_{L_i}$ and thus $(\chi_L, \chi_V) = n_L$.

Thus if two representations have the same character, then the irreducible representations appear with the same multiplicities n_i, and both representations are isomorphic to the direct sum $\oplus_{i=1}^r n_i L_i$. □

Corollary 4.6.13 Let $s \in G$ and let $c(s)$ be the number of group elements in the conjugacy class of s. Then we have

$$\sum_{i=1}^r \chi_i(s)\chi_i(s^{-1}) = \frac{|G|}{c(s)} \ ;$$

If $t \in G$ is not conjugate to s, then we have

$$\sum_{i=1}^r \chi_i(s)\chi_i(t^{-1}) = 0 \ .$$

Proof. For $s \in G$ let f_s be the class function that takes the value one on the conjugacy class of s and zero on all other conjugacy classes. Since the characters form an orthonormal basis for the class functions by Theorem 4.6.11, we can expand

$$f_s = \sum_{i=1}^r \lambda_i \chi_i \qquad \text{with coefficients} \qquad \lambda_i = (f_s, \chi_i) = \frac{c(s)}{|G|}\chi_i(s^{-1}).$$

Then we have

$$f_s(t) = \frac{c(s)}{|G|} \sum_{i=1}^r \chi_i(s^{-1})\chi_i(t) \ . \qquad \square$$

We specialize to the case of complex group algebras.

Corollary 4.6.14 Consider on the dual of the complex group algebra $\mathbb{C}[G]$ the (hermitian) inner product $\langle \cdot, \cdot \rangle$ given by

$$\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi(g)\overline{\psi(g)} \ .$$

Then the simple characters form an orthonormal basis in the space of class functions.

Proof.

- For every character $\chi = \chi_V$ over $\mathbb{C}$ we will show

  $$\chi(g^{-1}) = \overline{\chi(g)} \, .$$

  For every complex vector space $(V, +, \cdot)$ there exists another complex vector space $(\overline{V}, +, *)$ which is equal as abelian group, but with the scalar multiplication twisted by conjugation:

  $$\lambda * v := \overline{\lambda} \cdot v \qquad \text{for all } \lambda \in \mathbb{C}, v \in V \, .$$

  Here $\overline{\lambda} \in \mathbb{C}$ is the complex conjugate of $\lambda \in \mathbb{C}$.

- If V is a G-representation, then so is $\overline{V}$ (with the same structure map!). With respect to the chosen basis of V the action is described by matrices with complex conjugate entries. Thus we have

  $$\chi_{\overline{V}}(g) = \overline{\chi_V(g)} \, .$$

- On the other hand we know from Remarks 4.6.7(4), that for the contragradient representation we have
$$\chi_{V^*}(g) = \chi_V(g^{-1})$$
It thus suffices to exhibit an isomorphism of G-representations
$$V^* \cong \overline{V}.$$
By Lemma 4.3.14 there exists a G-invariant inner product on V. We define a linear map
$$\iota \colon V^* \to \overline{V}$$
by requiring for $\varphi \in V^*$
$$\varphi(v) = \langle v, \iota(\varphi) \rangle$$
for all $v \in V$. Since $\langle \cdot, \cdot \rangle$ is non-degenerate, this defines a bijection. The map ι is even a G-morphism, because for all $g \in G$, $v \in V$, and $\varphi \in V^*$ we have:
$$\langle v, \iota(g\varphi) \rangle = g\varphi(v) = \varphi(g^{-1}v) = \langle g^{-1}v, \iota(\varphi) \rangle = \langle v, g\iota(\varphi) \rangle .$$
Here we used the definition of ι, the action of g on V^*, again the definition of ι, and the G-invariance of the inner product. □

Remark 4.6.15 The values of characters of the irreducible complex representations of a finite group G are collected in the form of a character table. The columns of such a table are indexed by representatives of conjugacy classes, and the the rows are indexed by irreducible representations. The table contains the values of the characters of the irreducible representations on the elements of the conjugacy class. Above the conjugacy classes one typically records in a separate row their sizes, so that one can also read off the values of the inner product on the space of class functions.

Examples 4.6.16

1. The irreducible complex representations of the symmetric group S_3 Are the trivial representation triv, the sign representation sign and the 2-dimensional reflection representation refl on $\mathbb{C}^3/\mathbb{C}(1,1,1)^t$ induced by permuting coordinates in $\mathbb{C}^3$. This results from extending scalars from $\mathbb{R}$ to $\mathbb{C}$ in the familiar interpretation of S_3 as the symmetry group of an equilateral triangle. In this picture, the odd permutations act by reflections in three lines through the origin in $\mathbb{R}^2$, which are spaced at 60 degree angles relative to each other.

   If we choose two odd transpositions $s, t \in S_3$, then the elements of are $S_3 = \{e, s, t, sts, ts, st\}$. The character table has the form

	1	3	2
	e	s, t, sts	ts, st
triv	1	1	1
sign	1	-1	1
refl	2	0	-1

   Only the lowest row poses any challenges. To see that it is plausible, note that every reflection in a line in the plane has trace zero, and every rotation by 120 degrees has trace $-1 = \zeta_3 + \overline{\zeta}_3$ with ζ_3 a primitive third root of unity. Checking the orthogonality relations from Corollary 4.6.14 and Corollary 4.6.13 is left as an exercise.

2. To determine the one-dimensional complex irreducible representations of a cyclic group $C_n = \langle g \rangle$ with a generator g and relation $g^n = e$ we make the ansatz $\rho(g) = w$ with $w \in GL(1, \mathbb{C}) \cong \mathbb{C}^\times$. The relation implies $1 = \rho(g^n) = \rho(g)^n = w^n$. We thus find n one-dimensional irreducible representations with

$$\chi_h(g^k) = \exp(2\pi \mathrm{i} \frac{kh}{n}) \ ,$$

indexed by $h \in \mathbb{Z}/n\mathbb{Z}$. The characters are apparently orthogonal, as we have:

$$\frac{1}{n} \sum_{k=0}^{n-1} \mathrm{e}^{\frac{2\pi \mathrm{i} k}{n}(h-h')} = \ \delta_{h,h'}^{\bmod n\mathbb{Z}} \ .$$

For the tensor product of these representations we see $\chi_h \chi_{h'} = \chi_{h+h' \bmod n}$. In fact we have found all irreducible representations: in an abelian group all conjugacy classes have exactly one element. For a finite abelian group there are as many isomorphism classes of simple representations as group elements. The square sum of dimensions of the n one-dimensional representations equals the order of the group $|C_n| = n$.

3. The dihedral group D_n is defined as the symmetry group of the regular n-gon. It contains the rotations by multiples of $\frac{2\pi}{n}$ as cyclic subgroup of order n. Additionally it contains n reflections in lines. As generator we choose the rotation r by $\frac{2\pi}{n}$ and one reflection s. Then er have the relations

$$r^n = 1, \quad s^2 = 1 \quad \text{and} \ \ rs = sr^{-1} \ .$$

The group elements are all of the form r^k, sr^k with $k \bmod n$, and so there are $2n$ group elements.

Suppose that n is even. Then there exist four isomorphism classes of one-dimensional representations

	r^k	sr^k
ψ_1	1	1
ψ_2	1	-1
ψ_3	$(-1)^k$	$(-1)^k$
ψ_4	$(-1)^k$	$(-1)^{k+1}$

where k is taken modulo n. To find two-dimensional representations we choose a primitive nth root of unity $w := \exp(2\pi \mathrm{i}/n)$ and set for $h \in \mathbb{Z}$:

$$\rho^{(h)}(r^k) = \begin{pmatrix} w^{hk} & 0 \\ 0 & w^{-hk} \end{pmatrix} \qquad \rho^{(h)}(sr^k) = \begin{pmatrix} 0 & w^{-hk} \\ w^{hk} & 0 \end{pmatrix}$$

Clearly it suffices to consider h modulo n. Further, by exchanging the basis vectors e_1 and e_2 of the standard basis we get the isomorphism $\rho^{(h)} \cong \rho^{(n-h)}$. The representations $\rho^{(0)}$ and $\rho^{(n/2)}$ are decomposable because all matrices have the common eigenvectors $e_1 \pm e_2$. Thus we have the following decomposition into one-dimensional representations:

$$\rho^{(0)} \cong \psi_1 \oplus \psi_2 \quad \rho^{(n/2)} \cong \psi_3 \oplus \psi_4 \ .$$

For $0 < h < n/2$ the representations $\rho^{(h)}$ are irreducible, because the matrix $\rho^{(h)}(r)$ is diagonalizable with distinct eigenvalues but not simultaneously with $\rho^{(h)}(s)$. We thus get the additional characters

$$\chi_h(r^k) = 2 \cos \frac{2\pi kh}{n} \qquad \chi_h(sr^k) \ = 0 \quad \text{for} \quad h = 1, \ldots, n/2 - 1 \, .$$

One can check that these characters are all orthogonal in the sense of Theorem 4.6.11, which implies that the representations are pairwise non-isomorphic. By computing the square sum of dimensions

$$|D_n| \ = 2n = \ 4 \cdot 1^2 + (n/2 - 1) \cdot 2^2 \ ,$$

we deduce that we have found all $n/2 + 3$ isomorphism classes of irreducible representations. Also the number of conjugacy classes

$$\{e\}, \quad \{r^{n/2}\}, \quad \{r^k, r^{-k}\} \qquad k = 1, \ldots, \frac{n}{2} - 1$$

together with the two conjugacy classes of reflections in lines through edge bisectors resp. through corners $\{sr^i\}$ with i even resp. odd coincides with the number of isomorphism classes.

For odd n one finds only two one-dimensional representations and the character table

	r^k	sr^k
ψ_1	1	1
ψ_2	1	-1
χ_h	$2\cos\frac{2\pi kh}{n}$	0 with $0 < h < \frac{n}{2}$

In the case of odd n there exists only one conjugacy class of reflections.

4. The alternating group A_4 can be identified with the rotational symmetries of a regular tetrahedron, whose corners we number by $1, 2, 3, 4$. The 12 elements consist of

   - the neutral element,
   - three double transpositions

     $$x := (12)(34) \quad y := (13)(24) \quad z := (14)(23) \ ,$$

     which generate a normal subgroup $H \subset A_4$ isomorphic to the Klein four-group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Geometrically they correspond to rotations of the tetrahedron by π in an axis through the centres of opposite edges.
   - There also exist 8 cyclic permutations of order 3, which geometrically correspond to rotations by $\frac{2\pi}{3}$ in an axis through one of the four vertices and the centre of the opposite face.

   If we choose the rotation $t := (123)4$, then we find four conjugacy classes:

   $$\{1\} \quad \{x, y, z\} \quad \{t, tx, ty, tz\} \quad \{t^2, t^2x, t^2y, t^2z\} \ .$$

   Let $K := \{e, t, t^2\} \cong \mathbb{Z}/3\mathbb{Z}$ be a cyclic subgroup of A_4, then we find a short exact sequence of groups

   $$1 \to H \to A_4 \to K \to 1 \, ,$$

   in which the surjection onto K has kernel $\{1, x, y, z\}$.

   The characters of three one-dimensional irreducible representations can be found by pulling back the three irreducible characters of the cyclic group K. The fourth character we find via the orthogonality relations:

	1	3	4	4
	1	x	t	t^2
χ_0	1	1	1	1
χ_1	1	1	w	w^2
χ_2	1	1	w^2	w
ψ	3	-1	0	0

where w is a primitive third root of unity. It is straightforward to check the remaining orthogonality relations.

Finally we describe the irreducible three-dimensional representation: A_4 acts as subgroup of S_4 on $\mathbb{C}^4 = \mathbb{C}(e_1, e_2, e_3, e_4)$ by permuting the elements of the standard basis. The orthogonal complement of the trivial subrepresentation $\mathbb{C}(e_1 + e_2 + e_3 + e_4)$ is the sought-after three-dimensional irreducible representation.

Definition 4.6.17

1. The Quaternions are the real 4-dimensional associative unital algebra $\mathbb{H}$ with basis $1, \mathrm{i}, \mathrm{j}, \mathrm{k}$, for which the multiplication is determined on the basis elements by the relations

$$\begin{aligned} \mathrm{i}^2 &= \mathrm{j}^2 = \mathrm{k}^2 = -1 \\ \mathrm{ij} &= \mathrm{k}\,. \end{aligned}$$

2. An $\mathbb{H}$-module we will also call an $\mathbb{H}$-vector space or a quaternionic vector space.

The algebra $\mathbb{H}$ of quaternions is a skew field, or also called division algebra, because every $a_0 + a_1\mathrm{i} + a_2\mathrm{j} + a_3\mathrm{k} \in \mathbb{H} \setminus \{0\}$ has an inverse, $\frac{1}{\sum_i a_i^2}(a_0 - a_1\mathrm{i} - a_2\mathrm{j} - a_3\mathrm{k})$. A classical result of Frobenius says that there are only three finite-dimensional real division algebras: the fields $\mathbb{R}$ and $\mathbb{C}$ of real and complex numbers, as well as the quaternions.

The nomenclature "quaternionic vector space" is justified by the following theorem, which implies that all $\mathbb{H}$-modules are isomorphic to direct sums of a single irreducible $\mathbb{H}$-module.

Theorem 4.6.18 Let D be a division ring and V a finitely generated D-module. Then the ring $\mathrm{End}_D(V)$ is semisimple and all simple $\mathrm{End}_D(V)$-modules are isomorphic.

Proof. As in linear algebra one shows that V has a finite D-basis. Choose a D-basis $(e_1, \dots e_n)$ of V and consider

$$\begin{aligned} R := \mathrm{End}_D(V) &\to V \oplus \ldots \oplus V \\ f &\mapsto (f(e_1), \ldots, f(e_n))\ , \end{aligned}$$

which is a homomorphism of R-modules. Since a D-linear map can be uniquely determined by specifying values on a basis, the morphism is injective and surjective, thus an isomorphism of R-modules. Now since V is simple as $\mathrm{End}_D(V)$-module, and thus also semisimple, the ring $\mathrm{End}_D(V)$ is semisimple. By Theorem 4.3.10 every simple $\mathrm{End}_D(V)$-module is isomorphic to a submodule of $\mathrm{End}_D(V)$, i.e. isomorphic to V. Every $\mathrm{End}_D(V)$-module is thus a direct sum of simple $\mathrm{End}_D(V)$-modules, namely of copies of V. □

The following lemma establishes a connection to complex vector spaces:

Lemma 4.6.19 An $\mathbb{H}$-module is equivalent to a complex vector space V with an antilinear map J that satisfies $J^2 = -\mathrm{id}_V$.

Proof. Let V be a $\mathbb{H}$-module. We defined the action of the imaginary unit of $\mathbb{C}$ by acting with $\mathrm{i} \in \mathbb{H}$. This endows V with the structure of a complex vector space. Now set $J(v) = \mathrm{j}v$. The properties of J are easily checked.

Conversely, given a complex vector space V with an antilinear map J, then one defines the action of the quaternion i by the action of $\mathrm{i} \in \mathbb{C}$ and the action of j by the action J. The action of $\mathrm{k} = \mathrm{ij}$ is then determined. □

Theorem 4.6.20 Let G be a group and V a simple finite-dimensional representation of G over $\mathbb{C}$. Then exactly one of the following three cases applies:

(a) V is obtained from a simple real representation $V_{\mathbb{R}}$ by extension of scalars, i.e.

$$V = \mathbb{C} \otimes_{\mathbb{R}} V_{\mathbb{R}} = \mathrm{Ind}_{\mathbb{R}}^{\mathbb{C}}(V_{\mathbb{R}}) \ .$$

In this case we say that V is of real type.

(b) V is obtained from a simple quaternionic representation $V_{\mathbb{H}}$ on an $\mathbb{H}$-module by restriction of scalars onto $\mathbb{C} \subset \mathbb{H}$, i.e.

$$V = \mathrm{Res}_{\mathbb{C}}^{\mathbb{H}} \ V_{\mathbb{H}} \quad .$$

In this case we say that V is of quaternionic type.

(c) V is not isomorphic to $\overline{V}$. In this case we say that V is of complex type.

Proof. • If the representations V and $\overline{V}$ are not isomorphic, then by Schur's lemma 1.5.5 there are no nonzero G-intertwiners between them. If, on the other hand $V \cong \overline{V}$, then

$$\dim_{\mathbb{C}} \ \mathrm{Hom}_G(V, \overline{V}) = 1 \, .$$

For a nonzero homomorphism $J \in \mathrm{Hom}_G(V, \overline{V})$ we have

$$Jav = \overline{a} Jv \qquad \text{for all} \quad a \in \mathbb{C}, v \in V$$

i.e. J is antilinear. By applying the underlying $\mathbb{R}$-linear map twice, then we obtain a $\mathbb{C}$-linear map, to which we can apply Schur's lemma. Thus

$$J^2 = \lambda \mathrm{id}_V \quad \text{with } \lambda \in \mathbb{C}^\times \, ,$$

$$\lambda Jv = J^3 v = J(J^2 v) = J\lambda v = \overline{\lambda} Jv \, ,$$

which implies $\lambda = \overline{\lambda}$, and so $\lambda \in \mathbb{R}$. If we replace J by a complex multiple J', i.e. $J' = zJ$ with $z \in \mathbb{C}^\times$, then

$$(J')^2 = zJzJ = |z|^2 J^2 = |z|^2 \lambda \ \mathrm{id}_V \, .$$

In the case $V \cong \overline{V}$ we can thus find an antilinear G-isomorphism J with either (a) $J^2 = \mathrm{id}_V$ or (b) $J^2 = -\mathrm{id}_V$.

• In case (a) we consider the real vector subspace of J-fixed points $V^J \subset V$. The endomorphisms ρ_g commute with J and so V^J is a real G-representation:

$$J\rho_g v = \ \rho_g Jv = \ \rho_g v$$

and so we get for every $g \in G$ that $\rho_g v \in V^J$. The map

$$\begin{array}{rcl} V^J \otimes_{\mathbb{R}} \mathbb{C} & \to & V \\ v \otimes_{\mathbb{R}} (\lambda_1 + \mathrm{i}\lambda_2) & \mapsto & \lambda_1 v + \lambda_2 \mathrm{i} v \end{array}$$

with $\lambda_1, \lambda_2 \in \mathbb{R}$ is then an isomorphism of complex G-representations. (On the left-hand side G acts non-trivially only on V^J, but trivially on $\mathbb{C}$.) In case (b) the map J provides V with the structure of an $\mathbb{H}$-vector space by Lemma 4.6.19.

□

One can read off the type from the character table, cf. [S77, Proposition 39]: the expression $\frac{1}{|G|} \sum_{g \in G} \chi(g^2)$ takes the value 1 for real, -1 for quaternionic and 0 for complex representations.

5 Artinian and Noetherian modules

5.1 Noetherian modules

Let R be a unital ring.

Theorem 5.1.1 For a (left) R-module M the following are equivalent.

1. Every ascending chain $N_1 \subseteq N_2 \subseteq \cdots \subseteq N_k \subseteq N_{k+1} \subseteq \cdots$ of submodules of M becomes stationary, i.e. there exists an index k, such that $N_i = N_k$ for all $i \geq k$. We also say that M satisfies the ascending chain condition.

2. Every non-empty subset of submodules of M has a maximal element with respect to inclusion.

3. Every submodule of M is finitely generated.

Definition 5.1.2

- A left R-module M, that satisfies one (and thus all) conditions from Theorem 5.1.1 is called a Noetherian module.
- A ring R is called (left-)Noetherian, if it is Noetherian as left module over itself.
- Analogously one defines Noetherian right modules and right-Noetherian rings.
- A ring is called Noetherian, if it is both left- and right-Noetherian.

A left Noetherian ring is not automatically right-Noetherian. A counterexample will be discussed in the exercises.

Proof of Theorem 5.1.1.

(1) $\Rightarrow$ (2) Every non-empty set X of submodules satisfies the requirements of Zorn's lemma: let $N_1 \subseteq N_2 \subseteq \ldots$ be a chain in X, then $\bigcup_i N_i = N_k \in X$ is by (1) an upper bound for the family $\{N_i\}$. The existence of a maximal element thus follows from Zorn's lemma.

(2) $\Rightarrow$ (3) Let $N \subseteq M$ be a submodule. We consider the set

$$X := \{N' | N' \subseteq N \quad N' \text{finitely generated submodule of} M, \}$$

This set is non-empty because the it contains the zero module, $0 \in X$. Let $N_0 \in X$ be a maximal element. We claim that $N_0 = N$. Otherwise, for $x \in N \backslash N_0$, we would have $\langle N_0, x\rangle \in X$ and $\langle N_0, x\rangle \supsetneq N_0$, in contradiction to maximality of N_0.

(3) $\Rightarrow$ (1) Let $N_1 \subseteq N_2 \subseteq \cdots$ be a chain of submodules. The union $N' := \bigcup_i N_i$ is a submodule and finitely generated by (3), say $N' = \langle x_1, \ldots, x_r\rangle$. Now there exists a $k \in \mathbb{N}$ such that $x_i \in N_k$ for all $i = 1, \ldots, r$. Thus $N' \subseteq N_k$ and so the chain of submodules becomes stationary. □

Examples 5.1.3

1. If R is an algebra over a field K, then every R-module that is finite-dimensional over K is also Noetherian. If R is a finite-dimensional algebra over a field, then R is Noetherian.

2. Semisimple rings are Noetherian by Theorem 4.3.10

3. The submodules of a ring are its ideals. In the case of PIDs, these are generated by a single element, in particular they are all finitely generated. By Theorem 5.1.1 PIDs are thus Noetherian.

4. We give an example of a ring, that is not Noetherian:

$$\begin{aligned} R &= \{f(X) \in \mathbb{Q}[X] \mid f(0) \in \mathbb{Z}\} \\ &= \{m + Xg \mid m \in \mathbb{Z}, g \in \mathbb{Q}[X]\} \end{aligned}$$

Every subgroup G of $(\mathbb{Q}, +)$ defines an ideal

$$A_G := GX + X^2\mathbb{Q}[X]$$

of R. Consider for every $i \in \mathbb{N}$ the subgroup $G_i := \{\frac{m}{i} \mathfrak{m} m \in \mathbb{Z}\}$. Here we get an infinite ascending chain of ideals

$$A_{G_2} \subset A_{G_4} \subset A_{G_8} \subset \dots .$$

in R that does not become stationary. More examples of Noetherian rings will result from Corollary 5.1.7 below.

Theorem 5.1.4

1. Submodules and homomorphic images of Noetherian modules are Noetherian.

2. If U is a submodule such that U and M/U are Noetherian, then so is M.

Proof. 1. Let M be Noetherian and U a submodule of M. Every submodule U' of U is also a submodule of M, thus finitely generated. Thus the submodule U is also Noetherian by Theorem 5.1.1.

Let M' be a homomorphic image of M, i.e. $f\colon M \twoheadrightarrow M'$, so that $M' \cong M/\ker f$. Let V be a submodule of M' and $f^{-1}(V)$ its preimage under the surjection f. Then $f^{-1}(V)$ is a submodule of the Noetherian module M and thus finitely generated, say:

$$f^{-1}(V) = \langle v_1, \dots, v_r \rangle \quad \text{with } v_i \in M\,.$$

This implies

$$V = \langle v_1 + \ker f, \dots, v_r + \ker f \rangle\,,$$

and so V is also finitely generated. Thus the homomorphic image M' is Noetherian.

2. Let $N_1 \subseteq N_2 \subseteq \cdots$ be an ascending chain of submodules in M. Via the canonical surjection $p\colon M \twoheadrightarrow M/U$ we obtain an ascending chain of submodules in M/U

$$(N_1 + U)/U \subseteq (N_2 + U)/U \subseteq \cdots$$

and by intersecting with U an ascending chain of submodules in U:

$$N_1 \cap U \subseteq N_2 \cap U \subseteq \cdots$$

As both U and M/U were assumed to be Noetherian, there exists a $k \in \mathbb{N}$, such that

$$N_k + U = N_{k+1} + U = \cdots \qquad \text{and} \qquad N_k \cap U = N_{k+1} \cap U = \dots .$$

This implies $N_k = N_{k+1}$, because the stationary chain in the quotient implies that $x \in N_{k+1}$ can be written as $x = y + u$ with $y \in N_k$ and $u \in U$. Thus $u = x - y \in U \cap N_{k+1} = U \cap N_k \subset N_k$, which implies $x \in N_k$. □

Corollary 5.1.5 Finite direct sums of Noetherian modules are Noetherian.

Proof. Let U, V be Noetherian modules. Then also $(U \oplus V)/V \cong U$ is Noetherian. Now Theorem 5.1.4(2) implies that the direct sum $U \oplus V$ is Noetherian. □

Theorem 5.1.6 A module over a Noetherian ring is Noetherian if and only if it is finitely generated.

Proof. Every Noetherian module is finitely generated (since it is a submodule of itself). Conversely, let $M = \langle a_1, \ldots, a_r \rangle$ and let $F := R^r$. Consider the surjection

$$\begin{array}{rcl} F = R^r & \twoheadrightarrow & M \\ (\alpha_1, \alpha_2, \ldots, \alpha_r) & \mapsto & \sum_{i=1}^{r} \alpha_i a_i \end{array}$$

By Corollary 5.1.5 the direct sum R^r is Noetherian and by Theorem 5.1.4 (1) so is its homomorphic image M. □

Corollary 5.1.7

1. Finitely generated modules over PIDs are Noetherian.
2. The finitely generated abelian groups are the Noetherian $\mathbb{Z}$-modules.
3. Every subgroup of a finitely generated abelian group is finitely generated.

Proof.

1. Theorem 5.1.6 immediately implies that finitely generated modules over PIDs are Noetherian.
2. Since $\mathbb{Z}$ is a PID, this is a special case of (1).
3. Follows from Theorem 5.1.1, as a subgroup of an abelian group is also a $\mathbb{Z}$-submodule.

□

Theorem 5.1.8 [Hilbert's basis theorem] Let R be a commutative ring. If R is Noetherian, then so is the polynomial ring $R[X]$.

Proof. Let $I \subset R[X]$ be an ideal. Let $\mathfrak{a}_i \subset R$ be the ideal generated by the leading coefficients of all polynomials of degree i in the ideal I. The multiplication with the monomial X shows the following inclusion of ideals of R:

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots \mathfrak{a}_i \subseteq \mathfrak{a}_{i+1} \subseteq \ldots .$$

For this ascending chain of ideals in the Noetherian ring R there exists a j, such that

$$\mathfrak{a}_j = \mathfrak{a}_{j+1} = \ldots .$$

Each of the finitely many ideals $\mathfrak{a}_i$ with $i \leq j$ is finitely generated since R is Noetherian, see Theorem 5.1.6. Now we can choose finitely many polynomials from I, whose leading coefficients generated all ideals $\mathfrak{a}_i$ of R.

We claim that these finitely many polynomials generate the ideal I in the polynomial ring: let $p \in I$ of degree n, then we find $\alpha_i \in R$ with associated polynomial p_i, such that p and the polynomial $\sum_i \alpha_i X^{n_i} p_i$ have the same leading coefficient. The difference $p - \sum_i \alpha_i X^{n_i} p_i$ has degree less or equal than $n-1$. One now proceeds by induction to find that p is contained in the ideal generated by the polynomials p_i.

□

5.2 Artinian modules

Artinian modules behave similarly to Noetherian modules. We keep their discussion brief.

Definition 5.2.1

1. An R-module is called Artinian, if for every descending chain $M_0 \supset M_1 \supset M_2 \cdots$ of submodules in M there exists an index n, such that $M_i = M_n$ for all $i \geq n$. We say that M satisfies the descending chain condition.

2. A ring is called left-Artinian, if it is Artinian as a left module over itself.

3. Analogously one defines Artinian right modules and right-Artinian rings.

4. A ring is called Artinian, if it is both left- and right-Artinian.

Examples 5.2.2

1. If R is an algebra over a field K, then every R-module that is finite-dimensional over K, is also Artinian. If R is a finite-dimensional algebra over a field, then R is Artinian.

2. The ring $\mathbb{Z}$ is not Artinian, as shown by the chain $\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset \cdots$. For every positive $n \in \mathbb{Z}$ is the ring $\mathbb{Z}/n\mathbb{Z}$ is finite and thus Artinian. (Note that the ring $\mathbb{Z}$ is Noetherian, as it is a PID.)

One can show:

Theorem 5.2.3

1. Let M be an R-module and N a submodule of M. Then M is Artinian if and only if M/N and N are Artinian.

2. Let $M_1, M_2, \ldots, M_r$ be modules over R. Then the direct sum $\oplus_{i=1}^{r} M_i$ is Artinian if and only if all summands M_i are Artinian.

3. Every finitely generated module over a left-Artinian ring is Artinian.

Remark 5.2.4

- Note that an R-module is finitely generated if and only if for every family $(M_i)_{i\in I}$ of submodules with $\sum_{i\in I} M_i = M$ there exists a finite subset $J \subset I$, such that $M = \sum_{j\in J} M_j$. If M is finitely generated, $M = \langle x_1, \ldots x_r\rangle$, then we find submodules M_i with $x_i \in M_i$ and so $M = \sum_{i=1}^{r} M_i$. For the converse we use that $M = \sum_{m\in M} Rm$ and we can find a finite subset of M that generates M.

- Dually one now defines: An R-module M is called finitely cogenerated, if for every family $(M_i)_{i\in I}$ of submodules with $\cap_{i\in I} M_i = 0$ there exists a finite subset $J \subset I$ with $\cap_{j\in J} M_j = 0$.

- If N is a submodule of an R-module M, then the definition implies that the quotient module M/N is finitely cogenerated if and only for every family $(M_i)_{i\in I}$ of submodules of M with $\cap_{i\in I} M_i = N$ there exists a finite subset $J \subset I$ with $\cap_{j\in J} M_j = N$.

Theorem 5.2.5 Let M be an R-module. Then the following statements are equivalent:

1. M is Artinian.

2. Every non-empty set of submodules of M contains a minimal element with respect to inclusion.

3. Every quotient module of M is finitely cogenerated.

Proof.

(1) $\Rightarrow$ (2) is proved analogously to the corresponding statement (1) $\Rightarrow$ (2) in Theorem 5.1.1 for Noetherian modules.

(2) $\Rightarrow$ (3) Let N and $(M_i)_{i\in I}$ be submodules of M with $N = \cap_{i\in I} M_i$. Set $X = \{\cap_{j\in J} M_j | J \subset I \text{ finite}\}$. By assumption X contains a minimal element N_1. Then we have $N_1 \supset N$. If this were a proper inclusion, then we could find an $x \in N_1 \setminus N$. By $N = \cap_{i\in I} M_i$ there would exists an $i \in I$ with $x \notin M_i$, and so $x \notin N_2 = N_1 \cap M_i$. We thus have $N_2 \in X$ and $N_2 \subsetneq N_1$: a contradiction!

(3) $\Rightarrow$ (1) For a descending chain $M_0 \supset M_1 \supset M_2 \supset \cdots$ of submodules of M we set $N := \cap_{i\in\mathbb{N}} M_i$. As M/N is finitely cogenerated, there exists a finite subset $J \subset \mathbb{N}$ with $N = \cap_{j\in J} M_j$. Setting $n := \max(J)$, then we get $N = M_n$, and so $M_i = M_n$ for all $i \geq n$. □

We finally state without proof the following theorem of Hopkins: A left-Artinian ring is also left-Noetherian. (The converse is false, with the ring $\mathbb{Z}$ providing a counterexample.)

Definition 5.2.6
A ring R is called a simple, if it has no non-trivial two-sided ideals, i.e. no ideals except 0 and R itself.

Warning: a ring that is simple as a module over itself, is a simple ring. The submodules are exactly the left ideals, and the module has no non-trivial submodules. Thus there are no non-trivial left ideals, hence also no non-trivial two-sided ideals. The converse is false: there exist simple rings that are not simple as modules over themselves. For example, the ring $M(n\times n, K)$ of $n \times n$ matrics over a field K is simple, but not simple as a module over itself: it is a direct sum of n simple modules of dimension n.

Theorem 5.2.7 For a ring R the following are equivalent

1. R is a simple Artinian ring.
2. R is isomorphic to a matrix ring over a division ring.
3. R is semisimple and all simple R-modules are isomorphic.
4. R is semisimple as R-module and in the decomposition of the left module R one only finds a single isomorphism class of simple modules.
5. R is Artinian and has a faithful simple module.

Proof. We will only prove the implications (5) $\Rightarrow$ (4) and (1) $\Rightarrow$ (5). The others are simple consequences of definitions and the Artin–Wedderburn Theorem 4.4.3.

(5) $\Rightarrow$ (4) Consider for the faithful module M and for all n all R-module homomorphisms

$$R \to M^n \ .$$

The kernels of such morphisms are (left-)ideals of R; as R is Artinian, we can choose a morphism f with minimal kernel.

We show that this f must be injective. If $r \in R \setminus \{0\}$ with $f(r) = 0$, then we could use the faithful module M to find an $m \in M$ with $r.m \neq 0$. But then

$$\begin{array}{rcl} R & \to & M^n \oplus M \\ r & \mapsto & (f(r), r.m) \end{array}$$

would have strictly smaller kernel than f, in contradiction the minimality of the kernel of f. Now we have found R as a submodule of the homogenous (i.e. consisting of a single non-trivial isotypic component) semisimple module M^n, so it is itself homogenous and semisimple.

(1) $\Rightarrow$ (5) For every R-module M the annihilator $\mathrm{Ann}(M)$ is a two-sided ideal. As R is simple and $1 \notin \mathrm{Ann}(M)$ for a non-zero R-module M, the annihilator must vanish and thus every non-zero R-module is faithful.

As R is Artinian, simple modules exist: every descending chain of ideals becomes stationary and the smallest appearing ideal is a simple module. □

Corollary 5.2.8 Let K be a field and R a K-algebra. Let M be a simple R-module with $\dim_K M < \infty$, for which we have $\mathrm{End}_R(M) = K\mathrm{id}_M$. (For example, this is always the case if K is algebraically closed.) Then the structure map

$$\begin{array}{rcl} R & \to & \mathrm{End}_R(M) \\ r & \mapsto & r\mathrm{id}_M \end{array}$$

is surjective.

Proof. We factor the structure map

$$\begin{array}{ccc} R & \longrightarrow & \mathrm{End}_R(M) \\ \downarrow & \nearrow & \\ R/\mathrm{Ann}(M) & & \end{array}$$

Here M is a faithful $R/\mathrm{Ann}(M)$-module, such that the map $R/\mathrm{Ann}(M) \to \mathrm{End}_K(M)$ is injective. Thus $R/\mathrm{Ann}(M)$ is a finite-dimensional K-algebra and thus Artinian. Hence $R/\mathrm{Ann}(M)$ is an Artinian ring that is simple since M is a simple module. By Theorem 5.2.7.2 we have $R/\mathrm{Ann}(M) \cong \mathrm{End}_K(M)$.

Alternatively, we can use the Jacobson density theorem Theorem 4.5.1. Let $f \in \mathrm{End}_K(M) = \mathrm{End}_{\mathrm{End}_R(M)}(M)$. Let $m_1, \ldots m_n$ be afinite basis of the K-vector space M. The density Theorem 4.5.1 implies that there is $x \in R$ such that $x.m_i = f(m_i)$ for all $i = 1, \ldots, n$. Since a K-linear map is uniquely determined on a basis, f is in the image of the map $R \to \mathrm{End}_K(M)$. □

Here is a consequence:

Corollary 5.2.9 Let K be a field and R a simple, finite-dimensional K-algebra, $\dim_K R = n$, whose centre is $K1_R$. Then we have an isomorphism of rings:

$$R \otimes_K R^{\mathrm{opp}} \cong M(n \times n, K) \ .$$

Proof. We may consider R as an $R - R$-bimodule and, equivalently, as $R \otimes_K R^{\mathrm{opp}}$-module. The two-sided ideals are precisely the $R \otimes_K R^{\mathrm{opp}}$-submodules, and since R is a simple ring, it is also simple as $R \otimes_K R^{\mathrm{opp}}$-module. Now we have

$$\begin{array}{rcl} \mathrm{End}_{R \otimes_K R^{\mathrm{opp}}} R & \to & Z(R) \\ f & \mapsto & f(1) \ , \end{array}$$

since $r.f(1) = f(r \cdot 1) = f(1 \cdot r) = f(1).r$ for all $r \in R$. We thus have the isomorphism

$$\mathrm{End}_{R \otimes_K R^{\mathrm{opp}}} R \cong Z(R) \cong K \ .$$

By the previous corollary we get that

$$R \otimes_K R^{\mathrm{opp}} \to \mathrm{End}_K(R) \cong M(n \times n, K)$$

is surjective. The image and preimage are K-vector spaces of the same dimension n^2, thus the map is even an isomorphism. $\square$

6 Resolutions and derived functors

In an abelian category, the functor $\mathrm{Hom}(U,-)$ is exact if and only if U is a projective object; similarly $\mathrm{Hom}(-,U)$ is exact if and only if U is an injective object. The functor $U\otimes -$ is exact exactly for the flat objects in an abelian tensor category. We now aim to study these functors on general objects.

6.1 Projective and injective resolutions

Definition 6.1.1

1. An abelian category $\mathcal{C}$ has enough projective objects, if for every object $M\in\mathcal{C}$ there exists an epimorphism $P\to M\to 0$ from a projective object P.

2. It has enough injective objects, if for every object M there exists a monomorphism $0\to M\to I$ into an injective object I.

Examples 6.1.2

1. For every ring R, the category $R-$Mod has enough projective and injective objects. This is a consequence of the fact that every module is a submodule of a cofree module and the image of a free module, cf. Theorem 3.3.4.

2. The category Ab_{fin} of *finite* abelian groups has no projective or injective objects whatsoever, in particular not enough.

   Here we have to be careful: Ab_{fin} is a full subcategory of Ab, but in general the projective or injective objects of a subcategory are not simply the projective or injective objects, the happen to lie in the subcategory. For example, every vector space over the field $\mathbb{Z}/2\mathbb{Z}$ is an abelian group and every linear map is a group homomorphism. Thus $\mathrm{vect}_{\mathbb{Z}/2\mathbb{Z}}\subset\mathrm{Ab}$ is a subcategory. Every vector space is free and thus projective. In particular, $\mathbb{Z}/2\mathbb{Z}$ is projective in $\mathrm{vect}_{\mathbb{Z}/2\mathbb{Z}}$, but not in Ab.

   To see this we argue that for every $n\in\mathbb{N}$ the short exact sequence

   $$0\to\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/n^2\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}\to 0$$

   does not split. Thus the cyclic group $\mathbb{Z}/n\mathbb{Z}$ is neither projective nor injective. According to Corollary 4.2.4, every finite abelian group A can be written as $A=\bigoplus\mathbb{Z}/n_i\mathbb{Z}\equiv\prod\mathbb{Z}/n_i\mathbb{Z}$. As a sum (product) of non-projective (non-injective) modules it is non-projective (non-injective) in the category the finite abelian groups by Lemma 3.3.1.

3. The category of finitely generated abelian groups has enough projective objects (the free abelian group on a finite generating set is projective and maps surjectively onto such a group), but no injective objects. According to Corollary 4.2.4 any finitely generated abelian group A can be written as a finite product $\prod\mathbb{Z}/n_i\mathbb{Z}\times\mathbb{Z}^n$. By Lemma 3.3.1 it is injective in Ab, if every factor if injective. By Corollary 1.4.16 the injective abelian groups are exactly the divisible abelian groups; but the factors $\mathbb{Z}$ and $\mathbb{Z}/n_i\mathbb{Z}$ are not divisible. (Note that the coregular module is not finitely generated.)

Definition 6.1.3 Let M be an object in an abelian category $\mathcal{C}$.

1. A projective resolution of M is an exact sequence

   $$\cdots\to P_i\to P_{i-1}\to\cdots\to P_1\to P_0\to M\to 0$$

   in which all objects (except M) are projective. The surjective morphism $P_0\to M$ is known as the augmentation.

2. An injective resolution is an exact sequence

$$0 \to M \to Q_0 \to Q_1 \to \cdots \ ,$$

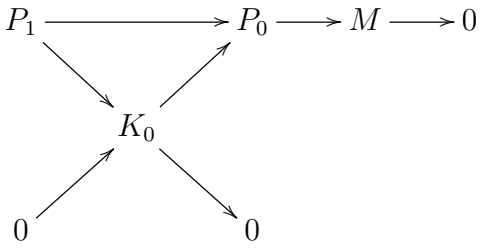
in which all objects Q_i are injective.

Free resolutions are special cases of projective resolutions. We have already seen in Observation 4.1.3 that modules over PIDs admit free resolutions of length 1:

$$0 \to F_1 \to F_0 \to M \ \to 0 \ .$$

Lemma 6.1.4 If a category $\mathcal{C}$ has enough projectives, then every object of $\mathcal{C}$ has a projective resolution. If $\mathcal{C}$ has enough injectives, then every object has an injective resolution.

Proof. We only prove the statement for projective resolutions; the statement for injective resolutions is the corresponding statement in $\mathcal{C}^{\mathrm{opp}}$. First we note that there exists an epimorphism $P_0 \to M \to 0$, as $\mathcal{C}$ has enough projectives. Let $K_0 := \ker(P_0 \to M)$. The object K_0 is in general not projective, but we can find an epimorphism $P_1 \to K_0$ from a projective object P_1. The resulting sequence



is exact. Iterating this procedure, one obtains a projective resolution. □

Remark 6.1.5 To motivate the appearance of resolutions, we start by discussing systems of linear equations. In contrast to linear algebra, the coefficients of the equations will now be elements of a K-algebra A, where K is a commutative ring. Thus let $B \in M(q \times p, A)$ a matrix with entries in A.

The solutions we are interested in are p-tuples $(u_j)_{j=1,\dots p}$ of elements in an arbitrary left A-module S. Indeed, in

$$(*) \qquad \sum_{j=1}^{p} B_{ij} u_j = v_i \quad \text{with} \quad i = 1, \dots, q \ .$$

Here $B_{ij}u_j$ is the left action of the element $B_{ij} \in A$ on the element u_j in the A-module S. The inhomogeneity $(v_j)_{j=1,\dots q}$ is an element in the A-module S^q.

Such a situation is realized in the following examples.

- Let K to be a field and $A = K[X_1, \dots, X_s]$ the polynomial ring over K in several indeterminates. We endow $S = K^n$ with the structure of an A-module as follows: any choice of s-tuples $(q_1, \dots, q_s) \in K^s$ gives an evaluation morphism $ev_{(q_1,\dots,q_s)} : A = K[X_1, \dots, X_s] \to K$. Pulling back the K-module structure on $S = K^n$ along this evaluation, we obtain an A-module structure on K^n. The homogeneous linear system $(*)$ is then a system of linear equations depending polynomially on s parameters in K.

- In another example we take $K = \mathbb{R}$ and A the algebra of real-valued smooth functions on a smooth manifold X. If X is compact, thenby the Serre-Swann theorem finitely generated projective A-modules are exactly the spaces of smooth sections in vector bundles over X. Let B be a linear differential operator (for example the Laplace operator if the manifold X has a metric). Then we are looking for solutions of inhomogeneous system of linear differential equations $Bu = v$.

We now describe the situation in terms of resolutions. To encode the matrix B, we observe that its action by right multiplication gives a morphism of free left A-modules

$$F_1 = A^q \xrightarrow{\cdot B} F_0 = A^p \ .$$

We form the quotient module $M := F_0/\mathrm{Im}\, B$ which comes with a canonical surjection $\psi\colon A^p \to M$. We obtain an exact sequence

$$F_1 = A^q \xrightarrow{B} F_0 = A^p \xrightarrow{\psi} M \to 0 \ .$$

1. We are in a first step interested in solutions of the homogeneous system associated to $(*)$ with values in an arbitrary A-module S. Apply the contravariant left-exact functor $\mathrm{Hom}_A(-, S)$ to this exact sequence to get the new exact sequence

   $$0 \to \mathrm{Hom}_A(M, S) \to S^p \xrightarrow{B\cdot} S^q \ ,$$

   where B now acts by left multiplication. We see that for any A-module S, the K-module $\mathrm{Hom}_A(M, S)$ is isomorphic to the kernel of B. and thus equal to the space of solutions of the homogeneous systems of equations to $(*)$ with values in the module S.

   The quotient module $M = A^p/A^qB$ can thus be considered as a "coordinate-free" version of the homogeneous linear system to $(*)$: the homomorphisms from the quotient module M into a module S is the space of solutions of the homogeneous system for the module S. Note that after choosing the standard basis $(e_i)_{i=1,\dots p}$ of A^p and setting $u_i := \psi(e_i) \in M$, the module M has generators $(u_i)_{i=1,\dots p}$ which obey the relations $\sum_{j=1}^p B_{ij}u_j$ for $i = 1, \dots, q$.

2. We now assume that A is left-Noetherian. For example, this is the case for the polynomial ring $A = K[X_1, \dots, X_s]$ over a field K. As a submodule of a finitely generated module, $\ker B$ is then finitely generated. This allows us to find a finitely generated free module $F_2 = A^r$ and a surjection $F_2 \to \ker B$. We extend the exact sequence above to find

   $$(**) \qquad F_2 \xrightarrow{X} F_1 = A^q \xrightarrow{B} F_0 = A^p \to M \to 0$$

   an exact sequence finitely generated free modules. Iterating, we find a free and thus, in particular, projective resolution of M.

   Again, we apply the left-exact contravariant functoir $\mathrm{Hom}_A(-, S)$ to obtain a chain complex

   $$0 \to \mathrm{Hom}_A(M, S) \to S^p \xrightarrow{B\cdot} S^q \xrightarrow{X\cdot} S^r$$

   of K-modules. A necessary condition for the inhomogeneous linear system $(*)$ with inhomogeity $(u_j)_{j=1,\dots q}$ to have solution is that v is in the image of B. Exactness implies that this is equivalent to $Xv = 0$. We have thus characterized the inhomogenuous terms for which solutions exist by a linear condition.

3. It remains to describe the solutions of the homogeneous system using the complex $(**)$.

   The images of r generators of F_2 are generators for the space of solutions of the homogeneous system $Bu = 0$ in F_0. Over rings, in contrast to fields, this is typically an over-parametrization: in general, the free resolution continues:

   $$\cdots F_3 \to F_2 = R^r \xrightarrow{X} F_1 = R^q \xrightarrow{B} F_0 = R^p \to R^p/BR^q \to 0 \ .$$

   The elements of the module F_3 describe dependencies between parametrizations; they are called syzygies. One can show that for the ring $K[X_1, \dots, X_s]$ the free resolution can be chosen to terminate after s steps. For a PID such as $K[X]$ we already know from Observation 4.1.3, that free resolutions of length 1 exist.

6.2 Homology and homotopy

We denote by $Ch_{\mathcal{C}}$ the category of chain complexes in an abelian category $\mathcal{C}$. Chain complexes were introduced in Definition 1.4.1. The morphisms in $Ch_{\mathcal{C}}$ are the "ladders" of morphisms in $\mathcal{C}$, i.e. commutative diagrams

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

that are called chain maps.

Remarks 6.2.1

1. There exist interesting (full) subcategories: e.g. the chain complexes supported in non-negative or non-positive degrees, or the bounded chain complexes, for which only finitely many objects C_i are nonzero in the abelian category $\mathcal{C}$. For simplicity we will denote all differentials in a chain complex by the symbol d in what follows.

2. In an exercise we will see that the category $Ch_{\mathcal{C}}$ is abelian.

Definition 6.2.2

1. Let $(C_\bullet, d_\bullet) \in Ch_{\mathcal{C}}$. The i-cycles are defined as $Z_i(C_\bullet, d_\bullet) := \ker(d_{i-1}) \subset C_i$.

2. The i-boundaries $B_i(C_\bullet, d_\bullet)$ are defined as the image of d_i in C_i.

3. The image B_i is a subobject of the chains C_i. By the chain complex condition $d^2 = 0$, the composite of inclusion $B_i \xrightarrow{\iota} C_i$ and the differential $C_i \xrightarrow{d} C_{i-1}$ vanishes. The inclusion hence factors over the kernel Z_i of d

$$\begin{array}{ccccc} B_i & \xrightarrow{\iota} & C_i & \xrightarrow{d} & C_{i-1} \\ & \searrow & \uparrow{\scriptstyle \ker d} & & \\ & & Z_i & & \end{array}$$

   with a monomorphism. The boundaries are thus a subobject of the cycles. The ith homology of the complex $C_\bullet$ is defined as the cokernel of this monomorphism.

   By realizing the abelian category explicitly as full subcategory of a category of modules over a ring, then we can compute with elements. The cycles in Z_i are exactly the elements

$$Z_i := \{c_i \in C_i \,|\, d_{i-1}c_i = 0\}$$

   and the boundaries

$$B_i := \{c_i \in C_i \,|\, \exists\, b_{i+1} \in C_{i+1} \text{ such that } d_i b_{i+1} = c_i \ \} \ .$$

   Then boundaries are, in particular, cycles because $c_i = d_i b_{i+1}$ implies $d_{i-1}c_i = d_{i-1} \circ d_i b_{i+1} = 0$. The homology is then the quotient

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

4. A chain complex $C_\bullet$ is called acyclic , if $H_n(C_\bullet) = 0$ holds for all $n \geq 1$. (This terminology is typically used in cases when $C_n = 0$ for $n < 0$. It then says that the complex has trivial homology, except possibly in degree zero.)

Remarks 6.2.3

1. For every $n \in \mathbb{Z}$ the assignment $H_n \colon Ch_{\mathcal{C}} \to \mathcal{C}$ is a functor, because every morphism of chain complexes maps kernels of d auf kernels of d and images of d to images of d. For a chain map f, one typically also writes f_n instead of $H_n(f)$ for the induced map.

2. Let $P_\bullet \to M \to 0$ be a projective resolution of an object $M \in \mathcal{C}$. Then the complex $P_\bullet \to 0$ is acyclic. It zeroth homology is $P_0/(\mathrm{Im}\,(P_1 \to P_0) = P_0/\ker(P_0 \to M) \cong M$, since $P_0 \to M$ is surjective.

3. Let $C_\bullet$ be a chain complex, concentrated in non-negative degrees, i.e. one that ends with $\ldots \to C_1 \to C_0 \to 0$. Then we have $H_0(C_\bullet) = C_0/\mathrm{Im}\,(C_1 \to C_0)$ and the canonical surjection provides a surjective morphism $C_0 \to H_0(C_\bullet)$. Then one can form the so-called augmented complex

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

   which is exact if and only if $C_\bullet$ is acyclic.

4. The notions of cycles and boundaries come from topology. There the differential $d_\bullet$ can often be interpreted as taking the geometric boundary of an object, e.g. of a manifold, and a cycles is an object without boundary.

5. Consider a ring R and an element $x \in R$. Then right multiplication by x defines the differential in a chain complex

$$0 \to R \xrightarrow{\cdot x} R \to 0.$$

   Here we have $H_0(C_\bullet) = R/R.x$ and $H_1(C_\bullet) = \{r \in R | r.x = 0\} = \mathrm{Ann}(x)$.

6. For a slightly more complicated example we consider two elements $a, b \in R$ of a commutative ring R and the complex

$$0 \longrightarrow R \xrightarrow{X} R^2 \xrightarrow{A} R \longrightarrow 0$$

   with matrices

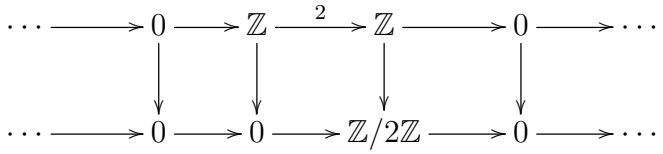
$$A = (a, b) \quad \text{and} \quad X = \begin{pmatrix} -b \\ a \end{pmatrix}$$

   Here we have $H_0(C_\bullet) = R/(ax + by)$ a measure to what extent the inhomogeneous linear equation $ax + by = c$ is solvable. The homology $H_1(C_\bullet) = \{(r_1, r_2) \in R^2 | r_1 a + r_2 b = 0\}/\{(-\lambda b, \lambda a)\}$ is the space of solutions of the homogeneous linear equation modulo the trivial solutions.

7. In some contexts it is usual to reverse the grading of chain complexes, i.e. with the differential mapping from C_i to C_{i+1}, and to call the resulting homology cohomology instead. For simplicity we do not reverse differentials and instead define the cohomology as $H^i(C_\bullet, d_\bullet) := H_{-i}(C_\bullet, d_\bullet)$ and also $C^i = C_{-i}$.

8. Note that a complex is exact if and only if its homology vanishes. The homology measures the failure of exactness.

9. It is possible that a map between two chain complexes is not an isomorphism, but that it induces an isomorphism upon passing to homology. Here is an example for $\mathcal{C} = Ab$:



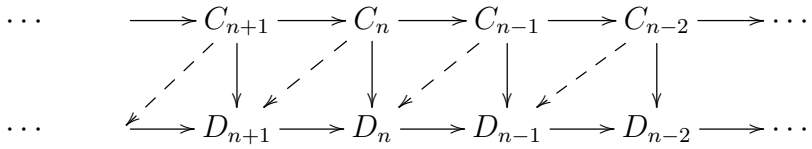
Degree	2	1	0	−1

In both cases is $H_0 = \mathbb{Z}/2\mathbb{Z}$, and all other homology groups vanish. A morphism of chain complexes $f_\bullet \colon C_\bullet \to D_\bullet$, that induces an isomorphism $H_n(f) \colon H_n(C_\bullet) \xrightarrow{\sim} H_n(D_\bullet)$ in every degree $n \in Z$, is called a quasi-isomorphism of complexes.

A subclass of quasi-isomorphisms is given by the chain homotopy equivalences.

Definition 6.2.4

1. Let $f, g \colon C_\bullet \to D_\bullet$ be two chain maps. A sequence of maps $h_n \colon C_{n-1} \to D_n$ with the property
$$f - g = h \circ d + d \circ h$$
is called (chain-)homotopy from g to f. Graphically:



where the vertical arrows are $(f-g)_n$ and the diagonal arrows are h_n. Note that this should *not* be read as a commutative diagram. If there exists a chain homotopy between f and g, then the two maps are called (chain) homotopic and we write $f \simeq g$.

2. If $f \colon C_\bullet \to D_\bullet$ and $g \colon D_\bullet \to C_\bullet$ are chain maps with the property $f \circ g \simeq \mathrm{id}_{D_\bullet}$ and $g \circ f \simeq \mathrm{id}_{C_\bullet}$, then we say the complexes $C_\bullet$ and $D_\bullet$ are (chain) homotopy equivalent and write $C_\bullet \simeq D_\bullet$. This defines an equivalence relation on chain complexes.

Remarks 6.2.5

1. A chain homotopy is not a chain map, already for degree reasons.

2. The following considerations give a hint why it makes sense to introduce chain homotopies. We consider only consider chain complexes $C_\bullet$ and $D_\bullet$ of modules, that are concentrated in degrees 1 and 0. We associate to the chain complex $C_\bullet$ the category $\mathcal{C}(C_\bullet)$ whose objects are the elements of C_0 and with morphisms $\mathrm{Hom}(c', c) := \{c_1 \in C_1 \mid dc_1 = c - c'\}$. The composition of morphisms is the addition in C_1.

   Then every chain map $f \colon C_\bullet \to D_\bullet$ defines a functor
$$\mathcal{C}(f) \colon \mathcal{C}(C_\bullet) \to \mathcal{C}(D_\bullet)$$
   This maps the object $c_0 \in C_0$ to the object $f(c_0) \in D_0$ and the morphism $c_0' \xrightarrow{c_1} c_0$ to $f(c_0') \xrightarrow{f(c_1)} f(c_0)$. Indeed, we have $f(c_1) \in \mathrm{Hom}\,(f(c_0), f(c_0'))$ since
$$df(c_1) = f(dc_1) = f(c_0 - c_0') = f(c_0) - f(c_0') \quad .$$

Let $f, g\colon C_\bullet \to D_\bullet$ be chain maps. A chain homotopy $h\colon g \rightsquigarrow f$ yields a a natural transformation $\mathcal{C}(h)\colon \mathcal{C}(g) \Rightarrow \mathcal{C}(f)$. The only non-zero component for such short chain complexes is $h_0\colon C_0 \to D_1$. By

$$f(c_0) - g(c_0) = h_{-1}(dc_0) + dh_0(c_0) = dh_0(c_0)$$

we have $h_0(c_0) \in \mathrm{Hom}(g(c_0), f(c_0))$. Furthermore, for a morphism $c_1 \in \mathrm{Hom}(c_0', c_0)$ the equation

$$f(c_1) - g(c_1) = h_0(dc_1) + dh_1(c_1) = h_0(dc_1) = h_0(c_0) - h_0(c_0')$$

implies the commutativity of the following diagram in $\mathcal{C}(D_\bullet)$

$$\begin{array}{ccc} g(c_0') & \xrightarrow{g(c_1)} & g(c_0) \\ {\scriptstyle h_0(c_0')}\downarrow & & \downarrow{\scriptstyle h_0(c_0)} \\ f(c_0') & \xrightarrow[f(c_1)]{} & f(c_0) \end{array}$$

Theorem 6.2.6

1. Chain homotopic maps induce the same map in homology.
2. Chain homotopy equivalences induce isomorphisms in homology.

Proof. Clearly the second statement follows immediately from the first one and Definition 6.2.4.2.

Let h be a chain homotopy. We have to show that $\hat{h} := (h \circ d + d \circ h)$ induces the zero map in homology. Restricting $\hat{h}_n$ to the cycles, we get: $\hat{h}_{|\ker d} = d \circ h$. This implies $\hat{h}_{|\ker d} \subseteq \mathrm{Im}\, d$ and thus $\hat{h}_* = 0$ in homology. □

In the Example 6.2.3.9 we have seen a chain map that induces an isomorphism in homology, i.e. a quasi-isomorphism. However, this chain map is *not* a chain homotopy equivalence: all chain maps from the lower complex to the upper complex are zero, so there cannot be an inverse up to homotopy.

6.3 The fundamental lemma of homological algebra

The following statement is central for the entire subject of homological algebra:

Theorem 6.3.1 Let $f\colon M \to N$ be a morphism in an abelian category, $P_\bullet \to M \to 0$ a chain complex of projective objects, and $N_\bullet \to N \to 0$ an arbitrary exact sequence.

1. Then there exists a extension $f_\bullet\colon P_\bullet \to N_\bullet$ of f to a morphism of chain complexes.
2. Any two such extensions $f_\bullet, f_\bullet'$ are chain homotopic.

Analogous statements hold for injective resolutions.

Proof. • Consider the diagram

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

As P_0 is projective, there exists a extension of the morphism $f \circ d$ to $P_0 \to N_0$, such that the resulting diagram commutes. This extension is typically not unique. Let $M' \subset P_0$ denote the kernel of the upper horizontal map, i.e. the kernel of the differential, and $N' \subset N_0$ the kernel of the lower map, then we consider the restriction of the map $P_0 \to N_0$ to M'. Let $x \in \ker d = M'$, then we have $df_0(x) = f_1(dx) = f_1(0) = 0$, thus by restriction to $\ker d$ we obtain a map $f' \colon M' \to N'$. Thus we have a new diagram

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

in which the lower row is again exact. Since P_1 is projective by assumption, we can proceed in the same fashion and obtain a morphism $P_1 \to N_1$. Inductively we find an extension of f over the entire resolutions.

- For the second part of the statement it is sufficient to show that every lift $f_\bullet$ of the zero map $M \xrightarrow{0} N$ 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:

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

Since $d \circ f_0 = 0 \circ d = 0$, the map f_0 gives a morphism $P_0 \to \ker(N_0 \to N)$. By exactness of the sequence $N_\bullet$ the morphism $N_1 \to \ker(N_0 \to N)$ is surjective. In the diagram

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

the projectivity of P_0 allows us to find a lift $h_0 \colon P_0 \to N_1$ over $N_1 \to \ker(N_0 \to N) \to 0$, such that $d \circ h_0 = f_0$. Similarly as before we can now repeat the argument for the morphism $f_1 - h_0 \circ d$:

$$\begin{array}{ccccccccc} & & P_1 & \xrightarrow{d} & P_0 & & & & \\ & \swarrow & \downarrow{\scriptstyle f_1} & {\scriptstyle h_0} \swarrow & \downarrow{\scriptstyle f_0} & & & & \\ N_2 & \xrightarrow[d]{} & N_1 & \xrightarrow[d]{} & \ker d & \longrightarrow & 0 & & \end{array}$$

Note that in the square only the lower triangle commutes! Then we have $d \circ (f_1 - h_0 \circ d) = d \circ f_1 - f_0 \circ d = 0$. Using this we can lift $f_1 - h_0 \circ d$ to a map h_1 with target N_2, such that $d \circ h_1 + h_0 \circ d = f_1$. Iterating the construction completes the proof. □

Corollary 6.3.2 Any two projective (injective) resolutions of an object are chain homotopy equivalent.

Proof. Let $P_\bullet$ and $P'_\bullet$ be two projective resolutions of an object $M \in \mathcal{C}$. Then by Theorem 6.3.1.1 we can extend the identity on M to chain maps $f \colon P_\bullet \to P'_\bullet$ and $f' \colon P'_\bullet \to P_\bullet$. Then $f \circ f'$ is an extension of the identity id_M to an endomorphism of the chain complex $P'_\bullet$. Another extension is given by the identity in every degree. By Theorem 6.3.1.2 these two extensions are homotopic. Thus f, f' are mutually inverse chain homotopy equivalences. □

We can now pursue the idea to replace objects of the category $\mathcal{C}$ by chain complexes of "better" objects, i.e. here projective or injective objects. As we have just seen, we can also lift morphisms, uniquely up to chain homotopy.

Let F be an additive functor, $F\colon \mathcal{C} \to \mathcal{D}$. By applying F termwise to a chain complex $P_\bullet$ in $Ch_{\mathcal{C}}$, we obtain another chain complex $F(P_\bullet)$ thanks to the additivity of F. However, F does not need to send exact chain complexes to exact chain complex: for an exact complex $P_\bullet$ the chain complex $F(P_\bullet)$ is guaranteed to be exact only if F is exact as a functor.

Definition 6.3.3 Let $\mathcal{C}, \mathcal{D}$ be abelian categories and $F\colon \mathcal{C} \to \mathcal{D}$ an additive functor.

1. If $\mathcal{C}$ has enough projectives, then the left derived functors $L_nF\colon \mathcal{C} \to \mathcal{D}$ of F are defined on objects by the homology of the complex $F(P_\bullet)$:

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

   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 defined analogously on objects by:

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

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

Remarks 6.3.4

- The derived functors vanish for $n \geq 1$ if the functor F is exact.
- By Theorem 6.3.1 the derived functors are well-defined up to isomorphism: if $P_\bullet$ and $P'_\bullet$ are two projective resolutions, then by Corollary 6.3.2 there exists a chain homotopy equivalence $P_\bullet \simeq P'_\bullet$; whose image under F yields a chain homotopy equivalence $F(P_\bullet) \simeq F(P_\bullet)$. Theorem 6.2.6 then implies that the homology groups are isomorphic.
- Theorem 6.3.1 also implies that the derived functors are indeed functors, i.e. also defined on morphisms. If $f\colon X \to Y$ is a morphism, then one can lift f to a morphism $f_\bullet\colon P_\bullet \to Q_\bullet$ between the projective resolutions $P_\bullet$ and $Q_\bullet$, unique up to homotopy. Thus one obtains a morphism $F(f_\bullet)\colon F(P_\bullet) \to F(Q_\bullet)$ of chain complexes, which induces a unique morphism $F(f_\bullet)_*$ on the homology. More precisely, Definition 6.2.2 implies that the final morphism does not depend on the choice of the lift $f_\bullet$. The functor axioms are easy to check.

Lemma 6.3.5 Let F be a right exact functor; then we have $L_0F = F$. Let F be left exact; then we have $R^0F = F$.

Proof. We only show the first part of the statement. If $P_\bullet \to X$ is a projective resolution, then the right exactness of F implies that the sequence

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

is exact. By the homomorphism theorem we have

$$F(X) \cong F(P_0)/(\ker(F(P_0) \to F(X)) \cong F(P_0)/\mathrm{Im}\,(F(P_1)) = H_0(F(P_\bullet)) \ . \qquad \square$$

From now on we will only consider left derived functors only for right exact functors and right derived functors only for left exact functors.

6.4 The long exact sequence

We have seen in Lemma 6.3.5 that the derived functors L_nF resp. R^nF vanish for $n \geq 1$ if the functor F is exact. To make statements in cases when the derived functors no not vanish, we need the long exact sequence of derived functors. This needs some preparations.

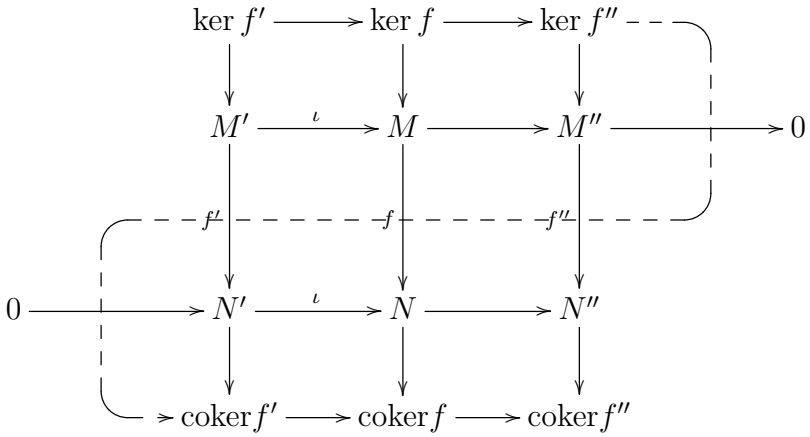
Lemma 6.4.1 [Snake lemma] Consider a commutative diagram of the following form in an abelian category $\mathcal{C}$ with exact rows:

$$(*) \qquad \begin{array}{ccccccc} & & M' & \xrightarrow{\iota} & M & \longrightarrow & M'' \longrightarrow 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} \\ 0 & \longrightarrow & N' & \xrightarrow{\iota} & N & \longrightarrow & N'' \end{array}$$

Then there exists an exact sequence

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

with a so-called connecting morphism ∂, that will be described in the proof. The name "Snake lemma" is motivated by adding the row $\ker f' \to \ker f \to \ker f''$ above and the row $\operatorname{coker} f' \to \operatorname{coker} f \to \operatorname{coker} f''$ below:



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

Proof. By diagram chase, where we may assume by the full embedding theorem that $\mathcal{C}$ is a full abelian subcategory of modules over a ring R. For proofs of this and similar results, which avoid the diagram chase, we refer to [McL71, pp. 202].

- We first construct the connecting morphism ∂. Let $m'' \in \ker f''$. As $M \to M''$ is surjective, there exists a preimage $m_0 \in M$, and by exactness at M every other such preimage has the form $m = m_0 + \iota(m')$ for some $m' \in M'$. Now $f(m_0) \in N$ maps under $N \to N''$ to 0, because we took $m'' \in \ker f''$. Exactness of the lower row at both sites implies that there exists a unique $n'_0 \in N'$ with $n'_0 \mapsto f(m_0)$. If we had picked $m \in M$ with $m := m_0 + \iota(m')$ where $m' \in M'$, then by $N' \ni n'_0 + f'(m') \mapsto f(m) \in N$ the element $n'_0 + f'(m')$ would be a preimage of $f(m)$. Thus the class $[n'_0] =: \partial(m'')$ is well-defined up to an image under f', i.e. well-defined in $\operatorname{coker} f'$. By construction ∂ is a module homomorphism.

- For the proof of exactness we restrict our attention to two sites, e.g. exactness at $\ker f$ and exactness at $\ker f''$. The additional statement about the injectivity of $\ker f' \to \ker f$ is clear. Then the exactness at $\operatorname{coker} f'$ and $\operatorname{coker} f$ as well as the statement about the surjectivity follow by proceeding to the opposite category $\mathcal{C}^{\mathrm{opp}}$.

- Exactness at $\ker f$: Exactness of the upper row implies that the image of $\ker f' \to \ker f$ is in the kernel of $\ker f \to \ker f''$. Conversely, let $m \in \ker f$ with $m \mapsto 0 \in M''$. By exactness of the upper row, there exists a preimage $m' \in M'$, but we still have to show that it is in the submodule $\ker f' \subset M'$. From $f(m) = 0$ we deduce $f(\iota(m)) = \iota f'(m') \mapsto 0 \in N$. Since the lower row is exact, the map $\iota\colon N' \to N$ is injective; and so we must have $f'(m') = 0$.

- Exactness at $\ker f''$: We retain the notation of elements from the first part of the proof, where the connecting morphism ∂ was constructed. First we show that the composite $\ker f \to \ker f'' \xrightarrow{\partial} \operatorname{coker} f'$ is zero. If $m'' \in M''$ is the image of an element $m \in \ker f$ under $M \to M''$, then $f(m) = 0$ and by construction of ∂ we have $\partial(m'') = 0$. This shows one inclusion.

  Let $m'' \in \ker \partial \cap \ker f''$; we look for a preimage in $\ker f$. By exactness of the upper row we find a preimage $m \in M$, which not necessarily lies in $\ker f$. But $f(m) \in N$ has a preimage n' in N' since $f(m) \mapsto 0 \in N''$. By assumption we have $\partial(m'') = 0$ and so there exists a preimage $m' \in M'$ of n' under f'. Let m_0 be the image of m' in M, so $m_0 = \iota(m')$. The difference $\delta := m - m_0 \in M$ has the same image as m in M'', i.e. the given m''. Then we also have
  $$f(\delta) = f(m) - f(m_0) = f(m) - \iota f'(m') = f(m) - \iota n' = 0 \ .$$
  In the last step we have used that n' is a preimage of $f(m) \in N$. Thus δ is the desired preimage of m'' in $\ker f$. □

Remark 6.4.2 (Naturality) The construction implies that the connecting morphism ∂ is natural, i.e., given a morphism of diagrams $D_1 \to D_2$ of the form $(*)$ in Lemma 6.4.1, we get a commutative diagram

$$\begin{array}{ccc} \ker(f''_{D_1}\colon M''_{D_1} \to N''_{D_1}) & \xrightarrow{\partial} & \operatorname{coker}(f'_{D_1}\colon M'_{D_1} \to N'_{D_1}) \\ \downarrow & & \downarrow \\ \ker(f''_{D_2}\colon M''_{D_2} \to N''_{D_2}) & \xrightarrow{\partial} & \operatorname{coker}(f'_{D_2}\colon M'_{D_2} \to N'_{D_2}) \end{array}$$

The category of chain complexes $Ch_{\mathcal{C}}$ of an abelian category is again an abelian category. Thus it is clear what a short exact sequence

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

of chain complexes is. In particular, for an exact sequence of chain complexes we have that for every n the sequence $0 \to M'_n \to M_n \to M''_n \to 0$ is exact.

Theorem 6.4.3 If $0 \to M'_\bullet \to M_\bullet \to M''_\bullet \to 0$ is a short exact sequence of chain complexes in $\mathcal{C}$, then there exists a long exact sequence in homology:

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

Proof. We again assume that $\mathcal{C}$ is a full subcategory of the category of R-modules over a ring R. The commuting diagram

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

together with the Snake Lemma 6.4.1 yields for all $n \geq 1$ a long exact sequence

$$0 \to Z_n M' \to Z_n M \to Z_n M'' \to \frac{M'_{n-1}}{B_{n-1}M'} \to \frac{M_{n-1}}{B_{n-1}M} \to \frac{M''_{n-1}}{B_{n-1}M''} \to 0$$

since the kernels of the differential d are the cycles and the images are the boundaries. Thus we have exact rows in the following commuting diagram

$$\begin{array}{ccccccc} & & M'_n/B_nM' & \longrightarrow & M_n/B_nM & \longrightarrow & M''_n/B_nM'' \longrightarrow 0 \\ & & \downarrow d & & \downarrow d & & \downarrow d \\ 0 & \longrightarrow & Z_{n-1}M' & \longrightarrow & Z_{n-1}M & \longrightarrow & Z_{n-1}M'' \end{array}$$

Here we have $\ker d = H_n$ and $\operatorname{coker} d = H_{n-1}$. Another application of the Snake Lemma 6.4.1 yields the long exact sequence in homology. □

Theorem 6.4.4 [Horseshoe lemma]

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

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

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

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

2. If $\mathcal{C}$ has enough projectives and if the functor F is right exact, then there exists a long exact sequence in $\mathcal{D}$

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

   The homomorphism ∂ is again called connecting morphism.

Proof. To compute derived functors we need to consider projective resolutions of $P'_\bullet \to M', P_\bullet \to M$ and $P''_\bullet \to M''$. To be able to apply Theorem 6.4.3, these resolutions should form a short exact sequence $0 \to P'_\bullet \to P_\bullet \to P''_\bullet \to 0$ of chain complexes, i.e. the diagram

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

should commute. Here ϵ' and ϵ'' are the augmentations of the projective resolutions of M' resp. M''. Then the claim follows from Theorem 6.4.3.

To construct such a diagram we choose two projective resolutions $P'_\bullet \to M'$ and $P''_\bullet \to M''$ and set $P_0 := P'_0 \oplus P''_0$. We consider on the first component $\iota \circ \epsilon'\colon P'_0 \to M$. For the second

component we note that $M \to M''$ is surjective and use the projectivity of P_0'' to lift ϵ'' to a morphism $P_0'' \to M$. Together we obtain a morphism $\epsilon\colon P_0 = P_0' \oplus P_0'' \to M$, such that the diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \ker(\epsilon') & \longrightarrow & \ker(\epsilon) & \longrightarrow & \ker(\epsilon'') & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P_0' & \longrightarrow & P_0 & \longrightarrow & P_0'' & \longrightarrow & 0 \\
 & & {\scriptstyle\epsilon'}\downarrow & & {\scriptstyle\epsilon}\downarrow & & {\scriptstyle\epsilon''}\downarrow & & \\
0 & \longrightarrow & M' & \xrightarrow{\iota} & M & \longrightarrow & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

commutes. The two lower rows are exact. The Snake Lemma 6.4.1 implies that the upper row is exact and $\operatorname{coker}(\epsilon) = 0$, and so $P_0 \to M$ is surjective.

Thus we have filled the first stage. Now we proceed to the situation

$$\begin{array}{ccccccccc}
 & & \downarrow & & & & \downarrow & & \\
 & & P_1' & & & & P_1'' & & \\
 & & \downarrow & & & & \downarrow & & \\
0 & \longrightarrow & \ker(\epsilon') & \longrightarrow & \ker(\epsilon) & \longrightarrow & \ker(\epsilon'') & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

which is again a horseshoe and proceed inductively. □

Remarks 6.4.5

1. The right derived functors of a left exact functor (for $n > 1$) vanish if and only if the functor F is exact. The exactness of F follows from the vanishing of R^1F resp. L_1F, cf. the exercises.

2. From the naturality of the connecting morphism we can deduce naturality statements: given

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M_\bullet' & \longrightarrow & M_\bullet & \longrightarrow & M_\bullet'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & N_\bullet' & \longrightarrow & N_\bullet & \longrightarrow & N_\bullet'' & \longrightarrow & 0
\end{array}$$

   a commutative diagram of exact sequences of chain complexes, then we obtain a morphism between the associated long exact sequences from Theorem 6.4.3, i.e. a commuting ladder

$$\begin{array}{ccccccccc}
\cdots & H_i(M_\bullet') & \longrightarrow & H_i(M_\bullet) & \longrightarrow & H_i(M_\bullet'') & \xrightarrow{\partial} & H_{i-1}(M_\bullet') & \longrightarrow \cdots \\
 & \downarrow & & \downarrow & & \downarrow & & \downarrow & \\
\cdots & H_i(N_\bullet') & \longrightarrow & H_i(N_\bullet) & \longrightarrow & H_i(N_\bullet'') & \xrightarrow{\partial} & H_{i-1}(N_\bullet') & \longrightarrow \cdots
\end{array}$$

If

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0 \end{array}$$

is a commutative diagram with short exact rows in a category $\mathcal{C}$ with enough projectives, then induced ladder from Theorem 6.4.4 also commutes:

$$\begin{array}{ccccccccccccc} \cdots & \longrightarrow & L_iF(M') & \xrightarrow{\iota_*} & L_iF(M) & \xrightarrow{p_*} & L_iF(M'') & \xrightarrow{\partial} & L_{i-1}F(M') & \xrightarrow{\iota_*} & \cdots & \longrightarrow & L_0F(M'') \to 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & & & \\ \cdots & \longrightarrow & L_iF(N') & \xrightarrow{\iota_*} & L_iF(N) & \xrightarrow{p_*} & L_iF(N'') & \xrightarrow{\partial} & L_{i-1}F(N') & \xrightarrow{\iota_*} & \cdots & \longrightarrow & L_0F(N'') \to 0 \end{array}$$

6.5 Tor and Ext

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

Definition 6.5.1 Let R be a ring.

1. Define for each R-right module X a functor $F_X\colon R\text{−Mod} \to \mathrm{Ab}$ by $F_X(Y) := X \otimes_R Y$. This functor is right exact (cf. Example 3.1.14.3). Its left derived functors are denoted
$$\mathrm{Tor}_n^R(X,Y) := L_nF_X(Y) \ .$$
2. Define for each R-module X a functor $G_X\colon (R\text{−Mod})^{\mathrm{opp}} \to \mathrm{Ab}$ by $G_X(Y) := \mathrm{Hom}_R(Y,X)$. The functor G_X is left exact (cf. Example 3.1.14.5). Its right derived functors are denoted
$$\mathrm{Ext}_R^n(Y,X) := R^nG_X(Y) \ .$$

In the definition of Ext, one uses an injective resolution in $(R\text{−Mod})^{\mathrm{opp}}$, which is the same as a projective resolution in R−Mod.

The following observations follow immediately from the definitions:

- $\mathrm{Tor}_n^R(X,Y) = 0$ for all Y and for all $n > 0$ if and only if the right module X is flat.
- $\mathrm{Ext}_R^n(Y,X) = 0$ for all Y and for all $n > 0$ if and only if the module X is injective.
- Tor and Ext are not only functors in the argument Y, but also in X.

Examples 6.5.2

1. Let $R = \mathbb{Z}$ and $Y = \mathbb{Z}/n\mathbb{Z}$. A free and thus also projective resolution of the $\mathbb{Z}$-module $Y = \mathbb{Z}/n\mathbb{Z}$ is given by the augmented complex
$$0 \to \mathbb{Z} \xrightarrow{n\cdot} \mathbb{Z} \to \mathbb{Z}_n \to 0\,.$$
We now compute $\mathrm{Tor}_k^{\mathbb{Z}}(X,Y)$ for the $\mathbb{Z}$-module $X = \mathbb{Z}/m\mathbb{Z}$. By $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}$ tensoring the projective resolution with $\mathbb{Z}/m\mathbb{Z}$ yields the complex
$$0 \to \mathbb{Z}/m\mathbb{Z} \xrightarrow{n\cdot} \mathbb{Z}/m\mathbb{Z} \to 0 \ ,$$
whose homology $\mathrm{Tor}_k^{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ is:
$$\mathrm{Tor}_k^{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \begin{cases} \mathbb{Z}_{\gcd(m,n)}; & \text{if } k = 0,1 \\ 0; & \text{otherwise.} \end{cases}$$

To see this we write $n = g \cdot x$ with $g := \gcd(m, n)$ and $x \in \mathbb{N}$. The multiplication by x acts on $\mathbb{Z}/m\mathbb{Z}$ as isomorphism since x is relatively prime to m. The kernel $\ker n\cdot = \ker g\cdot$ consists of all multiples of m/g, which form a cyclic group of order g. The cokernel $\mathrm{coker} n\cdot = \mathrm{coker} g\cdot$ is the quotient of $\mathbb{Z}/m\mathbb{Z}$ modulo all multiples of g, so again a cyclic group of order g.

By Lemma 6.3.5 Tor for $k = 0$ must coincide with the original functor: $\mathrm{Tor}_0(X, Y) = X \otimes_{\mathbb{Z}} Y$. Comparing with Examples 1.2.6.3, we find agreement.

The higher (i.e. $k \geq 2$) Tor-groups indeed vanish over $\mathbb{Z}$ for all $\mathbb{Z}$-modules: as $\mathbb{Z}$ is a PID, by Observation 4.1.3 one can always construct a free resolution that is concentrated in the degrees 0 and 1.

We also compute $\mathrm{Tor}_k^{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ as homology of the complex

$$0 \to \mathbb{Z} \xrightarrow{n\cdot} \mathbb{Z} \to 0$$

and find

$$\mathrm{Tor}_0^{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \quad \text{and} \quad \mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = 0 \ .$$

The functor $\mathrm{Tor}_1(-, \mathbb{Z}/n\mathbb{Z})$ on finitely generated abelian groups vanishes unless the groups have a torsion part, thus the name.

2. A very similar computation shows that

$$\mathrm{Ext}_{\mathbb{Z}}^k(\mathbb{Z}_m, \mathbb{Z}_n) \cong \begin{cases} \mathbb{Z}_{\mathrm{ggT}(m,n)}; & \text{if } k = 0, 1 \\ 0; & \text{otherwise.} \end{cases}$$

The notation Ext will be explained in Section 6.7.

3. In the following example there exist infinitely many non-trivial Tor-groups: Let $R = \mathbb{Z}[t]/(t^n - 1)$ be the group ring of the cyclic group $\mathbb{Z}/n\mathbb{Z}$ of order n over the integers.

The ring homomorphism $\epsilon : R \to \mathbb{Z}$ that sends $t \mapsto 1$ endows $\mathbb{Z}$ with the structure of an R-module with $t.m = m$, the trivial R-module. We choose $X = Y = \mathbb{Z}$ with trivial module structure. We claim that a projective (and indeed free) resolution is given by the projective part of the augmented complex

$$\cdots \xrightarrow{N} R \xrightarrow{1-t} R \xrightarrow{N} R \xrightarrow{1-t} R \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

where ϵ is defined as above by evaluating at 1, i.e. $\epsilon(t) = 1$ and $N := 1 + t + \cdots + t^{n-1}$. A quick computation shows $(1 - t)N = 1 - t^n$, so the differential squares to zero. We show exactness: the class of a polynomial $f \in \mathbb{Z}[t]$ in the quotient ring R vanishes if and only if f is a multiple of $1 - t^n$. The ring $\mathbb{Z}[t]$ is a unique factorization domain. Thus a multiple of N if also a multiple of $1 - t^n$ if and only if it is also divisible by $1 - t$. The complex is thus exact.

By tensoring the projective resolution over R with $\mathbb{Z}$, one obtains $R \otimes_R \mathbb{Z} \cong \mathbb{Z}$ in all degrees. The map induced by $1 - t$ is zero, because one evaluates at $t = 1$. Multiplication with N induces the multiplication by $n \in \mathbb{N}$. Thus we get the complex

$$\cdots \xrightarrow{n} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \to 0$$

and

$$\mathrm{Tor}_k^R(\mathbb{Z}, \mathbb{Z}) \cong \begin{cases} \mathbb{Z}; & \text{if } k = 0 \text{ (cf. Lemma 6.3.5)} \\ \mathbb{Z}_n; & \text{if } k \text{ odd} \\ 0 & \text{if } k > 0 \text{ even.} \end{cases}$$

4. It is clear that for a free $\mathbb{Z}$-module A one has $\mathrm{Ext}^1_{\mathbb{Z}}(A,\mathbb{Z}) = 0$. The converse, whether $\mathrm{Ext}^1_{\mathbb{Z}}(A,\mathbb{Z}) = 0$ implies that the $\mathbb{Z}$-module A is free, is a surprisingly subtle question, whose answer depends on the underlying set theory [HS1970, Second Edition, p. 330 "note to the third corrected printing"].

6.6 Symmetry of Tor and double complexes

It seems natural to define a second variant Tor' of Tor by using a projective resolution of the first variable. Similarly, there exists a variant Ext' of Ext, in which for a fixes the contravariant variable X and considers the right derived functors of the left exact functor $\mathrm{Hom}_R(X,-)\colon R\text{−Mod} \to Ab$.

We show the isomorphism of Tor and Tor', by showing that Tor is isomorphic to a third functor $\widetilde{\mathrm{Tor}}$, which is manifestly symmetric in both arguments; analogous statements hold for Ext. For all of this we need double complexes.

Definition 6.6.1

1. The category of double complexes in an abelian category $\mathcal{C}$ has as objects the triples (X_{ij}, d_h, d_v) consisting of objects X_{ij} of $\mathcal{C}$ for $i,j \in \mathbb{Z}$ and morphisms $d_h\colon X_{ij} \to X_{i-1,j}$ and $d_v\colon X_{ij} \to X_{i,j-1}$ such that

$$d_h d_v = -d_v d_h \quad \text{and} \quad d_h d_h = d_v d_v = 0\,.$$

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

2. The morphisms of double complexes are given by families of morphisms $f_{ij}\colon X_{ij} \to Y_{ij}$, that commute with the two differentials d_h and d_v.

3. Using the coproduct and product one assigns to a double complex two ordinary complexes

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

   for both of which the differential is given by $d = d_h + d_v$. Both complexes are called total complexes of the double complex.

Remark 6.6.2

1. Note that the indexing of double complexes is not the usual indexing of rows and columns of matrices!

2. The diagram

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

   does *not* commute! The anticommutativity of the differentials, $d_h d_v = -d_v d_h$, ensures that the total complexes $|X|$ and $\mathrm{Tot}X$ are again chain complexes: If $x \in X_{ij}$, then for $d = d_h + d_v$ we have

$$d(dx) = d(d_h x + d_v x) = d_h d_h x + d_h d_v x + d_v d_h x + d_v d_v x = 0\,.$$

Definition 6.6.3 Let R be a ring.

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

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

where the maps for $p \in P_i, q \in Q_j$ are given by $d_h(p \otimes q) = d(p) \otimes q$ and $d_v(p \otimes q) = (-1)^i p \otimes d(q)$. We call i the degree of p and write $|p| = i$. If we abstractly define the degree of d by -1 (since d takes P_n to P_{n-1}), then the sign convention above is a special case of the so-called Koszul sign rule:

Whenever an element of degree i commutes past an element of degree j, a sign $(-1)^{ij}$ appears.

2. We call the total complex $|P \otimes_R Q|$ the tensor product of the chain complexes $P_\bullet$ and $Q_\bullet$.

3. Let $(P_\bullet, d)$ be chain complex of R-modules, then we define a double complex $\mathrm{Hom}_R(P, Q)_{\bullet\bullet}$ of abelian groups by

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

Here the differentials of the double complex are given by pre- and postcomposing with the differentials of $P_\bullet$ and $Q_\bullet$.

Remark 6.6.4 Tensor products of chain complexes occur in the following problem, for example: let X and Y be topological spaces. Singular homology determines two chain complexes $C_\bullet(X)$ and $C_\bullet(Y)$. The Eilenberg–Zilber theorem says that the chain complex $C_\bullet(X \times Y)$ of the Cartesian product is chain homotopy equivalent to the tensor product chain complex $C_\bullet(X) \otimes C_\bullet(Y)$.

We need another auxiliary result to study total complexes:

Lemma 6.6.5 Let $X_{\bullet\bullet}$ be a double complex in an abelian category $\mathcal{C}$. If for every $j \in \mathbb{Z}$ we have that the row complex $X_{\bullet,j}$ is exact, then:

1. the total complex $|X|$ exact, if there exists an $N \in \mathbb{Z}$ such that $X_{ij} = 0$ for all rows $j < N$;

2. the total complex $\mathrm{Tot}X$ is exact, if there exists an $N \in \mathbb{Z}$, such that $X_{ij} = 0$ for all columns $i < N$.

Both conditions 1. and 2. automatically satisfied, if X is non-negatively graded in both indices. Neither condition is necessary; they are merely sufficient to ensure "convergence".

Proof. • For the proof of 1. we may assume without loss of generality that $N = 0$, otherwise we may shift the complex vertically. Likewise, it is enough to show exactness of the total complex at the site $|X|_0$, for otherwise we can shift any other total degree to zero by left or right shifts of X.

Then we have

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

Let $x = (x_{n_0}, x_{n_0-1}, \ldots, x_0) \in |X|_0$ be an element, with $x_n \in X_{-n,n}$, for which $d(x) = 0$ holds. By $d_h x_n \in X_{-n-1,n}$ and $d_v x_n \in X_{-n,n-1}$ this means for the homogeneous components

$$d_v(x_i) + d_h(x_{i-1}) = 0 \text{ in } X_{-i,i-1} \text{ for } 0 \leq i \leq n_0 + 1 \ . \qquad (*)$$

As $x_{n_0+1} = 0$ we have for $i = n_0 + 1$

$$d_h(x_{n_0}) = 0 \ .$$

Since the rows are exact by assumption, $d_h(x_{n_0}) = 0$ implies that there exists a $y_{n_0} \in X_{-n_0+1,n_0}$ with $d_h(y_{n_0}) = x_{n_0}$.

We now inductively find elements $y_n \in X_{-n+1,n}$, such that

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

It is possible to solve the second equation, because for $0 \leq i < n_0$ we have

$$d_h(x_i - d_v(y_{i+1})) = d_h(x_i) + d_v d_h(y_{i+1}) \stackrel{\text{I.H.}}{=} d_h x_i + d_v x_{i+1} - d_v d_v(y_{i+2}) \stackrel{(*)}{=} 0 \ ,$$

and by exactness of the rows we can find $y_i \in X_{-i+1,i}$ with

$$d_h y_i = x_i - d_v y_{i+1} \ .$$

Thus with $y = (y_{n_0}, ..., y_0) \in |X|_1$ we have found an element with $d(y) = x$. The total complex $|X|$ is thus exact.

- For the proof of the statement concerning $\mathrm{Tot}(X)$ we also assume $N = 0$ and consider $(\ldots, x_{-2}, x_{-1}, x_0) \in (\mathrm{Tot}X)_0$, which is allowed to have infinitely many non-vanishing entries $x_i \in X_{-i,i}$. We obtain equations $d_v(x_i) + d_h(x_{i-1}) = 0$ for all $i \leq 0$. The boundary conditions imply again that the 0th equation has the form $d_h x_0 = 0$, so that we can find a $y_0 \in X_{1,0}$ with $d_h y_0 = x_0$ by exactness of the rows. As before one inductively solves such a sequence equations to find $y_i \in X_{-i+1,i}$, which again may have infinitely many non-trivial entries, which is fine for an element of $\mathrm{Tot}X$. □

Let $P_\bullet \to X$ be a projective resolution of R^{opp}-modules and $Q_\bullet \to Y$ a projective resolution of R-modules. To get a complex that is symmetric in both resolutions, we consider the tensor product of the resolutions and the homology of the associated total complex and set

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

Theorem 6.6.6 For an R-right module X and an R-left module Y we have

$$\mathrm{Tor}^R_n(X, Y) = \widetilde{\mathrm{Tor}}^R_n(X, Y) \ .$$

As $\widetilde{\mathrm{Tor}}^R_n(X, Y)$ has been constructed via a double complex that is symmetric in both arguments, this shows that we could have also projectively resolved the other tensor factors.

Proof. • Let $P_\bullet \to X$ and $Q_\bullet \to Y$ be projective resolutions. We denote by $\tilde{P}_\bullet$ the augmented complex with $\tilde{P}_n := P_n$ for $n \geq 0$ and $P_{-1} = X$. The augmented complex $\tilde{P}_\bullet$ is exact and for every i the module Q_i is projective and thus flat by Theorem 1.4.10, which together imply that the double complex $\tilde{P} \otimes_R Q$ has exact rows. Thus the total complex $|\tilde{P} \otimes Q|$ which is concentrated in one quadrant is also exact by Lemma 6.6.5.

- Clearly
$$0 \to X[-1] \to \tilde{P}_\bullet \to P_\bullet \to 0$$
is a short exact sequence of complexes, where $X[-1]$ denotes the complex which has the module X in degree -1 and 0 everywhere else. Since Q_i is projective, tensoring with $Q_\bullet$ yields an exact sequence of double complexes. Since the functor $|-|$, which sends double complexes to complexes, is exact, we obtain a short exact sequence of total complexes
$$0 \to |X[-1] \otimes Q| \to |\tilde{P} \otimes Q| \to |P \otimes Q| \to 0$$
Since the middle complex $\tilde{P} \otimes_R Q$ is exact as we have seen in the first step of the proof, its homology vanishes, and the associated long exact sequence (from Theorem 6.4.3) breaks into small exact pieces
$$0 \to H_n|P \otimes Q| \to H_{n-1}|X[-1] \otimes Q| \to 0 \ ,$$
for $n \geq 0$, thus the connecting morphisms are isomorphisms.

- We now interpret the abelian groups that appear as the source and target of this isomorphism: by definition of $\widetilde{\mathrm{Tor}}$ the first one is
$$H_n|P \otimes Q| = \widetilde{\mathrm{Tor}}^R_n(X, Y) \ ;$$
and for the second we use the definition of Tor
$$H_{n-1}|X[-1] \otimes Q| = H_n(X \otimes Q) = \mathrm{Tor}^R_n(X, Y) \ .$$
Thus we shown the isomorphism of the functors Tor and $\widetilde{\mathrm{Tor}}$. □

For a commutative ring R both tensor products $X \otimes_R Y$ and $Y \otimes_R X$ are defined and isomorphic by swapping the factors. Let $P_\bullet \to X$ and $Q_\bullet \to X$ be projective resolutions. Then we have the isomorphism
$$\begin{array}{rcl} P \otimes Q & \to & Q \otimes P \\ v_p \otimes w_q & \mapsto & (-1)^{pq} w_q \otimes v_p \quad \text{for } v_p \in P_p \text{ and } w_q \in Q_q \end{array}$$
of double complexes. We thus find
$$\begin{array}{rcl} \mathrm{Tor}^R_*(X, Y) & \cong & \widetilde{\mathrm{Tor}}^R_*(X, Y) = H_*(|P \otimes_R Q|) \\ & \cong & H_*(|Q \otimes_R P|) = \widetilde{\mathrm{Tor}}^R_*(X, Y) = \mathrm{Tor}^R_*(Y, X) \end{array}$$
In the case of *commutative* rings R the derived functor Tor^R_* is thus commutative in both arguments. In the case of Ext we can also resolve the second argument injectively instead of resolving the first argument projectively:

Theorem 6.6.7 Let $X, Y \in R-\mathrm{Mod}$ and $Y \to I_\bullet$ be an injective resolution and $P_\bullet \to X$ a projective resolution. Set:
$$\mathrm{Ext}'^n_R(X, Y) := H^n(\mathrm{Hom}_R(X, I_\bullet)) \quad \text{and} \quad \widetilde{\mathrm{Ext}}^n_R(X, Y) := H_n(\mathrm{TotHom}_R(P_\bullet, I_\bullet)) \ .$$
Here we grade the complex of abelian groups by
$$\mathrm{Hom}(P_\bullet, I_\bullet)_{i,j} := \mathrm{Hom}(P_{-i}, I_j) \ .$$
Then we have
$$\mathrm{Ext}^n_R(X, Y) \cong \widetilde{\mathrm{Ext}}^n_R(X, Y) \cong \mathrm{Ext}'^n_R(X, Y)$$

Proof. Exercise. □

6.7 Extensions of modules

We have already seen in Examples 6.5.2 that the notation "Tor" can be motivated by considering torsion in abelian groups, but we have yet to make sense of the notation "Ext". In this section we discuss an alternative definition of Ext-groups via equivalence classes of extensions of R-modules by other R-modules, which goes back to Yoneda.

Let $\mathcal{C}$ be an abelian category and let M, N be two objects in $\mathcal{C}$. Consider for $n \geq 1$ the sets of *exact* sequences

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

where $\sim$ is the equivalence relation that is generated by declaring $E \sim E'$ if there exists a chain map $E \to E'$, which is the identity on the entries M and N. (Here it is not sufficient to require isomorphism on the entries M and N.) Note that the Nine Lemma 1.5.8 implies in the case $n = 1$ that the morphism $X_0 \to X_0'$ is an isomorphism. In general the components of the chain maps are not isomorphisms.

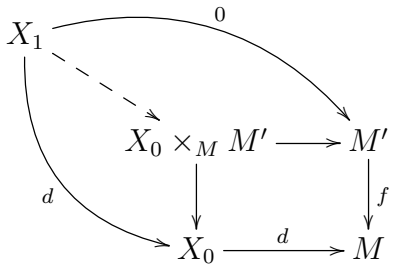
We now aim to turn Ex^n into a functor $\mathcal{C}^{\mathrm{opp}} \times \mathcal{C} \to \mathrm{Set}$. (In Lemma 6.7.2 we will see that it takes values in abelian groups.) To define the functor on morphisms, suppose we are given an extension

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

and morphisms

$$f\colon M' \to M \quad \text{and} \quad g\colon N \to N' .$$

Consider for f the pullback diagram



where the morphisms $X_1 \to X_0 \to M$ are taken from the exact sequence E, and thus compose to zero. Consider the complex

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

Dually we define by pushout under N a complex

$$g_*E\colon \quad 0 \to N' \to X_{n-1} \sqcup_N N' \to X_{n-2} \to \cdots \to X_0 \to M \to 0\,.$$

Lemma 6.7.1 Retain the notation from above.

1. The complexes f^*E and g_*E are again exact. Their equivalence classes do not depend on the choice of representatives E in Ex.

2. We obtain a functor $\mathcal{C}^{\mathrm{opp}} \times \mathcal{C} \to \mathrm{Set}$.

Proof. 1. To see that these constructions are well-defined, we need to check that f^* does not depend on the representatives E of the source equivalence class. Let

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

be an a elementary equivalence of exact sequences and $f\colon M' \to M$ a morphism. Then by functoriality of the pullback from Remarks 2.2.11.4, we obtain a map

$$X_0 \times_M M' \to X_0' \times_M M' \ ,$$

that, together with the other morphisms $X_i \to X_i'$, provides an elementary equivalence between the complexes f^*E and f^*E'. The dual argument applies to g_*.

2. We also need to show that f^*E is exact and thus an extension, as required.

   - The map $X \times_M M' \to M'$ is surjective: for any $m' \in M'$ we can find $x \in X_0$ with $f(m') = dx$ because $d\colon X_0 \to M$ is surjective. Then (x, m') is a preimage of $m' \in M'$ in the fibre product $X_0 \times_M M'$.
   - The morphism $X_1 \to X_0 \times_M M'$ is $x \mapsto (dx, 0)$, and by $d(dx) = 0 = f(0)$ this indeed lands in the fibre product $X_0 \times_M M'$. Thus we have the exactness condition

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

     by the exactness of the original sequence E.
   - 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 these we must have $dx = f(0) = 0$. By exactness of E this means $x \in \operatorname{Im}(X_1 \to X_0)$ and thus $(x, 0) \in \operatorname{Im}(X_1 \to X_0 \times_M M')$.

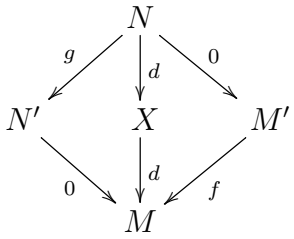
   The arguments for the exactness of the complex g_*E are again dual.

3. Now we consider the second part of the lemma, which concerns functoriality: let $M_2 \xrightarrow{f_1} M_1 \xrightarrow{f_0} M_0$ be two morphisms; we have to show that $(f_0 \circ f_1)^*E = f_1^* \circ f_0^* E$. This follows from the canonical isomorphism

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

   compare Remark 2.2.11.5.

4. Finally we have to show $f^*g_* = g_* f^*$ for $f\colon M' \to M$ and $g\colon N \to N'$. This is clear for $n \geq 2$, as both functors operate on different parts of the exact sequence. For $n = 1$, on the other hand, we consider the diagram

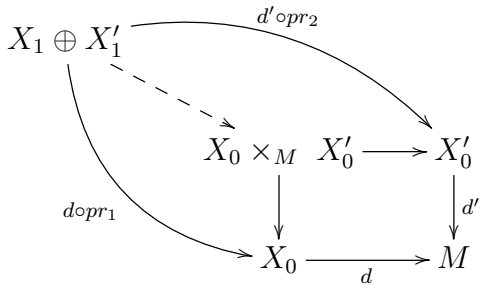
   and thus obtain an isomorphism

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

   (best checked on elements), which provides an equivalence of the sequences f^*g_*E and g_*f^*E.

□

We aim to equip the sets Ex^n with the structure of abelian groups. Let $E, E' \in \mathrm{Ex}^n(M,N)$. For $n \geq 2$ we consider the pullback diagram



and the dual pushout diagram. We define a complex $E + E'$ by direct sums and the dashed morphism in the diagram:

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

In case $n = 1$ we have to define the middle term of the complex $E + E'$ as

$$\{(x, x') \in X \oplus X' | d(x) = d'(x')\}/(d(n), 0) \sim (0, d'(n))(n \in N) \ .$$

Lemma 6.7.2 The sets $\mathrm{Ex}^n(M,N)$ are thus equipped with the structure of abelian groups.

Proof.

- We first verify the exactness of the complex $E + E'$.
  - The exactness is clear at the middle (direct sums-)groups.
  - Exactness at M is surjectivity: given $m \in M$, find $x_0 \in X_0$ and $x'_0 \in X'_0$ with $dx_0 = m$ and $d'x'_0 = m$ using the surjectivity in the extensions E, E'. Then (x_0, x'_0) is the desired preimage.
  - Exactness at $X_0 \times_M X'_0$: The kernel in $X_0 \times_M X'_0$ is exactly
  $$\ker(X_0 \to M) \times_M \ker(X'_0 \to M) = \mathrm{Im}\,(X_1 \oplus X'_1 \to X_0 \times_M X'_0).$$
  - The exactness at N and at $X_{n-1} \sqcup_N X'_{n-1}$ follows dually.
- The associativity and commutativity of the sum is manifest in the definition. We describe the neutral element; for $n \geq 2$ it is given by
  $$0 \to N \stackrel{\mathrm{id}}{\to} N \to 0 \to \cdots \to M \stackrel{\mathrm{id}}{\to} M \to 0$$
  resp. for $n = 1$ by the splitting short exact sequence.
- The proof of the existence of inverses is omitted.

□

The following theorem explains the notation Ext for the right derived functor of the Hom-functor. It also makes extensions of modules computable via projective resolutions.

Theorem 6.7.3 If the category $\mathcal{C}$ has enough projectives, then there exists a natural isomorphism of functors $\mathrm{Ex}^n \cong \mathrm{Ext}^n$.

Proof. • Let $P_\bullet \to M$ be a projective resolution of M. Let $E \in \mathrm{Ex}^n(M,N)$. Then by Theorem 6.3.1 the lifting problem for the identity id_M

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

has a solution. By commutativity of the leftmost square we have $f_n \circ d = 0$, so

$$f_n \in \ker(\mathrm{Hom}(P_n, N) \xrightarrow{d^*} \mathrm{Hom}(P_{n+1}, N)) \ .$$

We can thus consider the class

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

- We first show that $\Phi(E) \in \mathrm{Ext}^n(M,N)$ is well-defined: this element depends neither on the choice of lift $f_\bullet$ of the identity id_M nor on the choice of extension E within its equivalence class. Then we show that $\Phi\colon \mathrm{Ex}^n(M,N) \to \mathrm{Ext}^n(M,N)$ is an isomorphism of abelian groups.

  Theorem 6.3.1 shows that the lift $f_n\colon P_n \to N$ not only exists but is also unique up to homotopy. Thus every other solution is of the form $f_n + H \circ d = f_n + d^*(H)$, where $H\colon P_{n-1} \to N$ is part of a chain homotopy. Since this does not make any difference in homology, the first part of well-definedness is shown.

  Thus the class of f_n in $H^n(\mathrm{Hom}(P_\bullet, N)) = \mathrm{Ext}^n(M,N)$ is well-defined, provided we can show that it is invariant under the equivalence relation in Ex. If $E \to E'$ is an elementary equivalence, then we can choose the lift $P_\bullet \to E'$ of the identity in the special form of a lift $P_\bullet \to E$ of id_M, followed by the equivalence $E \to E'$. Since this is, by definition, the identity on N, we obtain the same element in Ext^n.

- We now set out to construct an inverse to Φ. Let $f\colon P_n \to N$ be a representative of an element of $\mathrm{Ext}^n(M,N)$. Consider the pushout diagram

$$\begin{array}{ccccc}
P_n & \xrightarrow{d} & P_{n-1} & & \\
{\scriptstyle f}\downarrow & & \downarrow & \searrow^{d} & \\
N & \longrightarrow & N \sqcup_{P_n} P_{n-1} & \dashrightarrow & \\
 & \searrow^{0} & & & P_{n-2}
\end{array}$$

  and construct from it (following arguments dual to those in the proof of Lemma 6.7.2) an exact sequence

$$0 \to N \to N \sqcup_{P_n} P_{n-1} \to P_{n-2} \to P_{n-3} \to \cdots \to P_0 \to M \to 0 \ .$$

  This determines an element in Ex^n. It is clear that the composite $\mathrm{Ext} \to \mathrm{Ex} \to \mathrm{Ext}$ is the identity; the other direction is given by the following diagram, that determines an equivalence in Ex:

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

- It is clear, that Φ sends the zero in Ex^n to the zero in Ext^n, because we can choose as lift on P_n the zero morphism.
- We still have to show that the bijection between Ext^n and Ex^n respects the addition. For this we first observe that we can characterize the addition in Ext^n as follows.

  Let $\Delta\colon M \to M \oplus M$ be the diagonal map and $\Sigma\colon N \oplus N \to N$ the sum map, then

  $$\mathrm{Hom}(M,N) \oplus \mathrm{Hom}(M,N) \to \mathrm{Hom}(M \oplus M, N \oplus N) \xrightarrow{\Sigma_*\Delta^*} \mathrm{Hom}(M,N)$$

  is by

  $$\Sigma \circ (f,g) \circ \Delta(m) = \Sigma\,(f(m), g(m)) = f(m) + g(m)$$

  the addition of abelian group $\mathrm{Hom}(M,N)$ and likewise

  $$\mathrm{Ext}(M,N) \oplus \mathrm{Ext}(M,N) \to \mathrm{Ext}(M \oplus M, N \oplus N) \xrightarrow{\Sigma_*\Delta^*} \mathrm{Ext}(M,N)$$

  is the addition the abelian group $\mathrm{Ext}(M,N)$: we have

  $$\Sigma_*\Delta^*(f \oplus g) = f + g\ .$$

  For Ex^n the functoriality for Δ^* was defined via a pullback and for Σ_* via a pushforward, see Lemma 6.7.1. Exactly the same operations also appear in the definition of the sum in Lemma 6.7.2. Thus we also have in Ex^n:

  $$E + E' \cong \Sigma_*\Delta^*(E \oplus E')\ ,$$

  where $E \oplus E'$ is the direct sum sequence from $N \oplus N$ to $M \oplus M$. If we choose a projective resolution $P_\bullet$ of M, then in the diagram

  $$\begin{array}{lccccccc}
  \cdots \longrightarrow & P_n \oplus P_n & \longrightarrow \cdots \longrightarrow & P_0 \oplus P_0 & \longrightarrow & M \oplus M & \longrightarrow 0 \\
  & \downarrow{\scriptstyle (f_n, f'_n)} & & \downarrow{\scriptstyle (f_n, f'_n)} & & \| & \\
  E \oplus E'\colon & N \oplus N & \longrightarrow \cdots \longrightarrow & X_0 \oplus X'_0 & \longrightarrow & M \oplus M & \longrightarrow 0
  \end{array}$$

  we can choose the lift as the direct sum of the lifts f, f' that correspond to E resp. E'. The application of $\Sigma_*\Delta^*$ then shows the additivity. □

Example 6.7.4 Let p be a prime number; then by Examples 6.5.2 we have $\mathrm{Ext}^1_{Ab}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z}$ in the category the abelian groups. We thus know that there are p equivalence classes of extensions:

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

For the non-trivial group elements of $\mathrm{Ext}^1_{Ab}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})$ we have $G \cong \mathbb{Z}/p^2\mathbb{Z}$, and for the neutral element $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

The interpretation via the Yoneda-Ext allows us to find more structure on the collection of groups $\mathrm{Ext}^*(M,N)$. If $E \in \mathrm{Ex}^n(M,N), E' \in \mathrm{Ex}^m(Q,M)$ with $m > 0$ and $n > 0$, then the composite $X_0 \to M \to X'_{m-1}$ gives a morphism. From the exactness of $X_1 \to X_0 \to M \to 0$ and $0 \to M \to X'_{m-1}$ we deduce that

$$\begin{array}{ccccccccccccc}
0 \longrightarrow & N & \longrightarrow & X_{n-1} & \longrightarrow \cdots \longrightarrow & X_0 & \longrightarrow & X'_{m-1} & \longrightarrow \cdots \longrightarrow & X'_0 & \longrightarrow & Q \\
 & & & & & & \searrow & \uparrow & & & & \\
 & & & & & & & M & & & &
\end{array}$$

is again an extension.

We define $\mathrm{Ex}^0(M,N)$ to be $\mathrm{Hom}(M,N)$; the multiplication $\mathrm{Ex}^0 \times \mathrm{Ex}^0 \to \mathrm{Ex}^0$ is simply the composition of morphisms. Further we set:

$$\begin{array}{rcl@{\qquad}rcl} \mathrm{Ex}^0 \times \mathrm{Ex}^n & \to & \mathrm{Ex}^0 \ , & \mathrm{Ex}^n \times \mathrm{Ex}^0 & \to & \mathrm{Ex}^0 \\ (f,E) & \mapsto & f^*E \ , & (E,g) & \mapsto & g_*E \end{array}$$

Theorem 6.7.5 [Yoneda product] If $E \in \mathrm{Ex}^n(M,N), E' \in \mathrm{Ex}^m(Q,M)$, then we define the Yoneda product $EE' \in \mathrm{Ex}^{n+m}(Q,N)$ to be represented by the extension

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

The map $(E,E') \mapsto E \cdot E'$ is a well-defined, bilinear, associative multiplication.

Proof. The associativity for $n,m > 0$ is immediately clear. Similarly the well-definedness, as any two elementary equivalences can be glued to an equivalence of the product.

The associativity for the cases $n = 0$ and $m = 0$ is a reformulation of the functoriality of Ex^n from Lemma 6.7.1. □

6.8 The Künneth formula

In Definition 6.6.3.2 we have defined the tensor product of chain complexes $X_\bullet$ and $Y_\bullet$ of R-modules as total complex $|X_\bullet \otimes_R Y_\bullet|$. We would like to express the homology of such a tensor product $C_\bullet \otimes_R D_\bullet$ in terms of the homologies of $C_\bullet$ and $D_\bullet$. Here we restrict to the case when R is a PID. In particular, R will be commutative.

Example 6.8.1 Let $R = \mathbb{Z}$ and let $C_\bullet = D_\bullet$ be complexes concentrated in degree zero with entry $\mathbb{Z}/2\mathbb{Z}$. Let $C'_\bullet$ be the complex with $\mathbb{Z}$ in degrees 0 and 1 and $0 \to \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \to 0$. By Remarks 6.2.3, the complexes $C_\bullet$ and $C'_\bullet$ are quasi-isomorphic, and thus have isomorphic homology,

$$H_p(C_\bullet) = H_p(C'_\bullet) \quad \text{for all } p \in \mathbb{Z} \ .$$

Now we have $H_1(C_\bullet \otimes D_\bullet) = 0$, but $H_1(C'_\bullet \otimes D_\bullet) = \mathbb{Z}/2\mathbb{Z}$ because

$$C'_\bullet \otimes D_\bullet : 0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{0} \mathbb{Z}/2\mathbb{Z} \to 0 \ .$$

The tensor product of the quasi-isomorphic complexes $C_\bullet$ and $C'_\bullet$ with the complex $D_\bullet$ are thus no longer quasi-isomorphic! The tensor product is not compatible with quasi-isomorphisms!

In particular, knowing the homology of the complexes is not sufficient to determine the homology of the tensor product. Put differently, if one considers complexes up to quasi-isomorphism as the fundamental objects, then one needs a different definition of the tensor product.

In the following theorem we make additional assumptions that, in particular, exclude torsion groups concentrated in a single degree, such as the ones in Example 6.8.1.

Theorem 6.8.2 [Künneth] Let $C_\bullet, D_\bullet$ be chain complexes of modules over a PID R. Suppose that one of the two complexes is flat, i.e. all involved modules are flat. Then there exists a natural short exact sequence

$$0 \to \bigoplus_{p+q=n} H_p(C_\bullet) \otimes_R H_q(D_\bullet) \xrightarrow{\zeta} H_n(C_\bullet \otimes D_\bullet) \to \bigoplus_{p+q=n-1} \mathrm{Tor}_1^R(H_p(C_\bullet), H_q(D_\bullet)) \to 0 \ ,$$

where ζ is induced by the inclusion

$$Z_p(C_\bullet) \otimes_R Z_q(D_\bullet) \to Z_{p+q}(C_\bullet \otimes_R D_\bullet)$$

of cycles. The sequence splits, though not naturally.

Proof. • Using the swap isomorphism of tensor product complexes over the ring R

$$\begin{array}{rcl} C_\bullet \otimes_R D_\bullet & \to & D_\bullet \otimes_R C_\bullet \\ c \otimes d & \mapsto & (-1)^{pq} d \otimes c \quad \text{for } c \in C_p \text{ and } d \in D_q \end{array}$$

we may assume without loss of generality that the complex $C_\bullet$ is flat.

- We introduce shorthand notation for cycles and boundaries

$$\begin{array}{ll} Z_p := Z_p(C_\bullet) & B_p := B_p(C_\bullet) \\ \overline{Z}_p := Z_p(D_\bullet) & \overline{B}_p := B_p(D_\bullet) \end{array}$$

and consider the the associated complexes with vanishing differential. We obtain an exact sequence of complexes

$$0 \to Z_\bullet \xrightarrow{\iota} C_\bullet \xrightarrow{\partial} B[-1]_\bullet \to 0 \ .$$

Since R is a PID, all these complexes are again flat, since they consist of subobjects of flat objects. As in the proof of Theorem 6.6.6 we obtain an exact sequence of complexes

$$0 \to Z_\bullet \otimes_R D_\bullet \xrightarrow{\iota\otimes\mathrm{id}} C_\bullet \otimes_R D_\bullet \xrightarrow{\partial\otimes\mathrm{id}} B[-1]_\bullet \otimes_R D_\bullet \to 0 \ .$$

By Theorem 6.4.3 this gives rise to a long exact sequence in homology, that we symbolically represent by:

$$\begin{array}{ccc} H(Z_\bullet \otimes_R D_\bullet) & \xrightarrow{(\iota\otimes\mathrm{id})_*} & H(C_\bullet \otimes_R D_\bullet) \ , \\ & {\scriptstyle\omega}\nwarrow \quad \swarrow{\scriptstyle(\partial\otimes\mathrm{id})_*} & \\ & H(B_\bullet[-1] \otimes_R D_\bullet) & \end{array}$$

where all morphisms have degree zero, except the morphism ω, which is generated by the connecting morphisms and which has degree -1. Undoing the degree shift at $B_\bullet$ we can also consider ω of degree zero and ∂ of degree -1.

- We inspect the homology $H(B[-1] \otimes_R D_\bullet)$. In the first tensor factor the differential is trivial and (after changing signs) we may work with the differential $\mathrm{id} \otimes \partial$. As all the B_n are flat, the kernels and images of this differential are tensor products of the kernel and images of the differential in $D_\bullet$. Thus we have

$$H_n(B[-1]_\bullet \otimes_R D_\bullet) = (B_\bullet \otimes_R H(D_\bullet))_{n-1}$$

Analogously we get

$$H_n(Z_\bullet \otimes_R D_\bullet) = (Z_\bullet \otimes_R H(D_\bullet))_n \ .$$

Thus we have a long exact sequence in homology

$$\begin{array}{ccc} Z_\bullet \otimes_R H(D_\bullet) & \xrightarrow{(\iota\otimes\mathrm{id})_*} & H(C_\bullet \otimes_R D_\bullet) \qquad (*) \\ & {\scriptstyle\omega}\nwarrow \quad \swarrow{\scriptstyle(\partial\otimes\mathrm{id})_*} & \\ & B_\bullet \otimes_R H(D_\bullet) & \end{array}$$

- We still have to inspect the morphism ω that comes from the connecting morphism. If we represent $\partial c \otimes [z] \in B \otimes_R H(D_\bullet)$ by $\partial c \otimes z$ then we see that $\omega(\partial c \otimes [z])$ is the homology class of $\partial c \otimes z$ in $Z_\bullet \otimes H(D_\bullet)$. Thus ω is induced by the inclusion $B_\bullet \to Z_\bullet$.

  Thus it is clear that $(\iota \otimes \mathrm{id})_*$ induces the map $H(C_\bullet) \otimes_R H(D_\bullet) \xrightarrow{\zeta} H_n(C_\bullet \otimes D_\bullet)$ when computing modulo boundaries, i.e. modulo the image of ω.

- We need another exact sequence: tensoring the short exact sequence

  $$0 \to B_\bullet \to Z_\bullet \to H(C_\bullet) \to 0$$

  with $H(D_\bullet)$ and noting $\mathrm{Tor}_1^R(Z_\bullet, H(D_\bullet)) = 0$, because $Z_\bullet$ is flat, the long exact sequence in homology yields the exact sequence

  $$0 \to \mathrm{Tor}_1^R(H(C_\bullet), H(D_\bullet)) \to B_\bullet \otimes_R H(D_\bullet) \xrightarrow{\omega} Z_\bullet \otimes_R H(D_\bullet) \to H(C_\bullet) \otimes_R H(D_\bullet) \to 0 \quad (**)$$

  of complexes.

  By $(*)$ the kernel of ζ is the image of ω. Thus we have $Z_\bullet \otimes_R H(D_\bullet)/\ker\zeta = \mathrm{coker}\omega \overset{(**)}{=} H(C_\bullet) \otimes_R H(D_\bullet)$ and we obtain the injection

  $$0 \to H(C_\bullet) \otimes_R H(D_\bullet) \xrightarrow{\zeta} H(C_\bullet \otimes_R D_\bullet) \ .$$

  We still have to compute the cokernel of ζ. We find

  $$\begin{array}{rcl} \mathrm{coker}\zeta & = & H(C_\bullet \otimes_R D_\bullet)/\mathrm{Im}\,\zeta \overset{(*)}{=} H(C_\bullet \otimes_R D_\bullet)/\ker(\partial \otimes \mathrm{id})_* \\ & \overset{(H)}{=} & \mathrm{Im}\,(\partial \otimes \mathrm{id})_* \overset{(*)}{=} \ker\omega \overset{(**)}{=} \mathrm{Tor}_1^R(H(C_\bullet), H(D_\bullet)) \ . \end{array}$$

  where we have used the homomorphism theorem at (H).

- For a proof of the fact that the Künneth sequence splits, we refer to [HS1970, V.2]. □

An important special case is when $C_\bullet$ is flat and $D_\bullet$ is an R-module A concentrated in degree 0.

Corollary 6.8.3 [Universal coefficient theorem in homology] Let R be a PID, $C_\bullet$ a flat chain complex of R-modules and A an R-module. Then there exists a natural short exact sequence

$$0 \to H_n(C_\bullet) \otimes_R A \xrightarrow{\zeta} H_n(C_\bullet \otimes_R A) \to \mathrm{Tor}_1^R(H_{n-1}(C_\bullet), A) \to 0 \ .$$

This exact sequence splits, naturally in A, though not naturally in $C_\bullet$.

Proof. Only the naturality statement is still open, and we refer again to [HS1970] for a proof. □

We also state the corresponding theorem for Ext, a proof appears in [HS1970, V.3].

Theorem 6.8.4 Let $C_\bullet, D_\bullet$ be chain complexes of modules over a PID R. Assume that the complex $C_\bullet$ is free. Then there exists a natural short exact sequence

$$0 \to \prod_{q-p=n+1} \mathrm{Ext}_R^1(H_p(C_\bullet), H_q(D_\bullet)) \to H_n(\mathrm{Hom}_R(C_\bullet, D_\bullet) \xrightarrow{\zeta} \bigoplus_{q-p=n} \mathrm{Hom}_R(H_p(C_\bullet), H_q(D_\bullet)) \to 0 \ ,$$

where ζ maps the morphism $f \in Z_n(\mathrm{Hom}_R(C_\bullet, D_\bullet))$ to the induced morphism $F_n \colon H_n(C_\bullet) \to H_n(D_\bullet)$. The sequence splits, though not naturally.

Analogously we get:

Corollary 6.8.5 [Universal coefficient theorem in cohomology] Let R be a PID, $C_\bullet$ a free chain complex of R-modules, and B an R-module. Then there exists a natural short exact sequence

$$0 \to \mathrm{Ext}^1_R(H_{n-1}(C_\bullet), B) \to H^n(\mathrm{Hom}_R(C_\bullet, B)) \xrightarrow{\zeta} \mathrm{Hom}_R(H_n(C_\bullet), B) \to 0 \ .$$

This exact sequence splits, naturally in B, though not naturally in $C_\bullet$.

7 Group cohomology

7.1 Definition and examples

Let G be a group. By a G-module we mean $\mathbb{Z}[G]$-module in this chapter. This is nothing but an abelian group M with a G-action $G \to \mathrm{Aut}_{\mathbb{Z}}(M)$ by morphisms of abelian groups. If A is an abelian group, then we may consider A as G-module with the trivial action, $\rho(g) = \mathrm{id}_A$ for all $g \in G$.

We first define:

Definition 7.1.1 The <u>invariants</u> M^G of a G-module M are the fixed points of the G-action:

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

i.e. the largest trivial submodule. The <u>coinvariants</u> M_G are defined as the quotient abelian group

$$M_G = M/(gm - m | g \in G, m \in M) \ ,$$

i.e. as the largest trivial quotient.

We turn invariants and coinvariants into additive functors

$$(-)^G, (-)_G \colon \mathbb{Z}[G]\text{−Mod} \to Ab \ ,$$

that are defined on $\mathbb{Z}[G]$-module homomorphism $f \colon M \to N$ as follows. By $g.m = m$ for all $g \in G$ we get $g.f(m) = f(g.m) = f(m)$ for all $g \in G$, and so the the restriction of f to the invariants M^G yields a homomorphism $f^G \colon M^G \to N^G$ of abelian groups. Since $f(gm - m) = gf(m) - f(m)$, the homomorphism $M \xrightarrow{f} N \xrightarrow{\mathrm{can}} N_G$ factors through a homomorphism of abelian groups $f_G \colon M_G \to N_G$ on the coinvariants,

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow{\scriptstyle \mathrm{can}} & & \downarrow{\scriptstyle \mathrm{can}} \\ M_G & \dashrightarrow & N_G \end{array}$$

Lemma 7.1.2 There exist natural isomorphisms $M^G \cong \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$ and $M_G \cong \mathbb{Z} \otimes_{\mathbb{Z}[G]} M$, where the abelian group $\mathbb{Z}$ is equipped with the trivial left- resp. right module structure. In particular, by Example 3.1.14.4, the functor of taking invariants $(-)^G$ is left exact and the functor of taking coinvariants $(-)_G$ is right exact by Example 3.1.14.3.

Proof. For the first isomorphism, we note that an element of $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, M)$ is uniquely determined by the value on $1 \in \mathbb{Z}$. For such a homomorphism to lie in $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M) \subset \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, M)$, we must have for all $g \in G$ that $g.f(1) = f(g.1) = f(1)$, hence $f(1) \in M^G$. Conversely, every such $x \in M^G$ defines a morphism in $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$.

For the second isomorphism we consider the surjective map

$$\begin{array}{rccl} \phi\colon & M & \to & \mathbb{Z} \otimes_{\mathbb{Z}[G]} M \\ & m & \mapsto & 1 \otimes m \end{array}$$

In the abelian group $\mathbb{Z} \otimes_{\mathbb{Z}[G]} M$ we have

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

and so the map ϕ descends to the quotient M_G, i.e. to the coinvariants. The map ϕ and thus also its induced map is surjective. It is clear that $1 \otimes m$ and $1 \otimes m'$ are equal if and only if $m \in M$ and $m' \in M$ represent the same class in the coinvariants. □

Definition 7.1.3 Let M be a $\mathbb{Z}[G]$-module.

1. The nth homology of the group G with coefficients in the $\mathbb{Z}[G]$-module M is defined as the nth left derived functor of the coinvariants:

$$H_n(G; M) := (L_n(-)_G)(M) \ = \ \mathrm{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, M) \ .$$

2. The nth cohomology of the group G with coefficients in the $\mathbb{Z}[G]$-module M is defined as

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

If M is the trivial G-module $\mathbb{Z}$, then we abbreviate $H_n(G) := H_n(G, \mathbb{Z})$ and $H^n(G) := H^n(G, \mathbb{Z})$.

Remark 7.1.4 The preceding definitions also make sense for monoids in place of groups G. Several effective methods work only for groups, so we restrict to this case.

Example 7.1.5 (homology of a cyclic group C_n)

1. Let $G = C_n = \langle t \rangle$ be a cyclic group of order $n \in \mathbb{N}$ with generator $t \in G$. Then $R := \mathbb{Z}[G] \cong \mathbb{Z}[t]/(t^n - 1)$, and we have already computed the homology in Example 6.5.2.3:

$$H_k(C_n) \cong \begin{cases} \mathbb{Z}, & \text{if } k = 0\,; \\ \mathbb{Z}/n\mathbb{Z}, & \text{if } k \text{ odd } ; \\ 0, & \text{otherwise.} \end{cases}$$

2. Now we consider the abelian group $A = \mathbb{Z}/n\mathbb{Z}$ with the trivial $\mathbb{Z}[G]$-module structure as coefficients. After tensoring the resolution from Example 6.5.2.3

$$\cdots \stackrel{N}{\to} R \stackrel{1-t}{\to} R \stackrel{N}{\to} R \stackrel{1-t}{\to} R \stackrel{\epsilon}{\to} \mathbb{Z} \to 0 \qquad (*)$$

(recall $N := 1 + t + \cdots + t^{n-1}$) with $\mathbb{Z}/n\mathbb{Z}$, we get the complex

$$\ldots \stackrel{0}{\to} \mathbb{Z}/n\mathbb{Z} \stackrel{0}{\to} \mathbb{Z}/n\mathbb{Z} \to 0$$

and thus $H_k(C_n; \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$ for all $k \geq 0$.

3. Next we consider an arbitrary module over a cyclic group C_n. The image of the multiplication by $N = 1 + t + \cdots + t^{n-1}$ is contained in the invariants M^G since $gN = N$ for all $g \in C_n$. The multiplication thus maps $M \to M^G$. Furthermore, $Ngm = Nm$ for all $g \in C_n$ and so the multiplication by N descends to a so-called norm map $\bar{N}\colon M_G \to M^G$ on the quotient M_G.

   In the case of a cyclic group with generator t we have for the invariants resp. coinvariants

$$\ker(1-t) = M^G \quad \text{resp.} \quad M/\mathrm{Im}\,(1-t) = M_G$$

   and thus

$$\ker N/\mathrm{Im}\,(1-t) = \ker \bar{N} \quad \text{resp.} \quad \ker(1-t)/\mathrm{Im}\, N = M^G/\mathrm{Im}\,\bar{N} = \mathrm{coker}\bar{N}\ .$$

   By tensoring the resolution $(*)$ from Example 6.5.2.3 with M we get the complex

$$\cdots M \overset{1-t}{\to} M \overset{N}{\to} M \overset{1-t}{\to} M \to 0$$

   and thus

$$H_k(\mathbb{Z}_n; M) \cong \begin{cases} M/\mathrm{Im}\,(1-t) = M_G, & \text{if } k = 0 \text{ (cf. Lemma 6.3.5);} \\ \ker(1-t)/\mathrm{Im}\, N = \mathrm{coker}\bar{N}, & \text{if } k \text{ odd;} \\ \ker N/\mathrm{Im}\,(1-t) = \ker \bar{N}, & \text{if } k > 0 \text{ and } k \text{ even.} \end{cases}$$

4. Analogously we can compute the cohomology. By applying $\mathrm{Hom}_R(-, M)$ to the resolution $(*)$ from Example 6.5.2.3 we get the complex

$$0 \to M \overset{1-t}{\to} M \overset{N}{\to} M \overset{1-t}{\to} M \overset{N}{\to} \cdots$$

   and thus

$$H^k(\mathbb{Z}_n; M) \cong \begin{cases} \ker(1-t) = M^G & \text{if } k = 0 \text{ (cf. Lemma 6.3.5);} \\ \ker N/\mathrm{Im}\,(1-t) = \ker \bar{N}, & \text{if } k \text{ odd;} \\ \ker(1-t)/\mathrm{Im}\, N = \mathrm{coker}\bar{N}, & \text{if } k > 0 \text{ even.} \end{cases}$$

Example 7.1.6 (homology of the free abelian group $\mathbb{Z}$) The group ring of the group $G = \mathbb{Z}$ is $\mathbb{Z}[G] \cong \mathbb{Z}[t, t^{-1}]$, i.e. the ring of Laurent polynomials $a_m t^m + \cdots + a_n t^n$ with $m \leq n$ and $n, \in \mathbb{Z}$ and $a_n \in \mathbb{Z}$. A free resolution of the trivial module $\mathbb{Z}$ as $\mathbb{Z}[G]$-module is given by the augmented complex

$$0 \to \mathbb{Z}[t, t^{-1}] \overset{1-t}{\to} \mathbb{Z}[t, t^{-1}] \overset{t\mapsto 1}{\to} \mathbb{Z} \to 0\ .$$

Tensoring the corresponding resolution with a module M over $\mathbb{Z}[G]$, one obtains the complex

$$0 \to M \overset{1-t}{\to} M \to 0$$

from which we get

$$H_0(G; M) = M/\mathrm{Im}\,(1-t) = M_G \quad \text{and} \quad H_1(G; M) = \ker(1-t) = M^G\ .$$

The result for $H_0(G, M)$ again agrees with Lemma 6.3.5. The application of $\mathrm{Hom}_{\mathbb{Z}}(-, M)$ yields the same complex, but with different grading, and thus

$$H_0(G; M) = H^1(G; M) = M_G \text{ and } H_1(G; M) = H^0(G; M) = M^G\ .$$

Alle higher homology and cohomology groups vanish since the resolution of the trivial $\mathbb{Z}[G]$-module $\mathbb{Z}$ has length 2.

Remark 7.1.7 (Maschke's theorem) We can interpret Maschke's theorem as a consequence of a statement concerning group cohomology. Let G be a finite group and K a field, whose characteristic does not divide the order $|G|$ of the group. One can show (cf. [HS1970, Lemma VI.16.7]) that for *every* $K[G]$-module W and all $n \geq 1$ one has $H^n(G, W) = 0$. We show that this vanishing result implies Maschke's Theorem 4.3.13.

To see this we let

$$0 \to V' \to V \to V'' \to 0$$

be an arbitrary short exact sequence of $K[G]$-modules. We aim to show that the induced sequence

$$0 \to \mathrm{Hom}_G(V'', V') \to \mathrm{Hom}_G(V, V') \to \mathrm{Hom}_G(V', V') \to 0 \qquad (*)$$

is exact. Then any preimage of the identity $\mathrm{id}_{V'}$ yields a retraction $V \to V'$ of $K[G]$-modules, so that the exact sequence $0 \to V' \to V \to V'' \to 0$ splits, cf. Theorem 1.4.3. To see the exactness of $(*)$, we consider the corresponding short exact sequence of K-vector spaces,

$$0 \to \mathrm{Hom}_K(V'', V') \to \mathrm{Hom}_K(V, V') \to \mathrm{Hom}_K(V', V') \to 0 \ ,$$

that we may interpret as exact sequence of $K[G]$-modules. The G-action on these vector spaces of linear maps is given by

$$\begin{array}{rcl} K[G] \times \mathrm{Hom}_K(V, W) & \to & \mathrm{Hom}_K(V, W) \\ (g, \varphi) & \mapsto & g.\varphi(g^{-1}-) \ . \end{array}$$

Since the elements of $\mathrm{Hom}_G(V, W)$ are exactly the G-invariants in the $K[G]$-module $\mathrm{Hom}_K(V, W)$ we have to show that the sequence of invariants

$$0 \to H^0(G, \mathrm{Hom}_K(V', V')) \to H^0(G, \mathrm{Hom}_K(V, V')) \to H^0(G, \mathrm{Hom}_K(V'', V')) \to 0$$

is exact. This follows via the long exact sequence 6.4.4 from $H^1(G, W) = 0$ with the $K[G]$-module $W = \mathrm{Hom}_K(V', V')$.

7.2 Functoriality

Homology and cohomology are functors, but the definition requires some care.

Definition 7.2.1 Let $GrpMod$ be the category, whose objects are pairs, consisting of a group G and a G-module M, and whose morphisms are defined by

$$\begin{array}{l} \mathrm{Hom}_{GrpMod}((G, M), (G', M')) := \{\alpha \colon G \to G', f \colon M \to M' | f(g.m) = \alpha(g) f(m) \\ \text{and } \alpha \text{ group homomorphism}\} \ . \end{array}$$

Remarks 7.2.2

1. A morphism $(\alpha, f) \colon (G, M) \to (G', N)$ is thus a morphism $f \colon M \to \alpha^* N$ of $K[G]$-modules, where $\alpha^* N$ denotes the $K[G]$-module obtained by pullback along α, i.e. restriction of scalars, from N.

2. For a fixed G one can consider the category $\mathrm{Mod}_{\mathbb{Z}[G]}$ as subcategory of $GrpMod$. This subcategory is not full, since $GrpMod$ has more morphisms, namely also those with $\alpha \neq \mathrm{id}_G$. We know that homology is a functor on this subcategory, because of the functoriality of Tor in the second argument.

3. On the other hand, one can fix an abelian group M and consider $Grp \hookrightarrow GrpMod$ as a subcategory by mapping the group G to (G, M) with the trivial G-module structure on M. Once we know that group homology is a functor, we obtain for every group homomorphism $\alpha\colon G \to H$ an induced map $\alpha_*\colon H_i(G) \to H_i(H)$ on the group homology with trivial coefficients.

Theorem 7.2.3 Group homology defines a functor $GrpMod \to Ab$ in every degree.

Proof. We have to define the functor on morphisms. Let $(\alpha, f)\colon (G, M) \to (H, N)$ be a morphism in $GrpMod$. Choose projective resolutions $P_\bullet \to M$ over the ring $\mathbb{Z}[G]$ and $Q_\bullet \to N$ over $\mathbb{Z}[H]$. We can pull back all H-modules Q_n in $Q_\bullet$ along α to G-modules, and thus consider $Q_\bullet$ as complex of $\mathbb{Z}[G]$-modules, with the same map as differential. This complex may no longer be projective; but since the differential is unchanged, the complex is still acyclic. By Theorem 6.3.1 there exists an up to homotopy unique lift $f_\bullet\colon P_\bullet \to \alpha^*(Q)_\bullet$ of the morphism $f\colon M \to \alpha^*(N)$ of G-modules. This induces a morphism of complexes of abelian groups

$$\mathrm{id} \otimes f_\bullet\colon \mathbb{Z} \otimes_{\mathbb{Z}[G]} P_\bullet \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} \alpha^*(Q)_\bullet \ .$$

The tensor product $\mathbb{Z} \otimes_{\mathbb{Z}[G]} \alpha^*(Q)_\bullet$ on the right hand side surjects to $H_i(H; N)$. Hence, we get a well-defined map $(\alpha, f)_*\colon H_i(G; M) \to H_i(H; N)$. The functoriality is a consequence of the uniqueness of the lift up to homotopy. □

Example 7.2.4 We show that the surjective group homomorphism $\alpha\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ induces a surjective morphism on the homology group $H_1(-; \mathbb{Z})$. We consider the standard resolutions of the trivial modules from Example 7.1.5 and Example 7.1.6 and an obvious lift of the identity on the trivial module $\mathbb{Z}$:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}[t,t^{-1}] & \xrightarrow{1-t} & \mathbb{Z}[t,t^{-1}] & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle t\mapsto t} & & \downarrow{\scriptstyle t\mapsto t} & & \| & & \\
\cdots & \xrightarrow{N} & \mathbb{Z}[t]/(t^n-1) & \xrightarrow{1-t} & \mathbb{Z}[t]/(t^n-1) & \longrightarrow & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

By passing to coinvariants on the resolutions we obtain the chain map

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{0} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \| & & \| & & \\
\cdots & \xrightarrow{n} & \mathbb{Z} & \xrightarrow{0} & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

and so the map on $H_1(-, \mathbb{Z})$ is the standard reduction $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ of abelian groups.

Theorem 7.2.5 Let G be a group and M a G-module. Let $g_0 \in G$ and consider the automorphism $(\alpha, f)\colon M \to M$ in $GrpMod$ given by $\alpha(g) := g_0 g g_0^{-1}$ and $f(m) := g_0.m$. [3] This induces the identity in homology, $(\alpha, f)_* = \mathrm{id}_{H_*(G;M)}$.

Proof. Let $P_\bullet \to M$ be a projective resolution of M over the ring $\mathbb{Z}[G]$. Define an automorphism of $P_\bullet$ by $\tau(x) = g_0.x$ for $x \in P_n$, for all n. Then τ is an automorphism of chain complexes, that extends the morphism $f\colon M \to M$, thus the morphism $(\alpha, f)_*$ can be computed as the map induced by τ in homology. But upon tensoring with the trivial module $\mathbb{Z}$, on which g_0 acts trivially, we have that

$$\mathrm{id}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \tau\colon \mathbb{Z} \otimes_{\mathbb{Z}[G]} P_n \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} P_n$$

is the identity. □

[3] Then we have $f(gm) = g_0 g m = g_0 g g_0^{-1} g_0 m = \alpha(g) f(m)$.

Remark 7.2.6 If G is a group, then the automorphism that can be represented as conjugation are called the inner automorphisms; these form a normal subgroup $\mathrm{Inn}(G) \subset \mathrm{Aut}(G)$. The quotient group $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the group of outer automorphisms. Then Theorem 7.2.5 shows, that the group homology $H_*(G)$ carries an action of the quotient group $\mathrm{Out}(G)$.

7.3 The bar resolution

In the previous examples we have always constructed resolutions by hand and in an ad hoc way. It is natural to ask whether there is a canonical, functorial way to construct a resolution of a module over $\mathbb{Z}[G]$. Indeed there ist, but only rarely is it helpful for explicitly computating the entire group homology, because it is so large.

Definition 7.3.1 Let R be a ring and M an R-module. To define the bar complex $B_\bullet(R;M)$, we consider for $n \geq 0$ the abelian groups

$$B_n(R;M) := R^{\otimes n+1} \otimes_{\mathbb{Z}} M \equiv R \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} R \otimes_{\mathbb{Z}} \ M.$$

For historical reasons we use the notation $a|b$ for $a \otimes b$; this is where the name comes from. We equip the abelian group $B_n(R;M)$ with an R-module structure by left multiplication

$$r.(r_0|\cdots|r_n|m) := rr_0|r_1|\cdots|r_n|m \ .$$

Finally we define the differentials $d\colon B_n(R,M) \to B_{n-1}(R,M)$ by

$$d := \sum_{i=0}^{n} (-1)^i d_i \ \text{ with } \ d_i(r_0|\cdots|r_n|m) := r_0|\cdots|r_ir_{i+1}|\cdots|r_n|m \ ,$$

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

Theorem 7.3.2 The complex $B_\bullet(R;M)$ is a resolution of M over R, i.e. an acyclic complex of R-modules with surjection to M.

Proof. In order to show that $B_\bullet(R;M)$ a complex is, we note that

$$d_i \circ d_j = d_j \circ d_{i+1} \text{ if } i \geq j \qquad (*)$$

holds. It is instructive to check that for $i = j+1$ this equation uses the associativity of the multiplication in R and the module properties of M. Now we compute

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

Here we first split the sum, then apply the relation $(*)$ to the first summands and finally reorder the first sum.

We have to show that the complex $B_\bullet(R;M)$ is exact upon augmenting with the obvious surjection to M, which we temporarily denote by $M =: B_{-1}(R;M)$. To this end we construct a contracting homotopy, i.e. a chain homotopy $h\colon B_n(R;M) \to B_{n+1}(R;M)$ for $n \geq -1$, such that $h \circ d + d \circ h = \mathrm{id}$. For this we use the unit $1 \in R$ and set

$$h(r_0|\cdots|r_n|m) := 1|r_0|\cdots|r_n|m \ .$$

Then we have $h \circ d_i = d_{i+1} \circ h$ for $i = 0, \ldots, n$ and thus

$$d \circ h + h \circ d \stackrel{\text{def}}{=} \sum_{i=0}^{n+1} (-1)^i d_i \circ h + \sum_{i=0}^{n} (-1)^i h \circ d_i = d_0 \circ h = \mathrm{id}\,. \qquad \square$$

Remarks 7.3.3

1. The R-module $B_n(R, M)$ is not necessarily projective; for example when $R = \mathbb{Z}$ and $M = \mathbb{Z}/n\mathbb{Z}$, we have $B_n(R; M) = R^{\otimes n+1} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$. However, if the ring R and the module M are free as abelian groups, then $B_n(R; M)$ is a free R-module for all n, since we tensor over $\mathbb{Z}$. We have found a free and, in particular, projective resolution.

2. Group rings $R = \tilde{R}[G]$ are always free as abelian groups, whenever the ground ring $\tilde{R}$ is free as abelian group.

3. More generally, if K is a commutative ground ring, R is a K-algebra, and if all tensor products in $B_n(R; M)$ are formed over K instead if $\mathbb{Z}$, then $B_n(R; M)$ is a free R-module whenever R and M are free K-modules. For a field K this is always the case.

We can now give a concrete interpretation of the first homology group in terms of classical algebraic notions.

Example 7.3.4 (First homology)

- We recall the concept of abelianization: Let G be an arbitrary group, and denote by G_{ab} the abelianization, i.e. the maximal abelian quotient of G. Then $G_{ab} = G/G'$, where G' is the normal subgroup generated by the commutators $[x, y] := xyx^{-1}y^{-1}$ with $x, y \in G$.

  By Examples 2.3.2.5 abelianization is the left adjoint functor to the inclusion functor $Ab \to Grp$. For every abelian group A we thus have

  $$\mathrm{Hom}_{Grp}(G, A) \cong \mathrm{Hom}_{\mathbb{Z}}(G_{ab}, A)\ .$$

  The corresponding universal property determines G_{ab} up to unique isomorphism.

- We claim that for all groups we have $H_1(G; \mathbb{Z}) \cong G_{ab}$. To see this, we consider the start of the bar resolution of the trivial module $\mathbb{Z}$ over $\mathbb{Z}[G]$ and note:

  $$B_n(\mathbb{Z}[G], \mathbb{Z}) = \mathbb{Z}[G]^{\otimes_{\mathbb{Z}}(n+1)} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}[G]^{\otimes_{\mathbb{Z}}(n+1)}$$

  The first differentials are:

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

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

  $$g_0|g_1 \longmapsto g_0g_1 - g_0$$

  Note that on the trivial module the rightmost element acts trivially. Since $\mathbb{Z}$ is a free $\mathbb{Z}$-module, we have found a free resolution of the trivial $\mathbb{Z}[G]$-module $\mathbb{Z}$. To compute the

homology $H_1(G,\mathbb{Z})$ with coefficients in the trivial module $\mathbb{Z}$, we tensor this sequence on the left with the trivial $\mathbb{Z}[G]$-module $\mathbb{Z}$ over $\mathbb{Z}[G]$ and obtain

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

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

$$g \longmapsto 0$$

Thus we have

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

- The map

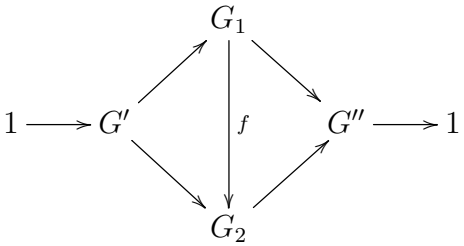
$$G \to \mathbb{Z}[G] \overset{\text{can}}{\to} \mathbb{Z}[G]/(g_1+g_2-g_1g_2 \,\|\, g_1,g_2\in G) \cong H_1(G;\mathbb{Z})$$

is an epimorphism of groups because in the quotient the class of $ng \in \mathbb{Z}[G]$ equals the class of g^n. It thus suffices to show that this map satisfies the universal property of the abelianization, i.e. that every group homomorphism $f\colon G \to A$ into an abelian group factors uniquely through $H_1(G;\mathbb{Z})$. Since A is abelian, one can extend f *uniquely* to a homomorphism $\mathbb{Z}[G]\to A$, namely by $\sum_g a_g g \mapsto \sum_g a_g f(g)$. Under this map an element of the form $g_1+g_2-g_1g_2$ is sent to zero because f is a group homomorphism. Thus $H_1(G;\mathbb{Z})$ satisfies the universal property of the abelianization, see Example 2.3.2.3.

7.4 Group cohomology and group extensions

Observation 7.4.1

1. Let $G'\triangleleft G$ be a normal subgroup in a group G with quotient group G''. We take the liberty to encode this by an exact sequence $1\to G'\to G\to G''\to 1$, even though the category of groups is not abelian. In this case we call G an extension of G'' by G'. Two extensions are said to be equivalent, if there exists a commutative diagram of group homomorphisms:



In this case f is automatically an isomorphism: The commutativity of the right triangle means $\ker f \subset \ker(G_1\to G'')$. If $x\in\ker f\subset\ker(G_1\to G'') = \operatorname{Im}(G'\to G_1)$, then we can find a preimage $y\in G'$, which is mapped injectively into G_2. There the image $f(x)$ is the neutral element, and so the two elements $y\in G'$ and also $x\in G_1$ are both the neutral elements. Thus f is injective.

To verify surjectivity, consider $x_2\in G_2$ and its image $x''\in G''$, for which we can find a preimage $x_1\in G_1$. Then $f(x_1)$ and x_2 have the same image in G'', and so $f(x_1)x_2^{-1}\in \ker(G_2\to G'') = \operatorname{Im}(G'\to G_2)$. Thus $f(x_1) = x_2\iota_2(g') = x_2 f(\iota_1 g')$ for some $g'\in G'$. We have $x_2 = f(x_1\iota_1(g')^{-1})$ and so f is surjective.

2. Consider an extension $1 \to G' \to G \to G'' \to 1$ with *abelian* normal subgroup G'. Then the quotient group G'', which is not necessarily abelian, acts on the abelian group G' as follows. Let $g \in G$ be a preimage of $g'' \in G''$. For $g_0 \in G'$ we set

$$g''.g_0 := gg_0g^{-1} \ .$$

As G' is a normal subgroup, the element $g''.g_0$ is again in G'. The choice of preimage g of g'' is immaterial, since any two choices differ by conjugation by an element of the abelian group G', and conjugation by elements of G' is the identity on on the abelian group G'.

3. Conversely, every action $\alpha\colon G'' \to \mathrm{Aut}(G')$ of G'' on *an arbitrary group* G' by group automorphisms gives rise to an extension $G = G' \rtimes_\alpha G''$, called the semi-direct product . The underlying set of G is $G' \times G''$, and the multiplication is defined by

$$(g'_1, g''_1) \cdot (g'_2, g''_2) := (g'_1(g''_1.g'_2), g''_1g''_2) \ .$$

This defines a group, and we sometimes suppress the datum α from the notation $G' \rtimes_\alpha G''$ by simply writing $G' \rtimes G''$ instead. The group homomorphisms

$$\begin{array}{ccc} G' & \to & G' \rtimes G'' \\ g' & \mapsto & (g', e) \end{array}$$

and

$$\begin{array}{ccc} G' \rtimes G'' & \to & G'' \\ (g', g'') & \mapsto & g'' \end{array}$$

give an extension $1 \to G' \to G' \rtimes G'' \to G'' \to 1$. In particular, G' is a normal subgroup. (The mnemonic for the symbol $\rtimes$: the pointy end of the triangle is towards the normal subgroup). More specifically, one can verify that conjugation by (e, g'') in $G' \rtimes G''$ recovers the automorphism α:

$$(e, g'')(g', e)(e, g'')^{-1} = (\alpha(g'')(g'), e) \ .$$

4. The extension $1 \to G' \to G' \rtimes G'' \to G'' \to 1$ splits, with a section given by the group homomorphism $s_0\colon G'' \to G' \rtimes G''$ that sends $g'' \mapsto (1, g'')$. Two sections $s_1, s_2\colon G'' \to G' \rtimes G''$ are said to be equivalent, if they differ by conjugation with an element from G', i.e. if $s_2(g'') = g's_1(g'')(g')^{-1}$ for some $g' \in G'$ and for all $g'' \in G''$. Conversely, every split extension exhibits the middle group as isomorphic to a semi-direct product of the outer two groups.

5. Two natural questions arise:

   - Do all extensions split, so that we have a semi-direct product? If not, how can one classify extensions up to equivalence?
   - in case we have a semidirect product: is s_0 the only possible section? If not, how can one describe the set of all sections up to equivalence?

6. Group cohomology answers both questions, at least for abelian normal subgroups G'. We first consider the second item. A section $s = (\delta, \mathrm{id})\colon G'' \to G' \rtimes G''$ must be the identity on the second coordinate. We write the first component with values in an abelian group G' additively. The section is required to be a group homomorphism,

$$(\delta g''_1, g''_1) \cdot (\delta g''_2, g''_2) = (\delta g''_1 + g''_1.\delta g''_2, g''_1g''_2) \stackrel{!}{=} (\delta(g''_1g''_2), g''_1g''_2) \ ,$$

and so the function $\delta\colon G'' \to G'$, that determines the section s, must satisfy the equation

$$\delta(g''_1g''_2) = \delta(g''_1) + g''_1.\delta(g''_2) \ . \tag{3}$$

7. If two functions $\delta_1, \delta_2 \colon G'' \to G'$ both satisfy the equation (3), then so does their sum $\delta_1 + \delta_2$; this defines an abelian group structure on the set of all sections. A section δ is equivalent to the zero section s_0 if and only if there exists a $g' \in G'$ such that

$$\delta(g'') = g' - g''.(g') \quad \text{for all } g'' \in G'' \ .$$

Theorem 7.4.2 Let G' be an abelian group; let G'' be a group that acts by group automorphisms on G' via $\alpha \colon G'' \to \mathrm{Aut}(G')$. Then the group of sections $G'' \to G' \rtimes_\alpha G''$ up to equivalence is isomorphic to $H^1(G'', G')$, where we consider the abelian group G' as a G''-module using the action α.

Proof. • As in Example 7.3.4 we consider the bar resolution of the trivial G''-module $\mathbb{Z}$ and study the complex of abelian groups with

$$C^n := \mathrm{Hom}_{\mathbb{Z}[G'']}(\mathbb{Z}[G'']^{\otimes n+1}, G') \ .$$

Then by definition of group cohomology we have $H^n(G'', G') = H^n(C^\bullet)$. A 1-cochain in C^1 is a $\mathbb{Z}[G'']$-linear morphism with values in the abelian group G',

$$f \colon \mathbb{Z}[G''] \otimes_{\mathbb{Z}} \mathbb{Z}[G''] \to G' \quad .$$

By the isomorphism for induced $\mathbb{Z}[G'']$-modules

$$\begin{array}{rcl} \mathrm{Hom}_{\mathbb{Z}[G'']}(\mathbb{Z}[G''] \otimes_{\mathbb{Z}} \mathbb{Z}[G''], G') & \to & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G''], G') \\ f & \mapsto & s(-) = f(1, -) \end{array}$$

this function is equivalent to a $\mathbb{Z}$-linear morphism $s \colon \mathbb{Z}[G''] \to G'$. (Conversely $f(g_1''|g_2'') = g_1''.s(g_2'')$.) The morphism of abelian groups $s \colon \mathbb{Z}[G''] \to G'$ is determined by its values on the basis $G'' \subset \mathbb{Z}[G'']$ and thus equivalent to a function $\delta \colon G'' \to G'$. The function f is a cocycle in the resolution if and only if

$$0 = df(g_0''|g_1''|g_2'') = f(g_0''g_1''|g_2'') - f(g_0''|g_1''g_2'') + f(g_0''|g_1'')$$

gilt, i.e. if and only if (for $g_0'' = 1$) the function δ satisfies

$$0 = g_1''\delta(g_2'') - \delta(g_1''g_2') + \delta(g_1'') \ . \tag{4}$$

In other words, δ satisfies the equation (3). So 1-cochains correspond to sections.

• Furthermore, f is a coboundary if and only if there exists a $\mathbb{Z}[G]$-linear morphism $\tilde{f} \colon \mathbb{Z}[G] \to G'$ such that

$$f(g_0''|g_1'') = \tilde{f}(g_0'') - \tilde{f}(g_1'') \ ,$$

i.e. iff there exists an $g' = \tilde{f}(1) \in G'$, such that

$$\delta(g_1'') = f(1, g_1'') = \tilde{f}(1) - \tilde{f}(g_1'') = g' - g_1''(g') \ . \tag{5}$$

By Observation 7.4.1.7 this is the case if and only if the section is equivalent to the zero section s_0. □

In preparation for Theorem 7.4.3 we describe the elements of the cohomology group $H^2(G'', G')$ as equivalence classes of functions $f \colon G'' \times G'' \to G'$ with

$$(df)(g_1'', g_2'', g_3'') = g_1''.f(g_2'', g_3'') - f(g_1''g_2'', g_3'') + f(g_1'', g_2''g_3'') - f(g_1'', g_2'') = 0 \ , \tag{6}$$

modulo the equivalence relation generated by declaring two functions equivalent if they differ by an expression of the form

$$da(g_1'', g_2'') := a(g_1'') - a(g_1''g_2'') + g_1''.a(g_2'')$$

for some function $a \colon G'' \to G'$.

Theorem 7.4.3 Let G'' be a group, that acts on the abelian group G' by group automorphisms. Then there exists a bijection from the set of extensions of G'' by G' up to equivalence as in Observation 7.4.1.1 to $H^2(G'', G')$, where we consider the abelian group G' as G''-module as before.

Proof. • Let $E\colon 1 \to G' \to G \to G'' \to 1$ be such an extension. In general, one will not be able to find a section $G'' \to G$ that is a group homomorphism. We thus choose a section $s\colon G'' \to G$ of sets. Then we have $s(g_1'')s(g_2'')s(g_1''g_2'')^{-1}$ in $\ker(G \to G'') = \mathrm{Im}\,(G' \to G) \cong G'$. We can thus define the function

$$\begin{array}{rcl} f_{E,s}\colon G'' \times G'' & \to & G' \\ (g_1'', g_2'') & \mapsto & s(g_1'')s(g_2'')s(g_1''g_2'')^{-1}\ . \end{array}$$

One can check that the cocycle condition (6) is satisfied; so $f_{E,s}$ defines a class in $H^2(G'', G')$.

- If $s'\colon G'' \to G$ is another section for the same extension, then we set $a := s's^{-1}\colon G'' \to G'$. Then we have

$$\begin{array}{rcl} (f_{E,s'} - f_{E,s})(g_1'', g_2'') & = & a(g_1'')s(g_1'')a(g_2'')s(g_2'')s(g_1''g_2'')^{-1}a(g_1''g_2'')^{-1}s(g_1''g_2'')s(g_2'')^{-1}s(g_1'')^{-1} \\ & = & a(g_1'')s(g_1'')a(g_2'')s(g_1'')^{-1}a(g_1''g_2'')^{-1} \\ & = & a(g_1'') - a(g_1''g_2'') + g_1''.a(g_2'') = (da)(g_1'', g_2'')\ . \end{array}$$

Here we have written the last row additively, since all terms lie in the abelian subgroup G'. The class of f in $H^2(G'', G')$ is thus independent of the choice of the section s. One also checks that equivalent extensions define the same function f.

- Conversely, let an arbitrary function $f\colon G'' \times G'' \to G'$ be given. We shall try to define a group structure G_f on the set $G' \times G''$ by setting:

$$(g_1', g_1'')(g_2', g_2'') := (g_1' + g_1''.g_2' + f(g_1'', g_2''), g_1''g_2'')$$

The projection $G_f \to G''$ gives a short exact sequence $E_f\colon 1 \to G' \to G_f \to G'' \to 1$. A straightforward check shows that G_f has inverses. However, the associativity of the multiplication is not automatic:

$$\begin{array}{rcl} [(g_1', g_1'')(g_2', g_2'')](g_3', g_3'') & = & (g_1' + g_1''.g_2' + f(g_1'', g_2''), g_1''g_2'') \cdot (g_3', g_3'') \\ & = & (g_1' + g_1''.g_2' + f(g_1'', g_2'') + (g_1''g_2'').g_3' + f(g_1''g_2'', g_3''), g_1''g_2''g_3'')\ . \\ (g_1', g_1'')[(g_2', g_2'')(g_3', g_3'')] & = & (g_1', g_1'')(g_2' + g_2''.g_3' + f(g_2'', g_3''), g_2''g_3'') \\ & = & (g_1' + g_1''.(g_2' + g_2''.g_3' + f(g_2'', g_3'')) + f(g_1'', g_2''g_3''), g_1''g_2''g_3'') \end{array}$$

The G'-component of the difference of the two expressions is:

$$g_1''f(g_2'', g_3'') - f(g_1''g_2'', g_3'') + f(g_1'', g_2''g_3'') - f(g_1'', g_2'') = (df)(g_1'', g_2'', g_3'')\ .$$

Thus f defines a group structure if and only if $df = 0$. If $f = f_{E,s}$, then E_f is equivalent to E, and so we obtain a bijection

$$\left\{ \begin{array}{l} \text{extensions of } G'' \text{ by } G' \\ \text{modulo equivalence} \end{array} \right\} \cong \left\{ \begin{array}{l} \text{functions } f\colon G'' \times G'' \to G' \text{ with } df = 0 \\ \text{modulo functions } da \text{ for } a\colon G'' \to G' \end{array} \right\}\ .$$

By the preceding discussion, the right-hand side is exactly $H^2(G'', G')$. □

Observation 7.4.4

- Let K/k be a Galois extension and $G := \mathrm{Gal}(K/k)$ the Galois group. Then the groups $H^n(G, K^*)$ are called the Galois cohomology groups of the extension K/k with coefficients in K^*.

- A version of Hilbert's Theorem 90 says that for finite Galois extensions $H^0(G, K^*) = k^*$ and $H^1(G, K^*) = 1$.

- We first investigate H^1. A function $\varphi\colon G \to K^*$ that represents a class in $H^1(G, K^*) = 1$ satisfies by (4) the equation

$$\varphi(\sigma\tau) = \tau\left(\varphi(\sigma)\right)\varphi(\tau)\ . \qquad (*)$$

  Classically such functions are called crossed homomorphisms. By equation (5) this is a coboundary if and only if there exists an element $\alpha \in K^*$ such that

$$\varphi(\sigma) = \frac{\alpha}{\sigma(\alpha)}\ .$$

  In that case one says that the crossed homomorphism splits. Hilbert's Theorem 90 says that this is indeed the case for finite Galois extensions.

- If the field extension is cyclic, i.e. $G = \langle\sigma\rangle$, then for every crossed homomorphism φ we have:

$$\begin{aligned} N(\varphi(\sigma)) &\overset{\text{def}}{=} \sigma^{n-1}(\varphi(\sigma))\ldots\sigma^2(\varphi(\sigma))\cdot\sigma(\varphi(\sigma))\cdot\varphi(\sigma) \\ &\overset{(*)}{=} \sigma^{n-1}(\varphi(\sigma))\ldots\sigma^2(\varphi(\sigma))\cdot\varphi(\sigma^2) \\ &\overset{(*)}{=} \sigma^{n-1}(\varphi(\sigma))\ldots\varphi(\sigma^3) = \ \varphi(\sigma^n) = 1 \end{aligned}$$

  One can also check that, conversely, for every element $\gamma \in K$ of norm $N(\gamma) = 1$ there exists a unique crossed homomorphism that is defined on the generator by $\varphi(\sigma) = \gamma$.

- For cyclic field extensions we recover the classical statement: an element $\gamma \in K^*$ has norm 1 if and only if there exists a crossed homomorphism with $\varphi(\sigma) = \gamma$, i.e. an $\alpha \in K^*$ with $\gamma = \varphi(\sigma) = \frac{\alpha}{\sigma(\alpha)}$. This statement is used to investigate under which conditions K can be obtained from k by adjoining an nth root of unity.

The cohomology $H^2(G, K^*)$ also has classical applications. For additional background for the following remarks we refer to [FD1993].

Definition 7.4.5

1. An algebra A over a commutative ring R is called central, if the centre is $Z(A) = R$.

2. An algebra is called central simple, if it is central and simple, i.e. if it is central has no non-trivial two-sided ideals.

Examples 7.4.6

1. The quaternions $\mathbb{H}$ are a central simple $\mathbb{R}$-algebra.

2. Every full matrix algebra $M(n \times n, k)$ over a field k is central simple.

3. A proper field extension K/k is not central simple, because $Z(K) = K \supsetneq k$.

4. Division algebras are not necessarily central simple, e.g. the real division algebra $\mathbb{C}$ is not semisimple.

Remarks 7.4.7

1. If R and S are central simple algebras, then so is $R \otimes S$. For example, the algebras $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}$ and $M(n \times n, k) \otimes S$ for a central simple algebra S are central simple.

2. For a finite-dimensional central simple k-algebra R one has $R \otimes R^{\mathrm{opp}} \cong M(n \times n, k)$ with $n := \dim_k R$.

3. Let D be a division algebra over k. A field extension K/k such that $D_K := D \otimes_k K \cong M(n \times n, K)$ is called a splitting field for D.

   Every maximal subfield $K \subset D$ is a splitting field of D and $[K : k] =: n$.

Definition 7.4.8

1. Let S and T be finite-dimensional central simple k-algebras. We say that S and T are similar, $S \sim T$, if one of the following equivalent conditions are satisfied:

   (a) If $S \cong M(n \times n, D)$ and $T \cong M(m \times m,\ E)$ with division algebras D, E, then $D \cong E$.

   (b) There exist m, n, such that $S \otimes_k M_m(k) \cong T \otimes_k M_n(k)$.

   (c) There exist m, n, such that $M_m(S) \cong M_n(T)$.

2. The Brauer group $Br(k)$ of a field k is defined on the set of equivalence classes of finite-dimensional simple k-algebras under similarity. The group operation is induced by the tensor product and the class $[k]$ is the neutral element.

The Brauer group is abelian and it classifies division algebras over k.

Examples 7.4.9

1. We have $Br(k) = 0$ if k is an algebraically closed field, because in that case, there exist no non-trivial division algebras.

2. For a finite field k we have $Br(k) = 0$. In particular, is every finite division ring is commutative (Wedderburn's theorem).

3. We have $Br(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$. A representative of the generator are the quaternions $\mathbb{H}$. Indeed, one has $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \cong M(4 \times 4, \mathbb{R})$.

Remark 7.4.10

1. For every field extension K/k there exists a homomorphism, given by extension of scalars:

$$\begin{array}{rcl} Br(k) & \to & Br(K) \\ [S] & \mapsto & [S_K] := [S \otimes_k K] \end{array}$$

2. The relative Brauer group is

$$Br(K/k) = \ker(Br(k) \to Br(K))$$

   i.e. the set of finite-dimensional central division algebras over k, which split over the field K.

3. One can show that for every division algebra D with centre k and $\dim_k D = n^2$, there exists a finite Galois extension K/k, such that D splits over K.

4. Thus one has $Br(k) = \cup Br(K/k)$, where K runs over all finite Galois extensions of k.

5. We have the following isomorphism of groups

$$Br(K/k) = H^2(\mathrm{Gal}(K/k), K^*)$$

Here we note that for a 2-cocycle $a_{\sigma,\tau}$ with $\sigma, \tau \in G := \mathrm{Gal}(K/k)$, the freely generated K-vector space over G with multiplication

$$(\alpha e_\sigma) \cdot (\beta e_\tau) := \alpha\sigma(\beta) a_{\sigma,\tau} e_{\sigma\tau}$$

is a central simple algebra.

Let S be a central simple algebra and K a field, over which S splits. We first observe that by the Skolem-Noether theorem for every $\sigma \in G$ there exists a $x_\sigma \in S$ with

$$\sigma(a) = x_\sigma \cdot a \cdot x_\sigma^{-1} \ ,$$

and the x_σ unique up to factors in K. Thus there exists a function $a\colon G \times G \to K^*$ with

$$x_\sigma x_\tau = a(\sigma, \tau) x_{\sigma\tau} \ .$$

From the associativity of the multiplication of the x_σ

$$x_\rho a(\sigma, \tau) \cdot x_{\sigma\tau} = a(\rho, \sigma) x_{\rho\sigma} \cdot x_\tau$$

and thus

$$\rho(a(\rho, \sigma)) a(\rho, \sigma\tau) x_{\rho\sigma\tau} = a(\rho, \sigma) a(\rho\sigma, \tau) x_{\rho\sigma\tau}$$

we deduce that a satisfies the equation (6), and thus defines a class in $H^2(G, K^*)$. One also shows that the family $(x_\sigma)_{\sigma \in G}$ forms a K-basis of S.

A Zorn's lemma

Let S be a set. We recall the following notions and results from set theory:

1. A <u>partial order</u> on S is a relation $x \leq y$ with the following properties:

$$\begin{array}{rcrcll} & & x \leq x & & & \text{reflexive}\,, \\ x \leq y & \wedge & y \leq z & \Rightarrow & x \leq z & \text{transitive}\,, \\ x \leq y & \wedge & y \leq x & \Rightarrow & x = y & \text{antisymmetric}\,. \end{array}$$

2. A <u>total order</u> on S is a partial order, for which any two elements are comparable:

$$x, y \in S \quad \Rightarrow \quad x \leq y \quad \text{or} \quad y \leq x\,.$$

3. Let S be partially ordered and $T \subset S$ a subset.

   A element $b \in S$ is called an <u>upper bound</u> for the subset T, if

$$x \leq b \quad \text{for all} \quad x \in T\,.$$

4. Let S be partially ordered. An element $m \in S$ is called a <u>maximal element</u>, if

$$m \leq x \quad \Rightarrow \quad m = x\,.$$

   A maximal element need not be unique. For example, consider the set of ideals of the rings $\mathbb{Z}$ with partial ordered given by inclusion. All prime ideals (p) (with p a prime) are maximal.

5. A partially ordered set S is called <u>induktively ordered</u>, if every non-empty, totally ordered subset of S has an upper bound.

6. <u>Zorn's lemma</u> Let S be a non-empty, inductively ordered set. Then S has maximal elements.

B Glossary German-English

For the benefit of German speaking students, we include a table with German versions of important notions.

English	German
abelian Lie algebra	abelsche Lie-Algebra
absolutely simple object	absolut einfaches Objekt
adjoint functor	adjungierter Funktor
alternating algebra	alternierende Algebra
augmentation ideal	Augmentationsideal
character	Charakter
class function	Klassenfunktion
coinvariant	Koinvariante
companion matrix	Begleitmantrix
convolution product	Konvolutionsprodukt, Faltungsprodukt
counitality	Kounitarität
derivation	Derivation
enriched category	angereicherte Kategorie
essentially small category	wesentlich kleine Kategorie
exterior algebra	äußere Algebra
forgetful functor	Vergissfunktor
free vector space	freier Vektorraum
invariant factor	Invariantenteiler
Horseshoe lemma	Hufeisenlemma
left adjoint functor	linksadjungierter Funktor
left module	Linksmodul
monic polynomial	normiertes Polynom
opposite algebra	opponierte Algebra
projective module	projektiver Modul
pullback of a representation	Pullback einer Darstellung
representation	Darstellung
right adjoint functor	rechtsadjungierter Funktor
semisimple algebra	halbeinfache Algebra
semisimple module	halbeinfacher Modul (der)
separable algebra	separable Algebra
simple module	einfacher Modul (der)
trace	Spur
trivial module	trivialer Modul (der)

References

[A15] S. Axler: *Linear Algebra Done Right* Third edition. Springer Undergraduate Texts in Mathematics, 2015.

[B94] F. Borceux: *Handbook of Categorical Algebra.* Volume 2: Categories and Structures. Cambridge University Press, Cambridge, 1994.

[B16] M. Brandenburg: *Einführung in die Kategorientheorie.* Springer Verlag, Berlin, 2016

[DSPS19] C.L. Douglas, C. Schommer-Pries, and N. Snyder: *The balanced tensor product of module categories.* Kyoto J. Math. 59 (2019) 167, `math.QA/1406.4204`

[FD1993] B. Farb and R.K. Dennis: *Noncommutative algebra.* Springer Graduate Texts in Mathematics 144, 1993.

[F05] R. Farnsteiner: *Self injective algebras I: The structure of the projective indecomposable modules.* Available at `https://www.math.uni-bielefeld.de/~sek/selected.html`

[FSS20] J. Fuchs, G. Schaumann, and C. Schweigert: *Eilenberg-Watts calculus for finite categories and a bimodule Radford S^4 theorem.* Trans. AMS 373 (2020) 1, `math.RT/1612.04561`

[HS1970] P.J. Hilton and U. Stammbach: *A Course in Homological Algebra.* Springer, New York, 1970

[JS06] J. Jantzen, J. Schwermer: *Algebra*, Springer, 2006

[K07] A. Knapp: *Advanced Algebra.* Birkhäuser Cornerstones, Boston, 2007

[K61] H.J. Kowalsky: *Linear algebra*, De Gruyter, 1961

[K80] E. Kunz: *Einführung in die kommutative Algebra und algebraische Geometrie.* vieweg studium Aufbaukurs Mathematik, volume 46.

[L02] S. Lang: *Algebra.* Springer Graduate Texts in Mathematics volume 211.

[McL71] S. MacLane: *Categories for the Working Mathematician.* Springer Graduate Text in Mathematics 5, 1971.

[Mi65] B. Mitchell: *Theory of categories.* Academic Press 1965, London-New York.

[N03] Jet Nestruev: *Smooth Manifolds and Observables.* Springer Graduate Texts in Mathematics volume 211.

[P97] B. Pareigis: *Algebra II.* Summer term 1997. Lecture notes available at `https://www.mathematik.uni-muenchen.de/~ pareigis/`

[R16] E. Riehl: *Category Theory in Context.* Dover Publications, New York, 2016. Available at `https://math.jhu.edu/~ eriehl`

[S77] J.-P. Serre: *Linear Representations of Finite Groups.*Springer Graduate Text 48, New York, 1977

[W60] C.E. Watts: *Intrinsic characterizations of some additive functors.* Proc. Amer. Math. Soc. 11 (1960) 5

Index