Modules and Homological Algebra

Karl-Heinz Fieseler

Uppsala 2012

Note:

These lecture notes are intended to give a presentation of the course "Modules and Homological Algebra" closer to the actual lectures than the text book. They are almost self contained, only sometimes refer to the book of Grillet, e.g. the proof of the long exact homology sequence is not given. The essentially new contributions are

1. Group and quiver algebras.

2. Singular homology.

Furthermore, in order to make derived functors more digestible we define functorial free resp. injective resolutions, postponing the discussion of arbitrary projective resolutions of a given module to a later section.

Finally, sections 6,7 and 8 as well as injective resolutions can presumably not be discussed in detail during the course, they are intended for private reading.

Uppsala, August 2012 Karl-Heinz Fieseler

Contents

1 Base rings

The theory of modules requires the choice of a base ring. Our base ring usually is denoted R and assumed to be "unital", i.e. to admit a unit element $1 \in R$. In particular there is its group of units

$$R^* := \{a \in R; \exists\ b \in R : ab = ba = 1\}.$$

We remark that an element $a \in R$ is a unit iff it has both a left and a right inverse.

Sometimes it is also useful to consider the "opposite ring":

Definition 1.1. Given the ring R, we denote R^{op} the ring, whose underlying additive group is that of R, but carries the "opposite multiplicative structure": If $(a, b) \mapsto ab$ denotes the multiplication in R, then

$$a * b := ba$$

is the multiplication in R^{op}.

Special cases we often are interested in are the following: The base ring R is

1. commutative,
2. an integral domains, i.e. commutative without zero divisors $\neq 0$,
3. a principal ideal domain (PID), i.e. an integral domain where all ideals are principal ideals,
4. an associative k-algebra with 1, where k denotes a field.

Definition 1.2. Let k be a field. A k-algebra is a k-vector space R together with a bilinear map

$$R \times R \longrightarrow R, (a, b) \mapsto ab.$$

If in addition the above product is associative and there is a unit element $1 \in R$, our k-algebra is a ring as well, and we call R an associative k-algebra with 1.

Example 1.3. 1. **Matrix algebras**: Let k be a field. We denote

$$\mathrm{Mat}_n(k) \quad \text{or} \quad k^{n,n}$$

the k-algebra of all $n \times n$-matrices with entries in k. Note that

$$\mathrm{Mat}_n(k)^{\mathrm{op}} \cong \mathrm{Mat}_n(k), A \mapsto A^T.$$

2. **Endomorphism rings**: For a vector space V the set

$$\mathrm{End}(V) := \{f : V \longrightarrow V; f \text{ linear}\}$$

of its endomorphisms, endowed with pointwise addition and the composition of linear maps as multiplication, is a ring with unit element id_V. If $n := \dim_k V < \infty$, any choice of a base $B = (v_1, ..., v_n)$ induces an isomorphism

$$\Phi_B : \mathrm{End}(V) \xrightarrow{\cong} \mathrm{Mat}_n(k), f \mapsto A = (\alpha_{ij}),$$

where

$$f(v_j) = \sum_{j=1}^{n} \alpha_{ij} v_i.$$

3. **The vector space generated by a set**: Given a set M and a field k, we consider the vector space

$$k[M] := \{f : M \longrightarrow k; |f^{-1}(k^*)| < \infty\}$$

of all k-valued functions on M with finite support $f^{-1}(k^*)$, where $k^* := k \setminus \{0\}$. With other words, a function $f \in k[M]$ satisfies $f(a) = 0$ for all but finitely many $a \in M$.

The Kronecker functions

$$e_a, \ a \in M, \quad (\text{i.e. we have } e_a(x) = \delta_{ax})$$

constitute a basis of $k[M]$. Indeed, because of the support condition every $f \in k[M]$ admits the finite expansion

$$f = \sum_{a \in M, f(a) \neq 0} f(a) e_a =: \sum_{a \in M} f(a) e_a.$$

For convenience of notation one often writes simply a instead of e_a, such that any element in $k[M]$ is a finite "formal" sum

$$f = \sum_{a \in M} \lambda_a a,$$

where $\lambda_a \neq 0$ for at most finitely many $a \in M$. We thus regard M as a subset $M \subset k[M]$, indeed a basis of the k-vector space $k[M]$.

4. **Group algebras**: For a group G we endow the vector space $k[G]$ with the following product

$$(fg)(a) := \sum_{xy=a} f(x)g(y);$$

the resulting ring is called the group ring (or algebra) of G over k. The products of the base elements are easily computed

$$e_a e_b = e_{ab}.$$

For the additive group $\mathbb{Z}$ the above formula reads $e_m e_n = e_{m+n}$ and we obtain an isomorphism

$$k[\mathbb{Z}] \longrightarrow k[T, T^{-1}], e_n \mapsto T^n,$$

with the k-algebra

$$k[T, T^{-1}] := \left\{ \sum_{n=r}^{s} a_n T^n; r, s \in \mathbb{N}, a_n \in k \right\} \subset k(T) := Q(k[T])$$

of all Laurent polynomials with coefficients in k.

5. **Quiver algebras** to be discussed in the remaining part of this section:

Definition 1.4. A *quiver* Q consists of two finite sets $V = V(Q) \neq \emptyset, A = A(Q)$ together with two maps $t, h : A \longrightarrow V$. The elements $x \in V$ are called *vertices*, the elements $\alpha \in A$ are called *arrows*, the vertex $h(\alpha)$ is called the *head* of the arrow α while $t(\alpha)$ is its *tail*.

Example 1.5. 1. $V = \{x_0\}, A = \{\alpha\}$, i.e. there is exactly one vertex and one arrow, together with the obvious maps t, h.

2. $V = \{x_0\}, A = \{\alpha, \beta\}$, i.e. there is exactly one vertex and two arrows, together with the obvious maps t, h.

3. $V = \{x_1, x_2\}, A = \{\alpha, \beta\}$ with $t(\alpha) = t(\beta) = x_1, h(\alpha) = h(\beta) = x_2$.

Definition 1.6. 1. A path of length $r > 0$ in a quiver is a finite sequence $f = (\alpha_r, ..., \alpha_1)$ of arrows $\alpha_i \in A(Q)$, such that $t(\alpha_{i+1}) = h(\alpha_i)$ for $1 \leq i < r$. The vertex $t(\alpha_1)$ is also called the origin (or starting point) of the path and denoted $S(f)$, and $h(\alpha_r)$ its terminus (or end point) $E(f)$. Furthermore there is (by definition!) for every vertex $x \in V(Q)$ a path e_x of length 0 having x both as its start and end point, the "lazy path at $x \in V$". We denote $\mathbb{P}(Q)$ the set of all paths in the quiver Q.

2. Paths $f, g \in \mathbb{P}(Q)$ with $E(f) = S(g)$ can be concatenated to a new path gf. Furthermore $e_y f := f$, if $y = E(f)$ and $ge_x = g$ for $x = S(g)$.

Example 1.7. 1. For the quiver Q with one vertex x and one arrow α we have
$$\mathbb{P}(Q) = \{e_x, \alpha, \alpha^2, \alpha^3, ...\}.$$

2. For the quiver Q with one vertex x and two arrows α, β we obtain the following paths
$$e_x, \alpha, \beta, \alpha^2, \alpha\beta, \beta\alpha, \beta^2, \alpha^3, \alpha^2\beta, \alpha\beta\alpha, \beta\alpha^2, \alpha\beta^2, \beta\alpha\beta, \beta^2\alpha, \beta^3, \alpha^4, ...$$

3. If Q has two different vertices x, y and one arrow α with tail x and head y, we find
$$\mathbb{P}(Q) = \{e_x, e_y, \alpha\}.$$

4. We have $|\mathbb{P}(Q)| < \infty$ if and only if there are no loops in Q, i.e. paths of length > 0 with the same start and end point.

We want to make the vector space $k[\mathbb{P}(Q)]$ a ring. In order to define a product we generalize the concatenation to arbitrary pairs of paths and "extend it by linearity".

Definition 1.8. Let Q be a quiver.

1. If $f, g \in \mathbb{P}(Q), S(g) \neq E(f)$, we set

$$gf := 0 \in k[\mathbb{P}(Q)].$$

2. The quiver algebra kQ is the vector space $k[\mathbb{P}(Q)]$ endowed with the linear extension of the concatenation product

$$\mathbb{P}(Q) \times \mathbb{P}(Q) \longrightarrow k[\mathbb{P}(Q)], (g, f) \mapsto gf.$$

Remark 1.9. 1. kQ is a ring with unit $e := \sum_{x \in V(Q)} e_x$.

2. $\dim kQ < \infty$ iff Q does not loops.

Example 1.10. 1. For the quiver Q with one vertex x and one arrow α there is an isomorphism

$$k[T] \longrightarrow kQ, 1 \mapsto e_x, T^n \mapsto \alpha^n,$$

with the ring of polynomials in one variable over the base fiield k.

2. For the quiver Q with one vertex x and two arrows α, β the k-algebra kQ is the "polynomial algebra in the two noncommuting variables α, β".

3. If Q has two different vertices x, y and one arrow α with tail x and head y, there is an isomorphism

$$kQ \cong \begin{pmatrix} k & 0 \\ k & k \end{pmatrix}$$

namely:

$$e_x \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \ e_y \mapsto \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \ \alpha \mapsto \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

2 Modules

Definition 2.1. A (left/right) R-module M is a vector space where the base field k is replaced with R as base ring. So there is an addition

$$M \times M \longrightarrow M, (u, v) \mapsto u + v$$

endowing M with the structure of an (additively written) abelian group, and

1. a left scalar multiplication

$$R \times M \longrightarrow M, (\lambda, u) \mapsto \lambda u$$

   resp.

2. a right scalar multiplication

$$M \times R \longrightarrow M, (u, \lambda) \mapsto u\lambda$$

satisfying the distributive law w.r.t. both arguments and

1. (a) $1u = u, \forall u \in M$
   (b) $\lambda(\mu u) = (\lambda\mu)u$

2. resp.

   (a) $u1 = u, \forall u \in M$
   (b) $(u\lambda)\mu = u(\lambda\mu)$.

Remark 2.2. The scalar multiplication of a left R-module M may also be regarded as a right R^{op}-scalar multiplication:

$$M \times R^{\mathrm{op}} \longrightarrow M, (u, \lambda) \mapsto \lambda u.$$

Of course the corresponding reasoning works for right R-modules, and thus we see, that left/right R-modules correspond to right/left R^{op}-modules. Hence, without loss of generality we may regard preferably left R-modules.

Example 2.3. 1. With the symbol 0 one denotes, by abuse of notation, the R-module $\{0\}$, whose underlying additive group is trivial, together with the obvious scalar multiplication.

2. The most basic ring is undoutedly the ring $\mathbb{Z}$ of all integers. Indeed, there is a one-to-one correspondence

$$\text{Abelian groups} \longleftrightarrow \mathbb{Z}\text{-modules}.$$

To come from a $\mathbb{Z}$-module to an abelian group simply forget the scalar multiplication. On the other hand, given an abelian group A, we get a scalar multiplication

$$\mathbb{Z} \times A \longrightarrow A, (n, a) \mapsto na$$

as follows

$$na := \begin{cases} \overbrace{a + ... + a}^{n\times} & , \text{ for } n > 0 \\ 0 & , \text{ for } n = 0 \\ |n|(-a) & , \text{ for } n < 0 \end{cases}.$$

3. Let k be a field. A k-module is nothing but a k-vector space: If we speak about a vector space, the base field is usually denoted k.

Let us compare linear algebra, i.e. the theory of vector spaces (and linear maps), with the theory of modules.

Example 2.4. Consider $R^n := \underbrace{R \times ... \times R}_{n \text{ times}}$ with the componentwise addition. It carries both a left and right scalar multiplication:

$$(\lambda, (x_1, ..., x_n)) \mapsto (\lambda x_1, ..., \lambda x_n)$$

and

$$((x_1, ..., x_n), \lambda) \mapsto (x_1\lambda, ..., x_n\lambda).$$

Obviously it thus becomes a left/right R-module, denoted

$${}_R R^n$$

resp.

$$R^n_R,$$

and furthermore, any $u \in R^n$ has a unique representation

$$u = \sum_{i=1}^{n} \lambda_i \cdot e_i$$

resp.

$$u = \sum_{i \in I} e_i \cdot \lambda_i,$$

where e_i denotes the i-th "unit vector" $e_i := (\delta_{i1}, ..., \delta_{in})$ and the coefficients λ_i are taken from the base ring: $\lambda_i \in R$. Indeed, if $u = (u_1, ..., u_n)$, then $\lambda_i = u_i$ is the unique choice of coefficients.

In the following we only deal with left modules, leaving the right modules to the reader.

Definition 2.5. A subset $B = \{e_i; i \in I\} \subset M$ of an R-module M is called a basis if each $u \in M$ has a unique representation

$$u = \sum_{i \in I} \lambda_i(u) \cdot e_i$$

as a finite(!) linear combination of elements in B with coefficients $\lambda_i(u) \in R$ in B. (For infinite B that means that for given $u \in M$ we have $\lambda_i(u) \neq 0$ for all but finitely many $i \in I$.) An R-module admitting a basis is called *free*.

Example 2.6. 1. R^n is a free R-module.

2. From linear algebra we know: For a field k every k-module (i.e. k-vector space) M is free, see also Th.14.6. Furthermore $|B| = |B'|$ for any two bases of M. The latter holds even for a free module over a commutative ring R (by reduction to the field case, to be seen later on), but not necessarily in the noncommutative case, where $R \cong R^2$ may occur.

3. The previous point may slightly be generalized: Modules over a division ring D are free: A *division ring* D is a (not necessarily commutative) ring, such that $D^* = D \setminus \{0\}$, i.e. all nonzero elements are invertible, have both a left and right inverse. Furthermore, any two bases of a given module have the same cardinality.

4. For an integral domain R the R-module $Q(R)$ is not free, if R is not a field: Since any two elements are linearly dependent, a basis should consist of one element $a \in Q(R)$ only. But $Q(R) = Ra$ implies that all elements in $R \setminus \{0\}$ are invertible.

5. In order to construct free modules with infinite bases we consider first for a set I the left or right R-module

$$R^I := \{f; f : I \longrightarrow R\}$$

of all R-valued functions on I - the scalar multiplication being

$$(\lambda f)(i) := \lambda \cdot f(i) \text{ resp.} (f\lambda)(i) := f(i) \cdot \lambda.$$

As a natural candidate for a basis one could consider the set $B := \{e_i; i \in I\}$ with the Kronecker functions $e_i : I \longrightarrow R, j \mapsto \delta_{ij}$. Unfortunately, for infinite I the set B is **not** a basis of R^I. Indeed a function $f : I \longrightarrow R$ is a finite linear combination of the Kronecker functions iff $f(i) = 0$ for all but finitely many $i \in I$. Even worse: The module R^I is in general not free — e.g. if R is a PID, but not a field, a non-trivial statement. On the other hand, for a field k the module k^I is of course free - but no human being has up to now found an explicit basis for $k^{\mathbb{N}}$!

So let us restrict our attention to the functions $f \in R^I$, which are finite linear combinations of the Kronecker functions $e_i, i \in I$. They form a submodule:

Definition 2.7. A submodule $L \subset M$ of a module M is a subgroup of the additive group of M stable under scalar multiplication. We write also $L \leq M$ in order to express that $L \subset M$ is a submodule of M.

Example 2.8.

1. A subset $\mathfrak{a} \subset R$ is a submodule of ${}_RR$ resp. R_R iff it is a left resp. right ideal.

2. The subset $R[I] \subset R^I$ of all R-valued functions on I with finite support $\text{supp} f := f^{-1}(R \setminus \{0\})$, i.e.

$$R[I] := \{f \in R^I; f(i) \neq 0 \text{ for at most finitely many } i \in I\},$$

forms a submodule. Obviously $R[I]$ is a free module with basis $B := \{e_i; i \in I\}$. The module $R[I]$ is also called **the free R-module generated by the set I.**

3. For $I_0 \subset I$ we may regard $R[I_0]$ as a submodule of $R[I]$, extending a function $f : I_0 \longrightarrow R$ to $\hat{f} : I \longrightarrow R$ with $\hat{f}|_{I \setminus I_0} = 0$.

4. If $\mathfrak{a} \subset R$ is a left/right ideal and M a left/right R-module then

$$\mathfrak{a}M := \{a_1u_1 + ... + a_ru_r; a_i \in \mathfrak{a}, u_i \in M\}$$

resp.

$$M\mathfrak{a} := \{u_1a_1 + ... + u_ra_r; a_i \in \mathfrak{a}, u_i \in M\}$$

is a submodule of M.

For an integral domain R there is the notion of the torsion submodule $T(M)$ of an R-module M:

Definition 2.9. Let R be an integral domain and M an R-module.

1. The *rank* $\mathrm{rk}(M) \in \mathbb{N} \cup \{\infty\}$ of M is defined to be the maximal number of linearly independent elements in M.

2. For $q \in R \setminus \{0\}$ we define its q-torsion module

$$T_q(M) := \{u \in M; qu = 0\}.$$

3. The torsion submodule of M is

$$T(M) := \{u \in M; \exists q \in R \setminus \{0\} : qu = 0\} = \bigcup_{q \in R\setminus\{0\}} T_q(M).$$

4. The module M is called torsion free if $T(M) = \{0\}$.

If R is a k-algebra, any R-module is also a k-vector space. So in order to describe such a module, one starts with a k-vector space and adds some additional data. Here are some examples:

Example 2.10. 1. Any vector space V is a left module over its endomorphism ring $\mathrm{End}(V)$ with the left scalar multiplication

$$\mathrm{End}(V) \times V \longrightarrow V, (f, v) \mapsto f(v).$$

The only submodules are V and $\{0\}$.

2. The dual space $V' := \mathrm{Hom}(V, k)$ of a vector space V is a right $\mathrm{End}(V)$-module with the scalar multiplication

$$V' \times \mathrm{End}(V) \longrightarrow V', (v', f) \mapsto v' \circ f.$$

The only submodules are V' and $\{0\}$.

3. Denote $k[T]$ the polynomial ring in one variable over the field k. There is a one-to-one correspondence

$$k[T]\text{-modules} \longleftrightarrow \text{pairs } (V, f), V \text{a } k\text{-vector space, } f \in \mathrm{End}(V).$$

Indeed, given a $k[T]$-module V we take

$$f := \mu_T : V \longrightarrow V, v \mapsto Tv,$$

to be scalar multiplication with the indeterminate T. Submodules are nothing but f-invariant subspaces.

4. Our interpretation of $k[G]$-modules is in terms of "k-linear representations of G", i.e. group homomorphisms from G to the general linear group of some k-vector space V. There is a one-to-one correspondence

$$k[G]\text{-modules} \longleftrightarrow \text{group homomorphisms } G \longrightarrow GL(V),$$

where V is a k-vector space. Given a $k[G]$-module with underlying vector space V, the corresponding group homomorphism is obtained as the restriction of the scalar multiplication to the standard basis $B = \{e_a; a \in G\} \subset k[G]$, i.e. it is

$$G \longrightarrow GL(V), a \mapsto \mu_{e_a}$$

with the scalar multiplication

$$\mu_{e_a} : V \longrightarrow V, \ v \mapsto e_a v.$$

On the other hand given $\varphi : G \longrightarrow GL(V), a \mapsto \varphi_a$, the scalar multiplication

$$k[G] \times V \longrightarrow V$$

is the linear extension of

$$B \times V \longrightarrow V, (e_a, v) \mapsto \varphi_a(v).$$

5. Modules over a quiver algebra: A *kQ-module* V looks as follows: As k-vector space it is a direct sum

$$V := \bigoplus_{x \in V(Q)} V_x$$

of k-vector spaces $V_x, x \in V(Q)$, together with linear maps $F_\alpha : V_{t(\alpha)} \longrightarrow V_{h(\alpha)}$ for every $\alpha \in A(Q)$. The scalar multiplication is obtained as the linear extension of

$$\mathbb{P}(Q) \times V_x \longrightarrow V, (f, v) \mapsto fv,$$

where for a path $f = (\alpha_r, ..., \alpha_1)$ of positive length $r > 0$ we define

$$fv := \begin{cases} F_{\alpha_r} \circ ... \circ F_{\alpha_1}(v), & \text{if } S(f) = x \\ 0\ , & \text{otherwise} \end{cases},$$

while in the case of a path e_y of length 0 we set instead

$$e_y v := \begin{cases} v, & \text{if } y = x \\ 0\ , & \text{otherwise} \end{cases}.$$

In order to see that every kQ-module V is of that form take

$$V_x := e_x V,$$

and define $F_\alpha : V_x \longrightarrow V_y$ for $x = t(\alpha), y = h(\alpha)$ by $F_\alpha := \alpha \cdot ..|_{V_x}$. (Note that $\alpha e_x = \alpha$, hence $\alpha \cdot ..|_{V_z} = 0$ for $z \neq x$ because of $e_x e_z = 0$.) A submodule is of the form $U := \bigoplus_{x \in V(Q)} U_x$ with subspaces $U_x \subset V_x$ such that $F_\alpha(U_{t(\alpha)}) \subset U_{h(\alpha)}$ for all arrows $\alpha \in A(Q)$.

Further modules can be obtained as factor modules:

Definition 2.11. Let $L \leq M$. The factor module M/L is, as an additive abelian group, the factor group endowed with the scalar multiplication

$$R \times M/L \longrightarrow M/L, (\lambda, u + L) \mapsto \lambda u + L.$$

3 A survey of module theory

The final goal of every algebraic theory is to classify the objects of interest. In order to compare different R-modules we need homomorphisms:

Definition 3.1. 1. A homomorphism $\varphi : M \longrightarrow N$ between the left/right R-modules M and N is a homomorphism of the underlying additive groups such that

$$\varphi(\lambda u) = \lambda\varphi(u)$$

resp.

$$\varphi(u\lambda) = \varphi(u)\lambda$$

holds for all $\lambda \in R, u \in M$. We denote

$$\mathrm{Hom}(M,N) := \{\varphi; \varphi : M \longrightarrow N \text{ module homomorphism}\}$$

the set of all R-module homomorphisms and

$$\mathrm{End}(M) := \mathrm{Hom}(M,M)$$

the ring of all endomorphisms. If there is some ambiguity about the choice of the base ring we write also

$$\mathrm{Hom}_R(M,N), \mathrm{End}_R(M).$$

2. A module homomorphism $\varphi : M \longrightarrow N$ is called an isomorphism, if it is bijective. We say that two modules are isomorphic, $M \cong N$, if there is an isomorphism $\varphi : M \longrightarrow N$.

Remark 3.2. 1. $\mathrm{Hom}(M,N)$ is an abelian group or rather a $Z(R)$-module, where

$$Z(R) := \{x \in R; xy = yx \ \forall\ y \in R\}$$

denotes the center of R. The module operations are argumentwise

$$(\varphi + \psi)(u) := \varphi(u) + \psi(u), (\lambda\varphi)(u) := \lambda \cdot \varphi(u).$$

2. If we think of elements of R_R^n as column vectors, homomorphisms

$$\varphi : R_R^m \longrightarrow R_R^n$$

are of the form

$$u \mapsto Au$$

with a (unique) matrix $A \in R^{n,m}$.

3. If we think of elements of ${}_RR^n$ as row vectors, homomorphisms

$$\varphi : {}_RR^m \longrightarrow {}_RR^n$$

are of the form

$$u \mapsto uA$$

with a (unique) matrix $A \in R^{m,n}$.

4. If R is commutative, the homomorphism $R^n \longrightarrow R^n, u \mapsto Au$, is an isomorphism or, equivalently, $A \in GL_n(R) := \mathrm{Mat}_n(R)^*$, iff $\det(A) \in R^*$. The implication "$\Longrightarrow$" follows from the fact that given an invertible matrix we have

$$1 = \det(E) = \det(AA^{-1}) = \det(A)\det(A^{-1})$$

as well as $\det(A^{-1})\det(A) = 1$. On the other hand, assuming $\det(A) \in R^*$, we have

$$A^{-1} = \det(A)^{-1}A^*$$

with the adjoint matrix $A^* \in \mathrm{Mat}_n(R)$.

5. If F, N are R-modules and F free with basis $B \subset F$, then

$$\mathrm{Hom}(F, N) \longrightarrow N^B, f \mapsto f|_N$$

is bijective, i.e. a homomorphism is uniquely determined by its values on the basis elements, and its values there can be prescribed arbitrarily.

6. Let V be a vector space. Show

$$\mathrm{End}_{\mathrm{End}(V)}(V) = k \cdot \mathrm{id}_V.$$

7. Homomorphisms $\varphi : V \longrightarrow W$ of kQ-modules V, W: Call $F_\alpha : V_{t(\alpha)} \longrightarrow V_{h(\alpha)}$ resp. $G_\alpha : W_{t(\alpha)} \longrightarrow W_{h(\alpha)}$ the linear map corresponding to the arrow $\alpha \in A(Q)$. Then a homomorphism $\varphi : V \longrightarrow W$ can be identified with a family $(\varphi_x : V_x \longrightarrow W_x)_{x \in V(Q)}$ of linear maps satisfying $\varphi_{h(\alpha)} \circ F_\alpha = G_\alpha \circ \varphi_{t(\alpha)}$ for all $\alpha \in A(Q)$. Furthermore, φ is an isomorphism if all maps $\varphi_x : V_x \longrightarrow W_x$ are linear isomorphisms.

We start our investigations by looking for modules generated by one element:

Definition 3.3. A left/right R-module M is called *cyclic* if one of the following equivalent conditions is satisfied:

1. There is an element $u \in M$, such that $M = Ru$ resp. $M = uR$.

2. $M \cong R/\mathfrak{a}$ with a left/right ideal $\mathfrak{a} \subset R$.

Proof of the equivalence. Given the generator $u \in M$ the map $R \longrightarrow M, \lambda \mapsto \lambda u / u\lambda$, induces an isomorphism

$$R/\mathrm{Ann}(u) \cong M$$

with the annihilator ideal

$$\mathrm{Ann}(u) := \{\lambda \in R; \lambda u = 0\} \text{ resp. } \mathrm{Ann}(u) := \{\lambda \in R; u\lambda = 0\}$$

of the element $u \in M$. On the other hand, for $M = R/\mathfrak{a}$ we may take $u := 1 + \mathfrak{a}$. □

But from a systematic point of view it is more promising to look for even more "atomic" modules:

Definition 3.4. A nonzero module M is called *simple* if $M, \{0\}$ are the only submodules of M.

Remark 3.5. Simple modules are cyclic: If M is, say, a left module and $u \in M \setminus \{0\}$, then $\{0\} \neq Ru \leq M$, hence $M = Ru$.

Proposition 3.6. *A (left/right) module M is simple iff*

$$M \cong R/\mathfrak{m}$$

with a maximal (left/right) ideal $\mathfrak{m} \subset R$.

Proof. We know already $M \cong R/\mathfrak{a}$. Denote $q : R \longrightarrow R/\mathfrak{a}$ the quotient map. Then

$$R/\mathfrak{a} \geq L \mapsto q^{-1}(L)$$

defines a bijective correspondence between the submodules of $R/\mathfrak{a}$ and the left/right ideals $\mathfrak{b} \subset R$ containing $\mathfrak{a}$. Hence $R/\mathfrak{a}$ is simple iff $\mathfrak{a}$ is a maximal left/right ideal. □

Corollary 3.7. *There are simple R-modules.*

Proof. There are maximal left/right ideals $\mathfrak{m} \subset R$, see Th.14.7. □

Example 3.8. Let V be a finite dimensional k-vector space. The left ideals of $\mathrm{End}(V) := \mathrm{End}_k(V)$ are of the form

$$I(U) := \{f \in \mathrm{End}(V); f|_U = 0\}$$

with a subspace $U \subset V$, and the right ideals look as follows

$$J(U) := \{f \in \mathrm{End}(V); f(V) \subset U\},$$

again with a subspace $U \subset V$. In particular for a maximal left ideal we have $\dim U = 1$, and $\dim U = \dim V - 1$ for a maximal right ideal. In any case we obtain V resp. V' as the only left/right simple $\mathrm{End}(V)$-modules: Take $u \in U \setminus \{0\}$ resp. $u' \in V' \setminus \{0\}, u'|_U = 0$. Then

$$\mathrm{End}(V) \longrightarrow V, f \mapsto f(u)$$

and

$$\mathrm{End}(V) \longrightarrow V', f \mapsto u' \circ f$$

induce isomorphisms

$$\mathrm{End}(V)/I(U) \cong V, \mathrm{End}(V)/J(U) \cong V'.$$

Example 3.9.

1. A vector space V is simple iff $\dim V = 1$.
2. A vector space V is a simple $\mathrm{End}(V)$-module.
3. A simple module M over an integral domain R, which is not a field, is a torsion module $M = T(M)$. In particular a torsion free module over an integral domain does not admit simple submodules.

The following proposition could be taken as a starting point for the study of general R-modules:

Proposition 3.10. *Any module M is a factor module of a free module F.*

Proof. The map

$$\sigma : F := R[M] \longrightarrow M, f \mapsto \sum_{u \in M} f(u)u$$

resp.

$$\sigma : F := R[M] \longrightarrow M, f \mapsto \sum_{u \in M} uf(u)$$

is onto, hence

$$M \cong F/L$$

with $L := \ker(\sigma)$. Note that $\sigma : R[M] \longrightarrow M$ is the unique homomorphism of left/right R-modules satisfying $\sigma(e_u) = u$ for the basis vectors $(e_u)_{u \in M}$. $\square$

The modules $R[M]$ are extremely large, unreasonably large:

Definition 3.11. 1. A subset $G \subset M$ is called a *set of generators* for M iff

$$\sigma|_{R[G]} : R[G] \longrightarrow M$$

is surjective.

2. The module M is called *finitely generated* if there is a finite set $G \subset M$ of generators. With other words, a left module M is finitely generated if there are elements $u_1, ..., u_n \in M$, such that

$$M = R \cdot u_1 + ... + R \cdot u_n := \{\lambda_1 u_1 + ... + \lambda_n u_n; \lambda_1, ..., \lambda_n \in R\}.$$

Remark 3.12. 1. A free module F is finitely generated iff $F \cong R^n$ for some $n \in \mathbb{N}$. We have $R^n = R \cdot e_1 + ... + R \cdot e_n$ with the standard basis vectors $e_i, i = 1, ..., n$. On the other hand assume that $F = R \cdot u_1 + ... + R \cdot u_r$ admits the basis $B \subset F$. Then the subset $B_0 \subset B$ of basis vectors appearing with a nonzero scalar coefficient in the representation of the elements $u_i, i = 1, ..., r$, as a linear combination in B is finite and generates F. Now a basis being a minimal set of generators we conclude $B = B_0$ and $F \cong R^n$ with $n = |B|$.

2. If R is an integral domain any two bases of a free module have the same cardinality. This follows from the vector space case since for any ideal $\mathfrak{a} \subset R$ we have

$$R[I]/\mathfrak{a}R[I] \cong (R/\mathfrak{a})[I]$$

and we may take $\mathfrak{a} := \mathfrak{m}$ to be a maximal ideal. Then with $K := R/\mathfrak{m}$ we obtain that $R[I] \cong R[J]$ implies $K[I] \cong K[J]$, and LA tells us $|I| = |J|$.

So in order to understand arbitrary finitely generated modules one can investigate submodules of R^n, an approach which works satisfactorily for a PID R, see section 4.

In an other approach one assumes that all simple modules are known. Then given a nonsimple module M, one hunts for submodules $L \leq M$, such that either L or M/L is simple. Then we have to deal with the question:

Question: Given $L \leq M$, what can be said about M, assuming that we know the submodule L and the factor module M/L?

The discussion of that problem leads us to a central question of homological algebra. We shall make a small detour and have a first glimpse at that subject:

The modules $L \leq M$ and $N := M/L$ are related by the "short exact sequence"

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0,$$

where $\varphi : L \longrightarrow M$ is the inclusion and $\psi : M \longrightarrow N$ the quotient map.

Definition 3.13. 1. A (finite or infinite) sequence of modules and module homomorphism

$$.... \longrightarrow M_{i-1} \xrightarrow{\varphi_{i-1}} M_i \xrightarrow{\varphi_i} M_{i+1} \longrightarrow ...$$

is called exact at M_i if $\ker(\varphi_i) = \varphi_{i-1}(M_{i-1})$ (such that in particular $\varphi_i \circ \varphi_{i-1} = 0$). It is called exact if it is exact at all intermediate positions.

2. A *short exact sequence* is a five term exact sequence

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0,$$

i.e.

   (a) φ is injective,

   (b) $\varphi(L) = \ker(\psi)$,

   (c) ψ is surjective.

3. A short exact sequence is called *split* (or said to split), if the submodule $\varphi(L) \leq M$ admits a complementary submodule $M_0 \leq M$, i.e. a submodule $M_0 \leq M$, such that

$$\psi|_{M_0} : M_0 \longrightarrow N$$

is an isomorphism.

Remark 3.14. 1. In a short exact sequence one has

$$L \cong \varphi(L), N \cong M/\varphi(L),$$

so one may always assume that $\varphi : L \longrightarrow M$ is the inclusion of a submodule $L \leq M$ and $N = M/L$ with ψ the quotient map.

In a split short exact sequence the middle term is the "direct sum" of the outer terms:

Definition 3.15. Let $M_i, i \in I$, be a family of R-modules.

1. The *direct product* of the $M_i, i \in I$, is

$$\prod_{i \in I} M_i := \{(u_i)_{i \in I}; \forall i \in I : u_i \in M_i\},$$

the set of all families $(u_i)_{i \in I}$ endowed with the componentwise module operations.

2. The *direct sum* of the $M_i, i \in I$, is the submodule

$$\bigoplus_{i \in I} M_i := \{(u_i)_{i \in I} \in \prod_{i \in I} M_i; u_i = 0 \text{ for all but finitely many } i \in I\}.$$

Example 3.16. 1. Let V be an n-dimensional vector space. Then we have

$$\mathrm{End}(V) \cong V^n,$$

an isomorphism of $\mathrm{End}(V)$-modules, the right hand side denoting the n-fold direct sum of the $\mathrm{End}(V)$-module V. Take a basis $v_1, ..., v_n \in V$; then

$$f \mapsto (f(v_1), ..., f(v_n))$$

provides an isomorphism.

2. Universal mapping property for the product: Homomorphisms $\varphi : L \longrightarrow \prod_{i\in I} M_i$ correspond to families $(\varphi_i)_{i\in I}$ of homomorphisms $\varphi_i : L \longrightarrow M_i$.

3. Universal mapping property for the direct sum: Homomorphisms $\psi : \bigoplus_{i\in I} M_i \longrightarrow N$ correspond to families $(\psi_i)_{i\in I}$ of homomorphisms $\psi_i : M_i \longrightarrow N$. Note that here it is essential that the families $(u_i)_{i\in I}$ only have finitely many nonzero components, since then we may define

$$\psi((u_i)_{i\in I})) := \sum_{i\in I} \psi_i(u_i)$$

for any family $(\psi_i)_{i\in I}$ of homomorphisms.

4. If $L, M_0 \leq M$ are submodules, we write

$$M = L \oplus M_0$$

if the natural map $L \oplus M_0 \longrightarrow M, (u, v) \mapsto u + v$, is an isomorphism. In that case we say that $M_0 \leq M$ is a submodule complementary to L. In particular

$$M_0 \hookrightarrow M \longrightarrow M/L$$

is an isomorphism.

5. For a split exact sequence

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0,$$

the middle term is the direct sum of the outer terms: The map

$$L \oplus N \cong L \oplus M_0 \xrightarrow{\cong} M, (x, y) \mapsto \varphi(x) + y$$

is an isomorphism.

6. Let $R = \mathbb{Z}$. The short exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\varphi} \mathbb{Z} \xrightarrow{\psi} \mathbb{Z}_n \longrightarrow 0,$$

where $\varphi(x) = nx$ and ψ is the quotient map, is not split for $n > 1$, the module $\mathbb{Z}$ being torsion free.

So in particular L and M/L don't determine the module M itself. But there are modules, for which any short exact sequence having them as first resp. third term splits:

Definition 3.17. 1. A module I is called *injective* if any short exact sequence

$$0 \longrightarrow I \longrightarrow M \longrightarrow N \longrightarrow 0$$

splits or, equivalently, if whenever $\varphi : I \hookrightarrow M$ is injective, then there is a submodule $M_0 \leq M$ with $M = \varphi(I) \oplus M_0$.

2. A module P is called *projective* if any short exact sequence

$$0 \longrightarrow L \longrightarrow M \longrightarrow P \longrightarrow 0$$

splits or, equivalently, if whenever $\psi : M \longrightarrow P$ is surjective, then there is a submodule $M_0 \leq M$ with $M = \ker(\psi) \oplus M_0$.

Remark 3.18. The above definitions differ slightly from the quite technical standard definitions of projective resp. injective modules in the literature, but they are equivalent, see Prop.11.1.

Example 3.19. 1. Free modules are projective: If F is free with basis $B = \{e_i, i \in I\} \subset F$ and

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} F \longrightarrow 0$$

a short exact sequence, choose $v_i \in M$ with $\psi(v_i) = e_i$ and set

$$M_0 = \sum_{i \in I} Rv_i.$$

Obviously $\psi|_{M_0} : M_0 \longrightarrow F$ is onto, while injectivity follows from the fact that the elements $e_i, i \in I$, are linearly independent.

2. Vector spaces are both injective and projective: Being free they are projective; as a consequence any short exact sequence of vector spaces splits, hence they are injective as well.

Theorem 3.20. *A module P is projective iff there is a module Q, such that $P \oplus Q$ is free.*

Proof. If $\psi : F \longrightarrow P$ is onto with a free module F, then choose $F_0 \leq F$, s.th. $\psi|_{F_0} : F_0 \longrightarrow P$ is an isomorphism. Then with $Q := \ker(\psi)$ we have

$$F = F_0 \oplus Q \cong P \oplus Q.$$

On the other hand, if $\psi : M \longrightarrow P$ is surjective, consider $\hat{\psi} := \psi \oplus \mathrm{id}_Q : \hat{M} := M \oplus Q \longrightarrow P \oplus Q$. We find a submodule $\hat{M}_0 \leq \hat{M}$, s.th.

$$\hat{M}_0 \hookrightarrow \hat{M} \xrightarrow{\hat{\psi}} P \oplus Q$$

is an isomorphism. Now choose $M_0 := \{u \in M; (u, 0) \in \hat{M}_0\}$. □

Remark 3.21.

1. From the previous point it follows that projective modules over an integral domain are torsion free.
2. A finite dimensional vector space V is a projective $\mathrm{End}(V)$-module, since $V \oplus V^{n-1} \cong V^n \cong \mathrm{End}(V)$ with $n = \dim V$. It is not free for $n > 1$.
3. We mention without proof: Projective modules over
   (a) a PID
   (b) a polynomial ring $k[T_1, ..., T_n]$
   (c) a local ring

   are free.
4. The integral domains which are closest to PIDs are the so called *Dedekind rings*, i.e. noetherian integral domains integrally closed in their field of fractions, with nonzero prime ideals being maximal. For such a ring R all its ideals $\mathfrak{a} \subset R$ are projective R-modules. In particular, if $\mathfrak{a}$ is not a principal ideal, then, being of rank one, it is not free. Indeed all the ideals of R can be generated by two elements. As a consequence there is always an R-module Q, s.th. $\mathfrak{a} \oplus Q \cong R^2$.

In order to give explicit examples of injective modules we need

Definition 3.22. A module D over an integral domain R is called *divisible* if

$$\mu_a : D \longrightarrow D, x \mapsto ax,$$

is surjective for all $a \in R \setminus \{0\}$.

Theorem 3.23. *1. An injective module I over an integral domain is divisible.*

2. A divisible module D over a PID is injective. In particular $Q(R)$ and $Q(R)/R$ are injective.

Proof. 1.) For any $a \in R\setminus\{0\}$ and $u \in I$ there is a module $M \geq I$, such that $u \in aM$. For example take $M := (I \oplus R)/R(u, -a)$; then $I \hookrightarrow I \oplus 0 \longrightarrow M$ is injective because of $R(u, -a) \cap (I \oplus 0) = 0$.

Since I is injective, we may write $M = I \oplus M_0$. Now we have $(u, 0) \in aM = aI \oplus aM_0$, whence $u \in aI$.

2.) Consider a module $M \geq D$. We have to show that D admits a complementary submodule $M_0 \leq M$. By Zorn's lemma there is a maximal submodule satisfying $M_0 \cap D = \{0\}$. Then $M_0 \hookrightarrow M \longrightarrow M/D$ is clearly injective, and we have to show that it is surjective as well, or equivalently $D + M_0 = M$. If not, take $u \notin D + M_0$. Since R is a PID, we have

$$\{\lambda \in R; \lambda u \in D + M_0\} = Rq$$

with a non-unit $q \in R \setminus R^*$. If $q = 0$, then we have obviously

$$(M_0 + Ru) \cap D = M_0 \cap D = \{0\},$$

a contradiction to the maximality of M_0. Now let us consider the case $q \neq 0$. Since D is divisible, we may write

$$qu = v + d = v + qd_0,\ v \in M_0, d, d_0 \in D.$$

If we now replace u with $\tilde{u} := u - d_0$, we have still $\tilde{u} \notin D + M_0$. Again hunting for the contradiction

$$(M_0 + R\tilde{u}) \cap D = \{0\},$$

we consider an element $w + \lambda\tilde{u}$ in that intersection, where $w \in M_0$. In particular

$$\lambda u = \lambda d_0 - w \in D + M_0,$$

hence $\lambda = \mu q$ and thus

$$w + \lambda\tilde{u} = w + \mu v \in D \cap M_0 = \{0\}.$$

□

Finally we ask what can be said about a module M, such that any exact sequence having M as middle term is split.

Theorem 3.24. *For a module M the following statements are equivalent.*

1. *All exact sequences*

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$$

   are split.

2. *Any submodule $L \leq M$ admits a complementary submodule $M_0 \leq M$, i.e. such that*

$$M = L \oplus M_0.$$

3. *The module M is the sum*

$$M = \sum_{i \in I} M_i$$

   of simple submodules $M_i \leq M$.

4. *The module M is a direct sum of simple modules, i.e.*

$$M \cong \bigoplus_{i \in I} M_i$$

   with simple modules $M_i, i \in I$.

A module M satisfying one of the above equivalent conditions is called semi-simple.

Proof. Statement *2.)* is just a reformulation of *1.*

2.) $\Longrightarrow$ 3.): We consider the sum $L \leq M$ of all simple submodules of M and show $L = M$. If not, write $M = L \oplus M_0$ and pick $u \in M_0 \setminus \{0\}$. We show that $Ru \leq M_0$ contains a simple submodule, a contradiction to $L \cap M_0 = \{0\}$. Denote $\mathfrak{m} \supset \mathrm{Ann}(u)$ a maximal left ideal containing the annihilator of u. We may write

$$M = \mathfrak{m}u \oplus N.$$

First of all $\mathfrak{m}u \subsetneqq Ru$ — otherwise we would have $u = \lambda u$ with some $\lambda \in \mathfrak{m}$, hence $1 - \lambda \in \mathrm{Ann}(u) \subset \mathfrak{m}$ resp. $1 \in \mathfrak{m}$. Hence $u = (\mu u, b) \in \mathfrak{m}u \oplus N$ with

$\mu \in \mathfrak{m}, b \neq 0$ and $\mathfrak{m}b = \{0\}$. Thus $Rb \cong R/\mathfrak{m}$ is simple and $Rb \leq Ru$ because of $b = (1-\mu)u$.

3.) $\Longrightarrow$ 4.): Let $M_i, i \in I$, be the simple submodules of M. We consider the subsets $J \subset I$, such that

$$\sum_{i \in J} M_i = \bigoplus_{i \in J} M_i,$$

a relation which holds iff it holds for all finite subsets $J_1 \subset J$. They form a set T partially ordered by inclusion. If $T_0 \subset T$ is a linearly ordered subset, then

$$J_\infty := \bigcup_{J \in T_0} J$$

is an upper bound. Obviously $J_\infty \in T$ by the above remark.

4.) $\Longrightarrow$ 2.): We choose $M_0 \leq M$ maximal with $L \cap M_0 = \{0\}$ and show $L + M_0 = M$. If not, we have $M_j \not\subset L \oplus M_0$ for some $j \in I$. Since M_j is simple, it follows $(L \oplus M_0) \cap M_j = \{0\}$ and thus $(L \cap (M_0 \oplus M_j) = \{0\}$, a contradiction to the maximality of M_0. □

Example 3.25. 1. Let V be a finite dimensional vector space. Then

$$R = \mathrm{End}(V) \cong V^n$$

is a semisimple module over itself.

2. For a PID R the module $M := R/(a)$ is semisimple iff $a \neq 0$ is square free, i.e. is the product of pairwise non-associated irreducible elements.

Semisimple modules (and rings) are studied in section 7. —

In order to achieve a classification of modules we try to decompose a given module as a sum so far as possible, with summands not admitting any further decomposition:

Definition 3.26. A module M is called *indecomposable* iff there are no non-trivial submodules $L, N \leq M$, such that $M = L \oplus N$.

Remark 3.27. An R-module M is indecomposable iff its endomorphism ring $\mathrm{End}(M) := \mathrm{End}_R(M)$ does not contain idempotents $\neq 0, \mathrm{id}_M$.

Example 3.28. 1. A torsion free module M of rank one over an integral domain R is indecomposable: If $M = P \oplus Q$ is a nontrivial decomposition, then P, Q are torsion free as well, hence M would have rank at least 2.

2. Let R be a PID and $a \in R$. The module $R/(a)$ is

   (a) simple iff a is irreducible, and

   (b) indecomposable iff $a = 0$ or a is associated to a power of an irreducible element: For an integral domain R we have

   $$\mathrm{End}_R(R/(a)) \cong R/(a),$$

   and the right hand side does not contain idempotents $\neq 0, 1$ iff $a = 0$ or a is associated to a prime power: If a is of that form, all zero divisors in $R/(a)$ are nilpotent, while idempotents $\neq 0, 1$ are non-nilpotent zero divisors. In the remaining cases we may write $a = bc$ with relatively prime non-units b, c and Th.4.12 gives the decomposition $R/(a) \cong R/(b) \oplus R/(c)$.

Often it is not difficult to show that a given module M is a finite direct sum of indecomposable modules. But in general the summands are not uniquely determined up to order: Take a Dedekind ring which is not a PID. As we have mentioned in Ex.3.19.7, for any non-principal ideal $\mathfrak{a} \subset R$, we have $\mathfrak{a} \oplus Q \cong R \oplus R$, where $\mathfrak{a}, Q, R$ are indecomposable. But for a PID uniqueness up to order holds, cf. the next section, and as well for modules of finite length, i.e. if there is a finite ascending sequence of submodules with simple successive factor modules (Th.6.11).

Example 3.29. For the fan Q with one arrow α and two vertices $x = t(\alpha)$ and $y = h(\alpha)$ the indecomposable modules V look up to isomorphy as follows

1. $V_x = 0, V_y \cong k, F_\alpha = 0$
2. $V_x \cong k, V_y = 0, F_\alpha = 0$
3. $V_x \cong k, V_y \cong k, F_\alpha = \mathrm{id}_k$.

Note that $V = V_x \oplus V_y$ has dimension 1,1 or 2, so in the first two cases the kQ-module V is simple, while in the third case $0 \oplus V_y \subset V$ is a nontrivial submodule.

Furthermore: Any kQ-module V is a direct sum of modules of the above type: Choose a basis $B = B_0 \cup B_1$ of V_x such that $\ker(F_\alpha) = \mathrm{span}(B_0)$ and a basis $C = F_\alpha(B_1) \cup C_2$ of V_y. Then V is the direct sum of the submodules

1. $0 \oplus kw, w \in C_2$

2. $kv \oplus 0, v \in B_0$

3. $kv \oplus kF(v), v \in B_1$.

So we have obtained a complete classification of all kQ-modules.

4 Finitely generated Modules over a PID

A finitely generated module is a factor module F/L with a free module $F \cong R^n$. In order to understand it, we study submodules $L \leq F$ of a free module F for a PID R. They are again free modules:

Lemma 4.1. *Let R be a PID. Every submodule $L \leq F$ of a finitely generated free R-module $F \cong R^n$ is itself a free module: $L \cong R^m$ with some $m \leq n$.*

Remark 4.2. The condition "finitely generated" is not really needed, it has only been imposed in order to simplify the proof. See also Th.14.8.

Proof. We prove the lemma by induction on n assuming $F = R^n$. For $n = 1$ it is true by assumption, the ring R being a PID. For $n > 1$ the exact sequence

$$0 \longrightarrow R^{n-1} \times \{0\} \longrightarrow R^n \xrightarrow{\pi} R \longrightarrow 0$$

with the projection $\pi : R^n \longrightarrow R$ onto the last component induces a split exact sequence

$$0 \longrightarrow L_0 \longrightarrow L \longrightarrow \pi(L) = Rq \longrightarrow 0,$$

where $L_0 := L \cap (R^{n-1} \times \{0\})$, the third term being free, either trivial or of rank one. If $q = 0$, we have $L = L_0 \leq R^{n-1} \times \{0\} \cong R^{n-1}$ and may apply the induction hypothesis. Otherwise $L \cong L_0 \oplus R$. □

The central result of this section assures the existence of a basis $B \subset F$ related in a simple way to a basis of L.

Theorem 4.3. *Let R be a PID and $L \leq F$ a submodule of the finitely generated free R-module $F \cong R^n$. Then there is a basis $B = \{b_1, ..., b_n\}$ of F together with elements $q_1, ..., q_n \in R$ such that*

1.

$$L = R \cdot q_1 b_1 \oplus .... \oplus R \cdot q_n b_n,$$

2. *and* $q_i | q_{i+1}$ *for* $i = 1, ..., n-1$.

Remark 4.4. 1. We remark that the elements $q_1, ..., q_n$ are, up to multiplication with a unit (or rather the descending sequence of ideals $\mathfrak{a}_i = Rq_i, i = 1, ..., n$) uniquely determined by $L \leq F$ as a consequence of Th.4.11. Note furthermore that there is some index $r \leq n$, such that $q_i = 0$ iff $i > r$.

2. The condition "finitely generated" is essential: Write $Q(R) \cong F/L$ with a free module $F \geq L$. Since $Q(R)$ is torsion free we would obtain $q_i = 0$ or $q_i = 1$ for all i. As a consequence $Q(R)$ would be a free R-module. Contradiction!

The proof of Th.4.3 is divided into several steps, formulated as lemmata. We are doing induction on n and start hunting for the first vector $b_1 \in B$. In any case it has to be a primitive vector:

Lemma 4.5. *Let F be a finitely generated free module over the PID R. Then for a vector $e \in F$ the following statements are equivalent:*

1. *The element $e \in F$ is primitive, i.e.*

$$e = \lambda w,\ \lambda \in R,\ w \in F \Longrightarrow \lambda \in R^*.$$

2. *There is a homomorphism $\pi : F \longrightarrow R$ with $\pi(e) = 1$.*

Proof. "1) $\Longrightarrow$ 2)": We may assume $F = R^n$ and $e = (r_1, ..., r_n)$ with $\gcd(r_1, ..., r_n) = 1$. Hence $R \cdot r_1 + ... + R \cdot r_n = R$ and thus there are elements $\lambda_1, ..., \lambda_n \in R$ with $\lambda_1 r_1 + ... + \lambda_n r_n = 1$, so we may define $\pi : F \longrightarrow R$ by $\pi(x_1, ..., x_n) = \lambda_1 x_1 + ... + \lambda_n x_n$.
"2) $\Longrightarrow$ 1)": Obvious. □

Definition 4.6. Let $u \in F \setminus \{0\}$ be a free module. We write

$$\mathrm{cont}(u) = \lambda$$

if $u = \lambda e$ with some primitive vector $e \in F$. For a nontrivial submodule $L \leq F$ we define

$$\mathrm{cont}(L) := \gcd\{\mathrm{cont}(u); u \in L \setminus \{0\}\}.$$

Remark 4.7. The *content* $\mathrm{cont}(u) \in R \setminus \{0\}$ is defined only up to multiplication with a unit. If $u = (u_1, ..., u_n) \in R^n$, we have

$$\mathrm{cont}(u) = \gcd(u_1, ..., u_n).$$

The essential argument in the proof of Th. 4.3 is the following:

Lemma 4.8. *Let* $L \leq F, L \neq \{0\}$. *If* $\mathrm{cont}(L) = 1$, *there is a vector* $v \in L$ *with* $\mathrm{cont}(v) = 1$.

Proof. We are hunting for a projection $\pi : F \longrightarrow R$ (= a surjective linear map), such that $\pi(L) = R$ and take $v \in L$ with $\pi(v) = 1$ as the primitive vector we are looking for.

Choose $\pi \in F^* := \mathrm{Hom}(F, R)$ with maximal $\pi(L) \leq R$. Such a π exists, since above an ideal $\mathfrak{a} = Ra \neq \{0\}$ there are only finitely many ideals, the ideals Rb with a divisor b of a. We have $\pi(L) = Rq$ and want to show $q \in R^*$. Pick $v \in L$ with $\pi(v) = q$. Indeed $q = \mathrm{cont}(v)$. To see that write $v = \lambda e$ with a primitive vector $e \in F$ and some $\lambda \in R$. We show that $\lambda \in R^*q$, thus may assume $\lambda = q$. By Lemma 4.5 there is $\tilde{\pi} \in F^*$ with $\tilde{\pi}(e) = 1$ resp. $\tilde{\pi}(v) = \lambda$, while $q = \lambda\pi(e)$. Thus $\tilde{\pi}(L) \supset R\lambda \supset Rq = \pi(L)$ resp. $\tilde{\pi}(L) = \pi(L)$ because of the maximality of $\pi(L)$. With other words $Rq = R\lambda$, i.e. λ and q differ only by a unit.

Now with $F_0 := \ker(\pi), L_0 := L \cap F_0$ we have direct sum decompositions

$$F = F_0 \oplus Re$$

as well as

$$L = L_0 \oplus R \cdot qe.$$

Assume $q \notin R^*$. Then, since $\mathrm{cont}(L) = 1$, there is a vector $v_0 = \mu e_0 \in L_0$ with $\mu \notin Rq$ and primitive $e_0 \in F_0$. Now apply Lemma 4.1 once again and obtain a projection $\pi_0 : F_0 \longrightarrow R$ with $\pi_0(e_0) = 1$. Then

$$\tilde{\pi} : F = F_0 \oplus Re \longrightarrow R,\ u_0 + \lambda e \mapsto \pi_0(u_0) + \lambda$$

is a linear form with $\mu, q \in \tilde{\pi}(L)$, in particular $\pi(L) = Rq \subsetneqq \tilde{\pi}(L)$, a contradiction. □

Proof of 4.3. We use induction on n. Take $q := \mathrm{cont}(L)$. We may apply Lemma 4.8 to $q^{-1}L \leq F$ and find a primitive vector $e \in q^{-1}L$. Choose a projection $\pi : F \longrightarrow R$ with $\pi(e) = 1$ and define $F_0 \geq L_0$ as in the proof of

4.8. By the induction hypothesis $L_0 \leq F_0 \cong R^{n-1}$ satisfies 4.3, so we find a basis $B_0 = \{b_2, ..., b_n\} \subset F_0$ of F_0, such that 4.3 is satisfied with suitable $q_2, ..., q_n \in R$. Now set $B := \{b_1 := e, b_2, ..., b_n\}$ and $q_1 := q$. Obviously $q|q_2$. □

Remark 4.9. 1. Let

$$L = AR^m = \{Au; u \in R^m\} \leq R^n$$

with a matrix $A = (\alpha_{ij}) \in R^{n,m}$, where we may assume $m \geq n$. We describe how one can find the elements $q_1, ..., q_n \in R$ and a corresponding basis $b_1, ..., b_n$ for $F := R^n$. Clearly

$$q_1 = \gcd(\alpha_{ij}; 1 \leq i \leq n, 1 \leq j \leq m).$$

Write

$$B = (b_1, ..., b_n),\ Q = \begin{pmatrix} q_1 & 0 & .. & .. & 0 \\ 0 & q_2 & 0 & & 0 \\ : & & & & : \\ 0 & & 0 & q_{n-1} & 0 \\ 0 & .. & .. & 0 & q_n \end{pmatrix}.$$

Th.4.3 tells us that there is matrix $T \in GL_m(R)$, such that

$$AT = (q_1 b_1, ..., q_n b_n, 0) = (BQ, 0)$$

with $0 \in R^{n,m-n}$ resp.

$$(Q, 0) = B^{-1}AT.$$

Now $(Q, 0)$ is obtained from A by elementary row and column operations corresponding to multiplication from the left with B^{-1} resp. to multiplication with T from the right. In particular B^{-1} is obtained from the unit matrix I_n by the row operations involved there. Hence B is obtained from I_n by the inverse row operations in reversed order: $R_i \mapsto R_i + \lambda R_j$ resp. $R_i \mapsto \lambda R_i$ with $\lambda \in R^*$ is replaced with $R_i \mapsto R_i - \lambda R_j$ resp. $R_i \mapsto \lambda^{-1} R_i$, while an exchange of rows is inverse to itself. Our first goal is to realize a transformation

$$A \mapsto \begin{pmatrix} q_1 & 0 \\ 0 & A_1 \end{pmatrix}$$

with $A_1 \in R^{n-1,m-1}$. Now either $A_1 = 0$ and $0 = q_2 = ... = q_n$ or q_2 is the greatest common divisor of the entries of A_1 and we can proceed with A_1 as with A.

2. Let us consider the case $m = n$. Since $\det(B), \det(T) \in R^*$, we obtain that $\det(A)$ and $\det(Q)$ only differ by a unit. In particular, for $R = \mathbb{Z}$ and assuming $q_i > 0, i = 1, ..., n$, we arrive at

$$|\mathbb{Z}^n / A\mathbb{Z}^n| = q_1 \cdot ... \cdot q_n = |\det(A)|.$$

Example 4.10. Let $N = A\mathbb{Z}^3$ with the matrix

$$A := \begin{pmatrix} 2 & 3 & 5 \\ 4 & 9 & 25 \\ 8 & 27 & 125 \end{pmatrix}.$$

Obviously $q_1 = 1$. We first perform column operations:

$$\begin{pmatrix} 2 & 3 & 5 \\ 4 & 9 & 25 \\ 8 & 27 & 125 \end{pmatrix} \mapsto \begin{pmatrix} 2 & 1 & 5 \\ 4 & 5 & 25 \\ 8 & 19 & 125 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 6 & 5 & 0 \\ 30 & 19 & 30 \end{pmatrix}.$$

Subtract the first column from the second, then twice resp. 5 $\times$ the middle column from the first resp. the third column and multiply finally the first column with -1. Now interchanging the first and the second column we get

$$\begin{pmatrix} 1 & 0 & 0 \\ 5 & 6 & 0 \\ 19 & 30 & 30 \end{pmatrix}.$$

Though one already can read of from that matrix everything we are looking for - no coordinate change in R^3 has been performed - , we follow the steps described above: The row operations $R_2 \mapsto R_2 - 5R_1, R_3 \mapsto R_3 - 19R_1, R_3 \mapsto R_3 - 5R_2$ result in the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 30 \end{pmatrix}.$$

Then we have

$$A_0 = \begin{pmatrix} 6 & 0 \\ 0 & 30 \end{pmatrix},$$

whence $q_2 = 6$ as well as $q_3 = 30$. Applying the row operations $R_3 \mapsto R_3 + 5R_2, R_3 \mapsto R_3 + 19R_1, R_2 \mapsto R_2 + 5R_1$ to the unit matrix E finally gives

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 5 & 1 & 0 \\ 19 & 5 & 1 \end{pmatrix}.$$

As a corollary we obtain the classification of all finitely generated modules over a PID:

Theorem 4.11. Fundamental Theorem on finitely generated modules over a PID: *Given a finitely generated module M over a principal ideal domain R, there are proper ideals $\mathfrak{a}_i \subsetneqq R, i = 1, ..., n$, such that M is isomorphic to the finite direct product of the cyclic modules $R/\mathfrak{a}_i$, i.e.:*

$$M \cong R/\mathfrak{a}_1 \oplus ... \oplus R/\mathfrak{a}_n \ ,$$

where the ideals $\mathfrak{a}_i$ satisfy one of the following two conditions:

1. *They form a descending sequence:*

$$\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset ... \supset \mathfrak{a}_n.$$

2. *The ideals $\mathfrak{a}_i$ are powers of prime ideals:*

$$\mathfrak{a}_i = (p_i^{k_i})$$

with prime elements $p_i \in R$ and $k_i \in \mathbb{N}_{>0}$.

The ideals $\mathfrak{a}_1, ..., \mathfrak{a}_n$ are unique in the first case and unique up to order in the second case 2). (PS: The number n need not be the same in both cases!).

Proof. Existence: *1.)* Let us start with the first case: We have $M \cong F/L$ and find a basis $(b_1, ..., b_n) \subset F \cong R^n$ as in Th.4.3; hence with $\mathfrak{a}_i = (q_i)$ we have

$$M \cong \frac{R \oplus ... \oplus R}{\mathfrak{a}_1 \oplus ... \oplus \mathfrak{a}_n} \cong R/\mathfrak{a}_1 \oplus ... \oplus R/\mathfrak{a}_n.$$

Here, obviously, w.l.o.g. $\mathfrak{a}_i \neq R$.

2.) Fix an index $i \leq r$ and apply the below theorem to $\mathfrak{b} = \mathfrak{a}_i = (q_i)$ and $\mathfrak{b}_j = (p_j^{k_j})$, where $q_i = p_1^{k_1} \cdot ... \cdot p_s^{k_s}$ is the factorization of q_i into prime elements.

Proposition 4.12 (Chinese Remainder Theorem)**.** *Let R be a commutative ring and $\mathfrak{b}_1, ..., \mathfrak{b}_s \subset R$ coprime ideals, i.e. $\mathfrak{b}_j + \mathfrak{b}_\ell = R$ for $\ell \neq j$, and $\mathfrak{b} := \bigcap_{j=1}^s \mathfrak{b}_j$. Then the natural map*

$$\psi : R/\mathfrak{b} \longrightarrow R/\mathfrak{b}_1 \oplus ... \oplus R/\mathfrak{b}_s,$$

$$x + \mathfrak{b} \mapsto (x + \mathfrak{b}_1, ..., x + \mathfrak{b}_s)$$

is an isomorphism of rings.

Proof. Injectivity being obvious, we have only to show surjectivity, which easily follows from the fact that every "unit vector" $e_j := (\delta_{j\ell} + \mathfrak{b}_\ell)_{\ell=1,...,s} \in R/\mathfrak{b}_1 \oplus ... \oplus R/\mathfrak{b}_s$ is in the image of ψ. Indeed for $\ell \neq j$ we can find $x_\ell \in \mathfrak{b}_\ell, y_\ell \in \mathfrak{b}_j$ with $x_\ell + y_\ell = 1$. Then with $x := x_1 \cdot ... \cdot x_{j-1} \cdot x_{j+1} \cdot ... \cdot x_s$ we have $\psi(x + \mathfrak{b}) = e_j$. □

Uniqueness: *2.)* Consider the power p^ℓ of a prime element $p \in R$. Then

$$T_{p^{\ell+1}}(M)/T_{p^\ell}(M) \cong K^s,$$

where $K = R/(p)$ and $s = s(p, \ell)$ is the number of the ideals $\mathfrak{a}_i = (p^j)$ with $j > \ell$. Obviously the numbers $s(p, \ell)$ determine the ideals $\mathfrak{a}_i \neq 0$ up to order. Finally the number of ideals $\mathfrak{a}_i = 0$ is nothing but the the rank of $M/T(M)$.

1.) Write $\mathfrak{a}_i = (q_i)$. Using what we already have seen in the first part we may assume $q_n \neq 0$. Given a prime element $p \in R$, denote $\mu(p, i) \geq 0$ the multiplicity of p as divisor of q_i. These numbers determine the q_i up to a unit, and can easily be read off from a decomposition of type *2.)* as follows: Since $q_i | q_{i+1}$, we have $\mu(p, i) \leq \mu(p, i + 1)$, so the exponent $\mu(p, n)$ necessarily is the highest exponent of a p-power occuring in a decomposition of the second type. Now remove one highest p-power for all prime elements $p \in R$ and continue with what is left in the same spirit. □

5 Chain conditions: Noetherian and artinian modules

We start with the following easy observation:

Lemma 5.1. *Let X be a set with a partial order "$\preceq$". Then the following statements are equivalent:*

1. *Any non-empty subset $Y \subset X$ admits a maximal element, i.e. there is some $y_0 \in Y$, such that "$y_0 \preceq y \Longrightarrow y_0 = y$" holds all $y \in Y$.*

2. *The "ascending chain condiition": Any ascending sequence $x_1 \preceq x_2 \preceq$ ..... of elements in X terminates, i.e. there is some index n_0, such that $x_n = x_{n_0}$ holds for all $n \geq n_0$.*

Proof. "$\Longrightarrow$": Take $Y := \{x_n; n \in \mathbb{N}_{>0}\}$. If x_{n_0} is a maximal element then $x_n = x_{n_0}$ for all $n \geq n_0$.
"$\Longleftarrow$": If $Y \subset X$ does not admit a maximal element, then there is for any $y \in Y$ some successor $s(y) \in Y$, i.e. $y \prec s(y)$. So take any $x_1 \in Y$ and define recursively $x_{n+1} := s(x_n)$. We thus obtain a strictly ascending sequence. Contradiction! □

Definition 5.2. For an R-module Mdenote

$$\mathrm{Sub}(M) := \{L; L \leq M\}$$

the set of its submodules. It is called

1. *noetherian*, if $\mathrm{Sub}(M)$ satisfies the ascending chain condition w.r.t. the partial order "$\preceq$" given by the inclusion of submodules, i.e.

$$L \preceq N \Longleftrightarrow L \subset N.$$

   One says that M satisfies the ascending chain condition.

2. *artinian*, if $\mathrm{Sub}(M)$ satisfies the ascending chain condition w.r.t. the partial order "$\preceq$" given by the reversed inclusion of submodules, i.e.

$$L \preceq N \Longleftrightarrow L \supset N.$$

   In that case one says that M satisfies the descending chain condition.

A ring R is called left/right noetherian/artinian if ${}_RR$ resp. R_R is noetherian/artinian.

Example 5.3. 1. A PID R is a noetherian: Since it is factorial, any non unit $\neq 0$ has (up to multiplication with a unit) only finitely many divisors. Hence for a nonzero ideal $\mathfrak{a}$ there are only finitely many ideals $\mathfrak{d} \supset \mathfrak{a}$ above it, since

$$(a) = \mathfrak{a} \subset \mathfrak{d} = (d) \Longleftrightarrow d|a.$$

2. A field is both noetherian and artinian.

3. An integral domain R, which is not a field, is not artinian: For a nonunit $a \neq 0$ the ideals $\mathfrak{a}_n := (a^n)$ form a strictly decreasing sequence.

4. Let $M := \left\{ \frac{a}{2^n} \in \mathbb{Q}; a \in \mathbb{Z}, n \in \mathbb{N} \right\}$. Then the $\mathbb{Z}$-module $M/\mathbb{Z}$ is artinian, but not noetherian, since it is not finitely generated. Indeed, any proper submodule of $M/\mathbb{Z}$ is of the form $\mathbb{Z} \cdot (\frac{1}{2^n} + \mathbb{Z}) \cong \mathbb{Z}_{2^n}$. Note that, as an abelian group, we have $M/\mathbb{Z} \cong C_{2^\infty} = \bigcup_{n=1}^{\infty} C_{2^n}$.

The ascending chain condition admits an important reformulation:

Proposition 5.4. *An R-module M is noetherian if and only if every submodule $N \leq M$ is finitely generated:*

$$N = Ru_1 + ... + Ru_s \ (\textit{resp.} \ = u_1R + ... + u_sR)$$

with suitable elements $u_1, ..., u_s \in N$.

Proof. "$\Longrightarrow$": Take a submodule $N \leq M$ and define $Y \subset \mathrm{Sub}(M)$ by

$$Y := \{L \leq N; L \text{ finitely generated}\}.$$

Now a maximal element of Y can not be a proper submodule $N_0 < N$, since otherwise one can pick some $u \in N \setminus N_0$ and obtains with $L := N_0 + Ru \in Y$ a module $L > N_0$. So $N \in Y$, i.e. N is finitely generated.
"$\Longleftarrow$": Consider an ascending chain of submodules $L_1 \leq L_2 \leq .....$ Then $L_\infty := \bigcup_{n=1}^{\infty} L_n$ is a submodule as well. Take a finite system $u_1, ..., u_r$ of generators of L_∞ together with indices n_i such that $u_i \in L_{n_i}$. Then for $n \geq n_0 := \max(n_1, ..., n_r)$ we have $L_{n_0} = L_\infty = L_n$. □

Proposition 5.5. *Let $N \leq M$. Then M is noetherian/artinian if and only if both N and M/N are noetherian/artinian.*

Proof. The claim is an immediate consequence of the fact that for submodules $L, \tilde{L} \leq M$ one has

$$L = \tilde{L} \Longleftrightarrow L \cap N = \tilde{L} \cap N \ \wedge \varrho(L) = \varrho(\tilde{L}).$$

Here $\varrho : M \longrightarrow M/N, u \mapsto u + N$, denotes the quotient map. □

Corollary 5.6. *Assume R is left/right noetherian/artinian and M a left/right R-module. Then M is*

1. *noetherian if and only if M is finitely generated,*

2. *artinian if M is finitely generated.*

Proof. By induction on n one shows that R^n is noetherian/artinian if R is: Take $M = R^{n+1}$ and $N = R^n \times \{0\}$. Furthermore recall that finitely generated modules are isomorphic to factor modules R^n/N. □

Theorem 5.7. *The polynomial ring $R[T]$ over a commutative noetherian ring is noetherian as well.*

Remark 5.8. The corresponding statement for artinian rings is obviously wrong: Consider the chain of ideals $\mathfrak{a}_n := (T^n)$.

Proof. We show that any ideal $\mathfrak{a} \subset R[T]$ is finitely generated. Consider the chain of ideals $\mathfrak{b}_n \subset R$

$$\mathfrak{b}_n := \{b \in R; \exists\ f = bT^n + \sum_{\nu=0}^{n-1} b_\nu T^\nu \in \mathfrak{a}\}.$$

Choose $n_0 \in \mathbb{N}$, such that $\mathfrak{b}_n = \mathfrak{b}_{n_0}$ for $n \geq n_0$, furthermore polynomials

$$f_{\mu n} = b_{\mu n} T^n + ... \in \mathfrak{b}_n, \mu = 1, ..., m_n,$$

such that $\mathfrak{b}_n = Rb_{1,n} + ... + Rb_{m_n,n}$. We leave it to the reader to check that indeed

$$\mathfrak{a} = \sum_{n=0}^{n_0} \sum_{\mu=1}^{m_n} R[T] f_{\mu,n}.$$

□

Corollary 5.9 (Hilberts Basissatz). *The polynomial ring $k[T_1, ..., T_n]$ in finitely many variables $T_1, ..., T_n$ over a field k is noetherian.*

Proof. Do induction on $n \in \mathbb{N}$ using the fact that

$$k[T_1, ..., T_{n+1}] = (k[T_1, ..., T_n])\,[T_{n+1}].$$

□

6 Modules of finite length

In this section we study modules which are both noetherian and artinian.

Definition 6.1. Let M be an R-module. The *length* $\lambda(M) \in \mathbb{N} \cup \{\infty\}$ of M is defined as

$$\lambda(M) := \sup \{r; \exists\ 0 = M_0 < M_1 < ... < M_r = M\},$$

i.e. $\lambda(M)$ is the supremum of the lengths of strictly increasing finite chains of submodules in M.

Example 6.2. 1. A module M is simple iff $\lambda(M) = 1$.

2. For an algebraically closed field k a $k[T]$-module V with $\dim_k V < \infty$ is indecomposable iff $\mu_T = \lambda \mathrm{id}_V + N$ with a nilpotent homomorphism $N : V \longrightarrow V$, $N^{\dim V - 1} \neq 0$. It is simple if in addition $\dim V = 1$ (and hence $N = 0$).

Proposition 6.3. *Let $M_0 \leq M$ be a submodule of the R-module M. Then we have $\lambda(M) = \lambda(M_0) + \lambda(M/M_0)$.*

Proof. Given ascending chains $0 = L_0 < L_1 < ... < L_r = M_0$ and $0 = N_0 < N_1 < ... < N_s = M/M_0$, we get a chain $0 = L_0 < ... < L_r = p^{-1}(N_0) < ... < p^{-1}(N_s) = M$; hence $\lambda(M) \geq \lambda(M_0) + \lambda(M/M_0)$.

On the other hand, given $0 = M_0 < M_1 < ... < M_t = M$ we have for all $i = 1, ..., t$ that $M_{i-1} \cap M_0 < M_i \cap M_0$ or $p(M_{i-1}) < p(M_i)$, where $p : M \longrightarrow M/M_0$ is the quotient projection. Hence $t \leq \lambda(M_0) + \lambda(M/M_0)$. □

Modules of finite length $\lambda(M) < \infty$ are obviously both noetherian and artinian. Given such a module, we want to investigate maximal strictly increasing chains of submodules:

Definition 6.4. A strictly increasing chain of submodules $0 = M_0 < M_1 < M_2 < ... < M_r = M$ is called a *composition series* for the module M if one of the following equivalent conditions is satisfied:

1. The sequence can not be refined by inserting modules between two successive modules M_i and M_{i-1}.

2. The factor modules M_i/M_{i-1}, also called the *factors* of the composition series, are (nonzero) simple modules.

Remark 6.5. 1. By 6.3 we see, that a module with a composition series of length r has length $\lambda(M) = r$; in particular two different composition series have the same length.

2. A module M which is both noetherian and artinian admits a composition series: Let $L \subset M$ be any submodule. Since M/L is artinian as well, there is a minimal nonzero submodule $N \leq M/L$ - it is automatically of length 1 - and set $\widetilde{L} := p^{-1}(N)$, where $p : M \longrightarrow M/L$ is the quotient homomorphism. Now take $M_0 := 0$ and $M_{i+1} := \widetilde{M_i}$. Since M is noetherian as well, the chain terminates, but that is only possible if we have $M_n = M$ for some $n \in \mathbb{N}$.

3. A module M is of finite length iff it is both noetherian and artinian.

4. Any finite strictly increasing chain of submodules in a module of finite length can be refined to a composition series: If $0 = M_0 < M_1 < .... < M_n = M$, we take a composition series for each factor M_i/M_{i-1} (being artinian) and insert the inverse images of its members with respect to $p : M_i \longrightarrow M_i/M_{i-1}$ between M_{i-1} and M_i. Note that for $L \leq N \leq M_i/M_{i-1}$ we have
$$p^{-1}(N)/p^{-1}(L) \cong N/L.$$
Hence the refined sequence is a composition series for M.

In order to compare the factors of different composition series we need the following observation:

Remark 6.6. A homomorphism $f : M \longrightarrow N$ between simple modules is either an isomorphism or $f = 0$, since for $\ker(f) \leq M$ and $F(M) \leq N$ we have
$$f \neq 0 \Longrightarrow \ker(f) \neq M \Longrightarrow \ker(f) = 0$$
as well as
$$f \neq 0 \Longrightarrow f(M) \neq 0 \Longrightarrow f(M) = N.$$

Corollary 6.7. *For a simple R-module M we have*

$$\mathrm{End}(M) = \mathrm{Aut}(M) \cup \{0\}.$$

In particular the ring $D := \mathrm{End}(M)$ is a division ring, i.e. $D \setminus \{0\}$ is a group with respect to the ring multiplication.

Remark 6.8. A commutative division ring is nothing but a field, a noncommative one is also called a *skew field*.

Remark 6.9. Let us comment briefly on division rings D: A division ring D is a vector space over its center

$$Z(D) := \{a \in D; ab = ba \ \forall\ b \in D\},$$

a field. Hence, given a field k one looks for "central k-division algebras", i.e. division rings D with $Z(D) \cong k$. Then D is a k-vector space, and we shall discuss here the finite dimensional situation $\dim_k D < \infty$. For a finite or an algebraically closed field, there are no nontrivial finite dimensional division algebras, i.e. one has necessarily $D = Z(D) = k$. For $k = \mathbb{R}$ the quaternion algebra $\mathbb{H}$ is the only nontrivial example. In general one knows that $\dim_k D = n^2$ is a square, and for $k = \mathbb{Q}_p$, the p-adic numbers, there are $\varphi(n)$ (with Eulers φ-function) pairwise non-isomorphic central k-division algebras of dimension n^2 over k.

Finite dimensional central $\mathbb{Q}$-division algebras then can be classified using their "base extensions" $D_{\mathbb{R}} := \mathbb{R} \otimes_{\mathbb{Q}} D$ and $D_{\mathbb{Q}_p} := \mathbb{Q}_p \otimes_{\mathbb{Q}} D$. That process of base extension is as follows: Take an isomorphism $D \cong \mathbb{Q}^m$ (with $m = n^2$) and use for the multiplication in $D_K := K^m$ (with $K = \mathbb{R}, \mathbb{Q}_p$) the same "structure constants $c_{ij}^{\ell} \in \mathbb{Q}$" as in $D \cong \mathbb{Q}^m$, i.e. multiplication looks as follows

$$e_i e_j = \sum_{\ell=1}^{m} c_{ij}^{\ell} e_{\ell}$$

both in D and D_K. In this way we get a central K-algebra D_K (i.e. $Z(D_K) = K$), which either is again a central K-division algebra or a matrix algebra $\mathrm{Mat}_r(E)$ with some central K-division algebra E. The technique of base extension is also behind the statement, that $\dim_k D$ is a square for an arbitrary central k-division algebra: If $K \supset k$ is the algebraic closure of k, then $\dim_k D = \dim_K(D_K)$ and $D_K \cong \mathrm{Mat}_n(K)$ for some $n \in \mathbb{N}_{>0}$.

Proposition 6.10. Theorem of Jordan-Hölder (Camille Jordan, 1838-1922, and Otto Hölder, 1859-1937) *Let M be an R-module admitting composition series $0 = L_0 < L_1 < ... < L_r = M$ as well as $0 = N_0 < N_1 < ... < N_r = M$. Then there is a permutation $f \in \mathbb{S}_r$, such that for $j = f(i)$ we have*

$$L_i/L_{i-1} \cong N_j/N_{j-1} \ .$$

Proof. We prove the statement for generalized composition serious, i.e. series, whose factors are either simple or 0. Assume first $r = 2$. Then our composition series are of the form $0 \leq L \leq M$ and $0 \leq N \leq M$. If M itself is simple or $N = L$, nothing remains to be shown. Otherwise we have $L \cap N \subsetneq N$. But then, N being simple, the proper submodule $L \cap N$ is trivial. Now consider the injective homomorphism $L \hookrightarrow M \longrightarrow M/N$: Its image is a nontrivial submodule of M/N, hence $L \cong M/N$. By symmetry we have $N \cong M/L$ as well.

In the general case we consider the submodules

$$M_{ij} := L_i \cap N_j \subset M$$

and generalized composition series of length $r + s$ starting with M_{00} and ending with M_{rr} and inclusion steps

$$M_{ij} \subset M_{i+1,j} \text{ or } M_{ij} \subset M_{i,j+1}.$$

Then the generalized composition series

$$M_{00} \subset M_{10} \subset ... \subset M_{r0} \subset M_{r1} \subset .... \subset M_{rr}$$

and

$$M_{00} \subset M_{01} \subset ... \subset M_{0r} \subset M_{1r} \subset .... \subset M_{rr}$$

have the same non-trivial factors as $N_0 < N_1 < ... < N_r$ resp. $L_0 < L_1 < ... < L_r$, and the first one can be connected to the second one by a chain of generalized composition series of length $2r$, such that two successive series differ only in two successive inclusions:

$$M_{ij} \subset M_{i+1,j} \subset M_{i+1,j+1}$$

is replaced with

$$M_{ij} \subset M_{i,j+1} \subset M_{i+1,j+1}.$$

But then it is clear from our initial argument (applied to the factor module $M_{i+1,j+1}/M_{ij}$) that the two successive generalized composition series have the same simple factors taken with multiplicities. □

So we may speak about the simple factors of an R-module M and their multiplicities in M (:= the number of times it shows up as a factor in a composition series). But, as we already have seen in section 3, the simple factors do not determine the module itself. Instead we have to consider indecomposable modules instead of simple ones. A decomposition as a finite direct sum of indecomposable modules is obviously possible for artinian modules. If it is even of finite length there is an analogue to the Jordan-Hölder theorem 6.10:

Theorem 6.11 (**Theorem of Krull-Schmidt).** (Wolfgang Krull, 1899-1971) *Let M be a module of finite length,*

$$M = L_1 \oplus ... \oplus L_r = N_1 \oplus ... \oplus N_s$$

with indecomposable submodules $L_i, N_j \leq M$. Then $s = r$, and there is a permutation $f \in \mathbb{S}_r$, such that for $j = f(i)$ we have

$$L_i \cong N_j \ .$$

Example 6.12. If V is a k-vector space with basis $e_1, ..., e_n$, then we get

$$\mathrm{End}(V) = \bigoplus_{i=1}^{n} \mathrm{End}(V)P_i$$

where $P_i : V \longrightarrow V, e_j \mapsto \delta_{ij} e_i$.

Remark 6.13. The assumption that M be of finite length is important; while for a PID and finitely generated M it holds as well (as we shall see later on), it is definitely false for arbitrary integral domains (though explicit counter examples are not easy at hand).

We need some preparatory lemmata dealing with the endomorphism ring of artinian resp. indecomposable modules:

Lemma 6.14. *For an endomorphism $f : M \longrightarrow M$ of a module of finite length the following statements are equivalent*

1. *f is bijective.*
2. *f is injective.*

3. f is surjective.

Proof. Assume $f : M \longrightarrow M$ is injective and $y \in M$. Then $M \geq f(M) \geq f^2(M) \geq ...$ is a strictly decreasing chain of submodules, so there is some $n \in \mathbb{N}$ with $f^{n+1}(M) = f^n(M)$. In particular $f^n(y) = f^{n+1}(x)$ with some $x \in M$. But then already $y = f(x)$, since with f its iterate f^n is injective as well.

Now assume that $f : M \longrightarrow M$ is surjective and consider the ascending chain $0 \leq \ker f \leq \ker f^2 \leq ....$ For some $n \in \mathbb{N}$ we have $\ker f^n = \ker f^{n+1}$. Hence $f|_{f^n(M)} = f|_M$ is injective. □

Lemma 6.15. *For an endomorphism $f : M \longrightarrow M$ of a module of finite length there is a positive natural number such that*

$$M = f^n(M) \oplus \ker(f^n).$$

In particular, if M is indecomposable, an endomorphism is either an automorphism or nilpotent.

Proof. Assume first that $g : M \longrightarrow M$ satisfies $\ker g^2 = \ker g$ as well as $g^2(M) = g(M)$. Then $M = g(M) \oplus \ker g$. The first condition is equivalent to $\ker(g) \cap g(M) = 0$. On the other hand, given any $y \in M$, we find some $x \in M$ with $g(y) = g^2(x)$. Then

$$y = g(x) + (y - g(x)) \in g(M) + \ker g = g(M) \oplus \ker g.$$

Now, since both chains $(f^i(M))_{i\in\mathbb{N}}$ and $(\ker f^i)_{i\in\mathbb{N}}$ terminate, we can take $g = f^n$ with a sufficiently big $n \in \mathbb{N}$. Finally, for indecomposable M we have either $f^n(M) = 0$ or $\ker f^n = 0$. It follows $f^n = 0$ or $\ker f = 0$; in the second case we obtain, according to 6.14, that f is an isomorphism. □

As a result of our discussion we obtain an algebraic characterization of the endomorphism ring $\mathrm{End}(M)$ of an indecomposable R-module, a generalization of Corollary 6.7:

Corollary 6.16. *For an indecomposable module M of finite length we have*

$$\mathrm{End}(M) = \mathrm{Aut}(M) \cup \mathrm{Nil}(M).$$

Furthermore the set $\mathrm{Nil}(M)$ *of nilpotent endomorphisms is even a two-sided ideal.*

Proof. The first part is a consequence of Lemma 6.15, while Lemma 6.14 yields $fg \in \mathrm{Aut}(M) \Longrightarrow f, g \in \mathrm{Aut}(M)$. Hence

$$\mathrm{Aut}(M) \circ \mathrm{Nil}(M),\ \mathrm{Nil}(M) \circ \mathrm{Aut}(M) \subset \mathrm{Nil}(M).$$

It remains to show that $\mathrm{Nil}(M)$ is additively closed. So take $f, g \in \mathrm{Nil}(M)$. If $f + g \notin \mathrm{Nil}(M)$, it is an automorphism, and thus we may even assume $f + g = \mathrm{id}_M$ - replace f, g with $f(f+g)^{-1}, g(f+g)^{-1}$. But then we get

$$f^2 + fg = f(f+g) = f = (f+g)f = f^2 + gf$$

and hence $fg = gf$. So, in order to compute $(f+g)^n$ we may use the binomial formula, and doing so we see easily that $f + g$ is nilpotent as well, contradiction! □

Proof of 6.11. We show by induction on k, that after a suitable permutation of the N_j we have

$$M = N_1 \oplus ... \oplus N_k \oplus L_{k+1} \oplus ... \oplus L_r$$

where $N_i \cong L_i$ for $i = 1, ..., k$. For $k = 0$ nothing has to be shown. Denote $p_i : M \longrightarrow N_i, i = 1, ..., k$ and $p_i : M \longrightarrow L_i, i = k+1, ..., r$ the projections belonging to the above direct sum decomposition, $q_j : M \longrightarrow N_j, j = 1, ..., s$ the projections for $M = N_1 \oplus ... \oplus N_s$. (We shall identify the projections p_i, q_j with the endomorphisms of M obtained by composing them with the injections $p_i(M), q_j(M) \hookrightarrow M$.)

We are now looking for an $\ell > k$ with $L_{k+1} \cong N_\ell$. Look at the following endomorphism

$$\mathrm{End}(L_{k+1}) \ni \mathrm{id}_{L_{k+1}} = \sum_{j=1}^{s} (p_{k+1} \circ q_j)|_{L_{k+1}} = \sum_{j=k+1}^{s} (p_{k+1} \circ q_j)|_{L_{k+1}},$$

since $p_{k+1}|_{N_j} = 0$ for $j = 1, ..., k$. The left hand side is not nilpotent, so by Corollary 6.16 there is an index $\ell \geq k+1$, such that $(p_{k+1} \circ q_\ell)|_{L_{k+1}} \in \mathrm{End}(L_{k+1})$ is not nilpotent either and hence $(p_{k+1} \circ q_\ell)|_{L_{k+1}} \in \mathrm{Aut}(L_{k+1})$. Obviously $q_\ell|_{L_{k+1}} : L_{k+1} \longrightarrow N_\ell$ is injective, but $(q_\ell \circ p_{k+1})|_{N_\ell}$ is not nilpotent either - otherwise $(p_{k+1} \circ q_\ell)|_{L_{k+1}}$ would be nilpotent as well! So as before $(q_\ell \circ p_{k+1})|_{N_\ell} \in \mathrm{Aut}(N_\ell)$ and hence q_ℓ is also surjective resp. $N_\ell \cong L_{k+1}$. Of course, after a reordering of the $N_j, j \geq k+1$, we may assume $\ell = k+1$. Finally

$$M = N_1 \oplus ... \oplus N_k \oplus N_{k+1} \oplus L_{k+2} \oplus ... \oplus L_r$$

is an immediate consequence of the direct sum decomposition

$$M = N_1 \oplus ... \oplus N_k \oplus L_{k+1} \oplus L_{k+2} \oplus ... \oplus L_r$$

and the fact that $q_{k+1}|_{L_{k+1}} : L_{k+1} \longrightarrow N_{k+1}$ is an isomorphism. □

7 Semisimple modules and rings

A module of finite length which is isomorphic to the direct sum of its simple factors (taken with multiplicities) is called *semisimple*. Indeed semisimplicity can be defined for any module (finite length is not needed): Semisimple modules are those ones which can be obtained as a (not necessarily finite) direct sum of simple modules. For details see Grillet, Ch, IX.2.

Here we prove a characterization of all rings which are semisimple as (left or right) module over itself.

Theorem 7.1 (Theorem of Artin-Wedderburn)**.** *For a ring R the following statements are equivalent:*

1. *${}_RR$ is a semisimple.*
2. *R_R is a semisimple.*
3. *There are natural numbers $n_1, ..., n_r \in \mathbb{N}_{>0}$ and division rings $D_1, ..., D_r$, such that*
$$R \cong \mathrm{Mat}_{n_1}(D_1) \times ... \times \mathrm{Mat}_{n_r}(D_r).$$

Proof. First of all we have isomorphisms

$$R \cong \mathrm{End}(R_R), a \mapsto \mu_a : x \mapsto ax$$

and

$$R^{\mathrm{op}} \cong \mathrm{End}({}_RR), a \mapsto \tilde{\mu}_a . x \mapsto xa.$$

On the other hand for a direct sum

$$M = \bigoplus_{i=1}^{r} M_i$$

of left/right R-modules we have

$$\mathrm{End}(M) \cong \bigoplus_{1 \leq i,j \leq r} \mathrm{End}(M_j, M_i), \varphi \mapsto (\varphi_{ij} := \mathrm{pr}_i \circ \varphi|_{M_j}),$$

where the right hand side is considered as a ring, namely endowed with "matrix multiplication". Now write

$$R = \bigoplus_{i=1}^{r} \mathfrak{a}_i^{n_i}$$

with simple pairwise non-isomorphic left/right ideals $\mathfrak{a}_i$. Since $\mathrm{End}(\mathfrak{a}_i, \mathfrak{a}_j) = 0$ for $i \neq j$ and $D_i = \mathrm{End}(\mathfrak{a}_i)$ is a division ring, we arrive at

$$\mathrm{End}(R) \cong \bigoplus_{i=1}^{r} \mathrm{Mat}_{n_i}(D_i),$$

where $\mathrm{End}(R)$ means either $\mathrm{End}({}_R R)$ or $\mathrm{End}(R_R)$. Combining with the first isomorphism we obtain the implication "2) $\Longrightarrow$ 3)", while for "1) $\Longrightarrow$ 3)" we get $R^{\mathrm{op}} \cong$ .... resp.

$$R \cong \bigoplus_{i=1}^{r} \mathrm{Mat}_{n_i}(D_i^{\mathrm{op}}),$$

since

$$\mathrm{Mat}_n(D^{\mathrm{op}}) \longrightarrow \mathrm{Mat}_n(D)^{\mathrm{op}}, A \mapsto A^T$$

is an isomorphism.
"3) $\Longrightarrow$ 1), 2)": Since a direct sum of semisimple rings is semisimple as well, it suffice to show that $\mathrm{Mat}_n(D)$ is both right and left semisimple. For $P_\ell := (\delta_{i\ell}\delta_{j\ell}) \in \mathrm{Mat}_n(D)$ we have

$$\mathrm{Mat}_n(D) = \bigoplus_{\ell=1}^{n} \mathrm{Mat}_n(D)P_i = \bigoplus_{\ell=1}^{n} P_i\mathrm{Mat}_n(D),$$

where each summand is isomorphic to the simple module D^n. Here we view the elements in D^n either as column or as row vectors: In the first case $\mathrm{Mat}_n(D)$ acts by multiplication from the left, in the second one by multiplication from the right. □

8 The Jacobson radical

For rings the artinian property is not completely analogous to the noetherian property. Indeed, in this section we shall see, that a ring which is left artinian automatically is left noetherian as well. The proof uses a new characterization of simple modules via the *Jacobson radical* of a ring.

Definition 8.1. 1. The nilradical $\sqrt{0} \subset R$ of a ring R is defined as the set of all nilpotent elements:

$$\sqrt{0} := \{x \in R; \exists\ r \in \mathbb{N}; x^r = 0\}.$$

2. The Jacobson radical $J(R) \subset R$ of a ring R is defined as the intersection of all maximal left ideals:

$$J(R) := \bigcap_{\mathfrak{m} \leq_R R} \mathfrak{m}.$$

Remark 8.2. 1. For a commutative ring R the nilradical $\sqrt{0}$ is an ideal, since obviously $R \cdot \sqrt{0} \subset \sqrt{0}$ and $x^m = 0 = y^n \Longrightarrow (x+y)^{n+m} = 0$ as a consequence of the binomial formula. One can even prove that

$$\sqrt{0} = \bigcap_{\mathfrak{p} \subset R \text{ prime ideal}} \mathfrak{p}$$

is the intersection of all prime ideals. Hence in particular

$$\sqrt{0} \subset J(R).$$

2. On the other hand, in the noncommutative case it can happen that $\sqrt{0}$ is not additively closed and that $R \cdot \sqrt{0} \not\subset \sqrt{0}$.

In order to get a more rewarding description of the Jacobson radical we need:

Remark 8.3. 1. For any left R-module M its annihilator

$$\mathrm{Ann}(M) := \{x \in R; xM = \{0\}\}$$

is a two sided ideal.

2. Denote $\mathfrak{a} \subset R$ a left ideal. For $M = R/\mathfrak{a}$ we have

$$\mathrm{Ann}(R/\mathfrak{a}) \subset \mathfrak{a}$$

with equality for a commutative ring R.

Proposition 8.4. *The Jacobson radical is the intersection of the annihilator ideals of simple R-modules:*

$$J(R) = \bigcap_{M \text{ simple } R\text{-module}} \mathrm{Ann}(M).$$

In particular $J(R) \subset R$ is a two sided ideal.

Proof. The inclusion "$\supset$" follows from $\mathfrak{m} \supset \mathrm{Ann}(R/\mathfrak{m})$ and the fact that a simple left R-module is of the form $R/\mathfrak{m}$. On the other hand, given $\lambda \in J(R)$ we have to show that $\lambda x = 0$ for any element $x \in M$ in a simple module M. For $x = 0$ this is obvious. Otherwise $M = Rx \cong R/\mathrm{Ann}(x)$, hence $\mathfrak{m} := \mathrm{Ann}(x)$ is a maximal left ideal and thus $\lambda \in \mathrm{Ann}(x)$. □

Lemma 8.5. *The Jacobson radical $J(R)$ of a ring R consists of all $x \in R$, such that $1 + \lambda x$ has a left inverse for all $\lambda \in R$, i.e.*

$$J(R) = \{x \in R; R(1 + \lambda x) = R, \ \forall \lambda \in R\}.$$

Proof. "$\subset$": If $x \in J(R)$, but $R(1 + \lambda x) \neq R$, then $R(1 + \lambda x) \subset \mathfrak{m}$ for some maximal left ideal $\mathfrak{m}$. But $\lambda x \in J(R) \subset \mathfrak{m}$ as well, hence $1 = (1 + \lambda x) - \lambda x \in \mathfrak{m}$, a contradiction.
"$\supset$": If $R(1 + \lambda x) = R$ for all $\lambda \in R$, but $x \notin \mathfrak{m}$ for some maximal left ideal $\mathfrak{m}$, then $R = \mathfrak{m} + Rx$ resp. $1 = y + \lambda x$ for some $y \in \mathfrak{m}, \lambda \in R$. But then $y = 1 + (-\lambda)x \in \mathfrak{m}$ has no left inverse, contradiction! □

The fact that the Jacobson radical is a two sided ideal motivates the question, whether it can be described without making a choice between "left" and "right". So it is, indeed:

Proposition 8.6. *For the Jacobson radical $J(R)$ of a ring R we have*

$$1 + J(R) \subset R^*,$$

and $J(R)$ contains all two sided ideals with that property, i.e. if $\mathfrak{a} \subset R$ is a two sided ideal, then

$$1 + \mathfrak{a} \subset R^* \Longrightarrow \mathfrak{a} \subset J(R).$$

So $J(R)$ is the unique maximal two sided ideal $\mathfrak{a}$ satisfying $1 + \mathfrak{a} \subset R^*$. In particular

$$J(R^{\mathrm{op}}) = J(R).$$

Proof. For $x \in J(R)$ we have $R = R(1+x)$, thus there is some $y \in R$ with $1 = y(1+x)$. But $y = 1 - yx$ has a left inverse $z \in R$ as well according to Lemma 8.5. That implies

$$z = z(y(1+x)) = (zy)(1+x) = 1 + x,$$

with other words $(1+x)y = 1$ as well and thus $1+x \in R^*$. Finally, for $x \in \mathfrak{a}$ we have $Rx \subset \mathfrak{a}$, hence $1 + Rx \subset R^*$ and thus in particular $x \in J(R)$. □

Definition 8.7. A left (or right) ideal $\mathfrak{n} \subset R$ is called nilpotent if there is some $r \in \mathbb{N}$ with $\mathfrak{n}^r = \{0\}$, i.e.

$$x_1, ..., x_r \in \mathfrak{n} \Longrightarrow x_1 \cdot .... \cdot x_r = 0.$$

Remark 8.8. Note that

$$\mathfrak{n} \subset \sqrt{0}$$

holds for a nilpotent ideal, but an ideal consisting of nilpotent elements only need not be nilpotent.

The relation between nilpotent ideals and the Jacobson radical is the following:

Lemma 8.9. *1. For a nilpotent left ideal $\mathfrak{n} \subset R$ we have $\mathfrak{n} \subset J(R)$.*

2. The Jacobson radical $J(R)$ of a left artinian ring R is itself nilpotent.

Proof. 1) Assume $\mathfrak{n}^r = \{0\}$. We show that $\mathfrak{n} \subset \mathrm{Ann}(M)$ for any simple left R-module M. If not, we find $\mathfrak{n}M = M$ and thus $\mathfrak{n}^\ell M = M$ for all $\ell \in M$. In particular $\{0\} = \mathfrak{n}^r M = M \neq \{0\}$, a contradiction.
2) First of all the descending sequence $J \supset J^2 \supset ...$ for $J := J(R)$ terminates, hence we find $m \in \mathbb{N}$ with $J^m = J^{m+1}$. We claim that $J^m = \{0\}$. Assume the contrary. The set of left ideals $\mathfrak{a} \leq {}_R R$ with $J^m\mathfrak{a} \neq \{0\}$ admits a minimal element, the ring R being artinian and $\mathfrak{a} = R$ being such an ideal. Take some element $a \in \mathfrak{a}$ with $J^m a \neq \{0\}$. Then we find $\mathfrak{a} = Ra$ because of the minimality of $\mathfrak{a}$ and even $J^m a = Ra$, using once again the minimality of $\mathfrak{a}$ together with the inclusion $J^m\mathfrak{a} \subset \mathfrak{a}$ and

$$J^m(J^m\mathfrak{a}) = J^{2m}\mathfrak{a} = J^m\mathfrak{a} \neq 0.$$

Hence $xa = a$ for some $x \in J^m$ resp. $0 = (1-x)a$. But that implies $a = 0$, since $1 - x \in R^*$ is a unit. Contradiction! □

Remark 8.10. 1. $J(R_1 \times ... \times R_s) = J(R_1) \times ... \times J(R_s)$, since the maximal left ideals of $R_1 \times ... \times R_s$ are of the form $R_1 \times ... \times R_{i-1} \times \mathfrak{m}_i \times R_{i+1} .... \times R_s$ with a maximal left ideal $\mathfrak{m}_i \subset R_i$.

2. $J(R/J(R)) = \{0\}$, since the maximal left ideals of $R/J(R)$ are of the form $\mathfrak{m}/J(R)$ with a maximal left ideal $\mathfrak{m} \leq {}_R R$.

3. For a division ring D we have $J(\mathrm{Mat}_n(D)) = \{0\}$, since the maximal left ideals of $\mathrm{Mat}_n(D)$ are of the form

$$\mathfrak{m} = I(L) := \{A \in \mathrm{Mat}_n(D)); A|_L = 0\}$$

with a "right line" $L \subset D^n$, i.e. $L = zD$ for some $z \in D^n \setminus \{0\}$.

4. For a semisimple ring R we have $J(R) = \{0\}$.

Theorem 8.11. *For a ring R the following statements are equivalent:*

1. *R is semisimple.*

2. *R is left artinian and $J(R) = \{0\}$*

3. *R is left artinian and has no nilpotent left ideals $\mathfrak{n} \neq \{0\}$.*

Proof. "1) $\Longrightarrow$ 2)": A semisimple ring is the direct sum of matrix rings over a division ring; hence Rem.8.10.1 and 3 give the result.
"2) $\Longrightarrow$ 1)": The Jacobson radical $J(R)$ of a left artinian ring R is the intersection of finitely many maximal left ideals

$$\{0\} = J(R) = \mathfrak{m}_1 \cap .... \cap \mathfrak{m}_s,$$

since otherwise one could construct an infinite strictly descending chain of left ideals (But that does not imply that $\mathfrak{m}_1, ..., \mathfrak{m}_s$ are the only maximal left ideals!). Then

$${}_R R \cong R/\mathfrak{m}_1 \times .... \times R/\mathfrak{m}_s$$

by the chinese remainder theorem Prop.4.12, hence ${}_R R$ is semisimple as a direct sum of simple modules.
"2) $\Longrightarrow$ 3)": Follows from the fact that nilpotent ideals are contained in the Jacobson radical.
"3) $\Longrightarrow$ 2)": The Jacobson radical $J(R)$ of a left artinian ring R is nilpotent according to Lemma 8.9. $\square$

Proposition 8.12. *A left module over a left artinian ring is semisimple iff* $J(R)M = \{0\}$.

Proof. "$\Longrightarrow$": Write $M = \bigoplus_{i=1}^{s} M_i$ as a direct sum of simple modules $M_i, i = 1, ..., s$. Then we have

$$J(R) \subset \bigcap_{i=1}^{s} \mathrm{Ann}(M_i),$$

hence $J(R)M = \{0\}$.
"$\Longleftarrow$": If $J(R)M = \{0\}$, the module M can be regarded as a $R/J(R)$-module. But $R/J(R)$ is a semisimple ring according to ...., hence M a semisimple $R/J(R)$- resp. R-module. □

Theorem 8.13. *For a left module M over a left artinian ring R the following statements are equivalent:*

1. *M is noetherian.*
2. *M is artinian.*
3. *M is of finite length.*

Proof. It suffices to prove the equivalence of 1) and 2).
"1) $\Longrightarrow$ 2)": If M is noetherian, it is in particular finitely generated and thus $M \cong {}_RR/K$ with some submodule $K \leq {}_RR$. Since ${}_RR$ is artinian, that implies that M is artinian as factor module of an artinian module.
"2) $\Longrightarrow$ 1)": Since $J = J(R)$ is nilpotent according to ...., say with $J^m = \{0\}$, we have a descending sequence

$$M \supset JM \supset J^2M \supset ... \supset J^{m-1}M \supset \{0\} = J^mM$$

with factors $Q_i := J^iM/J^{i+1}M$ annihilated by J. Thus they are as artinian semisimple modules finite direct products of simple modules. It follows that

$$\lambda(M) \leq \sum_{i=0}^{m-1} \lambda(Q_i) < \infty.$$

□

Taking $M = {}_RR$ we obtain finally:

Corollary 8.14. *A left artinian ring is left noetherian as well.*

9 Tensor product

The cartesian product $M \times N$ of two modules is the underlying set for the direct sum (or product) $M \oplus N$ of M and N. In this section we introduce a new construction, the tensor product $M \otimes N$ of M and N. It is an abelian group defined for a right R-module M and a left R-module N, its essential feature is that it transforms "bihomomorphisms" into homomorphisms.

Definition 9.1. Let M be a right R-module, N a left R-module and A an additively written abelian group. A map

$$\sigma : M \times N \longrightarrow A$$

is called a "bihomomorphism" if

1. σ is "biadditive", i.e. for $u \in M, v \in N$ the maps

   $$\sigma(u, ..) : N \longrightarrow A, \sigma(.., v) : M \longrightarrow A$$

   are homomorphism of abelian groups,

2. and

   $$\sigma(u\lambda, v) = \sigma(u, \lambda v)$$

   holds for $u \in M, v \in N, \lambda \in R$.

Example 9.2.

1. The map $\sigma : R_R \times {}_R R \longrightarrow R, (x, y) \mapsto axyb$, with $a, b \in R$ is a bihomomorphism.

2. A bihomomorphism $\sigma : R_R \times {}_R R \longrightarrow A$ is of the form $\sigma(x, y) = \varphi(xy)$ with a group homomorphism $\varphi : R \longrightarrow A$. Given σ, take $\varphi(\lambda) := \sigma(\lambda, 1)$.

3. The bihomomorphisms form an abelian group w.r.t. argumentwise addition.

4. Let I, J be sets. The bihomomorphisms

   $$\sigma : R[I]_R \times {}_R R[J] \longrightarrow A$$

   correspond to families of group homomorphisms $\varphi_{ij} : R \longrightarrow A, i \in I, j \in J$, as follows: Given σ we define

   $$\varphi_{ij} : R \longrightarrow A, \lambda \mapsto \sigma(e_i\lambda, e_j).$$

On the other hand, given a family $\varphi_{ij} : R \longrightarrow A$, we take

$$\sigma(f,g) := \sum_{i,j} \varphi_{ij}(f(i)g(j)),$$

a finite sum. Remember that f, g are finite sums

$$f = \sum_{i \in I} f(i)e_i, g = \sum_{j \in J} g(j)e_j.$$

Definition 9.3. Let M be a right R-module, N a left R-module. The tensor product of M and N is the pair $(M \otimes N, \beta)$ with the abelian group

$$M \otimes N := \mathbb{Z}[M \times N]/I(M,N),$$

where $I(M,N)$ is the subgroup ($\mathbb{Z}$-submodule) generated by three different families of generators

1. $e_{(u+\tilde{u},v)} - e_{(u,v)} - e_{(\tilde{u},v)}, u, \tilde{u} \in M, v \in N,$
2. $e_{(u\lambda,v)} - e_{(u,\lambda v)}, u \in M, v \in N, \lambda \in R,$
3. $e_{(u,v+\tilde{v})} - e_{(u,v)} - e_{(u,\tilde{v})}, u \in M, v, \tilde{v} \in N,$

and the bihomomorphism

$$\beta : M \times N \longrightarrow M \otimes N, (u,v) \mapsto u \otimes v := e_{(u,v)} + I(M,N).$$

Remark 9.4. The map $\beta : M \times N \longrightarrow M \otimes N$ in general is not surjective: Not every element in $M \otimes N$ is of the form $u \otimes v$, but these elements are generators:

$$M \otimes N = \left\{ \sum_{i=1}^{r} u_i \otimes v_i, u_1, ..., u_r \in M, v_1, ..., v_r \in N, r \in \mathbb{N} \right\}.$$

The observation that the subgroup $I(M,N)$ is the minimal subgroup $H \leq \mathbb{Z}[M \times N]$ making the composition

$$\begin{array}{ccccc} M \times N & \longrightarrow & \mathbb{Z}[M \times N] & \longrightarrow & \mathbb{Z}[M \times N]/H \\ (u,v) & \mapsto & e_{(u,v)} & & \end{array}$$

a bihomomorphism leads to a very useful description of the tensor product: It satisfies the following *universal mapping property*:

Proposition 9.5. *Assume $\sigma : M \times N \longrightarrow A$ is a bihomomorphism to the abelian group A. Then there is a unique group homomorphism $\hat{\sigma} : M \otimes N \longrightarrow A$ making the following diagram commutative:*

$$\begin{array}{ccc} & M \otimes N & \stackrel{\hat{\sigma}}{\longrightarrow} & A \\ \beta & \uparrow & \nearrow & \sigma \\ & M \times N & & \end{array}$$

Proof. Existence: The homomorphism $\mathbb{Z}[M \times N] \longrightarrow A, e_{(u,v)} \mapsto \sigma(u,v)$ annihilates $I(M,N)$ and thus factors through $M \otimes N$.
Uniqueness: The commutativity of the above triangle means nothing but

$$\hat{\sigma}(u \otimes v) = \sigma(u,v), \forall (u,v) \in M \times N,$$

and the elements $u \otimes v, u \in M, v \in N$, generate $M \otimes N$. □

In order to do explicit calculations in a tensor product, it turns out to be convenient to refer only to its universal mapping property - handling factor modules is sometimes a bit tricky. Indeed, it determines the tensor product up to an isomorphism:

Proposition 9.6. *Let $\tau : M \times N \longrightarrow T$ be a bihomomorphism satisfying the universal mapping property of Prop. 9.5. Then the homomorphism*

$$\hat{\tau} : M \otimes N \longrightarrow T, u \otimes v \mapsto \tau(u,v),$$

is the unique isomorphism making the diagram

$$\begin{array}{ccccc} & M \otimes N & \stackrel{\cong}{\longrightarrow} & T & \\ \beta & \uparrow & & \uparrow & \tau \\ & M \times N & = & M \times N & \end{array}$$

commutative.

Proof. Given a bihomomorphism $\sigma : M \times N \longrightarrow A$ denote $\tilde{\sigma} : T \longrightarrow A$ the corresponding homomorphism. Then the commutative diagram

$$\begin{array}{ccccc} M \otimes N & & \stackrel{\hat{\beta}}{\longrightarrow} & & M \otimes N \\ \| & & & & \| \\ M \otimes N & \stackrel{\hat{\tau}}{\longrightarrow} & T & \stackrel{\tilde{\beta}}{\longrightarrow} & M \otimes N \\ \uparrow & & \uparrow & & \uparrow \\ M \times N & = & M \times N & = & M \times N \end{array}$$

gives $\mathrm{id}_{M\otimes N} = \hat{\beta} = \tilde{\beta} \circ \hat{\tau}$, while

$$\begin{array}{ccccc} T & & \xrightarrow{\tilde{\tau}} & & T \\ || & & & & || \\ T & \xrightarrow{\tilde{\beta}} & M \otimes N & \xrightarrow{\hat{\tau}} & T \\ \uparrow & & \uparrow & & \uparrow \\ M \times N & = & M \times N & = & M \times N \end{array}$$

yields $\mathrm{id}_T = \tilde{\tau} = \hat{\tau} \circ \tilde{\beta}$. □

Remark 9.7. In order to check the universal mapping problem for $\tau : M \times N \longrightarrow T$, one shows the existence of a factorization, while uniqueness usually follows from the fact that the elements $\tau(u, v), u \in M, v \in N$, generate the abelian group T.

Example 9.8. 1. **Tensor product of free modules**: We have

$$R[I]_R \otimes {}_R R[J] \cong R[I \times J],$$

an isomorphism of abelian groups. (Of course $R[I \times J]$ can be regarded as a left and a right R-module - how to understand that phenomenon in a general setting we shall discuss soon.) The isomorphism is given by

$$R[I] \otimes R[J] \xrightarrow{\cong} R[I \times J], f \otimes g \mapsto f * g,$$

where

$$f * g : I \times J \longrightarrow R, (i, j) \mapsto f(i)g(j),$$

in particular

$$e_i * e_j = e_{(i,j)}.$$

Indeed the map

$$\tau : R[I] \times R[J] \longrightarrow T := R[I \times J], (f, g) \mapsto f * g$$

is a bihomomorphism satisfying the universal mapping property: If $\sigma : R[I] \times R[J] \longrightarrow A$ is a bihomomorphism with corresponding group homomorphisms $\varphi_{ij} : R \longrightarrow A$, the map

$$\hat{\sigma} : R[I \times J] \longrightarrow A$$

is defined by the finite(!) sum

$$\hat{\sigma}(h) := \sum_{i,j} \varphi_{ij}(h(i,j)).$$

Uniqueness is a consequence of the fact that the functions of the form $f * g$ generate $R[I \times J]$ as abelian group.

2. Let $a, b \in R$ with a PID R and write $R_c := R/(c)$. Then we have

$$R_a \otimes R_b \cong R_d \text{ with } d := \gcd(a,b),$$

with the map

$$(x + (a)) \otimes (y + (b)) \mapsto xy + (d).$$

For a proof we consider the bihomomorphism

$$\tau : R_a \times R_b \longrightarrow T := R_d, (x + (a), y + (b)) \mapsto xy + (d).$$

and check, that it satisfies the universal mapping property. Assume $\sigma : R_a \times R_b \longrightarrow A$ is a bihomomorphism. Then define $\hat{\sigma}(z + (d)) := \sigma(z + (a), 1 + (b))$. The main point is to show that $\hat{\sigma}$ is well defined: The map $R \longrightarrow A, z \mapsto \sigma(z + (a), 1 + (b))$ annihilates d:

$$\sigma(d + (a), 1 + (b)) = \sigma(ra + sb + (a), 1 + (b)) = \sigma(sb + (a), 1 + (b))$$

$$= \sigma((s + (a))b, 1 + (b)) = \sigma(s + (a), b(1 + (b))) = \sigma(s + (a), 0) = 0.$$

3. For $M = R_R/\mathfrak{a}$ with a right ideal $\mathfrak{a} \leq R_R$ we have

$$R_R/\mathfrak{a} \otimes N \cong N/\mathfrak{a}N,$$

where $\mathfrak{a}N \subset N$ is the additive subgroup generated by the products $av, a \in \mathfrak{a}, v \in N$. In particular

$$R \otimes N \cong N.$$

The tensor product behaves naturally with respect to module homomorphisms:

Proposition 9.9. *Denote $f : M \longrightarrow \tilde{M}$ and $g : N \longrightarrow \tilde{N}$ homomorphisms of right resp. left R-modules. Then there is a homomorphism*

$$f \otimes g : M \otimes N \longrightarrow \tilde{M} \otimes \tilde{N}$$

of abelian groups satisfying

$$(f \otimes g)(u \otimes v) = f(u) \otimes g(v).$$

Remark 9.10. For a general element $\sum_{i=1}^{r} u_i \otimes v_i \in M \otimes N$ we have

$$f \otimes g \left(\sum_{i=1}^{r} u_i \otimes v_i \right) = \sum_{i=1}^{r} f(u_i) \otimes g(v_i).$$

But a priori we can not take this as a definition, since the LHS sum representation is not unique. The problem to show that the RHS indeed does not depend on the representation of an element as a finite sum of "tensor products" is circumvented by the use of the universal mapping property – see the below easy and short proof.

Proof. We consider the diagram

$$\begin{array}{ccccc} & M \otimes N & \xrightarrow{\hat{\sigma}} & \tilde{M} \otimes \tilde{N} & \\ \beta & \uparrow & \nearrow & \uparrow & \tilde{\beta} \\ & M \times N & \xrightarrow{(f,g)} & \tilde{M} \times \tilde{N} & \end{array},$$

where the skew arrow $\sigma : M \times N \longrightarrow \tilde{M} \otimes \tilde{N}$ is

$$\sigma := \tilde{\beta} \circ (f, g)$$

and define

$$f \otimes g := \hat{\sigma}.$$

□

In certain situations the tensor product carries in a natural way not only the structure of an abelian group. For this we need bimodules:

Definition 9.11. Let S, R be rings. An (S, R)-bimodule M, abbreviated as $M = {}_S M_R$, is an abelian group together with a left and a right scalar multiplication

$$S \times M \longrightarrow M$$

and

$$M \times R \longrightarrow M,$$

such that

$$(\mu u)\lambda = \mu(u\lambda)$$

holds for all $u \in M, \mu \in S, \lambda \in R$.

Since for $M = {}_S M_R$ scalar multiplication with elements in S is by R-module homomorphisms and scalar multiplication with elements in R is by S-module homomorphisms, we obtain from Prop. 9.9 the following corollary:

Corollary 9.12. *If $M = {}_S M_R$ and $N = {}_R N_T$, then*

$$M \otimes N = {}_S(M \otimes N)_T.$$

Remark 9.13. For a commutative ring R an R-module is an (R, R)-bimodule with the given scalar multiplication. Then

$$M \otimes N = {}_R(M \otimes N)_R,$$

with the same left and right scalar multiplication. Hence it is again just an R-module. Obviously $\beta : M \times N \longrightarrow M \otimes N$ is R-bilinear. We leave it to the reader to check that $(M \otimes N, \beta)$ satisfies the universal mapping property w.r.t. R-bilinear maps to R-modules A, transforming them to R-linear maps with the same target.

Example 9.14.

1. **Tensor product of k-vector spaces**: If V, W are k-vector spaces with bases $e_i, i \in I$, and $\tilde{e}_j, j \in J$, the k-vector space $V \otimes W$ has the basis $e_i \otimes \tilde{e}_j, i \in I, j \in J$.

2. **Base change**: Consider a ring homomorphism $\varphi : R \longrightarrow S$ and a left R-module N. We have $S = {}_S S_R$ with the right scalar multiplication

   $$S \times R \longrightarrow S, (s, \lambda) \mapsto s\varphi(\lambda).$$

   Then

   $$S \otimes N = {}_S(S \otimes N)$$

is a left S-module. In the same way for $M = M_R$ and $S = {}_RS_S$ we find

$$M \otimes S = (M \otimes S)_S.$$

3. **Tensor product of R-algebras**: Let R be a commutative ring and $\varphi : R \longrightarrow A, \psi : R \longrightarrow B$ ring homomorphisms, such that the elements in $\varphi(R)$ resp. $\psi(R)$ commute with all elements in A resp. B (one says, that A resp. B is an R-algebra). Regard $A = A_R$ and $B = {}_RB$ as right resp. left R-module. Then $A \otimes B$ carries as well the structure of an R-algebra. The product satisfies

$$(a \otimes b) \cdot (x \otimes y) = (ax) \otimes (by).$$

Once again, this is not a definition: We have to make sure that there is a (unique) product on $A \otimes B$ behaving in that way. The map

$$\mu : A \times B \longrightarrow \mathrm{End}_R(A \otimes B), (a, b) \mapsto \mu_a \otimes \mu_b,$$

is R-bilinear, thus gives rise to an R-module homomorphism

$$\hat{\mu} : A \otimes B \longrightarrow \mathrm{End}_R(A \otimes B), u \mapsto \hat{\mu}_u.$$

Then

$$A \otimes B \times A \otimes B \longrightarrow A \otimes B, (u, v) \mapsto \hat{\mu}_u(v),$$

is an R-bilinear map sending $(a \otimes b, x \otimes y)$ to $(ax) \otimes (by)$. As a consequence we see that it induces on $A \otimes B$ the structure of a ring resp. an R-algebra with the homomorphism

$$R \longrightarrow A \otimes B, \lambda \mapsto \lambda(1_A \otimes 1_B).$$

10 Categories and Functors

If one considers a complicated mathematical problem it is often useful to simplify or reformulate the given situation in a "natural way". What this exactly means is encoded in the Category-Functor language described in this section.

In the below definition the word "class" denotes an "entity" which contains as elements certain mathematical "objects". In particular classes may

be quite big - for example all sets should constitute the elements of a class. That is the reason why one does not use anymore the term "set", since then we could speak about the set of all sets and would have trouble with self-contradictory constructions of the type "the set of all sets which do not contain themselves as elements". So one introduces instead the notion of a "class" extending that of a set: Classes are, similar as sets are, completely determined by their elements, but the possibilities to produce new classes from given ones are much more limited than in the case of sets.

We shall not make that precise here, but instead remain at a more or less naive point of view.

Definition 10.1. A category $\mathcal{C}$ is determined by the following data:

1. A class $\mathrm{Ob}(\mathcal{C})$, the elements $X, Y \in \mathrm{Ob}(\mathcal{C})$ being called the *objects* of the category $\mathcal{C}$,
2. A set $\mathrm{Mor}(X, Y)$ for any two objects $X, Y \in \mathrm{Ob}(\mathcal{C})$, its elements being called "morphisms from X to Y" (with the notation $f : X \longrightarrow Y$ meaning nothing but $f \in \mathrm{Mor}(X, Y)$),
3. A map
$$\mathrm{Mor}(Y, Z) \times \mathrm{Mor}(X, Y) \longrightarrow \mathrm{Mor}(X, Z), (g, f) \mapsto gf$$
for any three objects X, Y, Z,
4. A distinguished element $\mathrm{id}_X \in \mathrm{Mor}(X, X)$ for any $X \in \mathrm{Ob}(\mathcal{C})$,

being subject to the following conditions

1. For $f \in \mathrm{Mor}(X, Y)$ we have
$$\mathrm{id}_Y f = f, \ f\mathrm{id}_X = f$$
2. For $f \in \mathrm{Mor}(X, Y), g \in \mathrm{Mor}(Y, Z), h \in \mathrm{Mor}(Z, W)$ one has
$$h(gf) = (hg)f$$
3. We have
$$\mathrm{Mor}(X, Y) \cap \mathrm{Mor}(Z, W) = \emptyset$$
except if $Z = X$ and $W = Y$.

Example 10.2. 1. The category $\mathcal{SET}$: Its objects are the sets, while

$$\mathrm{Mor}(X, Y) := \{(f, Y); f \in Y^X\},$$

i.e., a morphism is a map from X to Y with the additional datum of Y as target. This is in order to make the last condition in 10.1 hold. A similar convention is understood in all the following examples, where we usually only give the first component f when describing morphisms.

2. The category $\mathcal{TOP}$:= (topological spaces, continuous maps) of topological spaces with the continuous maps as morphisms.

3. The category $\mathcal{GRO}$:= (groups, group homomorphisms), i.e. the objects are the groups and the morphisms are the group homomorphisms (with prescribed source and target).

4. The category $\mathcal{AB}$:= (abelian groups, group homomorphisms) of abelian groups and group homomorphisms between such groups as morphisms.

5. For a ring R denote R-$\mathcal{MOD}$:= (left R-modules, module homomorphisms) the category of left R-modules with the module homomorphisms as morphisms. Note that $\mathcal{AB} = \mathbb{Z}$-$\mathcal{MOD}$.

6. Denote $C_*(R\text{-}\mathcal{MOD})$ the category whose objects are (homological) R-module complexes

$$(M_*, \partial_*) := (M_n, \partial_n)_{n\in\mathbb{Z}},$$

i.e. $\mathbb{Z}$-families of R-modules M_n and R-module homomorphisms $\partial_n : M_n \longrightarrow M_{n-1}$, such that

$$\partial_{n-1} \circ \partial_n = 0.$$

The maps ∂_n are also called *boundary maps* or *differentials*, and often simply denoted ∂, the correct index $n \in \mathbb{Z}$ being understood. The morphisms

$$\varphi_* : M_* \longrightarrow \widetilde{M}_*$$

are the chain maps, i.e. families $(\varphi_n)_{n\in\mathbb{Z}}$ of R-module homomorphisms $\varphi_n : M_n \longrightarrow \widetilde{M}_n$ satisfying

$$\widetilde{\partial}_n \varphi_n = \varphi_{n-1} \partial_n$$

for all $n \in \mathbb{Z}$.

7. In order to make certain operations on complexes more natural one also considers the category $C^*(R\text{-}\mathcal{MOD})$ of cohomological complexes

$$(M^*, \partial^*) := (M^n, \partial^n)_{n\in\mathbb{Z}}$$

with R-modules M^n and R-module homomorphisms $\partial^n : M^n \longrightarrow M^{n+1}$, such that

$$\partial^{n+1} \circ \partial^n = 0.$$

Definition 10.3. Let $\mathcal{C}$ be a category, $X, Y \in \mathrm{Ob}(\mathcal{C})$. A morphism $f : X \longrightarrow Y$ is called an isomorphism, if it has a left and right inverse $g : Y \longrightarrow X$, i.e. $gf = \mathrm{id}_X$ as well as $fg = \mathrm{id}_Y$. We call the objects X, Y isomorphic, written as $X \cong Y$, if there is an isomorphism $f : X \longrightarrow Y$.

Note that if $f : X \longrightarrow Y$ has a left inverse $g : Y \longrightarrow X$ and a right inverse $h : Y \longrightarrow X$ then necessarily $g = g(fh) = (gf)h = h$.

Definition 10.4. A (covariant) functor $F : \mathcal{C} \longrightarrow \mathcal{C}'$ between the categories $\mathcal{C}, \mathcal{C}'$ is given by the following data

1. A map $F : \mathrm{Ob}(\mathcal{C}) \longrightarrow \mathrm{Ob}(\mathcal{C}'), X \mapsto F(X)$,
2. Maps $F_{X,Y} : \mathrm{Mor}(X, Y) \longrightarrow \mathrm{Mor}(F(X), F(Y))$ for all $X, Y \in \mathrm{Ob}(\mathcal{C})$ (we write simply $F(f) = F_{X,Y}(f)$, if there is no danger of confusion)

satisfying

1. F is compatible with the "composition" of morphisms $f : X \longrightarrow Y, g : Y \longrightarrow Z$, i.e.
$$F(gf) = F(g)F(f).$$
2. $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$.

In particular $X \cong Y \Longrightarrow F(X) \cong F(Y)$.

Example 10.5. 1. The "forgetful functor" $R\text{-}\mathcal{MOD} \longrightarrow \mathcal{SET}$ associates to a module its underlying set, forgetting the module operations.

2. There is the functor

$$R[\ ] : \mathcal{SET} \longrightarrow R\text{-}\mathcal{MOD}, A \mapsto R[A],\ \varphi \mapsto \varphi_*,$$

which associates to a set A the free (left or right) R-module $R[A]$ generated by it (consisting of all functions $f : A \longrightarrow R$ with finite support) and to a map $\varphi : A \longrightarrow B$ the push forward homomorphism $\varphi_* : R[A] \longrightarrow R[B]$ defined as follows

$$\varphi_*(f)(b) = \sum_{\varphi(a)=b} f(a).$$

Indeed for the basis elements $e_a, a \in A$, that means simply

$$\varphi_*(e_a) = e_{\varphi(a)}.$$

3. "Abelization" $A : \mathcal{GRO} \longrightarrow \mathcal{AB}, G \mapsto A(G) := G/C(G)$ is a functor with the obvious maps on the level of morphisms. Note that the passage $f \mapsto A(f)$ preserves surjectivity, but not injectivity, e.g. $A(\mathbb{A}_n)$ is trivial for $n \geq 5$, while $A(C_n) = C_n$. Then for odd n consider $f : C_n \longrightarrow \mathbb{A}_n, e^{2\pi i/n} \longrightarrow \sigma$, where $\sigma = (1, 2, ..., n)$.

4. Denote A a right R-module. Then

$$M \mapsto A \otimes M, \varphi \mapsto \mathrm{id}_A \otimes \varphi$$

defines a functor

$$A \otimes .. : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}.$$

In the same way, given a left R-module B, there is a functor $...\otimes B$ from the category of all right R-modules to the category of abelian groups. Furthermore, if R is commutative, we may replace $\mathcal{AB}$ with $R\text{-}\mathcal{MOD}$.

5. For a left R-module A

$$\mathrm{Hom}(A, ..) : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}, M \mapsto \mathrm{Hom}(A, M)$$

is a functor with the following action on the level of morphisms:

$$\mathrm{Hom}(A, ..) : \mathrm{Mor}(M, N) \longrightarrow \mathrm{Mor}(\mathrm{Hom}(A, M), \mathrm{Hom}(A, N)),$$

$$f \mapsto (\mathrm{Hom}(A, f) : \varphi \mapsto f \circ \varphi).$$

The passage $f \mapsto \mathrm{Hom}(A, f)$ preserves injectivity, but not surjectivity: Consider $R = \mathbb{Z}, A = \mathbb{Z}_2$ and $f : \mathbb{Z} \longrightarrow \mathbb{Z}_2, n \mapsto \overline{n}$, the quotient projection.

6. The base change functor: Let $\psi : R \longrightarrow \hat{R}$ be a ring homomorphism. Then
$$R\text{-}\mathcal{MOD} \longrightarrow \hat{R}\text{-}\mathcal{MOD}, M \mapsto \hat{R} \otimes M, \varphi \mapsto \hat{R} \otimes \varphi$$
is called the base change functor w.r.t. ψ. For the quotient map $\psi : R \longrightarrow R/\mathfrak{a}$ with a two sided ideal $\mathfrak{a}$, there is a functorial isomorphism
$$(R/\mathfrak{a}) \otimes M \cong M/\mathfrak{a}M.$$
Finally, if R is an integral domain and and $S \subset R \setminus \{0\}$ a multiplicative subset and $\psi : R \hookrightarrow S^{-1}R$ the inclusion, then the base change functor may be described as well more down to earth: There is a functorial isomorphism
$$S^{-1}R \otimes M \cong S^{-1}M.$$

7. The n-th homology functor
$$H_n : C_*(R\text{-}\mathcal{MOD}) \longrightarrow R\text{-}\mathcal{MOD}, M_* \mapsto H_n(M_*)$$
associates to a complex its n-th homology module
$$H_n(M_*) := Z_n(M_*)/B_n(M_*),$$
where
$$Z_n(M) := \ker \partial_n \ \leq M_n$$
is the submodule of "n-cycles" and
$$B_n(M) := \partial_{n+1}(M_{n+1}) \ \leq Z_n(M_*)$$
the submodule of "n-boundaries". A complex is called *acyclic*, if $H_n(M_*) = 0$ holdes for all $n \in \mathbb{Z}$.

8. The n-th cohomology (module) of a cohomological complex M^* is
$$H^n(M^*) := Z^n(M^*)/B^n(M^*),$$
where
$$Z^n(M) := \ker \partial^n \ \leq M^n$$
is the submodule of "n-cocycles" and
$$B^n(M) := \partial^{n-1}(M^{n-1}) \ \leq Z^n(M^*)$$
the submodule of "n-coboundaries".

In the above examples we have seen some "functorial isomorphisms". In technical terms one calls them "natural equivalences":

Definition 10.6. Let $F, G : \mathcal{C} \longrightarrow \mathcal{C}'$ be functors.

1. A natural transformation $\Phi : F \longrightarrow G$ from F to G is a collection

$$\Phi := (\Phi_A)_{A \in \mathrm{Ob}(\mathcal{C})}$$

of morphisms

$$\Phi_A : F(A) \longrightarrow G(A)$$

such that given any morphism $\varphi : A \longrightarrow B$, the diagram

$$\begin{array}{ccc} F(A) & \xrightarrow{\Phi_A} & G(A) \\ F(\varphi) \downarrow & & \downarrow G(\varphi) \\ F(A) & \xrightarrow{\Phi_B} & G(B) \end{array}$$

is commutative.

2. A natural equivalence between two functors is a natural transformation, such that all the morphisms $\Phi_A : F(A) \longrightarrow G(A)$ are isomorphisms.

Let us come back to the abelian group $\mathrm{Hom}(M, B)$. It depends on two variables: If we fix the first variable M we obtain the functor $B \mapsto \mathrm{Hom}(M, B)$, while $M \mapsto \mathrm{Hom}(M, B)$ is a "contravariant" functor from R-$\mathcal{MOD}$ to $\mathcal{AB}$: A module homomorphism $f : M \longrightarrow N$ induces a homomorphism in the opposite direction:

$$\mathrm{Hom}(f, B) : \mathrm{Hom}(N, B) \longrightarrow \mathrm{Hom}(M, B), \varphi \mapsto \varphi^*(f) := \varphi \circ f.$$

Definition 10.7. A (contravariant) functor $F : \mathcal{C} \longrightarrow \mathcal{C}'$ between the categories $\mathcal{C}, \mathcal{C}'$ is given by the following data

1. A map $F : \mathrm{Ob}(\mathcal{C}) \longrightarrow \mathrm{Ob}(\mathcal{C}'), X \mapsto F(X)$,

2. Maps $F_{X,Y} : \mathrm{Mor}(X, Y) \longrightarrow \mathrm{Mor}(F(Y), F(X))$ for all $X, Y \in \mathrm{Ob}(\mathcal{C})$ (we write simply $F(f) = F_{X,Y}(f)$, if there is no danger of confusion)

satisfying

1. F is compatible with the "composition" of morphisms $f : X \longrightarrow Y, g : Y \longrightarrow Z$, i.e.
$$F(gf) = F(f)F(g).$$
2. $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$.

Example 10.8. 1. There is the functor
$$\mathcal{SET} \longrightarrow R\text{-}\mathcal{MOD}, A \mapsto R^A, \varphi \mapsto \varphi^*,$$
which associates to a set A the (left or right) module of all R-valued functions on A and to a map $\varphi : A \longrightarrow B$ the pull back homomorphism
$$\varphi^* : R^B \longrightarrow R^A, f \mapsto f \circ \varphi.$$

2. For an R-module B
$$\mathrm{Hom}(.., B) : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}, M \mapsto \mathrm{Hom}(M, B)$$
is a functor with the following action on the level of morphisms:
$$\mathrm{Hom}(f, B) : \mathrm{Mor}(M, N) \longrightarrow \mathrm{Mor}(\mathrm{Hom}(B, N), \mathrm{Hom}(B, M)),$$
$$f \mapsto (\mathrm{Hom}(B, f) : \varphi \mapsto \varphi \circ f).$$
The passage $f \mapsto \mathrm{Hom}(f, B)$ transforms surjective homomorphisms into injective ones, but not necessarily injective homomorphisms into surjective ones: Consider $R = \mathbb{Z}, B = \mathbb{Z}$ and $f : \mathbb{Z} \longrightarrow \mathbb{Z}, n \mapsto 2n$.

The following class of functors is of particular importance:

Definition 10.9. A functor
$$F : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$$
is called *additive* if

1. for covariant F the maps
$$\mathrm{Hom}(L, N) \longrightarrow \mathrm{Hom}(F(L), F(N))$$
$$f \mapsto F(f)$$
are homomorphisms of abelian groups for all $L, N \in R\text{-}\mathcal{MOD}$,

2. for contravariant F the maps

$$\mathrm{Hom}(L,N) \longrightarrow \mathrm{Hom}(F(N),F(L))$$

$$f \mapsto F(f)$$

are homomorphisms of abelian groups for all $L, N \in R\text{-}\mathcal{MOD}$.

Example 10.10. 1. For $A, B \in R\text{-}\mathcal{MOD}$ the functors $\mathrm{Hom}(A,-)$ and $\mathrm{Hom}(-,B)$ are additive.

2. For a right R-module A the functor $A \otimes -$ is additive.

3. For a commutative ring R we may define the functor $R\text{-}\mathcal{MOD} \longrightarrow R\text{-}\mathcal{MOD}, M \mapsto M \otimes M, f \mapsto f \otimes f$, and obtain a non-additive functor.

4. The (restricted) functor $R[\ ] : R\text{-}\mathcal{MOD} \longrightarrow R\text{-}\mathcal{MOD}$ is not additive, since $R[f] \neq 0$ for any homomorphism f because of $R[f](e_0) = e_{f(0)} = e_0$.

Remark 10.11. For an additive functor one has $F(0) = 0$, where 0 represents the trivial R-module resp. trivial abelian group. Indeed a module M is trivial if and only if $\mathrm{id}_M = 0$ and in that case we have $\mathrm{id}_{F(M)} = F(\mathrm{id}_M) = F(0) = 0$.

Proposition 10.12. *1. Given an additive covariant functor $F : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$ we may extend it to a functor*

$$C_*(R\text{-}\mathcal{MOD}) \longrightarrow C_*(\mathcal{AB}), M_* \mapsto F(M_*),$$

where

$$F(M_*) := (F(M_n), F(\partial_n))_{n\in\mathbb{Z}}.$$

2. Given an additive contravariant functor $F : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$ we may extend it to a functor

$$C_*(R\text{-}\mathcal{MOD}) \longrightarrow C^*(\mathcal{AB}), M_* \mapsto F(M_*),$$

where

$$F(M_*) := (F(M_n), F(\partial_n))_{n\in\mathbb{Z}}.$$

Proof. We have

$$F(\partial_n) \circ F(\partial_{n+1}) = F(\partial_n \circ \partial_{n+1}) = F(0) = 0.$$

□

An additive functor need not commute with the homology functors, i.e. in general we have

$$H_n(F(M_*)) \ncong F(H_n(M_*)).$$

Only for exact functors that turns out to be true, see Prop.12.5. Here is the definition:

Definition 10.13. A covariant/contravariant additive functor $F : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$ is called

1. *left exact* if given a short exact sequence

   $$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

   the sequence

   $$0 \longrightarrow F(L) \longrightarrow F(M) \longrightarrow F(N)$$

   resp.

   $$0 \longrightarrow F(N) \longrightarrow F(M) \longrightarrow F(L)$$

   is exact,

2. *right exact* if given a short exact sequence as above the sequence

   $$F(L) \longrightarrow F(M) \longrightarrow F(N) \longrightarrow 0$$

   resp.

   $$F(N) \longrightarrow F(M) \longrightarrow F(L) \longrightarrow 0$$

   is exact. It is called *exact* if it is both left and right exact, i.e. if it transforms short exact sequences into short exact sequences.

Example 10.14. 1. For a multiplicative subset $S \subset R\backslash\{0\}$ of an integral domain R the localization functor

   $$S^{-1}(-) : R\text{-}\mathcal{MOD} \longrightarrow S^{-1}R\text{-}\mathcal{MOD}$$

   is exact.

2. The functor $\mathrm{Hom}(A,-) : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$ is left exact. It is exact if and only if with f also $\mathrm{Hom}(A,f)$ is surjective.

3. The (contravariant) functor $\mathrm{Hom}(-,A) : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$ is left exact. It is exact if and only if injective f gives surjective $\mathrm{Hom}(f,A)$.

Proposition 10.15. *Let*

$$L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

be an exact sequence of left/right R-modules, i.e. $\ker(g) = f(L)$ *and* $g(M) = N$*, and A a right/left R-module. Then the induced sequence*

$$A \otimes L \xrightarrow{\mathrm{id}_A \otimes f} A \otimes M \xrightarrow{\mathrm{id}_A \otimes g} A \otimes N \longrightarrow 0$$

resp.

$$L \otimes A \xrightarrow{f \otimes \mathrm{id}_A} M \otimes A \xrightarrow{g \otimes \mathrm{id}_a} N \otimes A \longrightarrow 0$$

is exact as well.

Proof. We consider the case of left R-modules L, M, N only. It is clear that $\tilde{g}(A \otimes M) = A \otimes N$ and that the composition of $\tilde{f} := \mathrm{id}_A \otimes f$ and $\tilde{g} := \mathrm{id}_A \otimes g$ is trivial, or, with other words, that $\tilde{f}(A \otimes L) \subset \ker(\tilde{g})$. Now let us consider the homomorphism

$$(A \otimes M)/\tilde{f}(A \otimes L) \longrightarrow A \otimes N.$$

induced by $\tilde{g}$. We construct an inverse: Consider the following bihomomorphism

$$\sigma : A \times N \longrightarrow (A \otimes M)/\tilde{f}(A \otimes L), (a,v) \mapsto a \otimes u + \tilde{f}(A \otimes L),$$

where $u \in M, g(u) = v$. It is well defined, since if $g(\tilde{u}) = v$ as well, then $\ker g = f(L)$ shows that $\tilde{u} - u = f(t)$ for some $t \in L$, hence $a \otimes \tilde{u} - a \otimes u = a \otimes f(t) \in \tilde{f}(A \otimes L)$. So there is a homomorphism

$$\hat{\sigma} : A \otimes N \longrightarrow (A \otimes M)/\tilde{f}(A \otimes L),$$

a left inverse to the map induced by $\tilde{g}$. Hence that map is injective and thus $\tilde{f}(A \otimes L) = \ker(\tilde{g})$. □

Example 10.16. The tensor product does not preserve injectivity: The map

$$\mu_2 : \mathbb{Z} \longrightarrow \mathbb{Z}$$

induces the zero map

$$0 = \mathrm{id}_{\mathbb{Z}_2} \otimes \mu_2 : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2.$$

Definition 10.17. A right/left R-module is called *flat* if the functor $A \otimes - : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$ resp. $- \otimes A : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$ is right exact or, equivalently, preserves injectivity.

Remark 10.18. There are also names for modules P resp. I, such that $\mathrm{Hom}(P, -)$ resp. $\mathrm{Hom}(-, I)$ is an exact functor: We know them already, injective and projective modules. For the proof that Def.3.17 is equivalent to the exactness of the Hom-functors we refer to the next section.

Example 10.19. Free modules, more generally projective modules are flat. Namely

$$R[I] \otimes M \cong M[I],$$

where

$$M[I] := \bigoplus_{i \in I} M_i, \text{ with } M_i = M \ \forall \ i \in I.$$

Furthermore

$$(P \oplus Q) \otimes M \cong (P \otimes M) \oplus (Q \otimes M).$$

Finally coming back to the general situation, we show, that exact functors transform exact sequences into exact sequences in general:

Proposition 10.20. *Let $F : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$ be an exact co(ntra)variant functor. If $L \longrightarrow M \longrightarrow N$ is exact, so is $F(L) \longrightarrow F(M) \longrightarrow F(N)$ resp. $F(N) \longrightarrow F(M) \longrightarrow F(L)$.*

Proof. We only consider the covariant case and leave the contravariant one to the reader. Denote $M_0 \leq M$ the image of the first arrow and $N_0 \leq N$ the image of the second one. Apply the functor F to the following diagram

$$\begin{array}{ccccccccc} & & & & & & & & N \\ & & & & & & & \nearrow & \uparrow \\ 0 & \longrightarrow & M_0 & \hookrightarrow & M & \twoheadrightarrow & N_0 & & \longrightarrow 0 \\ & & \uparrow & \nearrow & & & & & \\ & & L & & & & & & \end{array}$$

with the horizontal sequence being short exact, and obtain

$$\begin{array}{ccccccccc} & & & & & & & & F(N) \\ & & & & & & & \nearrow & \uparrow \\ 0 & \longrightarrow & F(M_0) & \hookrightarrow & F(M) & \twoheadrightarrow & F(N_0) & & \longrightarrow 0\ . \\ & & \uparrow & \nearrow & & & & & \\ & & F(L) & & & & & & \end{array}$$

Since the left vertical arrow remains surjective when applying the exact functor F and the right one injective, the exactness of the horizontal short exact sequence implies the exactness of the skew sequence at the middle position. □

11 Projective and injective modules

For the construction of complexes associated to an R-module we need some considerations about injective and projective modules:

Proposition 11.1. *1. An R-module P is projective iff, given a surjective module homomorphism $\psi : M \longrightarrow N$, for any module homomorphism $\sigma : P \longrightarrow N$ there is a homomorphism $\hat{\sigma} : P \longrightarrow M$ with $\sigma = \psi \circ \hat{\sigma}$, i.e. the following diagram*

$$\begin{array}{ccc} & \overset{\psi}{} & \\ M & \twoheadrightarrow & N \\ \hat{\sigma} & \nwarrow & \uparrow \ \sigma \\ & & P \end{array}$$

is commutative.

2. An R-module I is injective iff, given an injective module homomorphism $\varphi : L \longrightarrow M$, for any module homomorphism $\sigma : L \longrightarrow I$ there is a homomorphism $\hat{\sigma} : M \longrightarrow I$ with $\sigma = \hat{\sigma} \circ \varphi$, i.e. the following diagram

$$\begin{array}{ccc} & L & \overset{\varphi}{\hookrightarrow} \ M \\ \sigma & \downarrow & \swarrow \ \hat{\sigma} \\ & I & \end{array}$$

is commutative.

Corollary 11.2. *1. The functor* $\mathrm{Hom}(A,-) : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$ *is exact iff* A *is projective.*

2. The functor $\mathrm{Hom}(-,A) : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$ *is exact iff* A *is injective.*

Proof of Prop.11.1. "$\Longleftarrow$":

1. Let $\psi : M \longrightarrow P$ be surjective. Taking $N = P$ and $\sigma = \mathrm{id}_P$ gives the defining property of a projective module: $M_0 := \hat{\sigma}(P)$ then is a submodule complementary to $\ker(\psi)$.

2. Let $\varphi : I \longrightarrow M$ be injective. Taking $L := I$ and $\sigma = \mathrm{id}_I$ gives the defining property of an injective module: $M_0 := \ker(\hat{\sigma})$ then is a submodule complementary to $\varphi(L)$.

"$\Longrightarrow$":

1. Let $\psi : M \longrightarrow N$ be a surjective homomorphism. We define

$$M \times_N P := \{(u,p) \in M \oplus P; \psi(u) = \sigma(p)\}$$

and obtain a commutative diagram

$$\begin{array}{ccccc} & & M & \overset{\psi}{\twoheadrightarrow} & N & \\ & & \uparrow & & \uparrow & \sigma \\ C & \hookrightarrow & M \times_N P & \twoheadrightarrow & P & \end{array}$$

where the arrows emanating from the "fibred product" $M \times_N P$ are the respective projections, the horizontal one being onto. So we find a submodule $C \leq M \times_N P$, such that $C \overset{\cong}{\longrightarrow} P$ and define

$$\hat{\sigma} := \mathrm{pr}_M \circ (\mathrm{pr}_P|_C)^{-1}.$$

2. Let $\varphi : L \longrightarrow M$ be an injective homomorphism. We define

$$I \oplus_L M := (I \oplus M)/\Delta,$$

where

$$\Delta := \{(\varphi(\ell), -\sigma(\ell)); \ell \in L\}$$

as well as $\iota_1 : I \longrightarrow I \oplus_L M, i \mapsto (i,0) + \Delta$ and $\iota_2 : M \longrightarrow I \oplus_L M, u \mapsto (0,u) + \Delta$. and obtain a commutative diagram

$$\begin{array}{cccccc} & L & \stackrel{\varphi}{\hookrightarrow} & M & & \\ \sigma & \downarrow & & \downarrow & & \\ & I & \longrightarrow & I \oplus_L M & = & \iota_2(I) \oplus C \end{array}$$

where the arrows pointing to the "fibred sum" $I \oplus_L M$ are the maps ι_1 resp. ι_2, the horizontal one, ι_1, being into. So we find a submodule $C \leq I \times_L M$ complementary to $\iota_I(I)$ and define

$$\hat{\sigma} := \mathrm{pr} \circ \iota_2$$

with the projection $\mathrm{pr} : \iota_1(I) \oplus C \longrightarrow \iota_1(I) \cong I$.

□

The main result of this section is:

Theorem 11.3. *There are functors*

$$R[\ ] : R\text{-}\mathcal{MOD} \longrightarrow R\text{-}\mathcal{MOD}$$

and

$$I : R\text{-}\mathcal{MOD} \longrightarrow R\text{-}\mathcal{MOD}$$

taking free resp. injective modules as values together with a surjective resp. injective natural transformation

$$\sigma : R[\ ] \longrightarrow \mathrm{id}_{R\text{-}\mathcal{MOD}}$$

and

$$\varepsilon : \mathrm{id}_{R\text{-}\mathcal{MOD}} \longrightarrow I.$$

Proof. Let us assume that we are considering left modules. The first functor has already been defined on $\mathcal{SET}$, compose it with the forgetful functor $R\text{-}\mathcal{MOD} \longrightarrow \mathcal{SET}$, the natural transformation is given by

$$\sigma_M : R[M] \longrightarrow M, f \mapsto \sum_{u \in M} f(u)u,$$

or, equivalently $e_u \mapsto u$ holds for the elements of the basis $(e_u)_{u \in M}$. (For a right R-module we take the map $f \mapsto \sum_{u \in M} uf(u)$.)

For the second part we first of all need the contravariant exact character dual functor

$$M \mapsto M^*$$

transforming left/right modules into right/left modules together with the injective biduality natural transformation

$$\beta_M : M \longrightarrow M^{**}$$

to be explained below. Now given M take

$$I(M) := R[M^*]^*$$

with

$$\varepsilon_M = (\sigma_{M^*})^* \circ \beta_M : M \longrightarrow M^{**} \longrightarrow R[M^*]^* = I(M)$$

and $\sigma_{M^*} : R[M^*] \longrightarrow M^*$. □

Definition 11.4. The "character dual" L^* (no standard terminology!) of an abelian group L is defined as

$$L^* := \mathrm{Hom}_{\mathbb{Z}}(L, \mathbb{Q}/\mathbb{Z}).$$

Remark 11.5. If L is even a left/right R-module, it is a right/left R-module with the scalar multiplication $(\chi\lambda)(u) := \chi(\lambda u)$ resp. $(\lambda\chi)(u) := \chi(u\lambda)$. Furthermore, given $u \in L \setminus \{0\}$ we find $\chi \in L^*$ with $\chi(u) \neq 0$, namely: There is a homomorphism $\mathbb{Z}u \longrightarrow \mathbb{Q}/\mathbb{Z}, u \mapsto d^{-1} + \mathbb{Z}$, with some $d \in \mathbb{N}_{>1}$: If u has infinite order we may take any $d > 1$, otherwise $d := \mathrm{ord}(u)$. And that homomorphism extends to a "character form" $\chi : L \longrightarrow \mathbb{Q}/\mathbb{Z}$ due to the injectivity of $\mathbb{Q}/\mathbb{Z}$.

As a consequence the evaluation

$$\varepsilon_u : L^* \longrightarrow \mathbb{Q}/\mathbb{Z}, \chi \mapsto \chi(u),$$

of functionals at a given element $u \in L$ is nontrivial for $u \neq 0$. With other words: The biduality homomorphism

$$\beta_L : L \longrightarrow L^{**}, u \mapsto \varepsilon_u,$$

is an injective homomorphism of left/right R-modules.

Proposition 11.6. *For a projective (left/right) R-module P the (right/left) R-module P^* is injective.*

Proof. Given an injection

$$j : P^* \hookrightarrow M$$

the dual map

$$j^* : M^* \longrightarrow P^{**}$$

is onto, since $\mathbb{Q}/\mathbb{Z}$ is injective. Hence, P being projective, there is a map $\hat{\beta}_P$ making the diagram

$$\begin{array}{ccccc} M^* & \overset{j^*}{\twoheadrightarrow} & P^{**} & & \\ \hat{\beta}_P & \nwarrow & \uparrow & \beta_P & \\ & & P & & \end{array}$$

commutative. If we dualize it we obtain $(\hat{\beta}_P)^* \circ j^{**} = (\beta_P)^*$. Now we shall show that the map

$$\pi := (\hat{\beta}_P)^* \circ \beta_M : M \longrightarrow M^{**} \longrightarrow P^*$$

satisfies

$$\pi \circ j = \mathrm{id}_{P^*},$$

hence $M_0 := \ker(\pi)$ is a complementary submodule for $j(P^*)$. In order to see that we consider the commutative diagram

$$\begin{array}{ccccc} & P^* & \overset{j}{\longrightarrow} & M & \\ \beta_{P^*} & \downarrow & & \downarrow & \beta_M \\ & P^{***} & \overset{j^{**}}{\longrightarrow} & M^{**} & \\ (\beta_P)^* & \downarrow & & \downarrow & (\hat{\beta}_P)^* \\ & P^* & \overset{\mathrm{id}}{\longrightarrow} & P^* & \end{array} .$$

The upper square is commutative since β is a natural transformation, the commutativity of the lower one we have already seen above. Finally use the following lemma:

Lemma 11.7. *For any module P we have*

$$\mathrm{id}_{P^*} = (\beta_P)^* \circ \beta_{P^*} : P^* \overset{\beta_{P^*}}{\longrightarrow} P^{***} \overset{(\beta_P)^*}{\longrightarrow} P^*.$$

Proof. Take some $\varphi \in P^*$, i.e. a homomorphism $\varphi : P \longrightarrow \mathbb{Q}/\mathbb{Z}$. It is first mapped to $\varepsilon_\varphi \in (P^*)^{**}$, then we have to compose it with β_P and to show that it is just φ. In order to see that we evaluate at sume $u \in P$ and obtain

$$(\varepsilon_\varphi \circ \beta_P)(u) = \varepsilon_\varphi(\beta_P(u)) = \varepsilon_\varphi(\varepsilon_u) = \varepsilon_u(\varphi) = \varphi(u).$$

□

□

12 Construction of Complexes

In this section we construct functors

$$\mathcal{TOP}, R\text{-}\mathcal{MOD} \longrightarrow C_*(R\text{-}\mathcal{MOD}).$$

They associate with a topological space or an R-module a complex, which itself is a quite big and unwieldy object, but the compositions with the homology functors

$$H_n : C_*(R\text{-}\mathcal{MOD}) \longrightarrow R\text{-}\mathcal{MOD}$$

lead to interesting information about the original objects.

12.1 Singular homology groups

Here we construct a functor

$$C_* : \mathcal{TOP} \longrightarrow C_*(R\text{-}\mathcal{MOD}), X \mapsto C_*(X) := C_*(X, R),$$

which associates to a topological space its "singular chain complex with coefficients in the ring R".

Definition 12.1. Let X be a topological space.

1. The standard n-simplex $\Delta_n \subset \mathbb{R}^{n+1}$ is defined as the convex hull of the standard base vectors $e_0, ..., e_n \in \mathbb{R}^{n+1}$, i.e. the set

$$\Delta_n := \left\{(t_0, ..., t_n) \in \mathbb{R}^{n+1}; t_i \geq 0, t_0 + ... + t_n = 1\right\}.$$

2. A singular n-simplex σ in a topological space X is a continuous map

$$\sigma : \Delta_n \longrightarrow X.$$

We denote

$$S_n(X) := \{\sigma : \Delta_n \longrightarrow X \text{ continuous}\}$$

the set of all singular n-simplices in X (in particular $S_0(X) = X$).

3. The n-**th singular chain module** of X, $n \geq 0$, with coefficients in R, is the free R-module with basis $S_n(X)$, i.e.

$$C_n(X) := C_n(X;R) := R\left[S_n(X)\right]$$

$$= \left\{ \sum_{\sigma \in S_n(X)} \lambda_\sigma e_\sigma ; \lambda_\sigma \in R \text{ and } = 0 \text{ for almost all } \sigma \in S_n(X) \right\}$$

$$= \left\{ \sum_{i=1}^{r} \lambda_i \sigma_i ; \lambda_i \in R, \sigma_i \in S_n(X) \right\},$$

replacing, for convenience of notation, e_σ with σ. Furthermore

$$C_n(X) := 0, \ n < 0.$$

The boundary homomorphism: Now let us describe the boundary homomorphisms

$$\partial_n : C_n(X) \longrightarrow C_{n-1}(X), \ n > 0.$$

Necessarily $\partial_n = 0$ for $n \leq 0$. There are natural embeddings

$$\varepsilon_i^n : \Delta_{n-1} \longrightarrow \Delta_n, (t_0, ..., t_{n-1}) \mapsto (t_0, ..., t_{i-1}, 0, t_i, ..., t_{n-1})$$

of Δ_{n-1} as the facet opposite to the vertex $e_i \in \Delta_n$. Now, for a singular n-simplex σ we set

$$\partial_n \sigma := \sum_{i=0}^{n} (-1)^i \sigma \circ \varepsilon_i^n \in C_{n-1}(X)$$

and extend by linearity to $C_n(X)$. To see that $\partial_{n-1}\partial_n = 0$ we may assume $n \geq 2$ and consider for $0 \leq k < \ell \leq n$ the maps

$$\varepsilon_{k\ell} : \Delta_{n-2} \longrightarrow \Delta_n,$$

$$(t_0, ..., t_{n-2}) \mapsto (t_0, ..., t_{k-1}, 0, t_k, ..., t_{\ell-2}, 0, t_{\ell-1}, ..., t_{n-2})$$

and remark

$$\varepsilon_i^n \circ \varepsilon_j^{n-1} = \begin{cases} \varepsilon_{i,j+1} & , \text{ if } i \leq j \\ \varepsilon_{ji} & , \text{ if } j < i \end{cases}.$$

So

$$\partial_{n-1}\partial_n\sigma = \sum_{i=0}^{n}(-1)^i\partial_{n-1}(\sigma\circ\varepsilon_i^n) = \sum_{i=0}^{n}\sum_{j=0}^{n-1}(-1)^{i+j}\sigma\circ\varepsilon_i^n\circ\varepsilon_j^{n-1}$$
$$= \sum_{0\le k<\ell\le n}((-1)^{k+\ell-1}+(-1)^{k+\ell})\sigma\circ\varepsilon_{k\ell} = 0\ .$$

Thus we obtain the singular chain complex

$$C_*(X) := (C_n(X), \partial_n)_{n\in\mathbb{Z}}$$

of the topological space X. Its n-th homology module

$$H_n(X) := H_n(X; R) := H_n(C_*(X))$$

is called the n-th (singular) homology module with coefficients in R (or homology group, if $R = \mathbb{Z}$) of the topological space X.

Note that a continuous map $f : X \longrightarrow Y$ induces a chain map

$$C_*(f) : C_*(X) \longrightarrow C_*(Y),$$

where

$$C_n(f) : C_n(X) \longrightarrow C_n(Y)$$

is the linear extension of

$$S_n(X) \longrightarrow S_n(Y), \sigma \mapsto f\circ\sigma,$$

and thus a homomorphism

$$f_n : H_n(X) \longrightarrow H_n(Y).$$

12.2 Derived Functors

Here we construct two functors

$$P_* : R\text{-}\mathcal{MOD} \longrightarrow C_*(R\text{-}\mathcal{MOD})$$

and

$$I^* : R\text{-}\mathcal{MOD} \longrightarrow C^*(R\text{-}\mathcal{MOD}),$$

which associate to an R-module its natural free resp. injective resolution $P_*(M)$ resp. $I^*(M)$.

To begin with we define in general what we mean by a projective or free resolution: First of all we may regard modules as complexes concentrated in degree 0: The functor

$$\Delta_* : R\text{-}\mathcal{MOD} \longrightarrow C_*(R\text{-}\mathcal{MOD}), L \mapsto \Delta_*(L),$$

where $\Delta_*(L)$ denotes the complex with

$$\Delta_n(L) = \begin{cases} L & , \text{ if } n = 0 \\ 0 & , \text{ if } n \neq 0 \end{cases}$$

(and, necessarily, trivial differential) identifies $R\text{-}\mathcal{MOD}$ with a subcategory of $C_*(R\text{-}\mathcal{MOD})$. It has as a left inverse the zeroth homology functor

$$H_0 : C_*(R\text{-}\mathcal{MOD}) \longrightarrow R\text{-}\mathcal{MOD}, M_* \mapsto H_0(M_*).$$

In this section we want to "approximate" in a functorial way the complex $\Delta_*(L)$ by the complex $P_*(L)$, whose chain modules $P_n(L)$ are "nice". Here "nice" could mean either free or projective, while an "approximation" of $\Delta_*(L)$ is any complex admitting a "quasi-isomorphism" to $\Delta_*(L)$.

Definition 12.2. 1. A complex M_* is called *acyclic*, if it has trivial homology modules: $H_n(M_*) = 0$ for all $n \in \mathbb{Z}$.

2. A morphism of complexes $\varphi_* : M_* \longrightarrow N_*$ is called a *quasi-isomorphism* if all the homology maps $H_n(\varphi_*) : H_n(M_*) \longrightarrow H_n(N_*)$ are isomorphisms.

3. A projective/free resolution of a module L is a quasi-isomorphism

$$\varepsilon_* : Q_* \longrightarrow \Delta_*(L),$$

where the complex Q_* consists of projective/free R-modules $Q_n, n \in \mathbb{N}$, and, furthermore, $Q_n = 0$ for $n < 0$.

Remark 12.3. 1. For a resolution Q_* of a module L we have

$$H_n(Q_*) = \begin{cases} L & , \text{ if } n = 0 \\ 0 & , \text{ if } n \neq 0 \end{cases} .$$

2. If one wants to avoid the use of the complex $\Delta_*(L)$ and quasi-isomorphisms, we might say as well that the data determining a projective/free resolution of a module L are the complex Q_* together with a homomorphism $\varepsilon : Q_0 \longrightarrow L$, such that the augmented complex

$$... \longrightarrow Q_1 \longrightarrow Q_0 \xrightarrow{\varepsilon} L \longrightarrow 0 \longrightarrow ....$$

is acyclic.

3. Since $H_0(Q_*) \cong L$ for a resolution Q_* of L, the complex Q_* contains all the information about L. So resolving a module means replacing it in the bigger category $C_*(R\text{-}\mathcal{MOD}) \supset R\text{-}\mathcal{MOD}$ by an in certain respects more well behaved object.

Example 12.4. For an integral domain R let $L := R/(a)$, where $a \in R\backslash\{0\}$. Then as a free resolution Q_* of L we can take the complex

$$... \longrightarrow 0 \longrightarrow Q_1 = R \xrightarrow{\mu_a} R = Q_0 \longrightarrow 0 \longrightarrow .....$$

with the multiplication map $\mu_a(x) = ax$ as differential ∂_1. And $\varepsilon_* = (\varepsilon_n)_{n\in\mathbb{Z}} : Q_* \longrightarrow \Delta_*(L)$ is composed of the quotient map $\varepsilon_0 : Q_0 = R \longrightarrow R/(a) = L$ and $\varepsilon_n = 0$ for $n \neq 0$.

Let us now construct the functor

$$P_* : R\text{-}\mathcal{MOD} \longrightarrow C_*(R\text{-}\mathcal{MOD}), L \mapsto P_*(L),$$

together with a natural transformation

$$\varepsilon_* : P_* \longrightarrow \Delta_*,$$

such that for every R-module L the chain map $\varepsilon_*(L) : P_*(L) \longrightarrow \Delta_*(L)$ provides a free resolution of L.

While for $n < 0$ we take $P_n(L) = \{0\}$ and thus necessarily $\partial_n = 0$, the construction of the $P_n(L), n \geq 0$, is by induction. We now take

$$P_0(L) := R[L], \partial_0 = 0, \varepsilon_0 := \sigma_L.$$

Assume now everything has been defined up to degree $n \geq 0$. With

$$K_n(L) := \begin{cases} \ker(\varepsilon_0) & , \text{ if } n = 0 \\ \ker(\partial_n) & , \text{ if } n > 0 \end{cases}$$

let

$$P_{n+1}(L) := R[K_n(L)]$$

and the boundary homomorphism is

$$\partial_{n+1} = \iota \circ \sigma : R[K_n(L)] \xrightarrow{\sigma} K_n(L) \overset{\iota}{\hookrightarrow} P_n(L),$$

where $\sigma := \sigma_{K_n(L)}$ and ι is the inclusion. We leave it to the reader to define, given a homomorphism $f : L \longrightarrow N$, the corresponding chain map $P_*(f) : P_*(L) \longrightarrow P_*(N)$.

Now let us pass to injective resolutions. The definition is analogous to that of a projective resolution, with all arrows reversed. Here we describe briefly the construction of the functor

$$I^* : R\text{-}\mathcal{MOD} \longrightarrow C^*(R\text{-}\mathcal{MOD}), L \mapsto I^*(L),$$

such that

1. the chain modules $I^n(L), n \in \mathbb{Z}$, are injective R-modules, $I^n(L) = 0$ for $n < 0$, and

2. there is a natural transformation

   $$\varepsilon^* : \Delta^* \longrightarrow I^*,$$

   where the functor $\Delta^* : R\text{-}\mathcal{MOD} \longrightarrow C^*(R\text{-}\mathcal{MOD})$ is defined in analogy to Δ_*, inducing a quasi-isomorphism

   $$\varepsilon^*(L) : \Delta^*(L) \longrightarrow I^*(L)$$

   for all R-modules L.

Taking $I^n(L) := 0$ for $n < 0$ and $I^0(L) := I(L)$, we define $I^n(L)$ and $\partial^n : I^n(L) \longrightarrow I^{n+1}(L)$ by induction on $n \in \mathbb{N}$. Assume $I^q(L)$ and ∂^{q-1} have been defined for $q \leq n$. Define

$$I^{n+1}(L) := \begin{cases} I(I(L)/\iota(L)) & , \text{ if } n = 0 \\ I(I^n(L)/\partial^{n-1}(I^{n-1}(L))) & , \text{ if } n > 0 \end{cases} .$$

with

$$\partial^0 := \iota \circ \varrho : I(L) \xrightarrow{\varrho} I(L)/\iota(L)) \xrightarrow{\iota} I^1(L)$$

and

$$\partial^n := \iota \circ \varrho : I^n(L) \xrightarrow{\varrho} I^n(L)/\partial^{n-1}(I^{n-1}(L)) \xrightarrow{\iota} I^{n+1}(L)$$

for $n > 1$.

In order to get complexes with interesting (co)homology one applies additive functors $F : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$ to resolutions. For exact functors we don't obtain something really new:

Proposition 12.5. *Let $F : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$ be an exact co(ntra)variant functor.*

1. *For covariant F there is a natural equivalence*

$$F \circ H_n \xrightarrow{\cong} H_n \circ F,$$

in particular

$$F(H_n(M_*)) \cong H_n(F(M_*)).$$

2. *For contravariant F we have*

$$F \circ H_n \xrightarrow{\cong} H^n \circ F,$$

in particular

$$F(H_n(M_*)) \cong H^n(F(M_*)).$$

Proof. We consider the covariant case and leave the contravariant one to the reader. Let $B_n := B_n(M_*), Z_n := Z_n(M_*), H_n := H_n(M_*)$. The sequence

$$M_{n+1} \twoheadrightarrow B_n \hookrightarrow M_n$$

is transformed into

$$F(M_{n+1}) \twoheadrightarrow F(B_n) \hookrightarrow F)M_n),$$

whence we obtain a natural isomorphism

$$F(B_n) \xrightarrow{\cong} B_n(F(M_*)).$$

On the other hand, the exact sequence

$$Z_n \hookrightarrow M_n \longrightarrow M_{n-1}$$

is transformed into the exact sequence

$$F(Z_n) \hookrightarrow F(M_n) \longrightarrow F(M_{n-1}),$$

whence we obtain a natural isomorphism

$$F(Z_n) \xrightarrow{\cong} Z_n(F(M_*)).$$

So we have established the upper two horizontal isomorphisms in the diagram

$$\begin{array}{ccc} 0 & & 0 \\ \downarrow & & \downarrow \\ F(B_n) & \xrightarrow{\cong} & B_n(F(M_*)) \\ \downarrow & & \downarrow \\ F(Z_n) & \xrightarrow{\cong} & Z_n(F(M_*)) \\ \downarrow & & \downarrow \\ F(H_n) & \xrightarrow{\cong} & H_n(F(M_*)) \\ \downarrow & & \downarrow \\ 0 & & 0 \end{array},$$

they induce the lower horizontal isomorphism on the homology level. □

Definition 12.6. 1. For a covariant additive functor $F : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$, the functor

$$L_nF := H_n \circ F \circ P_* : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$$

is called the n-th left derived functor of F.

2. For a contravariant additive functor $F : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$ the functor

$$R^nF := H^n \circ F \circ P_* : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$$

is called the n-th right derived functor of F.

3. For a covariant additive functor $F : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$ the functor

$$R^nF := H^n \circ F \circ I^* : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$$

is called the n-th right derived functor of F.

Remark 12.7. 1. If F is an exact covariant functor we have

$$L_nF(M) = 0,\ n > 0.$$

2. If F is an exact contravariant functor we have

$$R^nF(M) = 0,\ n > 0.$$

3. For a right exact covariant functor F there is a natural equivalence

$$L_0F \xrightarrow{\cong} F.$$

Indeed, the exact sequence

$$0 \longrightarrow Z_0(P_*(M)) \hookrightarrow P_0(M) \xrightarrow{\varepsilon} M \longrightarrow 0$$

yields the exact sequence

$$F(Z_0(P_*(M))) \longrightarrow F(P_0(M)) \xrightarrow{F(\varepsilon)} F(M) \longrightarrow 0.$$

Since the right exact functor F preserves surjectivity, we may replace the first term by $F(P_1(M))$ and obtain the exact sequence

$$F(P_1(M)) \xrightarrow{F(\partial_1)} F(P_0(M)) \xrightarrow{F(\varepsilon)} F(M) \longrightarrow 0,$$

inducing a natural isomorphism

$$L_0F(M) = \mathrm{coker}F(\partial_1) \cong F(M).$$

4. For a left exact contravariant functor F there is a natural equivalence

$$F \xrightarrow{\cong} R^0F.$$

The proof is anologous to that in the previous point.

5. Finally, for a left exact covariant functor F there is a natural equivalence

$$F \xrightarrow{\cong} R^0F.$$

Definition 12.8. 1. Fix a right R-module A and the functor $F(M) = A \otimes_R M$. Then we define

$$\mathrm{Tor}_n^R(A, M) := L_n F(M) = H_n(A \otimes P_*(M)).$$

2. Fix a left R-module B and consider the functor $F(M) = \mathrm{Hom}_R(M, B)$. Then we define

$$\mathrm{Ext}_R^n(M, B) := R^n F(M) = H^n(\mathrm{Hom}(P_*(M), B)).$$

Remark 12.9. 1. We have

$$\mathrm{Tor}_0^R(A, M) \cong A \otimes M$$

and

$$\mathrm{Ext}_R^0(M, B) \cong \mathrm{Hom}(M, B)).$$

2. Note that we can as well fix the second factor M and regard the functor $G(A) := A \otimes_R M$ (replacing left with right R-modules etc.). Then there is a natural isomorphism

$$L_n G(A) = H_n(P_*(A) \otimes M) \cong H_n(A \otimes P_*(M)) = \mathrm{Tor}_n^R(A, M).$$

For the proof we refer to Th.13.21.

3. Fix a left R-module M and consider the functor $G(B) = \mathrm{Hom}_R(M, B)$. Then there is a natural isomorphism

$$R^n G(B) = H^n(\mathrm{Hom}(M, I^*(B)) \cong H^n(P_*(M), B) = \mathrm{Ext}_R^n(M, B).$$

For the proof we refer to Th.13.21.

13 Computation of Homology

13.1 Comparing projective resolutions

The complex $P_*(L)$ is by far too big in order to be useful in computations. Indeed given a specific module L, we may replace $P_*(L)$ with a considerably smaller complex as in Example.13.1, since then we may adapt our construction to L, do not have to fulfill the naturality condition. A similar reasoning applies to injective resolutions; the necessary modifications, as for example arrows to be reversed, are left to the reader. The central result of this section is the following:

Theorem 13.1. *Let $P_* \longrightarrow \Delta_*(L)$ and $Q_* \longrightarrow \Delta_*(L)$ be projective resolutions of the R-module L. Then there is a chain map $\varphi_* : P_* \longrightarrow Q_*$, such that the triangle*

$$\begin{array}{ccc} P_* & \xrightarrow{\varphi_*} & Q_* \\ & \searrow \quad \swarrow & \\ & \Delta_*(L) & \end{array}$$

is commutative. Furthermore for any additive functor $F : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$, the induced chain map

$$F(\varphi_*) : F(P_*) \longrightarrow F(Q_*)$$

is a quasi-isomorphism, and the isomorphisms

$$H_n(F(\varphi_*)) : H_n(F(P_*)) \xrightarrow{\cong} H_n(F(Q_*))$$

are independent from the chain map fitting into the above commutative diagram.

Thus, in order to compute the value $L_nF(N)$ of a derived functor L_nF at some module N and to handle its elements we may use any projective resolution of the R-module N.

Example 13.2. The general construction of a projective resolution is similar to that one of $P_*(L)$, only that one may be more economic and less redundant: Set $Q_0 := R[B]$, where $B \subset L$ is a system of generators, and define $Q_{n+1} = R[B_n]$ with a system of generators B_n of $K_n := \ker(\partial_n) \leq Q_n$.

Let us now investigate how far we are from functoriality when working with arbitrary projective resolutions. Given a projective resolution $\varepsilon_* : P_* \longrightarrow \Delta_*(L)$, we shall treat the isomorphism

$$H_0(\varepsilon_*) : H_0(P_*) \xrightarrow{\cong} H_0(\Delta_*(L)) \cong L$$

as an identification.

Definition 13.3. Let $P_* \longrightarrow \Delta_*(L)$ and $Q_* \longrightarrow \Delta_*(N)$ be projective resolutions of the modules L, N. A complex homomorphism $\varphi_* : P_* \longrightarrow Q_*$ is

said to cover a homomorphism $f : L \longrightarrow N$, if $H_0(\varphi_*) = f$ or, equivalently, if the diagram

$$\begin{array}{ccc} P_* & \xrightarrow{\varphi_*} & Q_* \\ \downarrow & & \downarrow \\ \Delta_*(L) & \xrightarrow{\Delta_*(f)} & \Delta_*(N) \end{array}$$

commutes.

Lemma 13.4. *Given projective resolutions P_*, Q_* of the modules L, N and a homomorphism $f : L \longrightarrow N$, there is a complex homomorphism $\varphi_* : P_* \longrightarrow Q_*$ covering f.*

Proof. Exercise, alternatively Grillet. □

Example 13.5. The complex homomorphism $\varphi_* := P_*(f) : P_*(L) \longrightarrow P_*(N)$ is a covering homomorphism of $f : L \longrightarrow N$.

In order to compare different covering homomorphisms we need the following notion:

Definition 13.6. Two chain maps $\varphi_*, \widetilde{\varphi}_* : P_* \longrightarrow Q_*$ between complexes P_*, Q_* of R-modules are called "(chain) homotopic", written as $\varphi_* \backsimeq \widetilde{\varphi}_*$, if and only if there is a "chain homotopy" between φ_* and $\widetilde{\varphi}_*$, i.e. a family of R-module homomorphisms $(\kappa_n : P_n \longrightarrow Q_{n+1})_{n\in\mathbb{Z}}$ satisfying

$$\varphi_n - \widetilde{\varphi}_n = \partial_{n+1}\kappa_n + \kappa_{n-1}\partial_n$$

for all $n \in \mathbb{Z}$ (where we use the same letter to denote the differential in P_* and in Q_*!).

Remark 13.7. 1. Homotopic complex homomorphisms φ_* and $\widetilde{\varphi}_*$ induce the same homomorphisms in homology:

$$H_n(\varphi_*) = H_n(\widetilde{\varphi}_*).$$

2. Homotopy is an equivalence relation.

3. Composition can be defined on the level of homotopy classes of complex homomorphisms. As a consequence we can define a new category, the *homotopy category* $\mathcal{K}(R\text{-}\mathcal{MOD})$: Its objects are the complexes of R-modules, while the morphisms are the homotopy classes of complex homomorphisms: We denote $[\varphi_*]$ the homotopy class of a complex homomorphism φ_*.

4. The natural extension $F : C_*(R\text{-}\mathcal{MOD}) \longrightarrow C_*(\mathcal{AB})$ of an additive functor $F : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$ preserves homotopy:

$$\varphi_* \backsimeq \widetilde{\varphi}_* \Longrightarrow F(\varphi_*) \backsimeq F(\widetilde{\varphi}_*).$$

So the above extended functor $F : C_*(R\text{-}\mathcal{MOD}) \longrightarrow C_*(\mathcal{AB})$ "descends" to a functor $F : \mathcal{K}(R\text{-}\mathcal{MOD}) \longrightarrow \mathcal{K}(\mathcal{AB})$. Furthermore there are homology functors $H_n : \mathcal{K}(R\text{-}\mathcal{MOD}) \longrightarrow R\text{-}\mathcal{MOD}$ resp. $H_n : \mathcal{K}(\mathcal{AB}) \longrightarrow \mathcal{AB}$.

Lemma 13.8. *Given projective resolutions P_*, Q_* of the modules L, N, any two coverings $\varphi_*, \widetilde{\varphi}_* : P_* \longrightarrow Q_*$ of a homomorphism $f : L \longrightarrow N$ are chain homotopic:*

$$\varphi_* \backsimeq \widetilde{\varphi}_*.$$

Furthermore $[\varphi_*]$ is an isomorphism iff f is.

Proof. The construction of the homomorphisms $\kappa_n : P_n \longrightarrow Q_{n+1}$ is by induction: .....

For the second part note first of all that any covering $\varphi_* : P_* \longrightarrow P_*$ of id_L is homotopic to id_{P_*}, the latter being itself a covering homomorphism.

Now consider a covering homomorphism of an isomorphism: It determines an isomorphism in the category $\mathcal{K}(R\text{-}\mathcal{MOD})$: Given an isomorphism $f : L \longrightarrow N$ and covering homomorphisms φ_*, ψ_* of f, f^{-1}, the compositions $\psi_* \circ \varphi_*$ and $\varphi_* \circ \psi_*$ are coverings of id_L resp. id_N; hence

$$\psi_* \circ \varphi_* \backsimeq \mathrm{id}_{P_*}, \varphi_* \circ \psi_* \backsimeq \mathrm{id}_{Q_*}.$$

□

Proof of Th.13.1. The first part is Lemma 13.4. Furthermore

$$H_n(F(\varphi_*)) = H_n(F([\varphi_*])),$$

where $[\varphi_*]$ is a uniquely determined isomorphism in $\mathcal{K}(\mathcal{AB})$, the complex homomorphism $\varphi_* : P_* \longrightarrow Q_*$ being a cover of id_L. □

Corollary 13.9. *Consider the left (resp. right) derived functors L_nF (resp.R^nF) of a given co(ntra)variant additive functor $F : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$. Denote $Q_* \longrightarrow \Delta_*(M)$ a projective resolution of M. Then there are canonical isomorphisms*

$$L_nF(M) \cong H_n(F(Q_*))$$

and

$$R^nF(M) \cong H^n(F(Q_*)).$$

Remark 13.10. If Q_* is a free resolution of the left R-module M, say with finitely generated chain modules $Q_i \cong R^{n_i}$, we may explicitly describe the complexes $A \otimes Q_*$ and $\mathrm{Hom}(Q_*, B)$ using the fact that

$$A \otimes R^n \cong A^n, \mathrm{Hom}(R^n, B) \cong B^n.$$

Consider the free resolution

$$... \longrightarrow R^{n_2} \longrightarrow R^{n_1} \longrightarrow R^{n_0} \longrightarrow M$$

writing the elements in R^n as row vectors and the differential as

$$R^{n_i} \longrightarrow R^{n_{i-1}}, u \mapsto uD_i$$

with a matrix $D_i \in R^{n_i, n_{i-1}}$. Tensorizing with the right R-module A yields the complex

$$... \longrightarrow A^{n_2} \longrightarrow A^{n_1} \longrightarrow A^{n_0} \longrightarrow 0 \longrightarrow ....,$$

where the differential is nothing but

$$A^{n_i} \longrightarrow A^{n_{i-1}}, u \mapsto uD_i.$$

Applying the functor $\mathrm{Hom}(.., B)$ with a left R-module B leads to the cohomological complex

$$... \longleftarrow B^{n_2} \longleftarrow B^{n_1} \longleftarrow B^{n_0} \longleftarrow 0 \longleftarrow ....,$$

with the differential

$$B^{n_i} \longrightarrow B^{n_{i+1}}, v \mapsto D_{i+1}v,$$

acting now on column(!) vectors. Note that the differentials here are homomorphisms of abelian groups, not necessarily of right resp. left R-modules!

Example 13.11. We consider an integral domain R and $M := R/(c)$ for $c \in R \setminus \{0\}$..

1. Let us consider the resolution

$$... \longrightarrow 0 \longrightarrow R \xrightarrow{D_1} R \longrightarrow M = R/(a) \longrightarrow 0 \longrightarrow .....$$

of M with $D_1 = (c)$.

2. The complex $A \otimes Q_*$ now looks as follows

$$... \longrightarrow 0 \longrightarrow A \xrightarrow{D_1} A \longrightarrow 0 \longrightarrow .....$$

yielding

$$\mathrm{Tor}_n(A, M) \cong H_n(A \otimes Q_*) = \begin{cases} A/cA & , \text{ if } n = 0 \\ T_c(A) & , \text{ if } n = 1 \\ 0 & , \text{ otherwise} \end{cases}$$

with the c-torsion $T_c(A) := \{u \in A; cu = 0\}$.

3. Applying $\mathrm{Hom}(.., B)$ yields

$$... \longleftarrow 0 \longleftarrow B \xleftarrow{D_1} B \longleftarrow 0 \longleftarrow .....$$

and thus

$$\mathrm{Ext}^n(M, B) \cong H^n(\mathrm{Hom}(Q_*, B)) = \begin{cases} T_c(B) & , \text{ if } n = 0 \\ B/cB & , \text{ if } n = 1 \\ 0 & , \text{ otherwise} \end{cases} .$$

13.2 Long exact homology sequence

Definition 13.12. A short exact sequence of complexes

$$0 \longrightarrow A_* \xrightarrow{\varphi_*} B_* \xrightarrow{\psi_*} C_* \longrightarrow 0$$

consists of complex homomorphisms φ_*, ψ_*, such that all sequences

$$0 \longrightarrow A_n \xrightarrow{\varphi_n} B_n \xrightarrow{\psi_n} C_n \longrightarrow 0$$

are exact.

Remark 13.13. Often we treat φ_* as the inclusion of a subcomplex $A_* \leq B_*$.

Proposition 13.14. *For a short exact sequence*

$$0 \longrightarrow A_* \xrightarrow{\varphi_*} B_* \xrightarrow{\psi_*} C_* \longrightarrow 0$$

of complexes all the sequences

$$H_n(A_*) \xrightarrow{H_n(\varphi_*)} H_n(B_*) \xrightarrow{H_n(\psi_*)} H_n(C_*)$$

are exact.

Proof. We have $H_n(\psi_*) \circ H_n(\varphi_*) = H_n(\psi_* \circ \varphi_*) = H_n(0) = 0$. Now assume $H_n(\psi_*)([b]) = 0$ holds for a homology class $[b] \in H_n(B_*)$, i.e. $b \mapsto c = \partial\tilde{c}$ with some $\tilde{c} \in C_{n+1}$; choose $B_{n+1} \ni \tilde{b} \mapsto \tilde{c}$. Now $b - \partial\tilde{b} \mapsto 0$, so $a := b - \partial\tilde{b} \in Z_n(A_*)$. With other words $H_n(\varphi_*)([a]) = [b]$.

$$\begin{array}{ccccc} & & B_{n+1} & \twoheadrightarrow & C_{n+1} \\ & & \downarrow & & \downarrow \\ A_n & \hookrightarrow & B_n & \twoheadrightarrow & C_n \\ \downarrow & & \downarrow & & \\ A_{n-1} & \hookrightarrow & B_{n-1} & & \end{array}$$

□

The homomorphism $H_n(\varphi_*)$ is in general not injective nor needs $H_n(\psi_*)$ to be surjective. But we can concatenate the above "truncated" short exact sequences by linking them together with a "connecting homomorphism":

Definition 13.15. Given a short exact sequence

$$0 \longrightarrow A_* \xrightarrow{\varphi_*} B_* \xrightarrow{\psi_*} C_* \longrightarrow 0,$$

of complexes the "connecting homomorphism"

$$\delta_n : H_n(C_*) \longrightarrow H_{n-1}(A_*)$$

is defined by

$$\delta_n(c + B_n(C_*)) := a + B_{n-1}(A_*),$$

where

$$\varphi_{n-1}(a) = \partial b \text{ with any } b \in B_n, \psi_n(b) = c.$$

Remark 13.16. The connecting homomorphism δ_n is well defined: First of all, using $A_{n-1} \leq B_{n-1}$, we have $\partial a = \partial\partial b = 0$. Assume now $[c_1] = [c_2]$, i.e. $c_2 - c_1 = \partial\tilde{c}$ with some $\tilde{c} \in C_{n+1}$.. Let $B_{n+1} \ni \tilde{b} \mapsto \tilde{c}$, furthermore $B_n \ni b_i \mapsto c_i$. Then $b_2 - b_1 - \partial\tilde{b} \mapsto 0 \in C_n$, hence $b_2 - b_1 - \partial\tilde{b} = a \in A_n \subset B_n$, whence $\partial b_1 - \partial b_2 = \partial a \in B_n(A_*)$, i.e. $[\partial b_1] = [\partial b_2] \in H_n(A_*)$.

Theorem 13.17. *Let*

$$0 \longrightarrow A_* \xrightarrow{\varphi_*} B_* \xrightarrow{\psi_*} C_* \longrightarrow 0,$$

be a short exact sequence of complexes. Then

$$... \longrightarrow H_{n+1}(B_*) \longrightarrow H_{n+1}(C_*) \xrightarrow{\delta_{n+1}} H_n(A_*) \longrightarrow H_n(B_*) \longrightarrow$$

$$\longrightarrow H_n(C_*) \xrightarrow{\delta_n} H_{n-1}(A_*) \longrightarrow H_{n-1}(B_*) \longrightarrow ...$$

is exact. It is called the long exact homology sequence associated to the above short exact sequence of complexes.

Proof. The sequence is exact at

1. $H_n(A_*)$: The homomorphism $H_{n-1}(\varphi_*) \circ \delta_n$ maps $[c] \in H_n(C_*)$ to $[\partial b] = 0 \in H_{n-1}(B_*)$, where $b \mapsto c$. Now assume $[a] \mapsto 0$, i.e. $a = \partial b$ with some $b \in B_n$. Then for $c := \psi_n(b)$ we have $\partial_n([c]) = [a]$.

2. $H_n(C_*)$: The homomorphism $\delta_n \circ H_n(\psi_*)$ maps $[b] \in H_n(B_*)$ to $[\partial b] = [0] = 0 \in H_{n-1}(A_*)$. Now assume $[c] \mapsto 0$, i.e. for $b \mapsto c$ we have $\partial b = \partial\tilde{a}$ with some $\tilde{a} \in A_n$. So $b - \tilde{a} \in Z_n(B_*)$ and $[b - \tilde{a}] \mapsto [c]$.

□

Here is an application for derived functors:

Theorem 13.18. *Let $F : R\text{-}\mathcal{MOD} \longrightarrow \mathcal{AB}$ be an additive co- resp. contravariant functor. A short exact sequence*

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

of R-modules induces a long exact sequence of derived functors

$$\longrightarrow L_{n+1}F(N) \longrightarrow L_nF(L) \longrightarrow L_nF(M) \longrightarrow L_nF(N) \longrightarrow L_{n-1}F(L) \longrightarrow$$

for covariant F, resp. for contravariant F it looks as follows

$$\longrightarrow R^{n-1}F(L) \longrightarrow R^nF(N) \longrightarrow R^nF(M) \longrightarrow R^nF(L) \longrightarrow R^{n-1}F(N) \longrightarrow$$

Corollary 13.19. *A short exact sequence*

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

of R-modules induces a long exact Tor-sequence

$$... \longrightarrow \mathrm{Tor}_{n+1}(A,N) \longrightarrow \mathrm{Tor}_n(A,L) \longrightarrow \mathrm{Tor}_n(A,M)$$

$$\longrightarrow \mathrm{Tor}_n(A,N) \longrightarrow \mathrm{Tor}_{n-1}F(A,L) \longrightarrow ...$$

a long exact Ext-sequence

$$... \longrightarrow \mathrm{Ext}^{n-1}(L,B) \longrightarrow \mathrm{Ext}^n(N,B) \longrightarrow \mathrm{Ext}^n F(M,B)$$

$$\longrightarrow \mathrm{Ext}^n(L,B) \longrightarrow \mathrm{Ext}^{n-1}(N,B) \longrightarrow ...$$

Proof of Th.13.18. We first prove:

Proposition 13.20. *A short exact sequence*

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

of R-modules can be covered by a short exact sequence

$$0 \longrightarrow P_* \xrightarrow{\varphi_*} S_* \xrightarrow{\psi_*} Q_* \longrightarrow 0$$

of projective resolutions of L, M and N. More precisely

1. *the resolutions P_*, Q_* with differentials $\partial_n, \tilde{\partial}_n$ can be prescribed. Then there is, for every $n \in \mathbb{N}$, an isomorphism*

   $$S_n \cong P_n \oplus Q_n,$$

   such that the above short exact sequence of complexes looks as follows

   $$P_n \xrightarrow{\varphi_n} S_n \cong P_n \oplus Q_n \xrightarrow{\psi_n} Q_n$$

   with the complex homomorphisms $\varphi_* : P_* \longrightarrow S_*$ and $\psi_* : S_* \longrightarrow Q_*$ given by $\varphi_n(x) = (x,0)$ and $\psi_n(x,y) = y$ for $x \in P_n, y \in Q_n$,

2. *in particular, the differentials* $\hat{\partial}_n$ *of the complex* $S_* = (S_n = P_n \oplus Q_n)_{n\in\mathbb{N}}$ *are of the form*

$$\hat{\partial}_n(x, y) = (\partial_n x + (-1)^n \chi_n(x), \tilde{\partial}_n y)$$

with a complex homomomorphism $\chi_* : Q_* \longrightarrow P_*[-1]$. *Here the shifted complex* $P_*[-1]$ *satisfies*

$$P_*[-1]_n := P_{n-1}$$

with the obvious differential.

Proof. We define $S_n = P_n \oplus Q_n$ and define the differential $\hat{\partial}_n : S_n \longrightarrow S_{n-1}$ by induction on n. For convenience define $P_{-1} = L, S_{-1} = M, Q_{-1} = N$. Asasume $\hat{\partial}_i$ is defined for $i \leq n$. Since the complexes up to $i \leq n$ form an exact sequence with trivial homology in degrees $i < n$ the long exact homology sequence implies that the lower row of the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P_{n+1} & \longrightarrow & S_{n+1} & \longrightarrow & Q_{n+1} & \longrightarrow & 0 \\ & & \downarrow & & & \swarrow & \downarrow & & \\ 0 & \longrightarrow & Z_n(P_*) & \longrightarrow & Z_n(S_*) & \longrightarrow & Z_n(Q_*) & \longrightarrow & 0 \end{array}$$

is exact. The skew arrow $\sigma : Q_{n+1} \longrightarrow Z_n(S_*)$ exists, since Q_{n+1} is projective, then take

$$\hat{\partial}_{n+1}(x, y) := (\partial_{n+1} x, 0) + \sigma(y).$$

An easy diagram chase yields $\hat{\partial}_{n+1}(S_{n+1}) = Z_n(S_*)$.

□

Let us now prove Th.13.18. We take a covering exact sequence

$$0 \longrightarrow P_* \xrightarrow{\varphi_*} S_* \xrightarrow{\psi_*} Q_* \longrightarrow 0$$

as in Prop:13.20. Then, given an additive functor F, the sequence

$$0 \longrightarrow F(P_*) \longrightarrow F(S_*) \longrightarrow F(Q_*) \longrightarrow 0$$

is exact as well, since additive functors commute with direct sums

$$F(S_n) \cong F(P_n) \oplus F(Q_n).$$

So we may apply Th.13.17. □

We conclude this section by establishing an alternative way to compute the Tor- and Ext-functors:

Theorem 13.21. *Let $A = A_R$ and $M = {}_RM, B = {}_RB$, furthermore $Q_* \longrightarrow \Delta_*(A)$ a projective resolution and $\Delta^*(B) \longrightarrow I^*$ an injective resolution. Then there are natural isomorphism*

$$\mathrm{Tor}_n(A, M) \cong H_n(Q_* \otimes M)$$

and

$$\mathrm{Ext}^n(M, B) \cong H^n(\mathrm{Hom}(M, I^*)).$$

Corollary 13.22. *A short exact sequence*

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

of R-modules induces a long exact Tor-sequence

$$\begin{aligned} ... \longrightarrow \mathrm{Tor}_{n+1}(C, M) \longrightarrow \mathrm{Tor}_n(A, M) \longrightarrow \mathrm{Tor}_n(B, M) \\ \longrightarrow \mathrm{Tor}_n(C, M) \longrightarrow \mathrm{Tor}_{n-1}(A, M) \longrightarrow ... \end{aligned}$$

as well as a long exact Ext-sequence

$$\begin{aligned} ... \longrightarrow \mathrm{Ext}^{n-1}(M, C) \longrightarrow \mathrm{Ext}^n(M, A) \longrightarrow \mathrm{Ext}^n F(M, B) \\ \longrightarrow \mathrm{Ext}^n(M, C) \longrightarrow \mathrm{Ext}^{n+1}(M, A) \longrightarrow ... \end{aligned}$$

For the proof of Th.13.21 we need double complexes, an important tool in homological algebra:

Definition 13.23. A homological double complex consists of R-modules

$$C_{\mu\nu}, \mu, \nu \in \mathbb{Z}$$

s.th.

$$C_{\mu\nu} = 0,$$

whenever $\mu < -1$ or $\nu < -1$, and R-module homomorphism

$$\partial_{\mu\nu} : C_{\mu\nu} \longrightarrow C_{\mu-1,\nu}$$

and

$$\tilde{\partial}_{\mu\nu} : C_{\mu\nu} \longrightarrow C_{\mu,\nu-1},$$

such that

1. $C_{*\nu}$ and $C_{\mu *}$ are complexes and

2. all squares
$$\begin{array}{ccc} C_{\mu\nu} & \longrightarrow & C_{\mu-1,\nu} \\ \downarrow & & \downarrow \\ C_{\mu,\nu-1} & \longrightarrow & C_{\mu-1,\nu-1} \end{array}$$
for $(\mu, \nu) \in \mathbb{Z}^2$ are commutative.

A cohomological double complex $C^{\mu\nu}$ is defined in the analogous way, with all arrows reversed.

The crucial result we need is the following:

Proposition 13.24. *Let $C_{\mu\nu}$ be a double complex, s.th. the complexes $C_{*\nu}$ and $C_{\mu *}$ are acyclic for $\mu, \nu \in \mathbb{N}$. Then there is a natural isomorphism*

$$H_n(C_{*,-1}) \cong H_n(C_{-1,*})$$

for every $n \in \mathbb{N}$. For cohomological double complexes the analogous statement holds.

Proof of Th.13.21. Denote $P_* \longrightarrow \Delta_*(M)$ a projective resolution of M, set $P_{-1} := M, Q_{-1} := A, I^{-1} := B$. We obtain a homological *double complex* with
$$C_{\mu\nu} := \begin{cases} Q_\mu \otimes P_\nu & , \text{ if } (\mu,\nu) \neq (-1,-1) \\ 0 & , \text{ if } (\mu,\nu) = (-1,-1) \end{cases},$$
resp. a cohomological *double complex*
$$C^{\mu\nu} := \begin{cases} \mathrm{Hom}(P_\mu, I^\nu) & , \text{ if } (\mu,\nu) \neq (-1,-1) \\ 0 & , \text{ if } (\mu,\nu) = (-1,-1) \end{cases}.$$

Now Prop.13.24 gives our result because of
$$\mathrm{Tor}_n(A, M) \cong H_n(C_{-1,*}),\ H_n(Q_* \otimes M) \cong H_n(C_{*,-1})$$
and
$$\mathrm{Ext}^n(M, B) \cong H^n(C^{*,-1}),\ H^n(\mathrm{Hom}(M, I^*)) = H^n(C^{-1,*}).$$

□

Proof of Prop.13.24. We compare the homology of the "boundary complexes" $C_{-1,*}$ and $C_{*,-1}$ with the homology of the *associated total complex* $\hat{C}_*$:

Definition 13.25. Given a homological double complex $C_{\mu\nu}$ the associated "total complex" $\widehat{C}_*$ has the chain modules

$$\widehat{C}_n := \bigoplus_{\mu+\nu=n} C_{\mu,\nu}$$

and the differentials

$$\widehat{\partial}_n : \widehat{C}_n \longrightarrow \widehat{C}_{n-1}$$

defined as follows

$$\widehat{\partial}_n := \bigoplus_{\mu+\nu=n} \partial_{\mu\nu} + (-1)^{\nu+1}\tilde{\partial}_{\mu\nu}.$$

We show that the injections of the boundary complexes

$$C_{*,-1} \hookrightarrow \widehat{C}_*,\ C_{-1,*} \hookrightarrow \widehat{C}_*$$

are quasi-isomorphisms - of course, by symmetry, it suffices to consider the first one. We consider the short exact sequence

$$0 \longrightarrow C_{*,-1} \longrightarrow \hat{C}_* \longrightarrow K_* \longrightarrow 0,$$

where the quotient complex $K_* := C_*/C_{*,-1}$ satisfies

$$K_n = \bigoplus_{\mu+\nu=n,\nu\geq 0} C_{\mu\nu},$$

and show that the complex K_* is acyclic. Assume

$$u = \sum_{\mu+\nu=n,\nu\geq 0} u_{\mu\nu} \in Z_n(K_*)$$

is a cycle $\neq 0$. We show by induction on $\lambda := \max\{\nu; u_{\mu\nu} \neq 0\}$ that u is even a boundary. Then we have $u_{n-\lambda,\lambda} \in Z_\lambda(C_{*,n-\lambda}) = B_\lambda(C_{*,n-\lambda})$, say $u_{n-\lambda,\lambda} = \partial v$ with some $v \in C_{\lambda+1,n-\lambda}$. Then by induction hypothesis $u' := u - \hat{\partial}v$ is a boundary and thus u as well.

Note that for a proof of our statement in the cohomological case all arrows have to be reversed; in particular the boundary complexes are no subcomplexes, but quotient complexes. □

13.3 Singular Homology

Here we shall assume R commutative, the most important case being $R = \mathbb{Z}$. Let us start the computation of singular homology groups with one point spaces:

Proposition 13.26. *1. For a one point space* pt *we have*

$$H_n(\mathrm{pt}) \cong \begin{cases} R & , \quad \textit{if } n = 0 \\ 0 & , \quad \textit{otherwise} \end{cases} .$$

2. $H_0(X) \cong R$ for X path connected.

Proof. Since there is exactly one n-simplex in a one point space, the complex $C_*(\mathrm{pt})$ looks as follows

$$\ldots \xrightarrow{\mathrm{id}} R \xrightarrow{0} R \xrightarrow{\mathrm{id}} R \xrightarrow{0} R \cong C_0(\mathrm{pt}) \longrightarrow 0,$$

whence the result follows. For the second part we consider the "augmentation homomorphism"

$$\varepsilon \ : \ C_0(X) \longrightarrow R, \sum_{x \in X} \lambda_x \cdot x \mapsto \sum_{x \in X} \lambda_x,$$

where we identify 0-simplices with points in X. Since ε is onto and $\partial_0 = 0$, it suffices to show $\ker(\varepsilon) = B_0(X) := \partial C_1(X)$. The inclusion "$\supset$" follows from $\varepsilon\partial\sigma = \varepsilon(\sigma(0,1) - \sigma(1,0)) = 0$ for any $\sigma \in S_1(X)$. On the other hand, if $\sum_{x \in X} \lambda_x = 0$, we may pick $x_0 \in X$ and 1-simplices σ_x with $\sigma_x(1,0) = x_0, \sigma(0,1) = x$, and obtain

$$\sum_{x \in X} \lambda_x \cdot x = \sum_{x \in X} \lambda_x \cdot x - \sum_{x \in X} \lambda_x \cdot x_0 = \sum_{x \in X} \lambda_x \partial\sigma_x = \partial \left(\sum_{x \in X} \lambda_x \sigma_x \right).$$

□

Now let us pass to "stars":

Definition 13.27. A subset $X \subset \mathbb{R}^m$ is called starshaped with center $x_0 \in X$, if for any point $x \in X$ the line segment from x_0 to x is contained in X as well.

We want to show that the inclusion $\{x_0\} \hookrightarrow X$ induces an isomorphism $H_n(x_0) \xrightarrow{\cong} H_n(X)$:

Theorem 13.28. *Let $X \subset \mathbb{R}^m$ be starshaped with center x_0. Then we have $C_*(\mathrm{id}_X) \backsimeq \varphi_*$, where $\varphi_* : C_*(X) \longrightarrow C_*(X)$ satisfies $\varphi_0(..) := \varepsilon(..)x_0$ and $\varphi_n = 0$ for $n \neq 0$. In particular φ_* factorizes through the complex R_* (with $R_0 = R$ and $R_n = 0$ otherwise) and thus*

$$H_n(X) \cong H_n(\mathrm{pt}).$$

Proof. Given an n-simplex $\sigma : \Delta_n \longrightarrow X$ we define an $(n+1)$-simplex $\widehat{\sigma} : \Delta_{n+1} \longrightarrow X$ as follows:

1. $\widehat{\sigma}(0, t_1, ..., t_{n+1}) = \sigma(t_1, ..., t_{n+1})$ and
2. $\widehat{\sigma}(1, 0, ..., 0) = x_0$.
3. For $s \in [0,1]$ we have $\widehat{\sigma}(1-s, s(t_1, ..., t_{n+1})) = (1-s)x_0 + s\ \sigma(t_1, ..., t_{n+1})$, i.e. the line segment from $(1, 0..., 0)$ to $(0, t_1, ..., t_{n+1})$ is mapped to the line segment from x_0 to $\sigma(t_1, ..., t_{n+1})$.

More explicitly

$$\widehat{\sigma}(t_0, ..., t_{n+1}) = \begin{cases} x_0 & , \quad \text{if } t_0 = 1 \\ t_0 x_0 + (1-t_0)\sigma((1-t_0)^{-1}t_1, ..., (1-t_0)^{-1}t_{n+1}) & , \quad \text{otherwise} \end{cases}.$$

Then, for $n > 0$, we have

$$\partial\widehat{\sigma} = \sigma + \sum_{i=0}^{n}(-1)^{i+1}\widehat{\sigma}_i = \sigma - \widehat{\partial\sigma}$$

with $\sigma_i := \sigma \circ \varepsilon_i^n : \Delta_{n-1} \hookrightarrow \Delta_n \longrightarrow X$, while

$$\partial\widehat{x} = x - x_0 \in C_0(X),$$

– please note that the expression $x - x_0$ is a difference of base elements in $C_0(X)$ and not a point in $\mathbb{R}^m$. Define $\kappa_n : C_n(X) \longrightarrow C_{n+1}(X)$ by $\kappa_n(\sigma) := \widehat{\sigma}$ for the basis elements $\sigma \in S_n(X) \subset C_n(X)$. Then the above equalities mean

$$\partial_{n+1}\kappa_n + \kappa_{n-1}\partial_n = \mathrm{id}_{C_n(X)} - \varphi_n = C_n(\mathrm{id}_X) - \varphi_n.$$

□

Theorem 13.29 (Homotopy invariance)**.** *Let $f, g : X \longrightarrow Y$ be homotopic continuous maps, i.e. there is a continuous map $F : X \times [0,1] \longrightarrow Y$ with $F_0 = f, F_1 = g$ (where $F_t(x) := F(x,t)$). Then $H_n(f) = H_n(g)$ for all $n \in \mathbb{N}$.*

Proof. The idea of the proof is quite intuitive: Assume that for all $q \in \mathbb{N}$ we can define an R-linear map

$$.. \times I : C_q(X) \longrightarrow C_{q+1}(X \times I), \xi \mapsto \xi \times I,$$

such that the "Leibniz rule"

$$\partial(\xi \times I) = (\partial\xi) \times I + (-1)^q(\xi \times 1 - \xi \times 0)$$

holds with the obvious definition of $\xi \times t$ for $t \in I$. Then we get for a cycle $\xi \in Z_q(X)$ the following:

$$F_1(\xi) - F_0(\xi) = F(\xi \times 1 - \xi \times 0) = F((-1)^q \partial(\xi \times I)) = \partial F((-1)^q \xi \times I),$$

where we have written simply F_t resp. F in order to denote $C_n(F_t)$ resp. $C_{n+1}(F)$.

The definition of $.. \times I : C_n(X) \longrightarrow C_{n+1}(X \times I)$ could be done by subdividing $\Delta_n \times I$ into a number of $(n+1)$-simplices $j_\nu : \Delta_{n+1} \hookrightarrow \Delta_n \times I$ and then, given $\sigma \in C_n(X)$, taking

$$\sigma \times I := \sum_\nu (\sigma \times \mathrm{id}_I) \circ j_\nu.$$

But that requires a careful definition of the j_ν, while we are lazy and prefer an abstract reasoning: The definition of $.. \times I$ will be "natural" in X and uses induction on n. The case $n = 0$ is left to the reader. Let now $n > 0$ and assume that for degree $< n$ we already have a definition. We look first at the case $X = \Delta_n$ and $\sigma = \delta_n := \mathrm{id}_{\Delta_n} \in C_n(\Delta_n)$. Then the chain

$$\zeta := (\partial\delta_n) \times I + (-1)^n(\delta_n \times 1 - \delta_n \times 0) \in C_n(\Delta_n \times I)$$

is defined by induction hypothesis and even a cycle:

$$\partial\zeta = (-1)^{n-1}(\partial\delta_n \times 1 - \partial\delta_n \times 0) + (-1)^n(\partial\delta_n \times 1 - \partial\delta_n \times 0) = 0.$$

But $H_n(\Delta_n \times I) = 0$ according to Th. 13.28, so there is a chain

$\eta \in C_{n+1}(\Delta_n \times I)$ with $\partial\eta = \zeta$, and we set

$$\delta_n \times I := \eta,$$

a choice making the Leibniz rule hold. In the general case, given an n-simplex $\sigma \in C_n(X)$, we take the continuous map $\sigma \times \mathrm{id}_I : \Delta_n \times I \longrightarrow X \times I$ and define

$$\sigma \times I := C_{n+1}(\sigma \times \mathrm{id}_I)(\delta_n \times I),$$

assuring "naturality", i.e. we have

$$f(\sigma \times I) = f(\sigma) \times I$$

for every continuous map $f : X \longrightarrow Y$. □

In order to compute singular homology modules we have to consider relative homology groups:

Definition 13.30. Let $A \subset X$ be a subspace of the topological space X. The relative chain complex $C_*(X, A)$ is defined as the complex with chain modules

$$C_n(X, A) := C_n(X)/C_n(A),$$

the differential being that one induced by $\partial_n : C_n(X) \longrightarrow C_{n-1}(X)$. Its homology

$$H_n(X, A) := H_n(C_*(X, A))$$

is called the n-th relative (singular) homology module (group) of X mod A.

Note that in general

$$H_n(X, A) \ncong H_n(X)/j_n(H_n(A)),$$

where $j_n : H_n(A) \longrightarrow H_n(X)$ denotes the homomorphism induced by the inclusion $j : A \longrightarrow X$. Instead the relative homology $H_*(X, A)$ relates the homology of X with the homology of the subspace A as follows: The short exact sequence of complexes

$$0 \longrightarrow C_*(A) \longrightarrow C_*(X) \longrightarrow C_*(X, A) \longrightarrow 0$$

induces the long exact homology sequence

$$... \longrightarrow H_{n+1}(X, A) \longrightarrow H_n(A) \longrightarrow H_n(X) \longrightarrow H_n(X, A) \longrightarrow H_{n-1}(A) \longrightarrow ....$$

On the other hand, intuitively, $H_*(X, A)$ should not depend on what is going on "inside A". Indeed we have:

Theorem 13.31 (Excision)**.** *Let $B \subset X$ be a subset with $\overline{B} \subset \overset{\circ}{A}$. Then the inclusion $(X \setminus B, A \setminus B) \hookrightarrow (X, A)$ induces an isomorphism*

$$H_n(X \setminus B, A \setminus B) \xrightarrow{\cong} H_n(X, A).$$

Barycentric Subdivision: In order to prove the above theorem one has to break singular chains into smaller pieces. This is done by "barycentric subdivision": For every topological space X we define a complex homomorphism

$$\beta_*(X) : C_*(X) \longrightarrow C_*(X),$$

such that

$$\beta_*(X) \backsimeq C_*(\mathrm{id}_X)$$

and, given a continuous map $f : X \longrightarrow Y$, we have

$$C_*(f) \circ \beta_*(X) = \beta_*(Y) \circ C_*(f),$$

i.e. the construction of $\beta_*(X)$ is "natural in X". We define $\beta_n(X)$ for every topological space X by induction on n. Take $\beta_0(X) := \mathrm{id}_{C_0(X)}$. Now assume $n > 0$ and that $\beta_q(X) : C_q(X) \longrightarrow C_q(X)$ is defined for all topological spaces X and $q < n$. First we consider again $X = \Delta_n$ and the singular n-simplex $\delta_n := \mathrm{id}_{\Delta_n}$. The standard n-simplex $\Delta_n \subset \mathbb{R}^{n+1}$ is starshaped with center $x_0 := (\frac{1}{n+1}, ..., \frac{1}{n+1})$. For any simplex $\sigma \in C_q(\Delta_n)$ denote $\widehat{\sigma} \in C_{q+1}(\Delta_n)$ the cone over σ with vertex x_0, see the prof of 13.28. Extend the cone construction linearly to all chains $\xi \in C_q(\Delta_n)$. Then, writing simply β_n instead of $\beta_n(\Delta_n)$ etc, we define

$$\beta_n(\delta_n) := \widehat{\beta_{n-1}(\partial\delta_n)},$$

the expression $\beta_{n-1}(\partial\delta_n)$ being defined by induction hypothesis. As before, for arbitrary $\sigma : \Delta_n \longrightarrow X$, we take

$$\beta_n(\sigma) := C_n(\sigma)(\beta_n(\delta_n)).$$

Let us check that this gives a chain map: Indeed, the formula

$$\partial\widehat{\sigma} = \sigma - \widehat{\partial\sigma}$$

yields

$$\partial\beta(\delta_n) = \partial(\widehat{\beta\partial\delta_n}) = \beta\partial\delta_n - (\widehat{\partial\beta\partial\delta_n}) = \beta\partial\delta_n,$$

since, again by induction hypothesis, $\partial_{n-1}\beta_{n-1}\partial_n = \beta_{n-2}\partial_{n-1}\partial_n = 0$. In the general case $\sigma \in C_n(X)$ we apply $C_*(\sigma) : C_*(\Delta_n) \longrightarrow C_*(X)$ using $C_n(\sigma)(\delta_n) = \sigma$.

It remains to define a chain homotopy $(\kappa_n(X) : C_n(X) \longrightarrow C_{n+1}(X))_{n\in\mathbb{Z}}$ between $\beta_*(X)$ and $C_*(\mathrm{id}_X)$ for all topological spaces X. Since $\beta_0(X) = \mathrm{id}_{C_0(X)}$ we may choose $\kappa_n(X) = 0$ for $n \leq 0$. Now assume $n > 0$ and $\kappa_q(X)$ defined for $q < n$. Again we consider first $X = \Delta_n$ and define $\kappa_n(\delta_n) := \kappa_n(\Delta_n)\delta_n$. We need to have

$$\partial_{n+1}\kappa_n(\delta_n) + \kappa_{n-1}\partial_n(\delta_n) = \beta_n(\delta_n) - \delta_n.$$

In order to find a good candidate for $\kappa_n(\delta_n)$, we check that

$$\zeta := \beta_n(\delta_n) - \delta_n - \kappa_{n-1}\partial_n(\delta_n)$$

is a cycle:

$$\partial_n(\zeta) = \partial_n\beta_n(\delta_n) - \partial_n(\delta_n) - \partial_n\kappa_{n-1}\partial_n(\delta_n)$$
$$= \beta_n(\partial_n\delta_n) - \partial_n\delta_n - \partial_n\kappa_{n-1}\partial_n(\delta_n) = \kappa_{n-2}\partial_{n-1}(\partial_n\delta_n) = 0,$$

the middle equality holding by induction hypothesis. Now, since $H_{n+1}(\Delta_n) = 0$, there is a singular chain $\eta \in C_{n+1}(\Delta_n)$ with $\partial_{n+1}\eta = \zeta$. Then set

$$\kappa_n(\delta_n) := \eta.$$

Finally, for general $\sigma : \Delta_n \longrightarrow X$ take

$$\kappa_n(\sigma) := C_{n+1}(\sigma)(\kappa_n(\delta_n)).$$

Remark 13.32.

1. If $A \subset X$ is a subspace of the topological space X, we have
$$\beta_*(X)|_{C_*(A)} = \beta_*(A), \kappa_*(X)|_{C_*(A)} = \kappa_*(A),$$
in particular there is an induced relative barycentric subdivision homomorphism
$$\beta_*(X, A) : C_*(X, A) \longrightarrow C_*(X, A)$$
homotopic to the identity.

2. For all simplices $\delta \in C_n(\Delta_n)$ entering in the chain $\beta^q(\delta_n) \in C_n(\Delta_n)$ we have
$$\mathrm{diam}(\delta(\Delta_n)) \leq (\frac{n}{n+1})^q \cdot \mathrm{diam}(\Delta_n).$$

3. If $\mathcal{U} := (U_j)_{j\in J}$ is an open cover of X, we define the subcomplex $C_*(\mathcal{U}) \subset C_*(X)$ of "$\mathcal{U}$-small chains" as

$$C_n(\mathcal{U}) := \sum_{j\in J} C_n(U_j).$$

Then, as a consequence of the first part of this remark, given a chain $\xi \in C_n(X)$ there is an exponent $s \in \mathbb{N}$, such that $\beta^s(\xi) \in C_n(\mathcal{U})$ holds for $\beta := \beta_n(X)$.

Proof of 13.31. We consider the open cover $\mathcal{U} := (U := X \setminus \overline{B}, V := \overset{\circ}{A})$.

1. Surjectivity: Denote $[\xi + C_n(A)] \in H_n(X, A)$ a relative homology class, i.e. $\partial\xi \in C_{n-1}(A)$. As a consequence of Rem.13.32.1 and 3 we may assume that ξ is $\mathcal{U}$-small, i.e.

$$\xi = \zeta + \eta$$

with n-chains $\zeta \in C_n(U) \hookrightarrow C_n(X \setminus B), \eta \in C_n(V)$. Then we have $\partial\xi, \partial\eta \in C_{n-1}(A)$, hence $\partial\zeta \in C_{n-1}(A)$ as well and $\zeta + C_n(A \setminus B) \in Z_n(X \setminus B, A \setminus B)$. Now

$$\zeta + C_n(A \setminus B) \mapsto \zeta + C_n(A) = \xi + C_n(A).$$

2. Injectivity: Assume $\zeta + C_n(X \setminus B) \in Z_n(X \setminus B, A \setminus B)$, i.e. $\partial\zeta \in C_{n-1}(A \setminus B)$, lies in the kernel of the homomorphism $H_n(X \setminus B, A \setminus B) \longrightarrow H_n(X, A)$, i.e.

$$\zeta = \partial\eta + \vartheta$$

with $\eta \in C_{n+1}(X), \vartheta \in C_n(A)$. Choose $s \in \mathbb{N}$, such that

$$\beta^s(\eta) = \eta_1 + \eta_2$$

with $n+1$-chains $\eta_1 \in C_{n+1}(U), \eta_2 \in C_{n+1}(V)$. Now we find

$$\zeta = (\zeta - \beta^s(\zeta)) + \beta^s(\zeta) = (\partial\kappa_n(\zeta) + \kappa_{n-1}(\partial\zeta)) + \beta^s(\partial\eta) + \beta^s(\vartheta),$$

where κ_* is our homotopy between the identity and $\beta^s = \beta_*(X)^s$. So

$$\zeta = \partial(\kappa_n(\zeta)) + \eta_1) + (\kappa_{n-1}(\partial\zeta) + \partial\eta_2 + \beta^s(\vartheta)),$$

where $\kappa_n(\zeta)) + \eta_1 \in C_{n+1}(X \setminus B)$ and the second term lies in $C_n(A \setminus B) = C_n(X \setminus B) \cap C_n(A)$, as desired: Indeed it lies in $C_n(X \setminus B)$, since both ζ and the first term do, furthermore $\kappa_{n-1}(\partial\zeta) \in C_n(A)$ by the naturally of the chain homotopy κ_*.

□

Theorem 13.33. *The unit sphere $\mathbb{S}^n \subset \mathbb{R}^{n+1}, n > 0$, has the homology modules:*

$$H_q(\mathbb{S}^n) = \begin{cases} R & , \quad \text{if } q = 0, n \\ 0 & , \quad \text{otherwise} \end{cases} .$$

Remark 13.34. Denote $\sigma : \Delta_{n+1} \longrightarrow \mathbb{B}^{n+1}$ a homeomorphism. Then we have

$$H_n(\mathbf{S}^n) = R[\partial\sigma].$$

Denote $\mathbb{B}^n \subset \mathbb{R}^n$ the open unit ball. The map

$$\mathbb{S}^n \longrightarrow \mathbb{B}^{n+1} \setminus \{0\}, x \mapsto x/2$$

has the left inverse

$$\mathbb{B}^{n+1} \setminus \{0\} \longrightarrow \mathbb{S}^n, x \mapsto \frac{x}{||x||} ;$$

indeed, up to homotopy, it is also a right inverse. As a consequence

$$H_q(\mathbb{S}^n) \cong H_q(\mathbb{B}^{n+1} \setminus \{0\}).$$

Now we may apply:

Proposition 13.35. *Let $n \geq 1$.*

1. *The $(n+1)$-dimensional punctured (open) unit ball $\mathbb{B}^{n+1} \setminus \{0\}$ has the homology modules:*

$$H_q(\mathbb{B}^{n+1} \setminus \{0\}) = \begin{cases} R & , \quad \text{if } q = 0, n \\ 0 & , \quad \text{otherwise} \end{cases} .$$

2. *The open unit ball $\mathbb{B}^n \subset \mathbb{R}^n$ mod its puncture $\mathbb{B}^n \setminus \{0\}$ has the homology modules:*

$$H_q(\mathbb{B}^n, \mathbb{B}^n \setminus \{0\}) = \begin{cases} R & , \quad \text{if } q = n \\ 0 & , \quad \text{otherwise} \end{cases} .$$

Corollary 13.36. *Invariance of dimension: If*

$$\mathbb{R}^m \supset U \xrightarrow{f} V \subset \mathbb{R}^n$$

with open subsets $U \subset \mathbb{R}^m, V \subset \mathbb{R}^n$ and a homeomorphism $f : U \longrightarrow V$, then $n = m$.

The invariance of dimension seems natural, but is far from being trivial: E.g. there are curves in the plane, i.e. continuous maps $f : [0,1] \longrightarrow \mathbb{R}^2$, whose image is a triangle or a square!

Proof. Take any point $x_0 \in U$ and $y_0 := f(x_0)$. Then $f : U \longrightarrow V$ being a homeomorphism, induces an isomorphism $H_q(U, U \setminus \{x_0\}) \cong H_q(V, V \setminus \{y_0\})$. But $H_q(U, U \setminus \{x_0\}) \cong H_q(\mathbb{B}^n, \mathbb{B}^n \setminus \{x_0\})$. Take $\varepsilon > 0$ with $\overline{\mathbb{B}_\varepsilon(x_0)} \subset U$. Then by excision

$$H_q(U, U \setminus \{x_0\}) \cong H_q(\mathbb{B}^n_\varepsilon(x_0), \mathbb{B}^n_\varepsilon(x_0) \setminus \{x_0\}) \cong H_q(\mathbb{B}^n, \mathbb{B}^n_0).$$

So by looking at the "local homology group" $H_q(U, U \setminus \{x_0\})$ we can rediscover the dimension n. □

Proof of Prop. 13.35: Write $\mathbb{B}^n_0 := \mathbb{B}^n \setminus \{0\}$.

The statement 2_n for $n = 1$: We have $\mathbb{B}^1 = (-1, 1)$ and $\mathbb{B}^1_0 = (-1, 0) \cup (0, 1)$. Hence $H_q(\mathbb{B}^1) = 0 = H_q(\mathbb{B}^1_0)$ for $q > 0$, while

$$H_0(\mathbb{B}^1_0) \cong R^2 \longrightarrow R \cong H_0(\mathbb{B}^1)$$

is the map $(x, y) \mapsto x + y$. The long exact homology sequence of the pair $(\mathbb{B}^1, \mathbb{B}^1_0)$ then gives the claim.

The implication "$2_n \Longrightarrow 1_n$": We may replace the punctured ball $\mathbb{B}^{n+1}_0, n \geq 1$ with the unit sphere $\mathbb{S}^n$. Since $\mathbb{S}^n$ is (pathwise) connected, we obtain $H_0(\mathbb{S}^n) = R$. For $q > 0$ we consider the exact homology sequence of the pair $(\mathbb{S}^n, \mathbb{S}^n_-)$ with $\mathbb{S}^n_- := \mathbb{S}^n \setminus \{e_{n+1}\}$, the sphere with the north pole removed. But $\mathbb{S}^n_- \cong \mathbb{B}^n$, so $H_q(\mathbb{S}^n_-) = 0$ for $q > 0$, while $H_0(\mathbb{S}^n_-) \longrightarrow H_0(\mathbb{S}^n)$ is an isomorphism. Thus

$$H_q(\mathbb{S}^n) \cong H_q(\mathbb{S}^n, \mathbb{S}^n_-) \cong H_q(\mathbb{S}^n_+, \mathbb{S}^n_0) \cong H_q(\mathbb{B}^n, \mathbb{B}^n_0)$$

with $\mathbb{S}^n_+ := \mathbb{S}^n \setminus \{-e_{n+1}\}$, the sphere with the south pole removed, and the double punctured sphere $\mathbb{S}^n_0 := \mathbb{S}^n \setminus \{\pm e_{n+1}\}$. The second isomorphism is obtained by excision of the south pole $-e_{n+1}$.

The implication "$1_n \Longrightarrow 2_{n+1}$": The long exact homology sequence of the pair $(\mathbb{B}^{n+1}, \mathbb{B}_0^{n+1})$ gives for $q > 1$ a "connecting isomorphism"

$$H_q(\mathbb{B}^{n+1}, \mathbb{B}_0^{n+1}) \xrightarrow{\cong} H_{q-1}(\mathbb{B}_0^{n+1}),$$

since then $H_q(\mathbb{B}^{n+1}) = 0 = H_{q-1}(\mathbb{B}^{n+1})$, while the case $q \leq 1$ follows from the fact that $H_0(\mathbb{B}_0^{n+1}) \longrightarrow H_0(\mathbb{B}^{n+1})$ is an isomorphism for $n \geq 1$. □

Finally we discuss a method how to compute the singular homology of topological spaces, which are the (set theoretically) disjoint union of *cells*:

Definition 13.37. An n-cell is a topological space homeomorphic to the open ball $\mathbb{B}^n$. And, of course, a cell is an n-cell with a suitable $n \in \mathbb{N}$.

If X is a disjoint union of cells, we take X_q to be the union of all i-cells with $i \leq q$ and obtain thus an increasing filtration of X. The following result shows that in certain cases we can replace the very big singular chain complex $C_*(X)$ with a smaller complex $C_*(\mathfrak{X})$.

Proposition 13.38. *Given a filtration*

$$\mathfrak{X} := (X_0 \subset X_1 \subset ... \subset X_{n-1} \subset X_n = X)$$

of the topological space X, the corresponding cellular complex $C_*(\mathfrak{X})$ is defined as

$$C_*(\mathfrak{X}) := (H_q(X_q, X_{q-1}), \partial_q),$$

with the relative homology groups $H_q(X_q, X_{q-1})$ and the the boundary homomorphisms

$$H_q(X_q, X_{q-1}) \longrightarrow H_{q-1}(X_{q-1}) \longrightarrow H_{q-1}(X_{q-1}, X_{q-2}).$$

If furthermore $H_p(X_q, X_{q-1}) = 0$ holds for $p \neq q$, there is a natural isomorphisms

$$H_q(X) \cong H_q(C_*(\mathfrak{X})),$$

in particular $H_q(X) = 0$ for $q > n$.

Proof. First of all $\partial_{q-1} \circ \partial_q = 0$, since

$$H_{q-1}(X_{q-1}) \longrightarrow H_{q-1}(X_{q-1}, X_{q-2}) \longrightarrow H_{q-2}(X_{q-2})$$

is the zero homomorphism. For the second part we do induction on n. Let us assume we have established the isomorphism for $Y = X_n$ and consider $X := X_{n+1}$. We look at the long exact homology sequence of the pair (X, Y) and find

$$H_q(Y) \cong H_q(X), q < n.$$

We have $H_{n+1}(Y) = 0$ and consider the exact sequence

$$0 \longrightarrow H_{n+1}(X) \longrightarrow H_{n+1}(X, Y) \longrightarrow H_n(Y) \longrightarrow H_n(X) \longrightarrow 0.$$

Write $Z := X_{n-1}$. Since $H_n(Y) \hookrightarrow H_n(Y, Z)$ because of $H_n(Z) = 0$, we obtain $H_{n+1}(X) \cong H_{n+1}(C_*(\mathfrak{X}))$. On the other hand $H_n(X) \cong \operatorname{coker}(H_{n+1}(X, Y) \longrightarrow H_n(Y))$, while $H_n(Y, Z) \longrightarrow H_{n-1}(Z, X_{n-2})$ has the same kernel as $H_n(Y, Z) \longrightarrow H_{n-1}(Z)$ because of $H_{n-1}(Z) \hookrightarrow H_{n-1}(Z, X_{n-2})$. So $H_n(Y) \cong Z_n(\mathfrak{X})$ and $\operatorname{coker}(H_{n+1}(X, Y) \longrightarrow H_n(Y)) \cong H_n(C_*(\mathfrak{X}))$. □

Definition 13.39. A cellular space is a topological space X together with a filtration

$$\mathfrak{X} := (X_0 \subset X_1 \subset ... \subset X_{n-1} \subset X_n = X)$$

by closed subsets $X_q \hookrightarrow X$, such that

$$X_q \setminus X_{q-1} = \bigcup_{i=1}^{m} U_i, m = m_q$$

is the disjoint union of q-cells U_i, which are attached to the $q-1$-skeleton X_{q-1} by continuous maps

$$\varphi_i : \overline{\mathbb{B}}^q \longrightarrow X_q$$

restricting to a homeomorphism

$$\mathbb{B}^q \longrightarrow U_i$$

and satisfying

$$\varphi_i(\mathbb{S}^{q-1}) \subset X_{q-1}.$$

Proposition 13.40. *In the above situation let* $x_i := \varphi_i(0)$ *and*

$U_i^* := U_i \setminus \{x_i\}$. *Then we have*

$$H_p(X_q, X_{q-1}) \cong \bigoplus_{i=1}^{m} H_p(U_i, U_i^*) \cong \begin{cases} R^m & , \quad \textit{if } p = q \\ 0 & , \quad \textit{otherwise} \end{cases} .$$

Proof. The inclusion $X_{q-1} \hookrightarrow U := X_q \setminus \{x_1, ..., x_m\}$ is a homotopy equivalence. Now the inclusion of pairs $(X_q, X_{q-1}) \hookrightarrow (X_q, U)$ induces a "morphism" of the corresponding long exact homology sequences; between the absolute groups we have the identity resp. an isomorphism. A simple diagram chase now shows that the homomorphisms between the relative groups are isomorphisms as well. Finally, by excision

$$H_p(X_q, U) \cong H_p(X_q \setminus X_{q-1}, U \setminus X_{q-1}).$$

□

So in order to compute $H_*(X)$ we have to understand the boundary homomorphisms of the cellular complex $C_*(\mathfrak{X})$.

Example 13.41. 1. The two dimensional torus $X = I^2/\sim$ is obtained from the unit square I^2 by identifying the points $(t, 0)$ and $(t, 1)$ as well as the points $(0, t)$ and $(1, t)$. Denote $\pi : I^2 \longrightarrow X$ the quotient map. We consider the filtration

$$\mathfrak{X} = (\pi(0, 0) \subset \pi(\partial I^2) \subset X_2 = X)$$

with one zero cell, the 1-cells $\pi((0, 1) \times 0), \pi(0 \times (0, 1))$ and the 2-cell $\pi((0, 1)^2)$. Then $C_*(\mathfrak{X})$ looks as follows

$$0 \longrightarrow R \longrightarrow R^2 \longrightarrow R \longrightarrow 0.$$

Assume that $1 \in R \cong C_2(\mathfrak{X})$ is induced from a singular 2-simplex $\Delta_2 \longrightarrow I^2$, whose boundary corresponds to the positively oriented loop ∂I^2, while $(1, 0), (0, 1) \in R^2 \cong C_1(\mathfrak{X})$ are obtained from the loops $t \mapsto \pi(t, 0)$ and $t \mapsto \pi(0, t)$. Hence $\partial_1 = 0$, but $\partial_2 = 0$ as well: Indeed

$$\partial_2(1) = (1, 0) + (0, 1) - (1, 0) - (0, 1).$$

It follows

$$H_q(X) \cong C_q(\mathfrak{X}) = \begin{cases} R & , \text{ if } q = 0, 2 \\ R^2 & , \text{ if } q = 1 \\ 0 & , \text{ otherwise} \end{cases} .$$

2. Klein's bottle $Y = I^2/\sim$ is obtained from the unit square I^2 by identifying the points $(t,0)$ and $(t,1)$ as well as the points $(0,t)$ and $(1,1-t)$. Denote $\pi : I^2 \longrightarrow Y$ the quotient map. We consider the filtration

$$\mathfrak{Y} = (\pi(0,0) \subset \pi(\partial I^2) \subset Y_2 = Y).$$

Then $C_*(\mathfrak{Y})$ looks as follows

$$0 \longrightarrow R \longrightarrow R^2 \longrightarrow R \longrightarrow 0.$$

Assume that $1 \in R \cong C_2(\mathfrak{Y})$ is induced from a singular 2-simplex $\Delta_2 \longrightarrow I^2$, whose boundary corresponds to the positively oriented loop ∂I^2, while $(1,0),(0,1) \in R^2 \cong C_1(\mathfrak{Y})$ are obtained from the loops $t \mapsto \pi(t,0)$ and $t \mapsto \pi(0,t)$. Hence $\partial_1 = 0$, while

$$\partial_2(1) = (1,0) - (0,1) - (1,0) - (0,1) = (0,-2).$$

It follows

$$H_q(Y) \cong \begin{cases} R & , \text{ if } q = 0 \\ R \oplus R_2 & , \text{ if } q = 1 \\ 0 & , \text{ otherwise} \end{cases}.$$

3. Finally we discuss $Z := I^2/\sim$ with the boundary point identifications $(t,0) \sim (1-t,1)$ and $(0,t) \sim (1,1-t)$. We obtain two different zero cells $\pi(0,0), \pi(1,0)$ (inducing the basis vectors $(1,0)$ reap. $(0,1)$ in $R^2 \cong C_0(\mathfrak{Z})$), and the paths $t \mapsto \pi(t,0)$ and $t \mapsto \pi(0,t)$ are no longer loops (they correspond to $(1,0)$ reap. $(0,1)$ in $R^2 \cong C_1(\mathfrak{Z})$). Thus the complex $C_*(\mathfrak{Z})$ looks as follows:

$$0 \longrightarrow R \longrightarrow R^2 \longrightarrow R^2 \longrightarrow 0$$

with $\partial_2(1) = (2,-2), \partial_1(1,0) = (-1,1) = \partial_1(0,1)$, hence $Z_1(\mathfrak{Z}) = R(1,-1)$. Thus:

$$H_q(Z) \cong \begin{cases} R & , \text{ if } q = 0 \\ R_2 & , \text{ if } q = 1 \\ 0 & , \text{ otherwise} \end{cases}.$$

The surface Z in the previous example can also be thought of as the closed unit disk $\overline{\mathbb{B}}^2$, where antipodal points on the boundary circle $\mathbb{S}^1$ are

identified. With that description it admits an immediate generalizations to higher dimensions. The most satisfactory construction is as follows:

Real projective n-space $\mathbb{P}_n(\mathbb{R})$ is the set of all one dimensional subspaces of $\mathbb{R}^{n+1}$. We have a natural map

$$\mathbb{R}^{n+1} \setminus \{0\} \longrightarrow \mathbb{P}_n(\mathbb{R}), \mathbf{x} \mapsto [\mathbf{x}] := \mathbb{R}\mathbf{x}$$

and endow $\mathbb{P}_n(\mathbb{R})$ with the quotient topology. Indeed the restriction of the quotient map to the unit sphere yields a local homeomorphism

$$\pi : \mathbb{S}^n \longrightarrow \mathbb{P}_n(\mathbb{R}),$$

whose fibres are pairs of antipodal points $\pm\mathbf{x}$. So $\mathbb{P}_n(\mathbb{R})$ is obtained from $\mathbb{S}^n$ by identifying antipodal points. (In particular $\mathbb{P}_1(\mathbb{R}) \cong \mathbb{S}^1$.)

We want to establish a cell decomposition of $\mathbb{P}_n(\mathbb{R})$: For $q \leq n$ the inclusion

$$\mathbb{R}^{q+1} \cong \mathbb{R}^{q+1} \times 0 \hookrightarrow \mathbb{R}^{n+1}$$

realizes projective q-space as a subspace of the n-dimensional projective space:

$$\mathbb{P}_q(\mathbb{R}) \hookrightarrow \mathbb{P}_n(\mathbb{R}).$$

We thus obtain a filtration $\mathfrak{Z}$ of $Z := \mathbb{P}_n(\mathbb{R})$ with

$$Z_q := \mathbb{P}_q(\mathbb{R}).$$

Eventually, in order to see that $(Z, \mathfrak{Z})$ is a cellular space it suffices to find an "attaching map" for the n-cell $Z_n \setminus Z_{n-1}$ and to use induction on n. First note that $\mathbf{x} \mapsto (\mathbf{x}, \sqrt{1 - ||\mathbf{x}||^2})$ identifies $\overline{\mathbb{B}}^n$ with the northern hemisphere $\mathbb{S}^n_+$ of $\mathbb{S}^n$. We choose

$$\varphi : \overline{\mathbb{B}}^n \longrightarrow Z, \mathbf{x} \mapsto \left[\mathbf{x}, \sqrt{1 - ||\mathbf{x}||^2}\right].$$

So there is one q-cell for any $q, 0 \leq q \leq n$, and $C_q(\mathfrak{Z}) = R$ for $0 \leq q \leq n$. In order to find $\partial_q : R \longrightarrow R$ for $q \geq 1$ it obviously suffices to study the case $q = n$. To that end we consider the following diagram

$$\begin{array}{ccccccc} H_n(\overline{\mathbb{B}}^n, \mathbb{S}^{n-1}) & \longrightarrow & H_{n-1}(\mathbb{S}^{n-1}) & \longrightarrow & H_{n-1}(\mathbb{S}^{n-1}, \mathbb{S}^{n-2}) & \cong & H_{n-1}(\mathbb{S}^{n-1}_+, \mathbb{S}^{n-2})^2 \\ \downarrow & & & & \downarrow & & \\ H_n(\mathbb{P}_n, \mathbb{P}_{n-1}) & & \xrightarrow{\partial_n} & & H_{n-1}(\mathbb{P}_{n-1}, \mathbb{P}_{n-2}) & & \end{array},$$

it turns out to be nothing but

$$\begin{array}{ccccc} R & \stackrel{\cong}{\longrightarrow} & R & \longrightarrow & R^2 \\ \downarrow & & & & \downarrow \\ R & & \stackrel{?}{\longrightarrow} & & R \end{array}.$$

The left vertical map is an isomorphism, while the right one is $(x, y) \mapsto x+y$, and what we have to understand is the horizontal map $R \longrightarrow R^2$. The right upper isomorphism looks as follows

$$H_{n-1}(\mathbb{S}^{n-1}, \mathbb{S}^{n-2}) \cong H_{n-1}(\mathbb{S}^{n-1}_+, \mathbb{S}^{n-2}) \oplus H_{n-1}(\mathbb{S}^{n-1}_-, \mathbb{S}^{n-2}) \cong H_{n-1}(\mathbb{S}^{n-1}_+, \mathbb{S}^{n-2})^2,$$

where the second component of the second isomorphism, the map

$$H_{n-1}(\mathbb{S}^{n-1}_-, \mathbb{S}^{n-2}) \longrightarrow H_{n-1}(\mathbb{S}^{n-1}_+, \mathbb{S}^{n-2}),$$

is induced by the antipodal map $\mathbb{S}^{n-1} \longrightarrow \mathbb{S}^{n-1}, \mathbf{x} \mapsto -\mathbf{x}$. On the other hand, it induces a commutative diagram

$$\begin{array}{ccc} H_{n-1}(\mathbb{S}^{n-1}) & \stackrel{\cong}{\longrightarrow} & H_{n-1}(\mathbb{S}^{n-1}_-, \mathbb{S}^{n-2}) \\ \downarrow & & \downarrow \\ H_{n-1}(\mathbb{S}^{n-1}) & \stackrel{\cong}{\longrightarrow} & H_{n-1}(\mathbb{S}^{n-1}_+, \mathbb{S}^{n-2}) \end{array},$$

so it suffices to know the left vertical map.

Proposition 13.42. *The map $i_n : H_n(\mathbb{S}^n) \longrightarrow H_n(\mathbb{S}^n)$ induced by the antipodal map $\mathbb{S}^n \longrightarrow \mathbb{S}^n, \mathbf{x} \mapsto -\mathbf{x}$, satisfies*

$$i_n = \mu_{(-1)^{n+1}}.$$

Proof. A reflection induces μ_{-1}: It suffices to consider the reflection $g : \mathbb{R}^{n+1} \longrightarrow \mathbb{R}^{n+1}$ at the hyperplane $\mathbb{R}^n \times 0$. Choose a singular n-chain $\xi \in C_n(\mathbb{S}^n_+), \partial\xi \in C_n(\mathbb{S}^{n-1})$, such that the (relative) homology class of $\xi + C_n(\mathbb{S}^{n-1})$ generates $H_n(\mathbb{S}^n_+, \mathbb{S}^{n-1})$. Then $[\xi - g(\xi)]$ generates $H_n(\mathbb{S}^n)$ and g maps it to $[g(\xi) - \xi]$.

Finally the antipodal map is the product of $n+1$ reflections. □

As a consequence we get the upper horizontal map

$$R \longrightarrow R^2, x \mapsto (x, (-1)^n x),$$

hence the lower horizontal map

$$\partial_n : R \longrightarrow R$$

is

$$x \mapsto (1 + (-1)^n)x.$$

So the complex $C_*(\mathfrak{Z})$ looks as follows

$$... \xrightarrow{\mu_2} R \xrightarrow{0} R \xrightarrow{\mu_2} R \xrightarrow{0} R \longrightarrow 0$$

Theorem 13.43.

$$H_q(\mathbb{P}_n(\mathbb{R})) \cong \begin{cases} R & , \quad \textit{if } q = 0 \textit{ or } q = n = 2\ell + 1 \\ R_2 & , \quad \textit{if } q = 2\ell + 1 < n \\ 0 & , \quad \textit{otherwise} \end{cases} .$$

Complex projective n-space $\mathbb{P}_n(\mathbb{C})$ is defined in the same way as real projective n-space, replacing $\mathbb{R}$ with $\mathbb{C}$. We obtain again a filtration

$$Z_q = \mathbb{P}_q(\mathbb{C}) \hookrightarrow \mathbb{P}_n(\mathbb{C}),$$

but now $Z_q \setminus Z_{q-1}$ is a $2q$-cell. There are further differences: The restriction

$$\mathbb{S}^{2n+1} \longrightarrow \mathbb{P}_n(\mathbb{C})$$

of the quotient map

$$\mathbb{C}^{n+1} \setminus \{0\} \longrightarrow \mathbb{P}_n(\mathbb{C})$$

to the unit sphere $\mathbb{S}^{2n+1} \hookrightarrow \mathbb{C}^{n+1}$, the "Hopf fibration", is no longer a local homeomorphism: Its fibres are copies of $\mathbb{S}^1$ (though $\mathbb{S}^{2n+1} \ncong \mathbb{P}_n(\mathbb{C}) \times \mathbb{S}^1$). Nevertheless the attaching map

$$\varphi : \overline{\mathbb{B}}^{2n} \longrightarrow \mathbb{P}_n(\mathbb{C})$$

can be defined in the same way - indeed, the restriction $\varphi|_{\mathbb{B}^{2n}}$ may be factorized as follows

$$\mathbb{B}^{2n} \xrightarrow{\psi} \mathbb{C}^n \times \{1\} \xrightarrow{\pi} \mathbb{P}_n(\mathbb{C}) \setminus \mathbb{P}_{n-1}(\mathbb{C})$$

with the homeomorphism

$$\psi(\mathbf{z}) := \left(\frac{\mathbf{z}}{\sqrt{1 - ||\mathbf{z}||^2}}, 1 \right).$$

The spaces $\mathbb{P}_n(\mathbb{C})$ are the basic spaces in complex algebraic geometry: Many "algebraic varieties" are realized as subspaces of some $\mathbb{P}_n(\mathbb{C})$. The case $n = 1$ yields the "projective line" $\mathbb{P}_1(\mathbb{C}) \cong \mathbb{S}^2$, also known in complex analysis as the "Riemann sphere" or "extended complex plane $\mathbb{C} \cup \{\infty\}$.

Since all cells are of even dimension, the differentials of the cellular complex $C_*(\mathfrak{Z})$ are trivial and we find:

Theorem 13.44.

$$H_q(\mathbb{P}_n(\mathbb{C})) \cong \begin{cases} R & , \quad \text{if } q = 2\ell \leq 2n \\ 0 & , \quad \text{otherwise} \end{cases}.$$

Euler characteristic:

Definition 13.45. For a cell decomposition $\mathfrak{X}$ of X denote e_q the number of connected components of $X_q \setminus X_{q-1}$, i.e. the number of q-cells in the decomposition. Then we define the Euler characteristic $\chi(\mathfrak{X})$ of the decomposition as

$$\chi(\mathfrak{X}) := \sum_{q=0}^{n} (-1)^q e_q.$$

Theorem 13.46.

$$\chi(\mathfrak{X}) = \sum_{q=0}^{n} \operatorname{rank}(H_q(X)).$$

In particular $\chi(\mathfrak{X})$ only depends on the topological space X, not on the choice of the cell decomposition, it is called the Euler-Poincaré characteristic of X and denoted $\chi(X)$.

Proof. Since $K = Q(R)$ is a flat R-module, we have $H_q(X, K) \cong H_q(X) \otimes K$ and thus $\operatorname{rank}(H_q(X, R)) = \dim H_q(X, K)$; so we may assume that $R = K$ is a field. Then we have

$$\chi(\mathfrak{X}) = \sum_{q=0}^{n} (-1)^q \dim C_q(\mathfrak{X}),$$

while

$$\sum_{q=0}^{n}(-1)^q \dim H_q(V_*) = \sum_{q=0}^{n}(-1)^q \dim V_q$$

holds for any complex of finite dimensional vector spaces living in degrees $q = 0, ..., n$. □

Remark 13.47. Note that $\dim H_q(X)$ depends on (the characteristic of) K. For $K = \mathbb{Q}$ the numbers

$$b_q(X) := \dim H_q(X, \mathbb{Q})$$

are called the "Betti numbers" of the topological space X.

14 Annex: Zorns Lemma

If in algebra infinite or even uncountable sets are involved, it can be useful to know about the existence of certain objects even if there is no constructive method to create them: A generally accepted tool in this context is "Zorns lemma", which we shall discuss in this annex.

Definition 14.1. *A* **partial order** *on a set M is a relation "$\preceq$", which is reflexive, antisymmetric and transitive, i.e.*

1. $\forall\ x \in M :\ x \preceq x$,
2. $\forall\ x, y \in M :\ x \preceq y \wedge y \preceq x \Longrightarrow x = y$ *and*
3. $\forall\ x, y, z \in M : x \preceq y \wedge y \preceq z \Longrightarrow x \preceq z$.

Such a relation is sometimes simply called an order (relation) on M. A **total** *or* **linear** *order is a partial order, where any two elements $x, y \in M$ are related:*

$$\forall\ x, y \in M :\ x \preceq y \vee y \preceq x\ .$$

A **well ordering** *on M is a linear order, such that every non-empty subset $M_0 \subset M$ has a first element (with respect to $\preceq$), i.e.,*

$$\forall\ M_0 \subset M\ \exists\ a \in M_0 : \forall\ x \in M_0\ :\ a \preceq x\ .$$

An element $a \in M$ is called **maximal** *(w.r.t. the order $\preceq$), iff*

$$\forall\ x \in M :\ a \preceq x \Longrightarrow a = x,$$

i.e., there are no elements bigger than a.

Example 14.2. In many applications the set M is realized as a subset $M \subset \mathcal{P}(U)$ of the power set of some set U (the "universe") with the inclusion as order relation

$$A \preceq B \Longleftrightarrow A \subset B.$$

Remark 14.3. 1. If $x \preceq a$ for all $x \in M$, the element a is obviously maximal, but in general that need not hold for a maximal element: It is allowed for a maximal element $a \in M$, that there are elements in M not related to a.

2. The set $\mathbb{N} = \{0, 1, 2, ...\}$ of all natural numbers, endowed with the natural order, is well ordered, but $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$ are not. The set $\mathbb{N}^2$, endowed with the **lexicographic order**

$$(x, y) \preceq (x', y') \Longleftrightarrow x < x' \vee (x = x' \text{ and } y \leq y') \ .$$

is well ordered. A subset of a well ordered set has by definition a unique first element, but in general no last element, and every element has an immediate successor - the first element of the set of all elements after the given one, but not necessarily an immediate predecessor. An **initial segment** M_0 of a linearly ordered set M is a subset $M_0 \subset M$ satisfying $M \ni y \preceq x \in M_0 \Longrightarrow y \in M_0$, i.e., with an element $x \in M_0$ all elements $y \preceq x$ before x belong to M_0. If M is well ordered, such an initial segment satisfies either $M_0 = M$ or $M_0 = M_{\prec a} := \{x \in M; x \prec a\}$. Namely, given an initial segment $M_0 \neq M$, choose a as the first element in the complement $M \setminus M_0$.

Theorem 14.4. (Zorns lemma) *(Max August Zorn, 1906-1993): Let M be a set with the partial order $\preceq$. If for every (w.r.t. $\preceq$) linearly ordered subset $T \subset M$ there is an upper bound $b \in M$, i.e. such that $t \preceq b$ for all $t \in T$ (written briefly as $T \preceq b$), then there are maximal elements in M.*

Example 14.5. If $M \subset \mathcal{P}(U)$ as in Example 14.2, the upper bound B of a linearly ordered subset $T \subset M \subset \mathcal{P}(U)$ usually is taken as the union $B := \bigcup_{A \in T} A$ of all sets $A \in T$, and it remains to check that in fact $B \in M$.

Before we prove Zorns lemma we present three applications:

Theorem 14.6. *Given a linearly independent set $B_0 \subset V$ of a K-vector space V there is a basis $B \supset B_0$ of V. In particular*

1. *Every vector space admits a basis.*

2. *For every subspace $W \subset V$ there is a complementary subspace $V_0 \subset V$, i.e. such that*
$$V = W \oplus V_0.$$

Proof. Take $M \subset \mathcal{P}(V)$ as the set of all linearly independent subsets of V containing B_0. We can apply Zorns lemma as in Example 14.5. So there is a maximal set $B \in M$. Indeed B is a basis: We have to show that any vector $v \in V$ is a finite linear combination of vectors in B. So let $v \in V$. If $v \in B$, we are done, otherwise $B \cup \{v\} \notin M$ – the set $B \in M$ being maximal in M – and hence there is a non-trivial relation

$$0 = \lambda v + \lambda_1 v_1 + ... + \lambda_r v_r$$

with $v_1, ..., v_r \in B$ and $\lambda, \lambda_1, ..., \lambda_r \in K$. But $\lambda \neq 0$, since the vectors $v_1, ..., v_r$ are linearly independent, i.e., we may solve for $v \in V$.

For the first part of the second statement take $B_0 = \emptyset$, for the second take B_0 as a basis of W and set

$$V_0 := \sum_{v \in B \setminus B_0} Kv.$$

□

Theorem 14.7. *Every proper left/right ideal $\mathfrak{a} \subset R$ in a ring R is contained in a maximal left/right ideal $\mathfrak{m} \subset R$.*

Proof. Take $M \subset \mathcal{P}(R)$ as the subset of all proper left/right ideals in R containing $\mathfrak{a}$. Since an ideal $\mathfrak{a}$ is proper iff $1 \notin \mathfrak{a}$, it is obvious that the union of a linearly ordered set of proper ideals again is a proper ideal. □

Theorem 14.8. *A submodule $N \leq F$ of a free module F over a PID R is itself free.*

Proof. The proof is analogous to that of Lemma 4.1, the only difference is that the basis of N is not any longer constructed in finitely many steps, instead Zorns lemma gives its existence: We may assume $F = R[I]$ and consider the set of pairs

$$(J, B),$$

such that

1. $J \subset I$, and

2. the submodule $N \cap R[J]$ is free with basis B.

It is non-empty, since obviously $R[J] \cap N$ is free whenever $|J| = 1$, the ring R being a PID. We have to show that $J = I$ is possible. We define the partial order

$$(J, B) \preceq (J', B') \Longleftrightarrow J \subset J' \text{ and } B \subset B'.$$

Given a linearly ordered subset T, an upper bound for T is $(\hat{J}, \hat{B})$ with

$$\hat{J} := \bigcup_{(J,B)\in T} J, \ \hat{B} := \bigcup_{(J,B)\in T} B.$$

Zorns lemma assures the existence of a maximal pair $(J_{\max}, B_{\max})$. So it suffices to show that there is above any (J, B) with $J \neq I$ some other pair. Take $j \in I \setminus J$ and $J' := J \cup \{j\}$. We have to find a corresponding $B' \supset B$. Look at the projection map

$$\mathrm{pr}_j : R[J'] \longrightarrow R, \ \sum_{i\in J'} \lambda_i e_i \mapsto \lambda_j.$$

Since R is a PID, we may choose $u \in N \cap R[J']$ with

$$R \geq \mathrm{pr}_j(N) = R \cdot \mathrm{pr}_i(u).$$

If $\mathrm{pr}_j(u) = 0$, take $B' = B$, otherwise $B' := B \cup \{u\}$. □

Proof of Th.14.4. We assume that there is no maximal element in M, but that every linearly ordered subset $T \subset M$ has an upper bound $\gamma(T) \in M$. So there is a function

$$\gamma : \mathrm{Lin}(M) \longrightarrow M$$

from the set $\mathrm{Lin}(M) \subset \mathcal{P}(M)$ of all subsets linearly ordered with respect to $\preceq$, such that $T \preceq \gamma(T)$. We may even assume that $\gamma(T)$ is a strict upper bound: $T \prec \gamma(T)$ or, equivalently $\gamma(T) \notin T$. If only $\gamma(T) \in T$ is possible, the element $\gamma(T)$ would be a maximal element for the entire set M.

Then we use the function γ in order to produce recursively a linearly ordered, indeed even well ordered, subset not admitting an upper bound, contrary to our hypothesis. We take $x_1 := \gamma(\emptyset)$ as its first element. If $x_1, ..., x_n$ are found one defines $x_{n+1} := \gamma(\{x_1, ..., x_n\})$. In this way we obtain

a sequence $(x_n)_{n\in\mathbb{N}}$ with $x_1 \prec x_2 \prec ...$, but the chain $\{x_n; n \in \mathbb{N}\}$ can be extended further: Take $y_1 := \gamma(\{x_n; n \in \mathbb{N}\})$, $y_2 := \gamma(\{y_1, x_n; n \in \mathbb{N}\})$.

In order to make sure that this idea really works, we introduce the concept of a "γ-chain": We shall call a subset $K \subset M$ a γ-chain, if $(K, \preceq)$ is well ordered and for any $y \in K$ the initial segment $K_{\prec y} := \{x \in K;\ x \prec y\}$ satisfies

$$y = \gamma(K_{\prec y}) \ .$$

We shall see that given two γ-chains K, L one of them is an initial segment of the other. Taking this for granted the set

$$T := \bigcup_{K\ \gamma\text{-chain}} K$$

is obviously a maximal γ-chain. On the other hand $\hat{T} := T \cup \{\gamma(T)\}$ is γ-chain as well, so $\hat{T} \subset T$ resp. $\gamma(T) \in T$ – a contradiction!

It remains to show that of two γ-chains K, L one is an initial segment of the other: Denote $K_0 = L_0$ the union of all sets which are initial segments of both K and L. Obviously it is an initial segment of both K and L. If $K_0 = K$ or $L_0 = L$, we are done; otherwise $K_0 = K_{\prec a}$ and $L_0 = L_{\prec b}$. In that case we have

$$a = \gamma(K_{\prec a}) = \gamma(L_{\prec b}) = b \in L \ ,$$

i.e., $K_{\preceq a} = L_{\preceq b}$ is an initial segment of both K and L, a contradiction! □

Remark 14.9. The above proof of Zorns lemma is a naive one. The most problematic part is the existence of the function

$$\gamma : \mathrm{Lin}(M) \longrightarrow M,$$

since in general there is no recipe for an explicit construction, the set $\mathrm{Lin}(M)$ being quite big. Instead one has to derive it from the

Axiom of Choice: *Given a family $(A_i)_{i\in I}$ of pairwise disjoint subsets $A_i \subset M$ of a set M, there is a set $A \subset M$ containing precisely one element out of each set $A_i, i \in I$, i.e., it has the form $A = \{x_i; i \in I\}$ with $x_i \in A_i$ for all $i \in I$.*

The axiom of choice, though looking quite harmless, has striking consequences, as for example the fact, that every set admits a well ordering. Indeed, no human being has up to now succeeded in well ordering the set of all real numbers.