Categories and Modules

Lecture Notes by

PD Dr. Jörg Zintl

Winter Term 2018/19 (Tübingen)

Version: April 2019

Contents

1 Categories

1.1 Definitions and examples

Category theory aims to provide a meta language for mathematics. In many cases, analogous constructions in different areas can be understood as instances of the same universal concept.

For the purpose of this lecture it is enough to take a small glimpse into the basics of this theory. Even though, we need to be careful about the formal foundations. Throughout, we presume a given set theory.

1.1 Lemma: Russel's Paradox. *There exists no set $\mathcal{S}$, which contains all sets as elements.*

Proof. Suppose that such a set $\mathcal{S}$ exists. Then by basic set theory we can define the subset

$$\mathcal{S}' := \{S \in \mathcal{S} : \ S \notin S\}.$$

Again, by basic set theory, it must either hold $\mathcal{S}' \in \mathcal{S}'$ or $\mathcal{S}' \notin \mathcal{S}'$. In the first case, when $\mathcal{S}' \in \mathcal{S}'$ holds, the definition of $\mathcal{S}'$ implies $\mathcal{S}' \notin \mathcal{S}'$, which is a contradiction. In the same way, we see that the second case leads to a contradiction. Therefore, our assumption on the existence of $\mathcal{S}$ cannot be true. □

1.2 Remark. A popular, but obviously non-mathematical version of Russel's paradox is the oxymoron: "*The set of all sets is not a set*".

As its formal set theoretical framework, general category theory uses the concept of a fixed given *universe* $\mathfrak{U}$, in which there exists a *class* $\mathcal{S}$ of all sets in $\mathfrak{U}$. See for example the discussion in [Mac, I.6] for details.

In this course, we will pretend[1] that classes are (slight generalizations of) sets, and we will talk about elements of classes, and maps between classes, and so on.

1.3 Definition. A *category* $\mathcal{C}$ consists of the following data:

(1) a class of *objects*, which is denoted by $\mathrm{Ob}(\mathcal{C})$;

[1] In fact, there is a formal justification for doing this: to any given universe $\mathfrak{U}$ and any given class $\mathcal{C}$ in $\mathfrak{U}$, there exists a larger universe $\mathfrak{U}'$ containing $\mathfrak{U}$, such that $\mathcal{C}$ is a set in $\mathfrak{U}'$.

(2) a pairwise disjoint family of classes of *morphisms*, which are denoted by $\mathrm{Mor}_{\mathcal{C}}(A,B)$, for pairs of objects $A,B \in \mathrm{Ob}(\mathcal{C})$;

(3) a family of *composition maps*

$$\mu_{A,B,C} : \mathrm{Mor}_{\mathcal{C}}(B,C) \times \mathrm{Mor}_{\mathcal{C}}(A,B) \to \mathrm{Mor}_{\mathcal{C}}(A,C),$$

for triples of objects $A,B,C \in \mathrm{Ob}(\mathcal{C})$, satisfying for all quadruples of objects $A,B,C,D \in \mathrm{Ob}(\mathcal{C})$ the *associativity law*

$$\mu_{A,B,D} \circ (\mu_{B,C,D} \times \mathrm{id}_{\mathrm{Mor}_{\mathcal{C}}(A,B)}) = \mu_{A,C,D} \circ (\mathrm{id}_{\mathrm{Mor}_{\mathcal{C}}(C,D)} \times \mu_{A,B,C});$$

(4) a family of *identity morphisms* $\mathrm{id}_B \in \mathrm{Mor}_{\mathcal{C}}(B,B)$, for $B \in \mathrm{Ob}(\mathcal{C})$, such that for all $A,C \in \mathrm{Ob}(\mathcal{C})$ and all morphisms $f \in \mathrm{Mor}_{\mathcal{C}}(A,B)$ and all morphisms $g \in \mathrm{Mor}_{\mathcal{C}}(B,C)$ the equalities $\mu_{A,B,B}(\mathrm{id}_B, f) = f$ and $\mu_{B,B,C}(g, \mathrm{id}_B) = g$ hold.

1.4 Notation. The set of all morphisms in $\mathcal{C}$ is denoted by

$$\mathrm{Mor}(\mathcal{C}) := \dot{\bigcup_{A,B \in \mathrm{Ob}(\mathcal{C})}} \mathrm{Mor}_{\mathcal{C}}(A,B).$$

A morphism $f \in \mathrm{Mor}_{\mathcal{C}}(A,B)$ is written as an *arrow*

$$f : A \to B \quad \text{or} \quad A \xrightarrow{f} B.$$

The object A is called the *domain* of f, and B its *codomain*. The composition $\mu_{A,B,C}(g,f) \in \mathrm{Mor}_{\mathcal{C}}(A,C)$ of f with some morphism $g \in \mathrm{Mor}_{\mathcal{C}}(B,C)$ is denoted by $g \circ f : A \to C$, and it is depicted as a composed arrow

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "g\circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

1.5 Remark: Commutative diagrams. A *commutative triangle* in a category $\mathcal{C}$ is a triple (f,g,h), where $f : A \to B$, $g : B \to C$ and $h : A \to C$ are morphisms in $\mathcal{C}$, such that $h = g \circ f$. It is visualized by the picture

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "h"'] & & B \arrow[dl, "g"] \\ & C & \end{tikzcd}$$

In this case, one says that the morphism $h : A \to C$ *factors through* B *via* f *and* g.

The reader will have no difficulties in generalizing this idea to diagrams involving more than three arrows. For example, the associativity law of axiom (3) of definition 1.3 is equivalent to the requirement, that for all morphisms $f : A \to B$, $g : B \to C$, and $h : C \to D$, the diagram

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "g\circ f"'] & B \arrow[d, "h\circ g"] \\ C \arrow[r, "h"'] & D \end{tikzcd}$$

is a *commutative square*, that is, the equation $(h \circ g) \circ f = h \circ (g \circ f)$ holds.

1.6 Example: The category (Set) **of sets.** The class of objects Ob (Set) of this category consists of all sets[2]. For two given sets X and Y, we define $\mathrm{Mor}_{(\mathrm{Set})}(X, Y)$ as the set (!) of all maps from X to Y. For three sets X, Y and Z, and maps $f : X \to Y$ and $g : Y \to Z$, we define $\mu_{X,Y,Z}(g, f) := g \circ f$ by the usual composition of maps, which is associative by construction.

Obviously, for any non-empty set X, there exists the identity morphism $\mathrm{id}_X : X \to X$, mapping each element of X to itself. For formal consistency, for the empty set $\emptyset$ we need to define $\mathrm{Mor}_{(\mathrm{Set})}(\emptyset, \emptyset) := \{\odot\}$. Here, $\{\odot\}$ denotes a set which contains exactly one element. This element then necessarily equals $\mathrm{id}_\emptyset$. For any non-empty set X, the set $\mathrm{Mor}_{(\mathrm{Set})}(\emptyset, X)$ also contains exactly one element, which can be interpreted as the inclusion map $\emptyset \subset X$, while the set $\mathrm{Mor}_{(\mathrm{Set})}(X, \emptyset)$ is empty.

1.7 Example. We define a category $\mathcal{C}$ as follows. The class of objects $\mathrm{Ob}(\mathcal{C})$ is given by the set of all intervals I of the real line $\mathbb{R}$. For two intervals $I, J \subseteq \mathbb{R}$, we define $\mathrm{Mor}_{\mathcal{C}}(I, J) := \{f : I \to \mathbb{R} : f \text{ differentiable, and } f(I) \subseteq J\}$. Note that it requires an (easy) proof to verify that the composition of two differentiable functions is again differentiable, and hence a morphism in $\mathcal{C}$.

Consider the functions $f_1 : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ and $f_2 : \mathbb{R}_{\geq 0} \to \mathbb{R}$, which are given by $f_1(x) := f_2(x) := x^2$ for $x \in \mathbb{R}_{\geq 0}$. By definition, they are two different morphisms in $\mathcal{C}$. This distinction makes sense. Indeed, they have different properties: f_1 is surjective, while f_2 is not. Note that f_1 is even bijective, with set theoretic inverse map f_1^{-1}. However, f_1^{-1} is not differentiable, so f_1 has no inverse in $\mathcal{C}$.

[2]More precisely, of all sets in our given universe $\mathfrak{U}$.

1.8 Example: The category (Gp) **of groups.** The class of objects Ob (Gp) is given by the class of all groups. For two groups G and H we define $\mathrm{Mor}_{\,(\mathrm{Gp})}(G,H) := \mathrm{Hom}(G,H)$ by the set of all group homomorphisms from G to H.

Clearly, for any group G, the identity map id_G is a group homomorphism, and therefore contained in $\mathrm{Mor}_{\,(\mathrm{Gp})}(G,G)$. The composition of two (composable) group homomorphisms is again a group homomorphism, and the composition of three group homomorphisms is associative, satisfying the axioms 1.3(3) and (4).

1.9 Remark. Analogously to the example 1.8, other categories are defined in the obvious way:

(Fld)	fields and field homomorphisms;
(Rng)	rings and ring homomorphisms;
(CRng)	commutative rings and their homomorphisms;
(Top)	topological spaces and continuous maps;
(Mfd)	differentiable manifolds and differentiable maps;
	$\vdots$

1.10 Definition. Let $\mathcal{C}$ be a category. A *subcategory of* $\mathcal{C}$ is a category $\mathcal{B}$, such that $\mathrm{Ob}\,(\mathcal{B}) \subseteq \mathrm{Ob}\,(\mathcal{C})$, and for all pairs of objects $A, B \in \mathrm{Ob}\,(\mathcal{B})$ holds $\mathrm{Mor}_{\,\mathcal{B}}(A,B) \subseteq \mathrm{Mor}_{\,\mathcal{C}}(A,B)$. It is called a *full subcategory*, if for all pairs of objects $A, B \in \mathrm{Ob}\,(\mathcal{B})$ holds the equality $\mathrm{Mor}_{\,\mathcal{B}}(A,B) = \mathrm{Mor}_{\,\mathcal{C}}(A,B)$.

1.11 Example: The category (Ab) **of Abelian groups.** By taking all Abelian groups as objects, together with all of their group homomorphisms as morphisms, we obtain a full subcategory of the category (Gp) of groups.

1.12 Example: The category (K-VS) **of vector spaces.** Let K be a given field. The category (K-VS) of vector spaces over K consists of all K-vector spaces, together with K-linear maps as morphisms.

We obtain the *full subcategory* (K-VS$_{finite}$) *of finite dimensional vector spaces* if we define Ob (K-VS$_{finite}$) as the class of only those K-vector spaces, which are of finite dimension over K. For two finite dimensional K-vector spaces V and W, we put $\mathrm{Mor}_{\,(K-\mathrm{VS}_{finite})}(V,W) := \mathrm{Mor}_{\,(K-\mathrm{VS})}(V,W)$.

Note that in general (K-VS) is not a subcategory of the category (Gp) of groups. Even though every vector space is a group by definition, there may be more[3] than one way in which a given group carries the structure of a vector space. Therefore, by “forgetting” the extra structure on the vector spaces, we get a map $\mathrm{Ob}\,(K\text{-VS}) \to \mathrm{Ob}\,(\mathrm{Gp})$, but in general this is not an inclusion. Compare also example 2.4 below.

1.13 Example. Let S be a set. We want to show that S can be interpreted as a category $\mathcal{S}$. To do this, we define $\mathrm{Ob}\,(\mathcal{S}) := S$. For any element $s \in S$ we define $\mathrm{Mor}_{\mathcal{S}}(s,s)$ as a set containing exactly one element, which shall be denoted by id_s. For any two elements $s,t \in S$ we define

$$\mathrm{Mor}_{\mathcal{S}}(s,t) := \begin{cases} \emptyset, & \text{if } s \neq t, \\ \{\mathrm{id}_s\}, & \text{if } s = t. \end{cases}$$

The composition of morphisms in $\mathcal{S}$ shall be defined in the obvious way.

Via this construction, any set can be interpreted as a category! This is a special instance of a general idea: very often category theory not only describes structures of a theory (set theory in this case) from the outside, but also incorporates and generalizes the theory itself.

1.14 Example. Let G be a given group, with composition $g * h \in G$ for a pair of elements $g,h \in G$. We define a category $\mathcal{G}$ as follows. Let $\mathrm{Ob}\,(\mathcal{G}) := \{\odot\}$ be a set containing exactly one element. As morphisms, we define $\mathrm{Mor}_{\mathcal{G}}(\odot,\odot) := G$, and the composition of morphisms be given by the composition in G. Since the composition in G is associative, axiom (3) of definition 1.3 is satisfied. For axiom (4), we define $\mathrm{id}_{\odot} := 1_G$ by the identity element of G. In this way, any group can be interpreted as a category with certain special properties.

1.15 Example: Orders. A category $\mathcal{C}$ is called an *order*, if for any pair of objects $a,b \in \mathrm{Ob}\,(\mathcal{C})$ the union

$$\mathrm{Mor}_{\mathcal{C}}(a,b) \cup \mathrm{Mor}_{\mathcal{C}}(b,a) = \{\odot\}$$

consists of exactly one element. Let $a \neq b$. Since the union is disjoint by definition, we must either have $\mathrm{Mor}_{\mathcal{C}}(a,b) = \{\odot\}$ and $\mathrm{Mor}_{\mathcal{C}}(b,a) = \emptyset$, or vice versa. In the first case, we denote the unique element by $(a \leq b) \in \mathrm{Mor}_{\mathcal{C}}(a,b)$.

[3] For example, the additive group $\mathbb{R} \times \mathbb{R}$ can viewed in (at least) two different ways as a vector space over $\mathbb{C}$.

For three objects $a, b, c \in \mathrm{Ob}\,(\mathcal{C})$ and morphisms $(a \leq b)$ and $(b \leq c)$, the composition axiom 1.3(3) becomes the *transitivity law*

$$(b \leq c) \circ (a \leq b) \;=\; (a \leq c).$$

Suppose that both morphisms $(a \leq b)$ and $(b \leq a)$ exist. Since $\mathrm{Mor}_{\mathcal{C}}(a,b) \cup \mathrm{Mor}_{\mathcal{C}}(b,a)$ contains only one element, it must hold $(a \leq b) = (b \leq a)$, which is true if and only if $a = b$.

For any set Z, which is ordered by an order relation "$\leq$", we can define an order $\mathcal{Z}$ by putting $\mathrm{Ob}\,(\mathcal{Z}) := Z$, and

$$\mathrm{Mor}_{\mathcal{Z}}(x,y) := \begin{cases} \emptyset, & \text{if } x \not\leq y, \\ \{\odot\}, & \text{if } x \leq y. \end{cases}$$

Since the sets of morphisms in $\mathcal{Z}$ need to be pairwise disjoint, we use the notation (!) $(x \leq y)$ for the unique element in $\mathrm{Mor}_{\mathcal{Z}}(x,y)$ if $x \leq y$.

1.16 Remark. The above examples show that the notion of a "morphism" in a category is very versatile, and it includes much more than only maps and functions!

1.2 Monomorphisms, epimorphisms, and isomorphisms

1.17 Definition. Let $\mathcal{C}$ be a category, and let $B, C \in \mathrm{Ob}\,(\mathcal{C})$ be objects.
(i) A morphism $g : B \to C$ is called a *monomorphism*, if for all pairs of morphisms $f, f' : A \to B$ the equality $g \circ f = g \circ f'$ implies $f = f'$.
(ii) A morphism $g : B \to C$ is called an *epimorphism*, if for all pairs of morphisms $h, h' : C \to D$ the equality $h \circ g = h' \circ g$ implies $h = h'$.
(iii) A morphism $g : B \to C$ is called an *isomorphism*, if there exists a morphism $f : C \to B$, such that $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_C$.

1.18 Definition. Two objects B and C of a category $\mathcal{C}$ are called *isomorphic*, if there exists an isomorphism $g : B \to C$. We then write $B \cong C$.

1.19 Remark. a) In other words, a morphism is a monomophism, if and only if it can be *canceled on the left*, and an epimorphism, if and only if it can be *canceled on the right.*
b) It is easy to see that "being isomorphic" constitutes an equivalence relation on $\mathrm{Ob}\,(\mathcal{C})$.

1.20 Exercise. Let $f : A \to B$ and $g : B \to C$ be morphisms in a category $\mathcal{C}$. Prove the following implications:

$$\begin{array}{lccc} (i) & g \circ f \text{ is a monomorphism} & \Rightarrow & f \text{ is a monomorphism,} \\ (ii) & g \circ f \text{ is an epimorphism} & \Rightarrow & g \text{ is an epimorphism,} \\ (iii) & g \text{ is an isomorphism} & \Rightarrow & g \text{ is a mono- and an epimorphism.} \end{array}$$

1.21 Proposition. *For all morphisms* $g \in \operatorname{Mor}(\mathrm{Set})$ *in the category of sets the following equivalences hold:*

$$\begin{array}{lccc} (i) & g \text{ is a monomorphism} & \Leftrightarrow & g \text{ is injective,} \\ (ii) & g \text{ is an epimorphism} & \Leftrightarrow & g \text{ is surjective,} \\ (ii) & g \text{ is an isomorphism} & \Leftrightarrow & g \text{ is bijective.} \end{array}$$

Proof. We will prove the first equivalence only, and leave the second one as an exercise to the reader. Equivalence *(iii)* is the well-known result, that a map is bijective if and only if it has a set theoretic inverse.

Suppose at first, that $g : Y \to Z$ is a monomorphism in (Set). Let $x, y \in Y$ such that $f(x) = f(y)$. Consider the set $X := \{x, y\}$. Let $i : X \to Y$ denote the inclusion map, and let $f : X \to Y$ denote the constant map with $f(x) := x$ and $f(y) := x$. Then clearly $g \circ f = g \circ i$. By the definition of a monomorphism, this implies $f = i$, and hence $x = y$. This establishes the injectivity of g.

Conversely, suppose that $g : Y \to Z$ is injective. Let $f, f' : X \to Y$ be morphisms in (Set), such that $g \circ f = g \circ f'$. By definition of the composition, for all $x \in X$ holds $g(f(x)) = g(f'(x))$. The injectivity of f implies for all $x \in X$ the equality $f(x) = f'(x)$, and thus $f = f'$. $\square$

1.22 Remark. In general, the equivalences of proposition 1.21 are misleading. First of all, there are categories, where the words "injective" and "surjective" have no meaningful definition. But even if these notions can be defined, they may not correlate to monomorphisms and epimorphisms, as example 1.23 below shows.

Recall also example 1.7, where we found a morphism, which was both injective and surjective, but not an isomorphism in the given category. In particular, a morphism, which is both a monomorphism and an epimorphism, needs not be an isomorphism.

1.23 Example. Let X be a set. The *power set* of X is defined as the set of all subsets of X, i.e. $\mathcal{P}(X) := \{Y : Y \subseteq X\}$. We define a category $\mathcal{X}$ by $\mathrm{Ob}\,(\mathcal{X}) := \mathcal{P}(X)$, and

$$\mathrm{Mor}_{\mathcal{X}}(U,V) := \begin{cases} \{i_{U,V} : U \hookrightarrow V \text{ inclusion map}\}, & \text{if } U \subseteq V \\ \emptyset, & \text{if } U \not\subseteq V. \end{cases}$$

Clearly there exists an identity morphism $\mathrm{id}_U := i_{U,U} \in \mathrm{Mor}_{\mathcal{X}}(U,U)$, as well as an associative composition $i_{V,W} \circ i_{U,V} := i_{U,W}$ for $U \subseteq V$ and $V \subseteq W$.

Since there is at most one morphism from any given object U to another object V in $\mathcal{X}$, the cancellation rules from remark 1.19 hold trivially. In particular, any morphism in $\mathcal{X}$ is both a monomorphism and an epimorphism.

On the other hand, suppose that $i_{U,V}$ is an isomorphism in $\mathcal{X}$. Then there exists a second morphism $i_{V,W}$ satisfying the identity $i_{V,W} \circ i_{U,V} = \mathrm{id}_U$. By definition, $i_{V,W} \circ i_{U,V} = i_{U,W}$, so we must have $U = W$. Since $U \subseteq V \subseteq W$, this implies $U = V$. Therefore, the isomorphisms in $\mathcal{X}$ are exactly the identity morphisms id_U.

The situation looks more familiar, if all morphisms in the category considered are group homomorphisms.

1.24 Proposition. *Let* (Gp) *be the category of groups. Then for all morphisms* $g \in \mathrm{Mor}\,(\mathrm{Gp})$ *the following equivalences hold:*

(*i*)	g is a monomorphism	$\Leftrightarrow$	g is injective,
(*ii*)	g is an epimorphism	$\Leftrightarrow$	g is surjective,
(*iii*)	g is an isomorphism	$\Leftrightarrow$	g is a mono- and an epimorphism.

Proof. The third equivalence follows from the first two. Indeed, if $g : G \to H$ is both a monomorphism and an epimorphism of groups, then it is bijective by (*i*) and (*ii*). Hence there exists a set-theoretic inverse map $g^{-1} : B \to A$. An easy standard argument in group theory shows that g^{-1} is again a group homomorphism, and hence a morphism in (Gp). Conversely, if g is an isomorphism, then it is a monomorphism and an epimorphism by exercise 1.20(*iii*).

We will now prove the first equivalence only, and leave the second one as an exercise to the reader.

To show the implication "$\Rightarrow$", let $g : G \to H$ be a monomorphism in (Gp). Put $K := \ker(g) \in \mathrm{Ob}\,(\mathrm{Gp})$, and consider the group homomorphisms

$$\begin{array}{cccc} f: & K & \to & G \\ & a & \mapsto & a \end{array} \quad \text{and} \quad \begin{array}{cccc} f': & K & \to & G \\ & a & \mapsto & 0_G \end{array}$$

which are the inclusion homomorphism f of K into G, and the constant morphism f' mapping K to the identity element $0_G \in G$. For all elements $a \in K$, we compute

$$g \circ f(a) = g(a) = 0_H \quad \text{and} \quad g \circ f'(a) = g(0_G) = 0_H.$$

Thus $g \circ f = g \circ f'$, and since g is assumed to be a monomorphism, we conclude $f = f'$. This implies $\ker(g) = \{0_G\}$, and hence g is injective.

Conversely for the implication "$\Leftarrow$", let $g : G \to H$ be an injective morphism. Let $f, f' : A \to G$ be group homomorphisms with $g \circ f = g \circ f'$. Thus for all $a \in A$ holds $g \circ f(a) = g \circ f'(a)$, and then $f(a) = f'(a)$ by the injectivity of g. Hence $f = f'$. □

1.25 Exercise. Prove that the equivalences of proposition 1.24 hold in the category $\mathrm{Ob}\,(K\text{-VS})$, for any field K, too.

The above exercise 1.25 explains, why in the theory of vector spaces, we learned to use the words monomorphism and injective map as synonyms, as well as epimorphism and surjective map. Compare also lemma 2.10 below.

1.3 Products and coproducts

1.26 Definition. Let $\mathcal{C}$ be a category. Let $a : A \to C$ and $b : B \to C$ be morphisms in $\mathcal{C}$. A *product of* a *and* b is a triple (P, p_a, p_b), where $P \in \mathrm{Ob}\,(\mathcal{C})$ is an object, and $p_a : P \to A$ and $p_b : P \to B$ are morphisms in $\mathcal{C}$, such that $a \circ p_a = b \circ p_b$, and which satisfies the following *universal property of products*:

For any triple (D, f, g), with $Z \in \mathrm{Ob}\,(\mathcal{C})$, and $f : D \to A$ and $g : D \to B$ such that $a \circ f = b \circ g$, there exists a unique morphism $d : D \to P$ in $\mathcal{C}$, such that the following diagram commutes:

$$\begin{tikzcd} D \arrow[dr, "d"] \arrow[drr, bend left, "g"] \arrow[ddr, bend right, "f"'] & & \\ & P \arrow[r, "p_b"'] \arrow[d, "p_a"] & B \arrow[d, "b"] \\ & A \arrow[r, "a"'] & C \end{tikzcd}$$

1.27 Remark. Note the conceptual twist of the above definition 1.26. A product is not defined directly by writing down concrete objects and morphisms, but indirectly by postulating certain properties.

This approach has its obvious charm: What we obtain is tailor-made with exactly the properties we desire. On the downside, it is by no means clear, that what we defined really exists. And even, if it exists, how well-described is it by the postulated properties? If the postulates are too generic, our definition will be of little use.

Here a second subtlety of the definition comes into play: the idea of a *universal property*. We require that *all* triples (D, f, g) in the category $\mathcal{C}$, which have the same basic property $a \circ f = b \circ g$, are related to the "universal triple" in a unique (!) way. This determines the product (almost) uniquely, as we see in the following proposition 1.28

1.28 Proposition. *Let $\mathcal{C}$ be a category, and let $a : A \to C$ and $b : B \to C$ be morphisms in $\mathcal{C}$. Let (P, p_a, p_b) and (P', p'_a, p'_b) be products of a and b. Then there exists an isomorphism $p : P \to P'$ such that $p_a = p'_a \circ p$ and $p_b = p'_b \circ p$, and this isomorphism is unique.*

Proof. Since (P, p_a, p_b) is a product of a and b, we have $a \circ p_a = b \circ p_b$. Since (P', p'_a, p'_b) is also a product, the universal property of (P', p'_a, p'_b) applied to the triple (P, p_a, p_b) implies the existence of a unique morphism $p : P \to P'$, such that the diagram

$$\begin{tikzcd}
P \arrow[dr, "p"] \arrow[drr, "p_b"] \arrow[ddr, "p_a"'] & & \\
& P' \arrow[r, "p'_b"'] \arrow[d, "p'_a"] & B \arrow[d, "b"] \\
& A \arrow[r, "a"'] & C
\end{tikzcd}$$

commutes. We claim that this morphism p is in fact an isomorphism.

To see this, we use in an analogous way as before the universal property of (P, p_a, p_b) applied to the triple (P', p'_a, p'_b). This implies the existence of a unique morphism $p' : P' \to P$, such that $p'_a = p_a \circ p'$ and $p'_b = p_b \circ p'$.

Therefore the composed diagram

$$\begin{tikzcd}
P' \arrow[dr, "p'"] \arrow[drrr, "p'_b"] \arrow[dddrr, swap, "p'_a"] & & & \\
& P \arrow[dr, "p"] \arrow[drr, "p_b"] \arrow[ddr, "p_a"] & & \\
& & P' \arrow[r, swap, "p'_b"] \arrow[d, "p'_a"] & B \arrow[d, "b"] \\
& & A \arrow[r, swap, "a"] & C
\end{tikzcd}$$

commutes. In particular, we have two commutative diagrams

$$\begin{tikzcd}
P' \arrow[dr, "p \circ p'"] \arrow[drr, "p'_b"] \arrow[ddr, swap, "p'_a"] & & \\
& P' \arrow[r, swap, "p'_b"] \arrow[d, "p'_a"] & B \arrow[d, "b"] \\
& A \arrow[r, swap, "a"] & C
\end{tikzcd}
\qquad \text{and} \qquad
\begin{tikzcd}
P' \arrow[dr, "\mathrm{id}_{P'}"] \arrow[drr, "p'_b"] \arrow[ddr, swap, "p'_a"] & & \\
& P' \arrow[r, swap, "p'_b"] \arrow[d, "p'_a"] & B \arrow[d, "b"] \\
& A \arrow[r, swap, "a"] & C
\end{tikzcd}$$

where the second one commutes trivially. Finally, by applying the universal property of (P', p'_a, p'_b) to (P', p'_a, p'_b) itself, we obtain the existence of a unique (!) morphism $\pi : P' \to P'$ making the above diagrams commute. Therefore we must have $p \circ p' = \pi = \mathrm{id}_{P'}$.

Analogously, we prove the identity $p' \circ p = \mathrm{id}_P$. This shows that $p : P \to P'$ is an isomorphism, and that it is the unique morphism which satisfies the property $p_a = p'_a \circ p$ and $p_b = p'_b \circ p$. □

1.29 Notation. It is established practice, presuming the Axiom of Choice, to fix for any pair of morphisms $a : A \to C$ and $b : B \to C$ in a category $\mathcal{C}$, for which a product of a and b exists, one product, which is then denoted by $(A \times_{a,C,b} B, p_a, p_b)$. Often, one just writes $A \times_C B$, and calls it the *fibre product of A and B over C*.

1.30 Example: Cartesian product. Consider the category (Set) of sets. As before, let $\{\odot\}$ denote a one-elemented set. Let A and B be sets, together with the unique constant maps $a : A \to \{\odot\}$ and $b : B \to \{\odot\}$.

We claim that up to bijections the product of a and b is given by the Cartesian product $A \times B$, together with the projection maps $p_1 : A \times B \to A$ and $p_2 : A \times B \to B$. Obviously, we have $a \circ p_1 = b \circ p_2$. Suppose we are given a set X, together with a pair of maps $f : X \to A$ and $g : X \to B$. (Note that for the composed maps $a \circ f : X \to \{\odot\}$ and $b \circ g : X \to \{\odot\}$ the equality $a \circ f = b \circ f$ is trivially satisfied.) We define a map $h : X \to A \times B$ by $h(x) := (f(x), g(x))$ for $x \in X$. Consider the diagram

$$\begin{tikzcd}
X \arrow[dr, "{(f,g)}"] \arrow[drr, "g"] \arrow[ddr, "f"'] & & \\
& A \times B \arrow[r, "p_2"'] \arrow[d, "p_1"] & B \arrow[d, "b"] \\
& A \arrow[r, "a"'] & \{\odot\}
\end{tikzcd}$$

It is clear that this map satisfies $p_1 \circ h = f$ and $p_2 \circ h = g$, and it is the unique map with this property.

1.31 Remark. Analogously to example 1.30, other well-known constructions can be identified as products, for example:

- $G \times H$, the *product group* for groups $G, H \in \mathrm{Ob}\,(\mathrm{Gp})$;
- $V \oplus W$, the *direct sum* for K-vector spaces $V, W \in \mathrm{Ob}\,(K\text{-VS})$;
- $A \cap B$, the *intersection* of subsets $A, B \subseteq S$ of some given $S \in \mathrm{Ob}\,(\mathrm{Set})$.

1.32 Example: Preimages and fibres. Consider again the category (Set) of sets. Let $f : X \to Y$ be a map, and let $U \subseteq Y$ be a subset.

We claim that for the set-theoretic preimage of U there exists a bijection

$$f^{-1}(U) \;\cong\; U \times_{i,Y,f} X,$$

where $i : U \to Y$ is the inclusion map. More explicitly, if $j : f^{-1}(U) \to X$ denotes the inclusion map, then we claim that the triple $(f^{-1}(U), f|f^{-1}(U), j)$ is a product of i and f.

We clearly have $i \circ f|f^{-1}(U) = f \circ j$. Suppose that we are given a set S, together with maps $h : S \to U$ and $g : S \to X$, such that $i \circ h = f \circ g$.

Then for all $s \in S$, we have $f(g(s)) = (f \circ g)(s) = (i \circ h)(s) = h(s) \in U$. In particular, for all $s \in S$ holds $g(s) \in f^{-1}(U)$. Therefore, the map

$$g' : S \to f^{-1}(U) \text{ with } g'(s) := g(s)$$

is well-defined, and it satisfies both equalities $j \circ g' = g$ and $f|f^{-1}(U) \circ g' = h$. The commutative diagram looks like this:

$$\begin{tikzcd}
S \arrow[dr, "g'"] \arrow[drr, "g"] \arrow[ddr, "h"'] & & \\
& f^{-1}(U) \arrow[r, "j"'] \arrow[d, "f|f^{-1}(U)"] & X \arrow[d, "f"] \\
& U \arrow[r, "i"'] & Y
\end{tikzcd}$$

The map g' is the unique map satisfying the above two equalities. Indeed, suppose that there is another such map $\gamma : S \to f^{-1}(U)$. Then the map γ satisfies in particular $j \circ \gamma = g = j \circ g'$. The inclusion map j is injective, so it is a monomorphism by proposition 1.21. Thus $\gamma = g'$.

A *fibre* over a point $y \in Y$ is by definition the preimage of the subset $\{y\} \subseteq Y$ with respect to f. From this, the name “fibred product” is derived.

Note that this construction can be used to *define* preimages of morphisms even in a category $\mathcal{C}$, where no set-theoretic preimages exists, provided that products always exist in that category.

1.33 Definition. Let $\mathcal{C}$ be a category. Let $a : C \to A$ and $b : C \to B$ be morphisms in $\mathcal{C}$. A *coproduct of a and b* is a triple (Q, q_a, q_b), where $Q \in \mathrm{Ob}(\mathcal{C})$ is an object, and $q_a : A \to Q$ and $q_b : B \to Q$ are morphisms in $\mathcal{C}$, such that $q_a \circ a = q_b \circ b$, and which satisfies the following *universal property of coproducts*:

For any triple (Z, f, g), with $Z \in \mathrm{Ob}(\mathcal{C})$, and $f : A \to Z$ and $g : B \to Z$ such that $f \circ a = g \circ b$, there exists a unique morphism $z : Q \to Z$ in $\mathcal{C}$, such that the following diagram commutes:

$$\begin{tikzcd}
C \arrow[r, "b"] \arrow[d, "a"'] & B \arrow[d, "q_b"'] \arrow[ddr, "g"] & \\
A \arrow[r, "q_a"] \arrow[drr, "f"'] & Q \arrow[dr, dashed, "z"] & \\
& & Z
\end{tikzcd}$$

1.34 Exercise. Show that coproducts are unique up to a unique isomorphism. Compare the proof of proposition 1.28.

1.35 Example: Disjoint union. Consider the category (Set) of sets. Let A and B be sets, together with the unique inclusion maps $a : \emptyset \to A$ and $b : \emptyset \to B$.

We claim that up to bijections the coproduct of a and b is given by the disjoint union $A\dot{\cup}B$, together with the inclusion maps $i : A \to A\dot{\cup}B$ and $j : B \to A\dot{\cup}B$. The identity $i \circ a = j \circ b$ is trivial. Suppose that we are given a set X, together with a pair of maps $f : A \to X$ and $g : B \to X$. (Again, the condition $f \circ a = g \circ b$ is empty.) We define a map

$$h : A\dot{\cup}B \to X \qquad \text{by } h(x) := \begin{cases} f(x), & \text{if } x \in A, \\ g(x), & \text{if } x \in B. \end{cases}$$

Consider the diagram

$$\begin{tikzcd}
\emptyset \arrow[r, "b"] \arrow[d, "a"'] & B \arrow[d, "j"'] \arrow[ddr, "g"] & \\
A \arrow[r, "i"] \arrow[drr, "f"'] & A\dot{\cup}B \arrow[dr, "h"] & \\
 & & X
\end{tikzcd}$$

It is clear that this map satisfies $h \circ i = f$ and $h \circ j = g$, and it is the unique map with this property.

1.36 Exercise. Show that in the category of vector spaces over a given field K the direct sum $V \oplus W$ of $V, W \in \mathrm{Ob}\,(K\text{-VS})$ is a coproduct.

1.37 Example: Quotients. Consider the category of sets, and let a set $X \in \mathrm{Ob}\,(\mathrm{Set})$ be fixed. Recall that an *equivalence relation* on X is a subset $R \subseteq X \times X$, such that for all elements $x, y, z \in X$ the following hold

$$\begin{array}{llcl} (i) & & & (x,x) \in R, \\ (ii) & (x,y) \in R & \Rightarrow & (y,x) \in R, \\ (iii) & (x,y) \in R,\ (y,z) \in R & \Rightarrow & (x,z) \in R. \end{array}$$

Two elements $x, y \in X$ are called *equivalent*, if $(x, y) \in R$. The *equivalence class* of an element $x \in X$ with respect to R is the set $[x] := \{y \in R : (x, y) \in$

$R\}$. The set of all equivalence classes is denoted by $X/R := \{[x] : x \in R\}$ and called the *quotient* of X modulo R. There is a canonical surjective *quotient map* $\pi : X \to X/R$ given by $\pi(x) := [x]$.

Let $p_1 : R \to X$ and $p_2 : R \to X$ denote the projections onto the first and second coordinate, respectively. We claim that $(X/R, \pi, \pi)$ is a coproduct of p_1 and p_2.

Let $(x, y) \in R$. Then $\pi \circ p_1(x, y) = [x]$ and $\pi \circ p_2(x, y) = [y]$. But $[x] = [y]$ by definition, since $(x, y) \in R$. This shows the identity $\pi \circ p_1 = \pi \circ p_2$. To prove the universal property, consider a set Z, together with a pair of maps $f : X \to Z$ and $g : X \to Z$ such that $f \circ p_1 = g \circ p_2$. Thus, for all $(x, y) \in R$ holds $f(x) = g(y)$. In particular, since for all $x \in X$ holds $(x, x) \in R$, we find $f(x) = g(x)$, and hence $f = g$. We now define a map

$$\overline{f} : X/R \to Z \qquad \text{by } \overline{f}([x]) := f(x).$$

First, we need to verify that this is well defined. Let $x' \in X$ be another representative with $[x'] = [x]$. Then $(x', x) \in R$. We compute $f(x') = f \circ p_1(x', x) = g \circ p_2(x', x) = g(x) = f(x)$, by the previous observation. Hence the definition of the map $\overline{f}$ is independent of the chosen representative.

It satisfies the identity $\overline{f} \circ \pi = f$ by definition, and hence also $\overline{f} \circ \pi = g$, since $f = g$. It is the unique map with this property. Indeed, suppose there exists another map $z : X/R \to Z$ such that $z \circ \pi = f$. Then $z \circ \pi = \overline{f} \circ \pi$. Since π is an epimorphism by proposition 1.21, we conclude $z = \overline{f}$.

The corresponding diagram looks like this:

$$\begin{tikzcd}
R \arrow[r, "p_2"] \arrow[d, "p_1"'] & X \arrow[d, "\pi"'] \arrow[ddr, "g=f"] & \\
X \arrow[r, "\pi"] \arrow[drr, "f"'] & X/R \arrow[dr, "\overline{f}"] & \\
 & & Z.
\end{tikzcd}$$

1.38 Remark. In fact, what we discussed in example 1.37, is the *universal property of the quotient*: For any map $f : X \to Z$, which satisfies $f(x) = f(y)$ for any equivalent $x, y \in X$, there exists a unique map $\overline{f} : X/R \to Z$ such that $f = \overline{z} \circ \pi$.

1.39 Definition. Let $\mathcal{C}$ be a category. Let $C \in \mathrm{Ob}(\mathcal{C})$, and let I be a set. Let $A_I := \{a_i : A_i \to C\}_{i \in I}$ be a family of morphisms in $\mathcal{C}$. A *product of* A_I is an object $P \in \mathrm{Ob}(\mathcal{C})$ together with a family of morphisms $\{p_i : P \to A_i\}_{i\in I}$, such that $a_i \circ p_i = a_j \circ p_j$ holds for all pairs $i, j \in I$, and which satisfies the following *universal property of products*:

For any family $\{f_i : D \to A_i\}_{i\in I}$, such that $f_i \circ p_i = f_j \circ p_j$ or all pairs $i, j \in I$, there exists a unique morphism $f : D \to P$ in $\mathcal{C}$, such that the following diagram commutes for all $i, j \in I$:

$$\begin{tikzcd}
D \arrow[dr, "f"] \arrow[drr, "f_j"] \arrow[ddr, "f_i"'] & & \\
& P \arrow[r, "p_j"'] \arrow[d, "p_i"] & A_j \arrow[d, "a_j"] \\
& A_i \arrow[r, "a_i"'] & C
\end{tikzcd}$$

1.40 Remark. a) The diagram in definition 1.39 is drawn in analogy to the case of families consisting of two morphisms as in definition 1.26. For the universal property of arbitrary products it suffices to require the identity $f_i = p_i \circ f$ for all $i \in I$.

b) The definition of a *coproduct* of a family $A_I := \{a_i : C \to A_i\}_{i\in I}$ of morphisms generalizing definition 1.33 is completely analogous. Furthermore, the uniqueness statements for products and coproducts, as in proposition 1.28, carry over in a straightforward way.

c) In talking about products and coproducts, very often the morphisms involved are left unmentioned (but not forgotten!). The established notation is

$$\prod_{i\in I} A_i \text{ for a product, and } \coprod_{i\in I} A_i \text{ for a coproduct.}$$

1.41 Example. Let K be a field, and (K-VS) be the category of vector spaces over K. For a family of vector spaces $\{V_i\}_{i\in I}$, the Cartesian product

$$\prod_{i\in I} V_i := \Big\{ \{v_i\}_{i\in I} : v_i \in V_i \Big\}$$

has in a natural way the structure of a K-vector space. By definition, the *direct sum* of the family is the K-subspace

$$\bigoplus_{i\in I} V_i := \Big\{ \{v_i\}_{i\in I} : v_i \in V \text{ and } \{i \in I : v_i \neq 0\} \text{ is finite} \Big\}.$$

Obviously both constructions agree for finite sets of indices I.

Let $O := \{0\}$ denote the trivial vector space. We can identify the family $\{V_i\}_{i\in I}$ as well with a family of constant K-linear maps $\{V_i \to O\}_{i\in I}$, as with a family of trivial inclusion homomorphisms $\{O \to V_i\}_{i\in I}$. It is straightforward to verify that with respect to these families, $\prod_{i\in I} V_i$ is a product, and $\bigoplus_{i\in I} V_i$ is a coproduct.

To get an idea, why product and coproduct behave differently, consider two families of K-linear maps $\{f_i : U \to V_i\}_{i\in I}$, and $\{g_i : V_i \to W\}_{i\in I}$, and the corresponding diagrams of the universal properties:

$$
\begin{tikzcd}
U \arrow[dr, "f"] \arrow[drr, "f_j"] \arrow[ddr, "f_i"'] & & \\
& \prod_{i\in I} V_i \arrow[r, "p_j"'] \arrow[d, "p_i"] & V_j \arrow[d] \\
& V_i \arrow[r] & O
\end{tikzcd}
\quad \text{and} \quad
\begin{tikzcd}
O \arrow[r] \arrow[d] & V_j \arrow[d, "e_j"] \arrow[ddr, "g_j"] & \\
V_i \arrow[r, "e_i"] \arrow[drr, "g_i"'] & \bigoplus_{i\in I} V_i \arrow[dr, "g"] & \\
& & W
\end{tikzcd}
$$

Here, p_i and e_i, for $i \in I$, denote the obvious projection and embedding homomorphisms.

In the case of the product, we need to verify for each vector $u \in U$ the condition $f_i(u) = p_i \circ f(u)$ for all $i \in I$ simultaneously. In the case of the coproduct, we need to verify for each single $i \in I$ that for any vector $v \in V_i$ the condition $g_i(v) = g \circ e_i(v)$ is satisfied.

In a certain sense, the product $\prod_{i\in I} V_i$ is the *largest* vector space, making the diagram of definition 1.39 commutative, while the coproduct $\bigoplus_{i\in I} V_i$ is the *smallest* vector space, that makes the corresponding diagram commutative.

2 Functors

2.1 Definitions and examples

2.1 Definition. Let $\mathcal{B}$ and $\mathcal{C}$ be categories. A *functor* $\mathbf{F}$ from $\mathcal{B}$ to $\mathcal{C}$ consists of the following data:

(1) a map of classes

$$F : \mathrm{Ob}\,(\mathcal{B}) \to \mathrm{Ob}\,(\mathcal{C})$$

(2) a family of maps of classes

$$F_{A,B} : \mathrm{Mor}_{\mathcal{B}}(A, B) \to \mathrm{Mor}_{\mathcal{C}}(F(A), F(B))$$

for all $A, B \in \mathrm{Ob}\,(\mathcal{B})$, such that

(3) for all $A \in \mathrm{Ob}\,(\mathcal{B})$ holds

$$F_{A,A}(\mathrm{id}_A) = \mathrm{id}_{F(A)}$$

(4) for all $A, B, C \in \mathrm{Ob}\,(\mathcal{B})$, $f \in \mathrm{Mor}_{\mathcal{B}}(A, B)$ and $g \in \mathrm{Mor}_{\mathcal{B}}(B, C)$ holds

$$F_{A,C}(g \circ f) = F_{B,C}(g) \circ F_{A,B}(f)$$

2.2 Remark. Note that in part (4) of definition 2.1, the symbol "$\circ$" stands on the left hand side of the equation for the composition in $\mathcal{B}$, while on the right hand side it stands for the composition in $\mathcal{C}$.

Our notation for a functor $\mathbf{F}$ from a category $\mathcal{B}$ to a category $\mathcal{C}$ will be

$$\begin{array}{rccc} \mathbf{F}: & \mathcal{B} & \to & \mathcal{C} \\ & B & \mapsto & F(B) \\ & f : B \to B' & \mapsto & F_{B,B'}(f) : F(B) \to F(B') \end{array}$$

where B and B' are objects in $\mathcal{B}$, and $f : B \to B'$ is a morphism in $\mathcal{B}$. Often we will simply write $F(f)$ instead of $F_{B,B'}(f)$ for the image of a morphism $f \in \mathrm{Mor}_{\mathcal{B}}(B, B')$.

2.3 Example. Let $n \in \mathbb{N}_{>0}$ be fixed. For any field $(K, +, \cdot)$, we have the multiplicative group of invertible square matrices $(\mathrm{Gl}_n(K), \cdot)$ of size n. In fact, this assignment is *functorial* in the following sense: We define a functor by

$$\begin{array}{rccc} \mathrm{Gl}_n : & (\mathrm{Fld}) & \to & (\mathrm{Gp}) \\ & (K,+,\cdot) & \mapsto & (\mathrm{Gl}_n(K),\cdot) \\ & \alpha & \mapsto & \tilde{\alpha} \end{array}$$

For a homomorphism of fields $\alpha : K \to L$ we define the morphism $\tilde{\alpha} := \mathrm{Gl}_n(\alpha)$ as follows. Consider an invertible matrix $A = (a_{ij})_{1\le i,j\le n} \in \mathrm{Gl}_n(K)$. For any $a_{ij} \in K$, we obtain $\alpha(a_{ij}) \in L$, and thus a quadratic matrix $\tilde{\alpha}(A) \in \mathrm{Mat}(n,n,L)$. Recall that the determinant map is a polynomial in the coefficients of the matrix, and α is a homomorphism of fields. So we compute

$$\det\left((\alpha(a_{ij}))_{1\le i,j\le n}\right) = \alpha(\det\left((a_{ij})_{1\le i,j\le n}\right)) \neq 0.$$

The last inequality follows, since $\det(A) \neq 0$ by assumption, and α is injective as a homomorphism of fields. In particular, $\tilde{\alpha}(A) \in \mathrm{Gl}_n(L)$, so $\tilde{\alpha}$ is indeed a map from $\mathrm{Gl}_n(K)$ to $\mathrm{Gl}_n(L)$.

To verify that $\tilde{\alpha}$ is in fact a morphism in (Gp), we still need to prove that it is a group homomorphism. Indeed, for $A, B \in \mathrm{Gl}_n(K)$, an elementary computation shows $\tilde{\alpha}(AB) = \tilde{\alpha}(A)\cdot\tilde{\alpha}(B)$.

It is easy to verify for a second homomorphism of fields $\beta : L \to M$ the functorial property $(\beta\circ\alpha)^{\sim} = \tilde{\beta}\circ\tilde{\alpha}$ for compositions.

2.4 Example: Forgetful Functors. As the name suggests, these functors "forget" certain structures on objects, reducing them to objects in a more elementary category.

For example, any field $(K,+,\cdot)$ carries as part of its definition the structure of an Abelian group $(K,+)$. Any homomorphism of fields is in particular a homomorphism of the underlying Abelian groups. We thus have as a special case of a forgetful functor:

$$\begin{array}{rccc} \mathbf{F} : & (\mathrm{Fld}) & \to & (\mathrm{Ab}) \\ & (K,+,\cdot) & \mapsto & (K,+) \\ & \alpha & \mapsto & \alpha \end{array}$$

2.5 Definition. Let $\mathbf{F} : \mathcal{B} \to \mathcal{C}$ be a functor. The functor $\mathbf{F}$ is called *full*, if for all $A, B \in \mathrm{Ob}\,(\mathcal{B})$ the map $F_{A,B}$ is surjective. The functor $\mathbf{F}$ is called *faithful*, if for all $A, B \in \mathrm{Ob}\,(\mathcal{B})$ the map $F_{A,B}$ is injective.

2.6 Example. Let $\mathcal{B}$ be a subcategory of $\mathcal{C}$. Then the in the obvious way defined *inclusion functor* $\mathbf{i} : \mathcal{B} \to \mathcal{C}$ is faithful. Moreover, $\mathcal{B}$ is a full subcategory if and only if $\mathbf{i}$ is full.

2.7 Exercise. Let $\mathbf{F} : \mathcal{B} \to \mathcal{C}$ be a functor, and let $f \in \mathrm{Mor}\,(\mathcal{B})$.

a) Show that $F(f)$ is an isomorphism, if f is an isomorphism.

b) Suppose that $\mathbf{F}$ is full and faithful. Show that $F(f)$ is an isomorphism if and only if f is an isomorphism.

2.8 Definition. A *faithful category over* (Set) is a pair $(\mathcal{C}, \mathbf{F})$ consisting of a category $\mathcal{C}$ and a faithful functor $\mathbf{F} : \mathcal{C} \to$ (Set). In this case, a morphism $f \in \mathrm{Mor}\,(\mathcal{C})$ is called *injective*, if $F(f)$ is injective in (Set), and *surjective*, if $F(f)$ is surjective in (Set).

2.9 Example. Using the respective forgetful functors, all of the categories (Gp), (Ab), (Rng), (CRng), (Fld), (K-VS) are faithful over (Set). With respect to the forgetful functors, the notions of injectivity and surjectivity of definition 2.8 agree with the standard definitions.

2.10 Lemma. *Let* $(\mathcal{C}, \mathbf{F})$ *be a faithful category over* (Set). *Let* $f \in \mathrm{Mor}\,(\mathcal{C})$ *be a morphism. If* f *is injective, then it is a monomorphism. If* f *is surjective, then it is an epimorphism.*

Proof. We prove only the first claim, and leave the second one to the reader as an exercise.

Suppose that $g : B \to C$ is an injective morphism in $\mathcal{C}$. Then, by definition, $F(g)$ is injective in (Set), so it is a monomorphism by proposition 1.21. Consider two morphisms $f, f' : A \to B$ in $\mathcal{C}$ such that $g \circ f = g \circ f'$. Applying the functor $\mathbf{F}$, we obtain $F(g) \circ F(f) = F(g) \circ F(f')$. Hence $F(f) = F(f')$, and thus $f = f'$, since $\mathbf{F}$ is faithful. □

2.11 Remark: Category (Cat) **of categories.** By now, we have become familiar with a fundamental trait of mathematics: in a first step, one introduces interesting new "objects", and in a second step one studies their interrelations, which are formulated as "morphisms".

It is only natural to apply this strategy to the definition of categories itself, viewing them as objects in a category, where the morphisms are given by functors.

Let $\mathcal{A}, \mathcal{B}, \mathcal{C}$ be categories. Let $\mathbf{F} : \mathcal{A} \to \mathcal{B}$ and $\mathbf{G} : \mathcal{B} \to \mathcal{C}$ be functors between them, given by families of maps F and F_{A_1,A_2}, or G and G_{B_1,B_2}, respectively, where $A_1, A_2 \in \mathrm{Ob}\,(\mathcal{A})$ and $B_1, B_2 \in \mathrm{Ob}\,(\mathcal{B})$. There is a natural composition of functors $\mathbf{G} \circ \mathbf{F}$, which is given by $G \circ F$ for objects, and $G_{F(A_1),F(A_2)} \circ F_{A_1,A_2}$, for morphisms, with $A_1, A_2 \in \mathrm{Ob}\,(\mathcal{A})$. This rule for composition is associative, and clearly there is an identity functor for each category.

In this way, we construct the *category of categories* (Cat), where the class of objects consists of all categories, and the respective class of morphisms $\mathrm{Mor}_{\,(\mathrm{Cat})}(\mathcal{A}, \mathcal{B})$ consists of all functors from $\mathcal{A}$ to $\mathcal{B}$.

2.2 Duality

The concept of *duality* is a deeply embedded into the framework of mathematical language.

2.12 Definition. Let $\mathcal{C}$ be a category. The *opposite category* $\mathcal{C}^{op}$ is defined by

(1) the class of objects
$$\mathrm{Ob}\,(\mathcal{C}^{op}) := \mathrm{Ob}\,(\mathcal{C}),$$

(2) the classes of morphisms, for all $A, B \in \mathrm{Ob}\,(\mathcal{C})$
$$\mathrm{Mor}_{\,\mathcal{C}^{op}}(A, B) := \mathrm{Mor}_{\,\mathcal{C}}(B, A)$$
(i.e. a morphism $f^o : A \to B$ in $\mathcal{C}^{op}$ is a morphism $f : B \to A$ in $\mathcal{C}$),

(3) the composition maps, for all $A, B, C \in \mathrm{Ob}\,(\mathcal{C}^{op})$
$$\mu^{op}_{A,B,C}(g^o, f^o) := \mu_{C,B,A}(f, g)^o$$
where $f^o \in \mathrm{Mor}_{\,\mathcal{C}^{op}}(A, B)$, and $g^o \in \mathrm{Mor}_{\,\mathcal{C}^{op}}(B, C)$,

(4) identity morphisms, for all $A \in \mathrm{Ob}\,(\mathcal{C}^{op})$
$$\mathrm{id}\,^o_A := \mathrm{id}\,_A.$$

2.13 Remark. In shorthand notation, the composition rule for morphisms $f^o : A \to B$ and $g^o : B \to C$ in $\mathcal{C}^{op}$ is written as
$$g^o \circ f^o = (f \circ g)^o$$

where we need to keep in mind that the composition "$\circ$" on the left hand side is meant to be taken in $\mathcal{C}^{op}$, and on the right hand side in $\mathcal{C}$.

Using diagrams, the composition rule for the opposite category is visualized as follows: A diagram in the category $\mathcal{C}^{op}$

$$\begin{tikzcd} A \arrow[r, "f^o"] \arrow[rr, bend right, "g^o \circ f^o"'] & B \arrow[r, "g^o"] & C \end{tikzcd}$$

corresponds in $\mathcal{C}$ to a diagram

$$\begin{tikzcd} A & B \arrow[l, "f"'] & C \arrow[l, "g"'] \arrow[ll, bend left, "f \circ g"] \end{tikzcd}$$

Clearly, we have $(\mathcal{C}^{op})^{op} = \mathcal{C}$. Therefore, for a morphism $f \in \mathrm{Mor}\,(\mathcal{C}^{op})$ we can also write $f^o \in \mathrm{Mor}\,(\mathcal{C})$ for the corresponding morphism in $\mathcal{C}$.

In practice, the superscript " ^{o} " is usually omitted, when the direction of the morphisms is clear from the context.

2.14 Proposition. *Let $\mathcal{C}$ be a category. Let $f : A \to C$ and $g : B \to C$ be morphisms in $\mathcal{C}$. Then the following equivalences hold:*

(i) f is a monomorphism in $\mathcal{C}$ $\Leftrightarrow$ f^o is an epimorphism in $\mathcal{C}^{op}$,

(ii) (P, p_a, p_b) is a product of f and g in $\mathcal{C}$ $\Leftrightarrow$ (P, p_a^o, p_b^o) is a coproduct of f^o and g^o in $\mathcal{C}^{op}$.

Proof. The proof follows immediately from the definitions. □

2.15 Remark. Let $\mathcal{C}$ be a category, and let $\mathcal{C}^{op}$ be its opposite category. The *duality* on $\mathcal{C}$ is defined by the assignment

$$\begin{array}{rccc} \mathbf{D}: & \mathcal{B} & \to & \mathcal{B}^{op} \\ & A & \mapsto & A \\ & f : A \to B & \mapsto & f^o : B \to A \end{array}$$

The duality $\mathbf{D}$ is not a functor. Indeed, for two morphisms $f : A \to B$ and $g : B \to C$ we compute from the composition rule of the opposite category

$$D_{A,C}(g \circ f) = (g \circ f)^o = f^o \circ g^o = D_{A,B}(f) \circ D_{B,C}(g).$$

2.16 Definition. Let $\mathcal{B}$ and $\mathcal{C}$ be categories. A *contravariant functor* from $\mathcal{B}$ to $\mathcal{C}$ is a functor

$$\mathbf{F}: \ \mathcal{B}^{op} \to \mathcal{C}.$$

2.17 Remark. a) For emphasis, a functor $\mathbf{F} : \mathcal{B} \to \mathcal{C}$ as in definition 2.1 is also called a *covariant functor*.

b) Let a contravariant functor $\mathbf{F} : \mathcal{B}^{op} \to \mathcal{C}$ be given. By composition with the duality on $\mathcal{B}$ from 2.15, it can be viewed as an assignment $\mathbf{F}^{op} := \mathbf{F} \circ \mathbf{D}$ with

$$\begin{array}{rccc} \mathbf{F}^{op}: & \mathcal{B} & \to & \mathcal{C} \\ & A & \mapsto & F(A) \\ & f : A \to B & \mapsto & F_{B,A}(f^o) : F(B) \to F(A). \end{array}$$

Recall that a morphism $f : A \to B$ in $\mathcal{B}$ is sent under the duality to the morphism $f^o : B \to A$ in $\mathcal{B}^{op}$. Therefore we have $F^{op}_{A,B}(f) = F_{B,A}(f^o) \in \mathrm{Mor}_{\mathcal{C}}(F(B), F(A))$.

For a second morphism $g : B \to C$ in $\mathcal{B}$, the composition $g \circ f : A \to C$ corresponds to a morphism $(g \circ f)^o : C \to A$ in $\mathcal{B}^{op}$. The composition rule for the covariant functor on $\mathcal{B}^{op}$ implies

$$F_{C,A}((g \circ f)^o) = F_{C,A}(f^o \circ g^o) = F_{B,A}(f^o) \circ F_{C,B}(g^o),$$

and hence,

$$F^{op}_{A,C}(g \circ f) = F^{op}_{A,B}(f) \circ F^{op}_{B,C}(g).$$

Summing things up: covariant functors preserve orientations and compositions, while covariant functors reverse both. In everyday mathematics, one simply writes $\mathbf{F} : \mathcal{B} \to \mathcal{C}$ instead of $\mathbf{F}^{op} : \mathcal{B}^{op} \to \mathcal{C}$ when the orientations of the arrows are clear from the context.

2.18 Example: The Mor-Functors.

Let $\mathcal{C}$ be a category, such that for all $A, B \in \mathrm{Ob}\,(\mathcal{C})$ the class $\mathrm{Mor}_{\mathcal{C}}(A, B)$ is a set. Let an object $A \in \mathrm{Ob}\,(\mathcal{C})$ be fixed.

a) We define the *covariant* Mor *-functor* by

$$\begin{array}{rccc} \mathrm{Mor}\,(A, \bullet): & \mathcal{C} & \to & (\mathrm{Set}) \\ & B & \mapsto & \mathrm{Mor}_{\mathcal{C}}(A, B) \\ & \alpha : B \to B' & \mapsto & \alpha_* : \mathrm{Mor}_{\mathcal{C}}(A, B) \to \mathrm{Mor}_{\mathcal{C}}(A, B') \end{array}$$

where we define for a morphism $\alpha : B \to B'$ and $f \in \mathrm{Mor}_{\mathcal{C}}(A, B)$ the image $\alpha_*(f) := \alpha \circ f \in \mathrm{Mor}_{\mathcal{C}}(A, B')$. Note that for a second morphism $\beta : B' \to B''$ we clearly have

$$(\beta \circ \alpha)_*(f) = \beta \circ \alpha \circ f = \beta_*(\alpha \circ f) = \beta_*(\alpha_*(f)) = \beta_* \circ \alpha_*(f).$$

Hence $(\beta \circ \alpha)_* = \beta_* \circ \alpha_*$, so $\mathrm{Mor}\,(A, \bullet)$ is indeed a functor.

b) We define the *contravariant* Mor *-functor* by

$$\begin{array}{rccc} \mathrm{Mor}\,(\bullet, A): & \mathcal{C} & \to & (\mathrm{Set}) \\ & B & \mapsto & \mathrm{Mor}_{\mathcal{C}}(B, A) \\ & \alpha : B \to B' & \mapsto & \alpha^* : \mathrm{Mor}_{\mathcal{C}}(B', A) \to \mathrm{Mor}_{\mathcal{C}}(B, A) \end{array}$$

where we define for a morphism $\alpha : B \to B'$ in $\mathcal{C}$ and $f \in \mathrm{Mor}_{\mathcal{C}}(B', A)$ the image $\alpha^*(f) := f \circ \alpha \in \mathrm{Mor}_{\mathcal{C}}(B, A)$. In this case, for a second morphism $\beta : B' \to B''$ in $\mathcal{C}$ we find

$$(\beta \circ \alpha)^*(f) = f \circ \beta \circ \alpha = \alpha^*(f \circ \beta) = \alpha^*(\beta^*(f)) = \alpha^* \circ \beta^*(f).$$

Hence $(\beta \circ \alpha)^* = \alpha^* \circ \beta^*$, so $\mathrm{Mor}\,(\bullet, A)$ is contravariant.

2.19 Exercise. Let $\mathcal{C} = (\mathrm{Gp})$ be the category of groups. For all groups $G, H \in \mathrm{Ob}\,(\mathrm{Gp})$, the set of morphisms $\mathrm{Mor}_{\,(\mathrm{Gp})}(G, H) = \mathrm{Hom}(G, H)$ has in a natural way the structure of a group. Construct analogously to the previous example 2.18 *covariant* and *contravariant* Hom-*functors* from (Gp) to (Gp) itself.

2.20 Example. Let K be a field, and consider the category (K-VS) of K-vector spaces. Consider K as a vector space over itself. Then the contravariant Mor-functor $\mathrm{Hom}_K(\bullet, K)$ assigns a vector space V to its dual vector space $V^* := \mathrm{Hom}_K(V, K)$. We obtain a contravariant functor

$$\begin{array}{rccc} \mathrm{Mor}\,(\bullet, K): & (K\text{-VS}) & \to & (K\text{-VS}) \\ & V & \mapsto & V^* \\ & V \xrightarrow{\varphi} W & \mapsto & W^* \xrightarrow{\varphi^*} V^* \end{array}$$

Exercise: Show that the assignment of V to its double dual V^{**} defines a functor.

2.3 Natural transformations

Inside the category of categories, we have a well-defined notion of isomorphism between categories. In practice, however, a weakened notion of "almost isomorphic" is more useful. We will make this precise in definition 2.28 below.

2.21 Definition: Natural transformation. Let $\mathbf{F}, \mathbf{G} : \mathcal{B} \to \mathcal{C}$ be two functors. A *natural transformation* $\eta : \mathbf{F} \Rightarrow \mathbf{G}$ *between* $\mathbf{F}$ *and* $\mathbf{G}$ is a family of morphisms $\eta = \{\eta_A\}_{A \in \mathrm{Ob}\,(\mathcal{B})}$, with $\eta_A \in \mathrm{Mor}_{\mathcal{C}}(\mathbf{F}(A), \mathbf{G}(A))$, such that for all morphisms $f : A \to B$ in $\mathcal{B}$ the diagram

$$\begin{tikzcd} F(A) \arrow[r, "\eta_A"] \arrow[d, "F(f)"'] & G(A) \arrow[d, "G(f)"] \\ F(B) \arrow[r, "\eta_B"'] & G(B) \end{tikzcd}$$

commutes.

2.22 Example. Let $n \in \mathbb{N}_{>0}$. Consider the functors

$$\begin{array}{rccc} \mathrm{Gl}_n : & (\mathrm{Fld}) & \to & (\mathrm{Gp}) \\ & (K,+,\cdot) & \mapsto & (\mathrm{Gl}_n(K),\cdot) \\ & \alpha & \mapsto & \tilde{\alpha} \end{array} \quad \text{and} \quad \begin{array}{rccc} \mathbf{U} : & (\mathrm{Fld}) & \to & (\mathrm{Gp}) \\ & (K,+,\cdot) & \mapsto & (K^*,\cdot) \\ & \alpha & \mapsto & \alpha|K^* \end{array}$$

For the second functor, $(K^*, \cdot)$ denotes the multiplicative group of units, and for the first functor compare example 2.3.

Let $\det_K : \mathrm{Gl}_n(K) \to K^*$ denote the determinant map on invertible matrices of size n over the field K. For any homomorphism of fields $\alpha : K \to L$, the diagram

$$\begin{tikzcd} \mathrm{Gl}_n(K) \arrow[r, "\det_K"] \arrow[d, "\tilde{\alpha}"'] & K^* \arrow[d, "\alpha|K^*"] \\ \mathrm{Gl}_n(L) \arrow[r, "\det_L"'] & L^* \end{tikzcd}$$

commutes. Thus the family of all determinants $\det := (\det_K)_{K \in \mathrm{Ob}\,(\mathrm{Fld})}$ constitutes a natural transformation of functors

$$\det : \quad \mathrm{Gl}_n \Rightarrow \mathbf{U}.$$

2.23 Remark: Functor category. Let $\mathcal{B}$ and $\mathcal{C}$ be categories, and let $\mathbf{F}, \mathbf{G}, \mathbf{H} : \mathcal{B} \to \mathcal{C}$ be functors. Let $\eta = \{\eta_A\}_{A \in \mathrm{Ob}\,(\mathcal{B})}$ and $\varrho = \{\varrho_A\}_{A \in \mathrm{Ob}\,(\mathcal{B})}$ define natural transformations $\eta : \mathbf{F} \Rightarrow \mathbf{G}$ and $\varrho : \mathbf{G} \Rightarrow \mathbf{H}$, respectively. Then there is a composition $\varrho \circ \eta : \mathbf{F} \Rightarrow \mathbf{H}$ of natural transformations, which is given by $\varrho \circ \eta := \{\varrho_A \circ \eta_A\}_{A \in \mathrm{Ob}\,(\mathcal{B})}$.

It is straightforward to verify that the class of functors $\mathrm{Mor}_{\,(\mathrm{Cat})}(\mathcal{B}, \mathcal{C})$ can in this way be equipped with the structure of a category, where the morphisms are natural transformations between functors. The resulting category is called the *functor category* of $\mathcal{B}$ and $\mathcal{C}$, and it is denoted by $\mathcal{M}or(\mathcal{B}, \mathcal{C})$.

2.24 Definition. Let $\mathcal{B}$ and $\mathcal{C}$ be categories. Two functors $\mathbf{F}, \mathbf{G} : \mathcal{B} \to \mathcal{C}$ are called *naturally equivalent*, if there exists a natural transformation η between $\mathbf{F}$ and $\mathbf{G}$, such that for all $A \in \mathrm{Ob}\,(\mathcal{B})$, the morphisms η_A are isomorphisms in $\mathcal{C}$. In this case, η is called a *natural equivalence*.

2.25 Remark. A natural equivalence of two functors $\mathbf{F}, \mathbf{G} : \mathcal{B} \to \mathcal{C}$ as defined above is in fact an isomorphism in the category $\mathcal{M}or(\mathcal{B}, \mathcal{C})$.

2.26 Example. Consider the category $(K\text{-VS})$ of vector spaces over a given field K. We define a functor by

$$\begin{array}{rccc} \mathbf{F} : & (K\text{-VS}) & \to & (K\text{-VS}) \\ & V & \mapsto & \mathrm{Hom}_K(K, V) \\ & \alpha & \mapsto & \alpha_* \end{array}$$

where for a K-linear map $\alpha : V \to W$ and an element $f \in \mathrm{Hom}_K(K, V)$ we put $\alpha_*(f) := \alpha \circ f \in \mathrm{Hom}_K(K, W)$. For a vector space V we define

$$\begin{array}{rccc} \varrho_V : & \mathrm{Hom}_K(K, V) & \to & V \\ & f & \mapsto & f(1_K) \end{array} \quad \text{and} \quad \begin{array}{rccc} \eta_V : & V & \to & \mathrm{Hom}_K(K, V) \\ & v & \mapsto & f_v \end{array}$$

where $f_v : K \to V$ is given by $f(k) := k \cdot v$. It is straightforward to see that these families define natural transformations $\varrho : \mathbf{F} \Rightarrow \mathrm{id}_{\,(K\text{-VS})}$ and $\eta : \mathrm{id}_{\,(K\text{-VS})} \Rightarrow \mathbf{F}$. Moreover, we have $\eta \circ \varrho = \mathrm{id}_{\,\mathrm{id}_{\,(K\text{-VS})}}$ and $\varrho \circ \eta = \mathrm{id}_{\,\mathbf{F}}$. In other words, via η and ϱ, the functors $\mathrm{id}_{\,(K\text{-VS})}$ and $\mathbf{F}$ are natural equivalent.

2.27 Remark: Canonical and natural isomorphisms. In the setting of example 2.26, we would like to comment on two bits of mathematical jargon. For a vector space V, the map $\varrho_V : \mathrm{Hom}_K(K, V) \to V$ from example

2.26 is called a *canonical morphism*. By this one means, that it is a morphism that "comes for free" with every object V, without any extra assumptions or choices involved.

Moreover, one says that the vector spaces V and $\mathrm{Hom}_K(K, V)$ are *naturally isomorphic*. This is more than to say that there exists an isomorphism between the two vector spaces. The word "naturally" indicates, that the isomorphisms for all varying vector spaces V are compatible.

For contrast, consider a finite dimensional K-vector space V of dimension $n \in \mathbb{N}$. Since V and K^n have the same dimension over K, they are isomorphic. However, this isomorphism depends on the choice of a basis of V, so it is not a canonical isomorphism. See the examples 2.29 and 2.31 below for a discussion of the naturality of this isomorphism.

2.28 Definition. Two categories $\mathcal{B}$ and $\mathcal{C}$ are called *naturally equivalent*, if there exists a pair of functors $\mathbf{F} : \mathcal{B} \to \mathcal{C}$ and $\mathbf{G} : \mathcal{C} \to \mathcal{B}$, such that for the composed functors there are natural equivalences $\mathbf{F} \circ \mathbf{G} \cong \mathrm{id}_{\mathcal{B}}$ and $\mathbf{G} \circ \mathbf{F} \cong \mathrm{id}_{\mathcal{C}}$.

2.29 Example. Let K be a field, and consider the category $(K\text{-VS}_{finite})$ of vector spaces of finite dimension over K. We define a category $(K\text{-VS}_{basis})$ as follows. The objects of this category are pairs $(V, \mathcal{B})$, where V is a finite dimensional K-vector space, and $\mathcal{B} \subset V$ is a basis. A morphism from an object $(V, \mathcal{B})$ to an object $(W, \mathcal{B}')$ is defined as a K-linear map $\alpha : V \to W$. In other words, we have $\mathrm{Mor}\,(K\text{-VS}_{basis}) = \mathrm{Mor}\,(K\text{-VS}_{finite})$. Clearly, there is a forgetful functor $\mathbf{F} : \mathrm{Mor}\,(K\text{-VS}_{basis}) \to \mathrm{Mor}\,(K\text{-VS}_{finite})$, which is full and faithful.

Now, for any finite dimensional K-vector space V we choose once and for all a basis $\mathcal{B}_V$. We thus obtain a (non-canonical) functor

$$\begin{array}{rccc} \mathbf{G}: & (K\text{-VS}_{finite}) & \to & (K\text{-VS}_{basis}) \\ & V & \mapsto & (V, \mathcal{B}_V) \\ & \alpha & \mapsto & \alpha \end{array}$$

Clearly, it holds $\mathbf{F} \circ \mathbf{G} = \mathrm{id}_{(K\text{-VS}_{finite})}$. Conversely, let $(V, \mathcal{B})$ be an object of the category $(K\text{-VS}_{basis})$. Then $G \circ F(V, \mathcal{B}) = (V, \mathcal{B}_V)$. Note that in particular $\mathbf{G} \circ \mathbf{F} \neq \mathrm{id}_{(K\text{-VS}_{basis})}$.

By definition, id_V is a morphism from $(V, \mathcal{B}_V)$ to $(V, \mathcal{B})$, and it is even an isomorphism. For any morphism α from $(V, \mathcal{B})$ to $(W, \mathcal{B}')$ in $(K\text{-VS}_{basis})$, the diagram

$$\begin{tikzcd}
G\circ F(V,\mathcal{B}) = (V,\mathcal{B}_V) \arrow[r, "\mathrm{id}_V"] \arrow[d, "G\circ F(\alpha)=\alpha"'] & (V,\mathcal{B}) \arrow[d, "\alpha"] \\
G\circ F(W,\mathcal{B}') = (W,\mathcal{B}_W) \arrow[r, "\mathrm{id}_W"'] & (W,\mathcal{B}')
\end{tikzcd}$$

commutes trivially. Hence the family $\{\mathrm{id}_V\}_{V\in\mathrm{Ob}\,(K\text{-VS}_{basis})}$ is a natural transformation $\mathbf{G}\circ\mathbf{F} \Rightarrow \mathrm{id}_{(K\text{-VS}_{basis})}$. It is even a natural equivalence, since all morphisms of the family are isomorphisms.

Summing things up, we see that the categories $(K\text{-VS}_{basis})$ and $(K\text{-VS}_{finite})$ are naturally equivalent via the forgetful functor. The categories are not isomorphic, since the map $F : \mathrm{Ob}\,(K\text{-VS}_{basis}) \to \mathrm{Ob}\,(K\text{-VS}_{finite})$ is not injective.

2.30 Theorem. *A functor $\mathbf{F} : \mathcal{B} \to \mathcal{C}$ is an equivalence of categories if and only if $\mathbf{F}$ is full and faithful, and for any object $C \in \mathrm{Ob}\,(\mathcal{C})$, there exists an object $B \in \mathrm{Ob}\,(\mathcal{B})$, such that $F(B) \cong C$.*

Proof. (i) First, let $\mathbf{F}$ be an equivalence of categories. So there exists a functor $\mathbf{G} : \mathcal{C} \to \mathcal{B}$, together with natural equivalences $\eta : \mathbf{F}\circ\mathbf{G} \Rightarrow \mathrm{id}_{\mathcal{C}}$ and $\varrho : \mathbf{G}\circ\mathbf{F} \Rightarrow \mathrm{id}_{\mathcal{B}}$. For any morphism $f : B \to B'$ in $\mathcal{B}$, and any morphism $g : C \to C'$ in $\mathcal{C}$ we have commutative diagrams

$$\begin{tikzcd}
G\circ F(B) \arrow[r, "\varrho_B"] \arrow[d, "G\circ F(f)"'] & B \arrow[d, "f"] \\
G\circ F(B') \arrow[r, "\varrho_{B'}"'] & B'
\end{tikzcd}
\quad \text{and} \quad
\begin{tikzcd}
F\circ G(C) \arrow[r, "\eta_C"] \arrow[d, "F\circ G(g)"'] & C \arrow[d, "g"] \\
F\circ G(C') \arrow[r, "\eta_{C'}"'] & C'
\end{tikzcd}$$

Note that for any object $C \in \mathrm{Ob}\,(\mathcal{C})$, we have the morphism $\mathrm{id}_C \in \mathrm{Mor}\,(\mathcal{C})$, and thus for $B := G(C) \in \mathrm{Ob}\,(\mathcal{B})$ an isomorphism $\eta_C : F(B) \to C$.

Let $f, f' : B \to B'$ be two morphisms in $\mathcal{B}$ with $F(f) = F(f')$. Then, by the left diagram above, we have $f = \varrho_{B'}\circ G(F(f))\circ\varrho_B^{-1} = \varrho_{B'}\circ G(F(f'))\circ\varrho_B^{-1} = f'$. This shows the injectivity of F on the level of morphisms, and hence $\mathbf{F}$ is faithful. The analogous argument shows that $\mathbf{G}$ is faithful, too.

Now let $B, B \in \mathrm{Ob}\,(\mathcal{B})$, and $g : F(B) \to F(B')$ be a morphism. We define $f : B \to B'$ as the composed morphism

$$B \xrightarrow{\varrho_B^{-1}} G\circ F(B) \xrightarrow{G(g)} G\circ F(B') \xrightarrow{\varrho_{B'}} B'.$$

The left diagram from above gives

$$G \circ F(f) = \varrho_{B'}^{-1} \circ f \circ \varrho_B = \varrho_{B'}^{-1} \circ (\varrho_{B'} \circ G(g) \circ \varrho_B^{-1}) \circ \varrho_B = G(g).$$

Since **G** is faithful, this implies $F(f) = g$. Hence **F** is full.

(ii) Conversely, suppose that **F** is full and faithful, and for any object $C \in \mathrm{Ob}\,(\mathcal{C})$, there exists an object $B_C \in \mathrm{Ob}\,(\mathcal{B})$, together with an isomorphism $\eta_C : F(B_C) \to C$. Let $g : C \to C'$ be a morphism in $\mathcal{C}$. Consider the composed morphism

$$F(B_C) \xrightarrow{\eta_C} C \xrightarrow{g} C' \xrightarrow{\eta_{C'}^{-1}} F(B_{C'}).$$

Since **F** is full and faithful, there exists a unique morphism $f_g : B_C \to B_{C'}$ such that $F(f_g) = \eta_{C'}^{-1} \circ g \circ \eta_C$. With this construction, we define

$$\begin{array}{cccc} \mathbf{G} : & \mathcal{C} & \to & \mathcal{B} \\ & C & \mapsto & B_C \\ & g : C \to C' & \mapsto & f_g : B_C \to B_{C'} \end{array}$$

We claim that **G** is a functor. It is clear that $G(\mathrm{id}_C) = \mathrm{id}_{B_C}$. For two composable morphisms $g : C \to C'$ and $g' : C' \to C''$ in $\mathcal{C}$ we compute

$$\begin{array}{rcl} F(G(g' \circ g)) & = & F(f_{g' \circ g}) \\ & = & \eta_{C''}^{-1} \circ (g' \circ g) \circ \eta_C \\ & = & \eta_{C''}^{-1} \circ g' \circ \eta_{C'} \circ \eta_{C'}^{-1} \circ g \circ \eta_C \\ & = & F(f_{g'}) \circ F(f_g) \\ & = & F(f_{g'} \circ f_g) \\ & = & F(G(g') \circ G(g)). \end{array}$$

Since **F** is faithful, we conclude $G(g' \circ g) = G(g') \circ G(g)$, showing the functoriality of **G**.

Now we claim that there is a natural equivalence $\eta : \mathbf{F} \circ \mathbf{G} \Rightarrow \mathrm{id}_{\mathcal{C}}$ given by $\eta := \{\eta_C\}_{C \in \mathrm{Ob}\,(\mathcal{C})}$. Indeed, for any morphism $g : C \to C'$ in $\mathcal{C}$, the diagram

$$\begin{tikzcd} F \circ G(C) = F(B_C) \arrow[r, "\eta_C"] \arrow[d, "F \circ G(g) = F(f_g)"'] & C \arrow[d, "g"] \\ F \circ G(C') = F(B_{C'}) \arrow[r, "\eta_{C'}"'] & C' \end{tikzcd}$$

is commutative by the definition of f_g. Hence η is a natural transformation, and invertible by definition.

To prove that $\mathbf{F}$ is an equivalence of categories, it only remains to show that there is a natural equivalence $\varrho : \mathbf{G} \circ \mathbf{F} \Rightarrow \mathrm{id}_{\mathcal{B}}$. To this end, we construct a family $\varrho := \{\varrho_B\}_{B \in \mathrm{Ob}(\mathcal{B})}$ as follows. For an object $B \in \mathrm{Ob}(\mathcal{B})$ holds $F(B) \in \mathrm{Ob}(\mathcal{C})$, and hence we have the isomorphism $\eta_{F(B)} : F(B_{F(B)}) \to F(B)$. By the definition of the functor $\mathbf{G}$, we have $B_{F(B)} = G(F(B))$, and hence $\eta_{F(B)} \in \mathrm{Mor}_{\mathcal{C}}(F(G(F(B))), F(B))$. Since the functor $\mathbf{F}$ is full and faithful, there exists a unique morphism $\varrho_B \in \mathrm{Mor}_{\mathcal{B}}(G(F(B)), B)$ such that $F(\varrho_B) = \eta_{F(B)}$. By exercise 2.7, ϱ_B is an isomorphism.

For a morphism $f : B \to B'$ in $\mathcal{B}$, we compute from the definition of the functor $\mathbf{G}$

$$F \circ G \circ F(f) = F(f_{F(f)}) = \eta^{-1}_{F(B')} \circ F(f) \circ \eta_{F(B)}.$$

Therefore the diagram

$$\begin{tikzcd}
F \circ G \circ F(B) \arrow[r, "\eta_{F(B)}"] \arrow[d, "F\circ G\circ F(f)"'] & F(B) \arrow[d, "F(f)"] \\
F \circ G \circ F(B') \arrow[r, "\eta_{F(B')}"'] & F(B')
\end{tikzcd}$$

is commutative. Since the functor $\mathbf{F}$ is faithful, the diagram

$$\begin{tikzcd}
G \circ F(B) \arrow[r, "\varrho_B"] \arrow[d, "G\circ F(f)"'] & B \arrow[d, "f"] \\
G \circ F(B') \arrow[r, "\varrho_{B'}"'] & B'
\end{tikzcd}$$

commutes, too. In particular, ϱ is a natural equivalence of functors. □

2.31 Example: Skeletons. Let K be a field. We define a category $\mathcal{S}$ by

$$\mathrm{Ob}(\mathcal{S}) := \{K^n : n \in \mathbb{N}\} \quad \text{and} \quad \mathrm{Mor}_{\mathcal{S}}(K^n, K^m) := \mathrm{Mat}(m, n, K).$$

Recall $K^0 = \{0\}$, and for $m = 0$, we define $\mathrm{Mat}(0, n, K) = \{(0, \ldots, 0)\}$, where $(0, \ldots, 0) \in \mathrm{Mat}(1, n, K)$ denotes the trivial matrix, and analogously for $n = 0$.

The composition of morphisms in $\mathcal{S}$ is given by the usual multiplication of matrices.

We define a functor on the category of finite dimensional K-vector spaces with bases by

$$\begin{array}{rccc} \mathbf{F}: & (K\text{-VS}_{basis}) & \to & \mathcal{S} \\ & V & \mapsto & K^{\dim_K(V)} \\ & \alpha : (V,\mathcal{B}) \to (W,\mathcal{B}') & \mapsto & M_{\mathcal{B},\mathcal{B}'} : K^{\dim_K(V)} \to K^{\dim_K(W)} \end{array}$$

where $M_{\mathcal{B},\mathcal{B}'}$ denotes the matrix representing the K-linear map $\alpha : V \to W$ with respect to the bases $\mathcal{B}$ and $\mathcal{B}'$.

By elementary Linear Algebra, the functor $\mathbf{F}$ is full and faithful. Any n-dimensional K-vector space V is (non-canonically) isomorphic to K^n. Hence by theorem 2.30, the functor $\mathbf{F}$ is an equivalence of categories.

In fact, by choosing for each $n \in \mathbb{N}$ the standard basis $\mathcal{E}_n$ for K^n, we can view $\mathcal{S}$ as a subcategory of $(K\text{-VS}_{basis})$. Then any finite dimensional K-vector space is isomorphic to exactly one object of $\mathcal{S}$. One says that the category $\mathcal{S}$ is a *skeleton* of $(K\text{-VS}_{basis})$.

Note that the isomorphism $(V,\mathcal{B}) \cong (K^{\dim_K(V)}, \mathcal{E}_{\dim_K(V)})$ is even natural in the sense of remark 2.27.

2.4 Adjunction

2.32 Definition. Let $\mathcal{A}$ and $\mathcal{B}$ be categories. The *product category* $\mathcal{A} \times \mathcal{B}$ has as its class of objects $\mathrm{Ob}\,(\mathcal{A} \times \mathcal{B}) := \mathrm{Ob}\,(\mathcal{A}) \times \mathrm{Ob}\,(\mathcal{B})$, and for pairs of objects $(A,B), (A',B') \in \mathrm{Ob}\,(\mathcal{A} \times \mathcal{B})$ we define

$$\mathrm{Mor}_{\mathcal{A}\times\mathcal{B}}((A,B),(A',B')) = \mathrm{Mor}_{\mathcal{A}}(A,A') \times \mathrm{Mor}_{\mathcal{B}}(B,B').$$

The composition of morphisms is defined in the obvious way in the components of the products.

2.33 Definition. Let $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ be categories. A *bifunctor* from $\mathcal{A}$ and $\mathcal{B}$ to $\mathcal{C}$ is a functor $\mathbf{H} : \mathcal{A} \times \mathcal{B} \to \mathcal{C}$.

2.34 Example. Let K be a field, and let $\mathcal{V} := (K\text{-VS})$ be the category of K-vector spaces. We define a bifunctor by

$$\begin{array}{rccc} \mathbf{H}: & \mathcal{V}^{op} \times \mathcal{V} & \to & \mathcal{V} \\ & (V,W) & \mapsto & \mathrm{Hom}_K(V,W) \\ & (\alpha^o,\beta) & \mapsto & \alpha^*\beta_* \end{array}$$

For a pair of K-linear maps $(\alpha^o : V \to V', \beta : W \to W')$ in $\mathcal{V}^{op} \times \mathcal{V}$, we obtain for any $\varphi \in \mathrm{Hom}_K(V, W)$ by composition

$$V' \xrightarrow{\alpha} V \xrightarrow{\varphi} W \xrightarrow{\beta} W'$$

which is a K-linear map $\alpha^* \beta_*(\varphi) \in \mathrm{Hom}_K(V', W')$. Note the commutativity relation $\alpha^* \beta_* = \beta_* \alpha^*$.

Usually the dual notation is avoided, so we write $(\alpha : V' \to V, \beta : W \to W')$ for a morphism in $\mathcal{V}^{op} \times \mathcal{V}$.

For composable morphisms $(\alpha_1 : V' \to V, \beta_1 : W \to W')$ and $(\alpha_2 : V'' \to V', \beta_2 : W' \to W'')$ one computes

$$\begin{aligned} H((\alpha_2, \beta_2) \circ (\alpha_1, \beta_1)) &= H(\alpha_1 \circ \alpha_2, \beta_2 \circ \beta_1) \\ &= (\alpha_1 \circ \alpha_2)^* (\beta_2 \circ \beta_1)_* \\ &= \alpha_2^* \circ \alpha_1^* \circ \beta_{2*} \circ \beta_{1*} \\ &= (\alpha_2^* \beta_{2*}) \circ (\alpha_1^* \beta_{1*}) \\ &= H(\alpha_2, \beta_2) \circ H(\alpha_1, \beta_1) \end{aligned}$$

so **H** is indeed a covariant functor.

2.35 Remark. One defines *natural transformations of bifunctors* $\mathbf{G}, \mathbf{H}$ from $\mathcal{A}$ and $\mathcal{B}$ to $\mathcal{C}$ simply as natural transformations on the underlying functors on the product category.

2.36 Definition. Let $\mathcal{B}$ and $\mathcal{C}$ be categories. Two functors $\mathbf{F} : \mathcal{B} \to \mathcal{C}$ and $\mathbf{G} : \mathcal{C} \to \mathcal{B}$ are called *adjoint*, if there exists a natural equivalence

$$\mathrm{Mor}_{\mathcal{C}}(\mathbf{F}(\bullet), \bullet) \cong \mathrm{Mor}_{\mathcal{B}}(\bullet, \mathbf{G}(\bullet))$$

of bifunctors from $\mathcal{B}^{op} \times \mathcal{C}$ to (Set). In this case, $\mathbf{F}$ is called a *left adjoint of* $\mathbf{G}$, and $\mathbf{G}$ a *right adjoint of* $\mathbf{F}$.

We will meet an example of a pair of adjoint functors in proposition **??** below.

3 Categories in Linear Algebra

3.1 Example. In Linear Algebra, we are mostly concerned with categories, where the morphisms are in particular homomorphisms of groups. A few examples of such categories are

(Ab)	Abelian groups and group homomorphisms
(Rng)	rings and homomorphisms of rings
(CRng)	commutative rings with one, ring homomorphisms with one
(Fld)	fields and field homomorphisms
(K-VS)	vector spaces over a field K, and K-linear maps
(R-Mod)	R-modules and R-module homomorphisms (see remark 4.16)

In this section we want to collect a few concepts from category theory, which are particularly useful for such categories.

3.1 Kernels and cokernels

3.2 Definition. Let $\mathcal{C}$ be a category.
(*i*) An object $T \in \mathrm{Ob}(\mathcal{C})$ is called a *terminal object*, if for all $A \in \mathrm{Ob}(\mathcal{C})$ there exists one and only one morphism $t_A : A \to T$.
(*ii*) An object $I \in \mathrm{Ob}(\mathcal{C})$ is called an *initial object*, if for all $A \in \mathrm{Ob}(\mathcal{C})$ there exists one and only one morphism $i_A : I \to A$.
(*iii*) An object $N \in \mathrm{Ob}(\mathcal{C})$ is called a *null object*, if it is both initial and terminal in $\mathcal{C}$.

3.3 Examples. a) The trivial group $\{0\}$ is a null object in both (Gp) and in (Ab).

b) For any field K, the trivial space $\{0\}$ is a null object in (K-VS).

c) The empty set $\emptyset$ is the unique initial object in the category (Set). Any one-pointed set $\{\odot\}$ is terminal.

d) In the category of fields (Fld), there is neither an initial nor a terminal object.

3.4 Remark. If an initial, terminal or null object exists, then it is unique up to a (unique) isomorphism (see also the proof of lemma 3.6 below). We shall denote a null object in a category $\mathcal{C}$ by $O_{\mathcal{C}}$.

3.5 Definition. Let $\mathcal{C}$ be a category, in which a null object $O_{\mathcal{C}}$ exists. Let $A, B \in \mathrm{Ob}\,(\mathcal{C})$. The composed morphism

$$\begin{tikzcd} A \arrow[r, "t_A"] \arrow[rr, bend right, "o_{A,B}"'] & O_{\mathcal{C}} \arrow[r, "i_B"] & B \end{tikzcd}$$

is called the *null morphism* $o_{A,B} : A \to B$.

3.6 Lemma. *The null morphism $o_{A,B}$ ist uniquely determined.*

Proof. Let O, O' be two null objects in $\mathcal{C}$. Consider the commutative diagram

$$\begin{tikzcd} & O \arrow[dr, "i"] \arrow[dd, shift right, "\nu"'] & \\ A \arrow[ur, "t"] \arrow[dr, "t'"'] & & B \\ & O' \arrow[ur, "i'"'] \arrow[uu, shift right, "\nu'"'] & \end{tikzcd}$$

Note that the defining property of null objects implies that all arrows in the above diagram are uniquely determined. It also implies that the two morphisms $\nu' \circ \nu : O \to O$ and $\mathrm{id}_O : O \to O$ must be identical. Therefore we compute

$$i' \circ t' = i \circ \nu' \circ \nu \circ t = i \circ t.$$

This verifies that the null morphism $o_{A,B}$ is independent of the choice a null object in $\mathcal{C}$. $\square$

3.7 Example. Let (Ab) be the category of Abelian groups, with the trivial group $O_{\mathcal{C}} := \{0\}$ as its unique null object. For any pair of Abelian groups G and H, the null morphism $o_{G,H} : G \to H$ is by definition the group homomorphism, which factors through the trivial group. Hence $o_{G,H}$ is the group homomorphism mapping constantly to the identity element $0_H \in H$.

3.8 Lemma. *Let $\mathcal{C}$ be a category with a null object O. Then for all objects $A, B \in \mathrm{Ob}\,(\mathcal{C})$ and all morphism $f : A \to B$ hold*

$$o_{B,O} \circ f = o_{A,O} \quad \text{and} \quad f \circ o_{O,A} = o_{O,B}.$$

Proof. By definition, O is a terminal object in $\mathcal{C}$. Thus the set of morphisms from B to O is $\mathrm{Mor}_{\mathcal{C}}(A, O) = \{t_A\}$, i.e. it contains exactly one element. In particular $o_{B,O} \circ f = t_A = o_{A,O}$. The second identity follows analogously from the fact, that O is an initial object. $\square$

3.9 Definition. Let $\mathcal{C}$ be a category with a null object. Let A and B be objects in $\mathcal{C}$, and let $f : A \to B$ be a morphism. A *kernel* of f is a morphism $k : K \to A$ in $\mathcal{C}$ such that

$$f \circ k = o_{K,B}$$

and satisfying the following *universal property of the kernel*:

For any morphism $d : D \to A$ in $\mathcal{C}$ with $f \circ d = o_{D,B}$, there exists a unique morphism $d' : D \to K$, such that the diagram

$$\begin{tikzcd} D \arrow[d, "d'"'] \arrow[dr, "d"] & & \\ K \arrow[r, "k"'] & A \arrow[r, "f"] & B \end{tikzcd}$$

commutes.

3.10 Lemma. *Let $k_1 : K_1 \to A$ and $k_2 : K_2 \to A$ be two kernels of a morphism $f : A \to B$ in $\mathcal{C}$. Then there exists a unique isomorphism $u : K_1 \to K_2$ such that $k_1 = k_2 \circ u$.*

Proof. Indeed, by the universal property of K_2 and K_1, there exist morphisms $k'_1 : K_1 \to K_2$ und $k'_2 : K_2 \to K_1$ in $\mathcal{C}$, such that $k_2 \circ k'_1 = k_1$ and $k_1 \circ k'_2 = k_2$. Hence

$$k_1 \circ (k'_2 \circ k'_1) = (k_1 \circ k'_2) \circ k'_1 = k_2 \circ k'_1 = k_1.$$

The universal property of K_1, applied to the diagram

$$\begin{tikzcd} K_1 \arrow[d, shift right, "k'_2 \circ k'_1"'] \arrow[d, shift left, "\mathrm{id}_{K_1}"] \arrow[drr, "k_1"] & & & \\ K_1 \arrow[rr, "k_1"'] & & A \arrow[r, "f"] & B \end{tikzcd}$$

implies the identity $k'_2 \circ k'_1 = \mathrm{id}_{K_1}$. Analogously, we obtain $k'_1 \circ k'_2 = \mathrm{id}_{K_2}$, so $u := k'_1$ is an isomorphism. Its uniqueness follows from the universal property of the kernel k_2. $\square$

3.11 Proposition. *Consider the category* (Gp) *of groups. Let $\alpha : G \to G'$ be a homomorphism of groups. Let* $\ker(\alpha)$ *denote the group-theoretical kernel of α, i.e. the subgroup of G given by* $\ker(\alpha) := \{g \in G : \alpha(g) = 0_{G'}\}$. *Let $\iota : \ker(\alpha) \to G$ denote the inclusion homomorphism. Then ι is a kernel of α in the sense of definition 3.9.*

Proof. The identity $\alpha \circ \iota = o_{\ker(\alpha),G'}$ is trivial by the definition of $\ker(\alpha)$, see example 3.7. It only remains to verify that ι satisfies the universal property of the kernel. Let H be a group, and let $\beta : H \to G$ be a group homomorphism such that $\alpha \circ \beta = o_{H,G'}$. The latter identity is equivalent to saying that for all $h \in H$ holds $\alpha \circ \beta(h) = 0_{G'}$. Hence for all $h \in H$ holds $\beta(h) \in \ker(\alpha)$. In particular, the map

$$\begin{array}{rccc} \beta' : & H & \to & G \\ & h & \mapsto & \beta(h) \end{array}$$

is well-defined, and a homomorphism of groups. It clearly satisfies $\beta = \iota \circ \beta'$. Note that the inclusion ι is a monomorphism, so β' is uniquely determined by this property. □

3.12 Remark. a) It follows from lemma 3.10 that for any kernel $k : K \to G$ of a group homomorphism $\alpha : G \to G'$ there exists a unique isomorphism $u : K \to \ker(\alpha)$ such that $k = \iota \circ u$.

b) Note that the proof of proposition 3.11 goes through without changes for other categories "over" the category (Gp), like for example categories of vector spaces, or any other category from example 3.1.

3.13 Definition. Let $\mathcal{C}$ be a category with a null object. Let A and B be objects in $\mathcal{C}$, and let $f : A \to B$ be a morphism. A *cokernel* of f is a morphism $q : B \to Q$ in $\mathcal{C}$ such that

$$q \circ f = o_{A,Q}$$

and satisfying the following *universal property of the cokernel*:

For all morphisms $d : B \to D$ in $\mathcal{C}$ with $d \circ f = o_{A,D}$, there exists a unique morphism $\overline{d} : Q \to D$, such that the diagram

$$\begin{tikzcd} & & D \\ A \arrow[r, "f"'] & B \arrow[ur, "d"] \arrow[r, "q"'] & Q \arrow[u, "\overline{d}"'] \end{tikzcd}$$

commutes.

3.14 Lemma. *Consider the category (Gp) of groups. Let $\alpha : G \to G'$ be a homomorphism of groups. Let $\mathrm{im}(\alpha)$ denote the group-theoretical image of α, i.e. the subgroup of G' given by $\mathrm{im}(\alpha) := \{\alpha(g) : g \in G\}$. Suppose that $\mathrm{im}(\alpha)$ is a normal subgroup of G'. Let $\pi : G' \to G'/\mathrm{im}(\alpha)$ denote the canonical quotient homomorphism. Then π is a cokernel in the sense of definition 3.13.*

Proof. The identity $\pi \circ \alpha = o_{G,G'/\mathrm{im}(\alpha)}$ is clear by the definition of $G'/\mathrm{im}(\alpha)$. Hence it suffices to verify the universal property for π. Suppose that H is a group, together with a group homomorphism $\varrho : G' \to H$ such that $\varrho \circ \alpha = o_{G,H}$. We define a map

$$\begin{array}{rccc} \overline{\varrho} : & G'/\mathrm{im}(\alpha) & \to & H \\ & [g'] & \mapsto & \varrho(g') \end{array}$$

where $g' \in G'$ is a representative of the equivalence class $[g'] \in G'/\mathrm{im}(\alpha)$. We claim that $\overline{\varrho}$ is well-defined. Indeed, let $g', g'' \in G'$ be two representatives of $[g']$. Then $g'' - g' \in \mathrm{im}(\alpha)$, so there exists some element $g \in G$ such that $\alpha(g) = g'' - g'$. Now we compute

$$\varrho(g'') = \varrho(g' + \alpha(g)) = \varrho(g') + \varrho \circ \alpha(g) = \varrho(g')$$

by the assumption on ϱ. Note that $\overline{\varrho}$ is a group homomorphism, and by construction the diagram

$$\begin{tikzcd} & & H \\ G \arrow[r, "\alpha"'] & G' \arrow[ur, "\varrho"] \arrow[r, "\pi"'] & G'/\mathrm{im}(\alpha) \arrow[u, "\overline{\varrho}"'] \end{tikzcd}$$

commutes. Since π is surjective, it is an epimorphism by lemma 2.10. Hence the identity $\varrho = \pi \circ \overline{\varrho}$ determines $\overline{\varrho}$ uniquely. □

3.15 Remark. Analogously to remark 3.12, for any cokernel $q : G' \to Q$ of a group homomorphism $\alpha : G \to G'$, such that the image is a normal subgroup, there exists a unique isomorphism $u : G'/\mathrm{im}(\alpha) \to Q$, such that for the canonical quotient morphism $\pi : G' \to G'/\mathrm{im}(\alpha)$ holds $q = u \circ \pi$.

Note that if $\mathrm{im}(\alpha)$ is not a normal subgroup, then the canonical quotient map $\pi : G' \to G'/\mathrm{im}(\varphi)$ is *not* a morphism in the category (Gp).

3.16 Lemma. *Let $\mathcal{C}$ be a category with a null object. Let $f : A \to B$ be a morphism in $\mathcal{C}$. Let $k : K \to A$ be a kernel and $q : B \to Q$ be a cokernel of f. Then k is a monomorphism, and q is an epimorphism.*

Proof. Let $h, h' : D \to K$ be two morphisms in $\mathcal{C}$ such that $k \circ h = k \circ h'$. To verify that k is a monomorphism, we need to show that $h = h'$. To do this, we put $d := k \circ h = k \circ h'$. We compute $f \circ d = f \circ k \circ h = o_{K,B} \circ h = o_{D,B}$. Now consider the diagram

$$\begin{tikzcd} D \arrow[d, shift right, "h'"'] \arrow[d, shift left, "h"] \arrow[dr, "d"] & & \\ K \arrow[r, "k"'] & A \arrow[r, "f"'] & B \end{tikzcd}$$

The universal property of the kernel k now implies $h = h'$.

The proof of the corresponding statement for q is left to the reader as an exercise. $\square$

3.17 Lemma. *Let $\mathcal{C}$ be a category with a null object O. Let $f : A \to B$ be a morphism in $\mathcal{C}$.*
a) *If f is a monomorphism, then $o_{O,A} : O \to A$ is a kernel of f.*
b) *If f is an epimorphism, then $o_{B,O} : B \to O$ is a cokernel of f.*

Proof. As usual, we only prove the first claim, leaving the second one as an exercise to the reader.

For the morphism f clearly holds $f \circ o_{O,A} = o_{O,B}$. To verify the universal property, we consider an arbitrary morphism $d : D \to A$ such that $f \circ d = o_{D,B}$. We also have the identity $f \circ o_{D,A} = o_{D,B}$. Since f is a monomorphism, we conclude $d = o_{D,A}$, and hence by the definition of the null morphism, $d = i_A \circ t_D$. Thus we have a commutative diagram

$$\begin{tikzcd} D \arrow[d, "t_D"'] \arrow[dr, "d"] & & \\ O \arrow[r, "i_A"'] & A \arrow[r, "f"'] & B \end{tikzcd}$$

Since O is a terminal, the uniqueness of t_D is trivial. $\square$

3.18 Lemma. *Let $\mathcal{C}$ be a category with a null object. Let $f : A \to B$ be a morphism in $\mathcal{C}$. A morphism $k : K \to A$ is a kernel of f in $\mathcal{C}$ if and only if $k^o : A \to K$ is a cokernel of $f^o : B \to A$ on $\mathcal{C}^{op}$.*

Proof. This follows immediately from the definitions. □

3.19 Remark. The above lemma 3.18 states that the dual notion of "kernel" is "cokernel", and *not* "image". In fact, the definition of an image is somehow subtle.

3.20 Definition. Let $\mathcal{C}$ be a category, and let $f : A \to B$ be a morphism in $\mathcal{C}$. An *image of f* is a monomorphism $i : I \to B$, such that there exists an epimorphism $f' : A \to I$, such that $f = i \circ f'$, which satisfies the *universal property of the image*:

For any pair consisting of a monomorphism $m : J \to B$ and an epimoprhism $e : A \to J$ in $\mathcal{C}$, such that $m \circ e = f$, there exists a morphism $u : I \to J$ such that the diagram

$$\begin{tikzcd} & J \arrow[dr, "m"] & \\ A \arrow[ur, "e"] \arrow[r, "f'"] \arrow[rr, bend right, "f"'] & I \arrow[u, "u"] \arrow[r, "i"] & B \end{tikzcd}$$

commutes, i.e. the identity $i = m \circ u$ holds.

3.21 Remark. In the situation of definition 3.20, a number of implications hold.

- the epimorphism f' is uniquely determined by i. Indeed, if $i \circ f'' = f = i \circ f'$, then $f'' = f'$ follows, since i is a monomorphism;
- the identity $i = m \circ u$ implies the identity $e = u \circ f'$. Indeed, it follows from $m \circ e = f = i \circ f' = m \circ u \circ f'$, since m is a monomorphism;
- the morphism u is uniquely determined by m. Indeed, if $m \circ u = i = m \circ u'$, then $u = u'$ follows, since m is a monomorphism;
- the morphism u is a monomorphism and an epimorphism. Indeed, this follows from exercise 1.20, since $u \circ f' = e$ is an epimorphism and $m \circ u = i$ is a monomorphism.

In some sense, the image of $f : A \to B$ should be thought of as the "smallest subobject" of B, through which f factors. As before, it is unique up to a unique isomorphism.

3.22 Lemma. *Consider the category* (Set) *of sets. Let $f : A \to B$ be a map of sets, and let $f(A) := \{f(a) : a \in A\}$ denote the set-theoretic image of f. Then the inclusion map $i : f(A) \to B$ is an image of f.*

Proof. Obviously, f factors through the well-defined map

$$\begin{array}{cccc} f' : & A & \to & f(A) \\ & a & \mapsto & f(a) \end{array}$$

as $f = i \circ f'$, with f' surjective, and i injective. Let $f = m \circ e$ be another factorization with a surjective map $e : A \to C$ and an injective map $m : C \to B$. For an element $b \in f(A)$, there exists an element $a \in A$, such that $f(a) = b$. Hence $m(e(a)) = b$, so $b \in m(C)$. Since m is injective, there exists a unique $c_b \in C$, such that $m(c_b) = b$. This defines a map

$$\begin{array}{cccc} u : & f(A) & \to & C \\ & b & \mapsto & c_b \end{array}$$

which satisfies $m \circ u = i$. □

3.23 Exercise. Define and discuss the dual notion of a "coimage".

3.2 *Ab*-categories

3.24 Definition. A category $\mathcal{C}$ is called an *Ab-category*, if for all $A, B \in \mathrm{Ob}\,(\mathcal{C})$ the set $\mathrm{Mor}_{\mathcal{C}}(A, B)$ is an Abelian group, and the composition is *bilinear* in the sense that for all morphisms $f, f' : A \to B$ and $g, g' : B \to C$ in $\mathcal{C}$ holds

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

For $A, B \in \mathrm{Ob}\,(\mathcal{C})$, we call the identity element $0_{A,B} \in \mathrm{Mor}_{\mathcal{C}}(A, B)$ of the Abelian group the *zero morphism* from A to B.

Examples of *Ab*-categories are in particular all categories of example 3.1.

3.25 Lemma. *Let $\mathcal{C}$ be an Ab-category. Then for all objects $A, B, C \in \mathrm{Ob}\,(\mathcal{C})$ and all morphisms $f : A \to B$ and $g : B \to C$ holds*

$$g \circ 0_{A,B} = 0_{A,C} \quad \text{and} \quad 0_{B,C} \circ f = 0_{A,C}.$$

Proof. For $g : B \to C$ we compute in the group $\mathrm{Mor}_{\mathcal{C}}(A, C)$

$$g \circ 0_{A,B} = g \circ (0_{A,B} + 0_{A,B}) = g \circ 0_{A,B} + g \circ 0_{A,B},$$

and hence $g \circ 0_{A,B} = 0_{A,C}$. The proof of the second equality is completely analogous. □

3.26 *Lemma.* *Let $\mathcal{C}$ be an Ab-category, in which a null object O exists. Then for all objects $A, B \in \mathrm{Ob}(\mathcal{C})$ holds for the null morphism $o_{A,B} = 0_{A,B}$.*

Proof. Since the identity element of a group is unique, it is enough to prove for all $A, B \in \mathrm{Ob}(\mathcal{C})$ the identity $o_{A,B} + o_{A,B} = o_{A,B}$.

Recall that by definition $o_{A,B} = i_B \circ t_A$ for the unique morphisms satisfying $\mathrm{Mor}_{\mathcal{C}}(A, O) = \{t_A\}$ and $\mathrm{Mor}_{\mathcal{C}}(O, B) = \{i_B\}$. Because these two groups are trivial, we must have $t_A = 0_{A,O}$ and $i_B = 0_{O,B}$. In particular, it holds $t_A + t_A = t_A$. Now we compute

$$o_{A,B} + o_{A,B} = i_B \circ t_A + i_B \circ t_A = i_B \circ (t_A + t_A) = i_B \circ t_A = o_{A,B}$$

as desired. □

3.27 *Proposition.* *Let $\mathcal{C}$ be an Ab-category, in which a null object O exists. Let $f : A \to B$ be a morphism in $\mathcal{C}$. The morphism f is*
a) *a monomorphism if, and only if $o_{O,A} : O \to A$ is a kernel of f.*
b) *an epimorphism if, and only if $o_{B,O} : B \to O$ is a cokernel of f.*

Proof. One direction of the implications has already been shown in lemma 3.17. We only prove assertion **a)**, while **b)** follows from duality.

Suppose that $o_{O,A} : O \to A$ is a kernel of f. Consider two morphisms $d, d' : D \to A$ such that $f \circ d = f \circ d'$. Using the group structure on $\mathrm{Mor}_{\mathcal{C}}(A, B)$ this is equivalent to the identity $f \circ (d - d') = 0_{D,B}$. Put $\Delta := d - d'$. By the universal property of the kernel, we have a commutative diagram

$$\begin{tikzcd}
D \arrow[d, "\Delta'"'] \arrow[dr, "\Delta"] & & \\
O \arrow[r, "o_{O,A}"'] & A \arrow[r, "f"'] & B
\end{tikzcd}$$

Since O is a null object, we have $o_{O,A} = i_A$ and $\Delta' = t_D$, and thus $\Delta = i_A \circ t_D = o_{D,A} = 0_{D,A}$, using lemma 3.26. This implies $d = d'$. □

3.3 Additive and exact functors

3.28 Definition. Let $\mathcal{B}$ and $\mathcal{C}$ be *Ab*-categories.

a) A functor $\mathbf{F} : \mathcal{B} \to \mathcal{C}$ is called *additive* if for all $A, B \in \mathrm{Ob}\,(\mathcal{B})$ and all $f, g \in \mathrm{Mor}_{\mathcal{B}}(A, B)$ holds $F(f+g) = F(f) + F(g)$.

b) An additive functor $\mathbf{F} : \mathcal{B} \to \mathcal{C}$ is called *left exact* if for all $A, B \in \mathrm{Ob}\,(\mathcal{B})$ and all $f \in \mathrm{Mor}_{\mathcal{B}}(A, B)$ and all kernels $k : K \to A$ of f holds that $F(k) : F(K) \to F(A)$ is a kernel of $F(f)$.

c) An additive functor $\mathbf{F} : \mathcal{B} \to \mathcal{C}$ is called *right exact* if for all $A, B \in \mathrm{Ob}\,(\mathcal{B})$ and all $f \in \mathrm{Mor}_{\mathcal{B}}(A, B)$ and all cokernels $q : B \to Q$ of f holds that $F(q) : F(B) \to F(Q)$ is a cokernel of $F(f)$.

b) An additive functor $\mathbf{F} : \mathcal{B} \to \mathcal{C}$ is called *exact* if it is both left exact and right exact.

3.29 Lemma. *Let* $\mathbf{F} : \mathcal{B} \to \mathcal{C}$ *be an additive functor between Ab-categories. Then for all objects* $A, B \in \mathrm{Ob}\,(\mathcal{C})$ *holds* $F(0_{A,B}) = 0_{F(A),F(B)}$.

Proof. We compute $F(0_{A,B}) = F(0_{A,B} + 0_{A,B}) = F(0_{A,B}) + F(0_{A,B})$, and hence the claim follows from the properties of groups. $\square$

3.30 Example. Let $\mathcal{B}$ be one of the categories of example 3.1, and hence in particular an *Ab*-category. Let $A \in \mathrm{Ob}\,(\mathcal{B})$ be fixed.

As in example 2.18 we consider the covariant Mor-functor defined by

$$\begin{array}{rccc} \mathbf{Mor}\,(A, \bullet) : & \mathcal{B} & \to & (\mathrm{Ab}) \\ & B & \mapsto & \mathrm{Mor}_{\mathcal{B}}(A, B) \\ & \alpha & \mapsto & \alpha_* \end{array} .$$

a) The functor $\mathbf{Mor}\,(A, \bullet)$ is additive.

Indeed, let $\alpha, \beta : B \to B'$ be morphisms in $\mathcal{B}$. Then $(\alpha+\beta)_* : \mathrm{Mor}_{\mathcal{B}}(A, B) \to \mathrm{Mor}_{\mathcal{B}}(A, B')$ is a morphism in (Ab). In particular, for any $\varphi \in \mathrm{Mor}_{\mathcal{B}}(A, B)$, we have a morphism $(\alpha + \beta)_*(\varphi) \in \mathrm{Mor}_{\mathcal{B}}(A, B')$. To understand this morphism, we need to consider for all elements $a \in A$ the image element $(\alpha + \beta)_*(\varphi)(a) \in B'$. We compute from the definitions

$$(\alpha+\beta)_*(\varphi)(a) = (\alpha+\beta) \circ \varphi(a) = \alpha \circ \varphi(a) + \beta \circ \varphi(a) = \alpha_*(\varphi)(a) + \beta_*(\varphi)(a).$$

From this we obtain the identity of morphisms in $\mathrm{Mor}_{\mathcal{B}}(A, B')$

$$(\alpha+\beta)_*(\varphi) = \alpha_*(\varphi) + \beta_*(\varphi) \quad \text{for all } \varphi \in \mathrm{Mor}_{\mathcal{B}}(A, B),$$

and therefore the identity of morphisms in (Ab)

$$(\alpha+\beta)_* = \alpha_* + \beta_*.$$

b) The functor $\mathbf{Mor}\,(A, \bullet)$ is left exact.

Indeed, consider a kernel $\kappa : K \to B$ of $\alpha : B \to B'$ in $\mathcal{B}$. By definition, we have $\alpha \circ \kappa = o_{K,B'}$. Hence by the functoriality of $\mathbf{F} := \mathbf{Mor}\,(A, \bullet)$ we obtain $F(\alpha) \circ F(\kappa) = F(\alpha \circ \kappa) = F(o_{K,B'}) = 0_{F(K),F(B')}$. So it only remains to verify the universal property for $F(\kappa)$. Let $\delta : D \to F(B)$ be a morphism in (Ab), such that $F(\alpha) \circ \delta = 0_{D,F(B')}$. In terms of diagrams, we have

$$\begin{tikzcd}
D \arrow[d, dotted, "?"'] \arrow[dr, "\delta"] & & \\
F(K) \arrow[r, "F(\kappa)"'] & F(B) \arrow[r, "F(\alpha)"'] & F(B')
\end{tikzcd}$$

We need to construct the dotted arrow as a unique morphism, which makes the diagram commutative. Let $d \in D$. Then $\delta(d) \in F(B) = \mathrm{Mor}_{\mathcal{B}}(A, B)$. So we have a diagram

$$\begin{tikzcd}
A \arrow[d, "u_d"'] \arrow[dr, "\delta(d)"] & & \\
K \arrow[r, "\kappa"'] & B \arrow[r, "\alpha"'] & B'
\end{tikzcd}$$

Note that the existence of the vertical morphism $u_d : D \to E$ follows from the universal property of the kernel, since we compute

$$\begin{array}{rclcl}
\alpha \circ \delta(d) & = & \alpha_*(\delta(d)) & = & F(\alpha)(\delta(d)) \\
 & = & F(\alpha) \circ \delta(d) & = & 0_{D,F(B')}(d) = 0_{F(B')} = 0_{A,B'}.
\end{array}$$

By construction, $u_d \in \mathrm{Mor}_{\mathcal{B}}(A, K) = F(K)$. This defines a map

$$\begin{array}{rccc}
u : & D & \to & F(K) \\
 & d & \mapsto & u_d
\end{array}$$

Note that u is indeed a morphism in (Ab). To see this, consider elements $d, d' \in D$. Then $u(d + d') \in F(K) = \mathrm{Mor}_{\mathcal{B}}(A, K)$. For all elements $a \in A$

we compute for their images in B

$$\begin{aligned}\kappa \circ u(d+d')(a) &= \kappa \circ u_{d+d'}(a) \\ &= \delta(d+d')(a) \\ &= \delta(d)(a) + \delta(d')(a) \\ &= \kappa \circ u_d(a) + \kappa \circ u_{d'}(a) \\ &= \kappa \circ (u(d) + u(d'))(a)\end{aligned}$$

Since κ is a monomorphism, we conclude $u(d+d') = u(d) + u(d')$.

The identity $F(\kappa) \circ u = \delta$ follows immediately from the construction of u. So it finally remains to show that u is the unique morphism satisfying this identity. Suppose that $F(\kappa) \circ u' = \delta$ holds for some morphism u' in (Ab). By definition, for all $d \in D$, we compute

$$\kappa \circ u'(d) = \kappa_*(u'(d)) = F(\kappa) \circ u'(d) = F(\kappa) \circ u(d) = \kappa_*(u(d)) = \kappa \circ u(d).$$

Hence $\kappa \circ u' = \kappa \circ u$, and the claim follows again from the fact, that κ is a monomorphism.

c) The functor **Mor** $(A, \bullet)$ is (in general) not right exact.

As a counter example, consider for a prime number $p \in \mathbb{N}$ the homomorphism of Abelian groups $\alpha : \mathbb{Z} \to \mathbb{Z}$ with $\alpha(a) := pa$. The canonical quotient map $\pi : \mathbb{Z} \to \mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$ is a cokernel of α by lemma 3.14

Consider the functor **Mor** $(A, \bullet)$ for $A := \mathbb{Z}_p$ on the category (Ab) of Abelian groups. The cokernel diagram

$$\mathbb{Z} \xrightarrow{\alpha} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_p$$

maps to the diagram

$$\mathrm{Hom}(\mathbb{Z}_p, \mathbb{Z}) \xrightarrow{\alpha_*} \mathrm{Hom}(\mathbb{Z}_p, \mathbb{Z}) \xrightarrow{\pi_*} \mathrm{Hom}(\mathbb{Z}_p, \mathbb{Z}_p)$$

It is easy to see that $\mathrm{Hom}(\mathbb{Z}_p, \mathbb{Z}) = \{0\}$, but $0 \neq \mathrm{id}_{\mathbb{Z}_p} \in \mathrm{Hom}(\mathbb{Z}_p, \mathbb{Z}_p)$. Therefore π_* is not surjective, and hence not a cokernel by lemma 3.16.

4 Modules

The theory of modules is a straightforward generalization of the theory of vector spaces. The basic idea is to replace the field of scalars, over which a vector space is defined, by a commutative ring. Since the concept of a commutative ring is less restrictive than that of a field, a far more versatile theory arises.

As pre-requisites for the understanding of this sections, we assume the theory of vector spaces over fields at the level of a standard introductory course. Furthermore, the reader should be familiar with the concept of groups, their homomorphisms and their quotients, including the groups of congruent numbers.

4.1 Definitions and examples

There is a rich and beautiful theory of rings. It is time well-spent to look into some of the many books on the subject. For our purposes, it will be enough to consider the special case of commutative rings.

4.1 Definition. A *commutative ring* is a triple $(R, +_R, \cdot_R)$, where

(1) $(R, +_R)$ is an Abelian group,

(2) $(R, \cdot_R)$ is a commutative semi-group with identity element $1_R \in R$,

such that for all $r, s, t \in R$ holds

(3) $(r +_R s) \cdot_R t = r \cdot_R t \; +_R \; s \cdot_R t$.

4.2 Remark. Sometimes a triple $(R, +_R, \cdot_R)$ as defined in 4.1 is more precisely called a *commutative ring with a multiplicative identity element.* Since we will only be concerned with commutative rings, where a multiplicative identity element exists, we include this as apart of our definition. See also the convention adopted in [Bou], and others.

Note that we need not include the multiplicative identity element $1_R \in R$ as part of the defining data. In fact, if a multiplicative identity element exists, it is necessarily unique, as the following lemma shows.

4.3 Lemma. *Let $(R, +_R, \cdot_R)$ be a commutative ring. Then for all $r, s \in R$ the following equalities hold:*

$$\begin{array}{lll} (i) & 0_R \cdot_R r & = & 0_R \\ (ii) & (-1_R) \cdot_R r & = & -r \\ (iii) & (-r) \cdot_R (-s) & = & r \cdot_R s. \end{array}$$

If $e \in R$ is an element, such that $e \cdot_R r = r$ holds for all $r \in R$, then $e = 1_R$.

Proof. To prove (i), we apply 4.1(3) and compute $0_R \cdot r = (0_R + 0_R) \cdot r = 0_R \cdot r + 0_R \cdot r$, and hence, since $(R, +_R)$ is a group, $0_R \cdot r = 0_R$. From this we obtain $0_R = (1_R - 1_R) \cdot r = 1_R \cdot r + (-1_R) \cdot r$, so that $(-1_R) \cdot r$ is the unique additive inverse to r. This shows (ii). Combining (ii) with the associativity and commutativity of $(R, \cdot_R)$ implies (iii).

Finally, if $r = e \cdot r$ holds for all $r \in R$, then we have in particular for $r = 1_R$ the equality $1_R = e \cdot 1_R = e$. □

4.4 Exercise. Let $(R, +_R, \cdot_R)$ be a commutative ring such that $1_R = 0_R$. Show that in this case the set R must be bijective to $\{0\}$.

4.5 Examples. **a)** The prototype of all commutative rings is the *ring of integers* $(\mathbb{Z}, +, \cdot)$. Analogously, there are the rings of rational, real and complex numbers, denoted by $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$, respectively. More generally, any field $(K, +, \cdot)$ is in particular a commutative ring.

b) Let $n \in \mathbb{N}$ be a fixed natural number. Then the set of congruent numbers modulo n inherits from the ring of integers the structure of a commutative ring $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$.

c) For any commutative ring $(R, +_R, \cdot_R)$, there is a commutative *ring of polynomials* $(R[X], +, \cdot)$.

d) Let $(R, +_R, \cdot_R)$ be a commutative ring, and let $n \in \mathbb{N}_{>0}$ be fixed. We define the set of *diagonal matrices* by

$$D_n(R) := \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \in \mathrm{Mat}(n, n, R) : \ a_{ij} = 0 \text{ for } i \neq j \right\}.$$

It is easy to see, using the usual addition and multiplication of matrices, that the triple $(D_n(R), +, \cdot)$ is a commutative ring, where the multiplicative identity element is the identity matrix in $\mathrm{Mat}(n, n, R)$.

4.6 Remark. Note that the last example 4.5d exhibits two key features, which make the theory of rings so much broader the theory of fields.

Clearly, as the multiplicative structure $(R, \cdot_R)$ of a given commutative ring $(R, +_R, \cdot_R)$ is only assumed to be a semi-group, we cannot expect to find for each element $r \in R$ a multiplicative inverse $s \in R$, such that $r \cdot_R s = 1_R$. The example of the integers shows how to handle this situation: by enlarging[4] the ring of integers $(\mathbb{Z}, +, \cdot)$ to the ring of rational numbers $(\mathbb{Q}, +, \cdot)$.

The second phenomenon has a more profound impact. In a commutative ring $(R, +_R, \cdot_R)$, there may (and in the case of example 4.5d, with $n \geq 2$ there always will) exist elements $r, s \in R$, which are both non-zero, but such that $r \cdot_R s = 0_R$. These *zero divisors* will have a significant effect on our considerations below.

4.7 Definition. A commutative ring $(R, +_R, \cdot_R)$ is called an *integral domain*, if $1_R \neq 0_R$, and for all pairs of elements $r, s \in R$ with $s \neq 0_R$, the equality $r \cdot_R s = 0_R$ implies $r = 0_R$.

4.8 Examples. a) The ring of integers $(\mathbb{Z}, +, \cdot)$ is an integral domain.

b) All fields $(K, +_K, \cdot_K)$ are integral domains.

c) The ring $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is an integral domain if and only if $n = 0$ or n is a prime number.

d) If $(R, +_R, \cdot_R)$ is an integral domain, then $(D_n(R), +, \cdot)$ is an integral domain if and only if $n = 1$.

4.9 Definition. Let $(R, +_R, \cdot_R)$ be a commutative ring. An *R-module* is a triple $(M, +_M, \lambda)$, where

(1) $(M, +_M)$ is an Abelian group,

(2) $\lambda : R \times M \to M$ is a map,

such that for all $r, s \in R$ and all $m, n \in M$ holds

$$\begin{array}{lrcl}
(3) & \lambda(r, m +_M m') & = & \lambda(r, m) +_M \lambda(r, m'); \\
(4) & \lambda(r +_R s, m) & = & \lambda(r, m) +_M \lambda(s, m); \\
(5) & \lambda(r \cdot_R s, m) & = & \lambda(r, \lambda(s, m)); \\
(6) & \lambda(1_R, m) & = & m.
\end{array}$$

4.10 Remark. The map $\lambda : R \times M \to M$ of definition 4.9 is called the *operation* of R on M. Usually, one writes for elements $r \in R$ and $m \in M$ shorter $r \cdot_M m := \lambda(r, m)$, or simply rm.

In general, when there is no danger of confusion, the indices of compositions and operations are omitted, both for commutative rings and modules.

[4] In algebra, this is the extension of the *integral domain* $\mathbb{Z}$ to its *field of fractions* $\mathbb{Q}$.

4.11 Lemma. *Let $(R, +_R, \cdot_R)$ be a commutative ring, and let $(M, +_M, \cdot_M)$ be an R-module. Then for all $r \in R$ and all $m \in M$ hold:*

$$\begin{array}{lllll} (i) & 0_R \cdot_M m & = & 0_M \\ (ii) & r \cdot_M 0_M & = & 0_M \\ (iii) & (-1_R) \cdot_M m & = & -m. \end{array}$$

Proof. The proof is analogous to the proof of lemma 4.3. $\square$

4.12 Examples. a) For any commutative ring $(R, +, \cdot)$, the triple $(R, +, \cdot)$ itself is an R-module.

b) Let $(K, +, \cdot)$ be a field. Then a triple $(M, +, \cdot)$ is a K-module if and only if $(M, +, \cdot)$ is a K-vector space.

c) For a commutative ring $(R, +, \cdot)$, let $R[X]$ denote the set of polynomials in X with coefficients in R. Using the obvious operation of R on $R[X]$, one obtains an R-module $(R[X], +, \cdot)$. Analogously, there is an R-module of formal power series $(R[[X]], +, \cdot)$.

d) Let $n \in \mathbb{N}_{>0}$ be fixed. For a commutative ring $(R, +, \cdot)$, we define

$$\begin{array}{rccc} \lambda : & D_n(R) \times \mathrm{Mat}(n, n, R) & \to & \mathrm{Mat}(n, n, R) \\ & (D, A) & \mapsto & DA \end{array}$$

by the multiplication of matrices. It is easy to verify that in this way $(\mathrm{Mat}(n, n, R), +, \lambda)$ is a $D_n(R)$-module.

4.13 Definition. a) Let $(R, +_R, \cdot_R)$ and $(S, +_S, \cdot_S)$ be commutative rings. A *homomorphism of commutative rings*

$$\varphi : \quad (R, +_R, \cdot_R) \to (S, +_S, \cdot_S)$$

is a homomorphism of groups $\varphi : (R, +_R) \to (S, +_S)$, such that $\varphi(1_R) = 1_S$, and for all $r, s \in R$ holds

$$\varphi(r \cdot_R s) = \varphi(r) \cdot_S \varphi(s).$$

b) Let $(R, +_R, \cdot_R)$ be a commutative ring. Let $(M, +_M, \cdot_M)$ and $(N, +_N, \cdot_N)$ be R-modules. A *homomorphism of R-modules*

$$\alpha : \quad (M, +_M, \cdot_M) \to (N, +_N, \cdot_N)$$

is a homomorphism of groups $\alpha : (M, +_M) \to (N, +_N)$, such that for all $r \in R$, and all $m \in M$ holds

$$\alpha(r \cdot_M m) = r \cdot_N \alpha(m).$$

The set of all such homomorphisms is denoted by $\mathrm{Hom}_R(M, N)$.

4.14 Remark. **a)** If $(K,+,\cdot)$ is a field, then a homomorphism of K-modules is called a *homomorphism of K-vector spaces.*

b) In analogy with the theory of vector spaces, a homomorphism of R-modules is also called an *R-linear map.* When the defining structures are clear from the context, an R-linear map $\alpha : (M,+_M,\cdot_M) \to (N,+_N,\cdot_N)$ is usualy simply written as $\alpha : M \to N$.

4.15 Lemma. *Compositions of homomorphisms of commutative rings are homomorphisms of commutative rings. Compositions of homomorphisms of R-modules are homomorphisms of R-modules.*

Proof. Straightforward. □

4.16 Remark. **a)** Commutative rings (by definition with multiplicative identity elements) together with their homomorphisms form a category (CR). The ring of integers $(\mathbb{Z},+,\cdot)$ is an initial object in (CR), and the trivial ring $(\{0\},+,\cdot)$ is a terminal object. In particular, there exists no null object.

b) For any commutative ring $(R,+_R,\cdot_R)$, there is a category (R-Mod) of R-modules and their homomorphisms. The *trivial R-module* $(\{0\},+,\cdot)$ is a null object in (R-Mod).

4.17 Remark. **a)** Let $(R,+_R,\cdot_R)$ be a commutative ring. For a pair of R-modules $(M,+_M,\cdot_M)$ and $(N,+_N,\cdot_N)$, consider the set $\mathrm{Hom}_R(M,N)$ of all homomorphisms from $(M,+_M,\cdot_M)$ to $(N,+_N,\cdot_N)$. By lemma 4.31, the triple $(\mathrm{Hom}_R(M,N),+_{pw},\cdot_{pw})$ is an R-module, where the compositions are defined point-wise.

b) Let $(L,+_L,\cdot_L)$ be another R-module. Consider two pairs of homomorphisms $\alpha,\alpha' \in \mathrm{Hom}_R(L,M)$ and $\beta,\beta' \in \mathrm{Hom}_R(M,N)$. For any $\ell \in L$ we compute

$$(\beta +_{pw} \beta') \circ (\alpha +_{pw} \alpha')(\ell) = (\beta +_{pw} \beta')((\alpha +_{pw} \alpha')(\ell))$$

$$\begin{aligned}
&= \beta((\alpha +_{pw} \alpha')(\ell)) +_N \beta'((\alpha +_{pw} \alpha')(\ell)) \\
&= \beta(\alpha(\ell) +_M \alpha'(\ell)) +_N \beta'(\alpha(\ell) +_M \alpha'(\ell)) \\
&= \beta(\alpha(\ell)) +_N \beta(\alpha'(\ell)) +_N \beta'(\alpha(\ell)) +_N \beta'(\alpha'(\ell)) \\
&= (\beta \circ \alpha +_{pw} \beta \circ \alpha' +_{pw} \beta' \circ \alpha +_{pw} \beta' \circ \alpha')(\ell).
\end{aligned}$$

Thus $(\beta +_{pw} \beta') \circ (\alpha +_{pw} \alpha') = \beta \circ \alpha +_{pw} \beta \circ \alpha' +_{pw} \beta' \circ \alpha +_{pw} \beta' \circ \alpha'$ holds as an identity of homomorphisms. In other words, the composition of homomorphisms of modules is bilinear in the sense of definition 3.24, and hence (R-Mod) is an *Ab*-category .

4.18 Exercise. **a)** Let $(R, +_R, \cdot_R)$ be a commutative ring. Construct a functor

$$\mathbf{F}: \quad (R\text{-Mod}) \to (\mathbb{Z}\text{-Mod}).$$

b) Show that any Abelian group $(G, +)$ can be equipped in a natural way with the structure of a $\mathbb{Z}$-module, and construct an isomorphism of categories

$$\mathbf{F}: \quad (\mathbb{Z}\text{-Mod}) \to (\text{Ab}).$$

4.19 Remark. **a)** Let $\varphi : (R, +_R, \cdot_R) \to (S, +_S, \cdot_S)$ be a homomorphism of commutative rings. Let $(M, +_M, \cdot_M)$ be an S-module. We define an operation of R on M by

$$\begin{array}{rccc} \cdot_\varphi : & R \times M & \to & M \\ & (r, m) & \mapsto & \varphi(r) \cdot_N m. \end{array}$$

It is easy to verify that in this way, the triple $(M, +_M, \cdot_\varphi)$ is an R-module. Moreover, consider a homomorphism of S-modules $\alpha : (M, +_M, \cdot_M) \to (N, +_N, \cdot_N)$. For any $r \in R$ and any $m \in M$ one computes

$$\alpha(r \cdot_\varphi m) = \alpha(\varphi(r) \cdot_M m) = \varphi(r) \cdot_N \alpha(m) = r \cdot_\varphi \alpha(m)$$

directly from the definition of $\cdot_\varphi$ and the S-linearity of α. This shows that α is in fact a homomorphism of R-modules. Summing things up, we obtain a functor

$$\begin{array}{rccc} \mathbf{F}_\varphi : & (S\text{-Mod}) & \to & (R\text{-Mod}) \\ & (M, +_M, \cdot_M) & \mapsto & (M, +_M, \cdot_\varphi) \\ & \alpha : (M, +_M, \cdot_M) \to (N, +_N, \cdot_N) & \mapsto & \alpha : (M, +_M, \cdot_\varphi) \to (N, +_N, \cdot_\varphi). \end{array}$$

b) More generally, the above construction induces a contravariant functor from the category of commutative rings into the category of categories:

$$\begin{array}{rccc} \mathbf{F} : & (\text{CR}) & \to & (\text{Cat}) \\ & (R, +_R, \cdot_R) & \mapsto & (R\text{-Mod}) \\ & \varphi : (R, +_R, \cdot_R) \to (S, +_S, \cdot_S) & \mapsto & \mathbf{F}_\varphi : (S\text{-Mod}) \to (R\text{-Mod}). \end{array}$$

4.2 Submodules and quotients

Throughout the rest of this section let $(R, +_R, \cdot_R)$ be a commutative ring.

4.20 Definition. Let $(M, +_M, \cdot_M)$ be an R-module. An *R-submodule* of $(M, +_M, \cdot_M)$ is an R-module $(N, +_N, \cdot_N)$, such that $(N, +_N)$ is a subgroup of $(M, +_M)$, and for all $(r, n) \in R \times N$ holds $r \cdot_N n = r \cdot_M n$.

4.21 Lemma. *Let $(M, +_M, \cdot_M)$ be an R-module. Let $(N, +_N)$ be a subgroup of $(M, +_M)$, and let $\cdot_N := \cdot_M|(R \times N)$ denote the restriction of the composition map. Then $(N, +_N, \cdot_N)$ is an R-submodule of $(M, +_M, \cdot_M)$ if and only if for all $r \in R$ and all $n \in N$ holds $r \cdot_M n \in N$.*

Proof. If $(N, +_N, \cdot_N)$ is an R-submodule, then by definition for all $r \in R$ and all $n \in N$ holds $r \cdot_M n = r \cdot_N n \in N$. Conversely, if $(N, +_N)$ is a subgroup of $(M, +_M)$, such that for all $r \in R$ and all $n \in N$ holds $r \cdot_M n \in N$, then the map $\cdot_N : R \times N \to N$ with $r \cdot_N n := r \cdot_M n$ is well-defined and an operation of R on N. The triple $(N, +_N, \cdot_N)$ satisfies all defining axioms of an R-module, since the triple $(M, +_M, \cdot_M)$ does. $\square$

4.22 Example. Let $\alpha : (M, +_M, \cdot_M) \to (N, +_N, \cdot_N)$ be a homomorphism of R-modules. By definition, $\alpha : (M, +_M) \to (N, +_N)$ is a homomorphism of groups, so there exists a kernel $(\ker(\alpha), +_{\ker(\alpha)})$ as a subgroup of $(M, +_M)$, with $\ker(\alpha) := \{m \in M : \alpha(m) = 0_N\}$. For any $r \in R$ and any $m \in \ker(\alpha)$ we compute $\alpha(r \cdot_M m) = r \cdot_N \alpha(m) = r \cdot_N 0_N = 0_N$, hence $r \cdot_M m \in \ker(\alpha)$. We can therefore define an operation

$$\cdot_{\ker(\alpha)} : \begin{array}{ccc} R \times \ker(\alpha) & \to & \ker(\alpha) \\ (r, m) & \mapsto & r \cdot_M m \end{array}$$

with which $(\ker(\alpha), +_{\ker(\alpha)}, \cdot_{\ker(\alpha)})$ becomes an R-module. We call this the *kernel of the homomorphism α of R-modules.*

4.23 Exercise. Show that the forgetful functor $\mathbf{F} : (R\text{-Mod}) \to (\mathrm{Ab})$ is faithful. Use this to prove that for a homomorphisms $\alpha : (M, +_M, \cdot_M) \to (N, +_N, \cdot_N)$ of R-modules the following are equivalent:

(*i*) α is injective;
(*ii*) α is a monomorphism;
(*iii*) $\ker(\alpha) = \{0_M\}$.

4.24 Example. Consider $(R, +_R, \cdot_R)$ itself as an R-module. Then an *ideal* of the ring $(R, +_R, \cdot_R)$ is defined as a submodule $(I, +_I, \cdot_I)$ of $(R, +_R, \cdot_R)$.

4.25 Example. Let $(R, +, \cdot)$ be an integral domain, and let $(M, +_M, \cdot_M)$ be an R-module. We define

$$T(M) := \{m \in M : \exists\, 0_R \neq r \in R \text{ such that } r \cdot_M m = 0_M\}.$$

It is easy to verify that this defines a submodule of $(M, +_M, \cdot_M)$, which is called the *R-torsion submodule of M*.

For example, if M is a vector space over a field, then $T(M) = \{0_M\}$. However, if $M = \mathbb{Z}/n\mathbb{Z}$, for some $n \in \mathbb{N}_{>0}$, considered as a $\mathbb{Z}$-module, then $T(M) = M$.

4.26 Remark. Let $(M, +_M, \cdot_M)$ be an R-module, and let $(N, +_N, \cdot_N)$ be a submodule. Since $(N, +_N)$ is a normal subgroup of $(M, +_M)$, the quotient group $(M/N, +_{M/N})$ exists. It is again an Abelian group, and the canonical quotient map $\pi : M \to M/N$ is a homomorphism of groups.

Let $r \in R$ and $m, m' \in M$ such that $m - m' \in N$. Then we compute

$$r \cdot_M m - r \cdot_M m' = r \cdot_N (m - m') \in N,$$

hence we obtain a well-defined operation

$$\begin{array}{rccc} \cdot_{M/N} : & R \times M/N & \to & M/N \\ & (r, [m]) & \mapsto & [r \cdot_M m] \end{array}$$

where as usual $[m] := \pi(M)$ denotes the equivalence class of an element $m \in M$. One verifies directly from the definitions that $(M/N, +_{M/N}, \cdot_{M/N})$ is an R-module, and the canonical quotient map $\pi : M \to M/N$ becomes a homomorphism of R-modules.

4.27 Definition. Let $(M, +_M, \cdot_M)$ be an R-module, and let $(N, +_N, \cdot_N)$ be a submodule. The *quotient module* of $(M, +_M, \cdot_M)$ by $(N, +_N, \cdot_N)$ is the R-module $(M/N, +_{M/N}, \cdot_{M/N})$.

4.28 Example. Let $\alpha : (M, +_M, \cdot_M) \to (N, +_N, \cdot_N)$ be a homomorphism of R-modules. By definition, $\alpha : (M, +_M) \to (N, +_N)$ is a homomorphism of groups, so there exists an image $(\mathrm{im}(\alpha), +_{\mathrm{im}(\alpha)})$ as a subgroup of $(N, +_N)$. Let $r \in R$ and $n \in \mathrm{im}(\alpha)$. By definition, there exists an $m \in M$, such that $\alpha(m) = n$. From this we compute $r \cdot_N n = r \cdot_N \alpha(m) = \alpha(r \cdot_M m) \in \mathrm{im}(\alpha)$. Therefore there is a well-defined operation

$$\begin{array}{rccc} \cdot_{\mathrm{im}(\alpha)} : & R \times \mathrm{im}(\alpha) & \to & \mathrm{im}(\alpha) \\ & (r, n) & \mapsto & r \cdot_N n \end{array}$$

with which $(\mathrm{im}(\alpha), +_{\mathrm{im}(\alpha)}, \cdot_{\mathrm{im}(\alpha)})$ becomes an R-module. We call this R-module the *image of the homomorphism α of R-modules*. The quotient module $(N/\mathrm{im}(\alpha), +_{N/\mathrm{im}(\alpha)}, \cdot_{N/\mathrm{im}(\alpha)})$ is called the *cokernel* of α, and denoted by $\mathrm{coker}(\alpha) := N/\mathrm{im}(\alpha)$.

4.29 Exercise. Prove that for a homomorphisms $\alpha : (M, +_M, \cdot_M) \to (N, +_N, \cdot_N)$ of R-modules the following are equivalent:

(*i*) α is surjective;
(*ii*) α is a epimorphism;
(*iii*) $\mathrm{coker}(\alpha) = \{[0_N]\}$.

4.30 Exercise. Show that kernels and cokernels of homomorphisms of modules correspond to kernels and cokernels in the categorical sense.

4.3 Dual modules

4.31 Lemma. *Let $(R, +_R, \cdot_R)$ be a commutative ring, and let $(M, +_M, \cdot_M)$ be an R-module. Let X be a set, and let $\mathrm{Map}(X, M) := \mathrm{Mor}_{(\mathrm{Set})}(X, M)$ denote the set of all maps from X to M. For any $r \in R$ and any pair of maps $\varphi, \psi \in \mathrm{Map}(X, M)$ we define maps "point-wise" by*

$$\begin{array}{rccc} \varphi +_{pw} \psi : & X & \to & M \\ & x & \mapsto & \varphi(x) +_M \psi(x) \end{array}$$

and

$$\begin{array}{rccc} r \cdot_{pw} \varphi : & X & \to & M \\ & x & \mapsto & r \cdot_M \varphi(x). \end{array}$$

Then the triple $(\mathrm{Map}(X, M), +_{pw}, \cdot_{pw})$ is an R-module, and

$$\begin{array}{rccc} \mathbf{Map}(\bullet, M) : & (\mathrm{Set}) & \to & (R\text{-Mod}) \\ & X & \mapsto & \mathrm{Map}(X, M) \\ & f : X \to Y & \mapsto & f^* : \mathrm{Map}(Y, M) \to \mathrm{Map}(X, M) \end{array}$$

is a contravariant functor, where for a map $f : X \to Y$ of sets, and a map $\varphi \in \mathrm{Map}(Y, M)$ holds $f^*(\varphi) := \varphi \circ f$.

Proof. Proving that $\mathrm{Map}(X, M)$, together with point-wise defined compositions, is an R-module is a standard exercise. Consider now a map $f : X \to Y$ of sets. For any $\varphi \in \mathrm{Map}(Y, M)$ clearly holds $f^*(\varphi) := \varphi \circ f \in \mathrm{Map}(X, M)$, so f^* is well-defined as a map of sets. To show that f^* is indeed defined in the "right" category, we need to verify that it is a homomorphism of R-modules.

To do this, let $r \in R$, and $\varphi, \psi \in \mathrm{Map}(Y, M)$. Then for all $x \in X$ holds by definition

$$\begin{aligned} f^*(\varphi +_{pw} \psi)(x) &= (\varphi +_{pw} \psi) \circ f(x) = (\varphi +_{pw} \psi)(f(x)) \\ &= \varphi(f(x)) +_M \psi(f(x)) = f^*(\varphi)(x) +_M f^*(\psi)(x) \\ &= (f^*(\varphi) +_{pw} f^*(\psi))(x), \end{aligned}$$

and hence $f^*(\varphi +_{pw} \psi) = f^*(\varphi) +_{pw} f^*(\psi)$ as maps. An analogous computation shows $f^*(r \cdot_{pw} \varphi) = r \cdot_{pw} f^*(\varphi)$. Thus f^* is a homomorphism of R-modules.

We still need to verify that the assignment of morphisms through $\mathbf{Map}(\bullet, M)$ is functorial. Consider a pair of maps $f : X \to Y$ and $g : Y \to Z$ in (Set). As in the case of the contravariant **Mor**-functor in example 2.18, one finds the identity $(g \circ f)^* = f^* \circ g^*$. □

By composing the Map-functor from lemma 4.31 with the forgetful functor $\mathbf{F} : (R\text{-Mod}) \to (\text{Set})$, we obtain a contravariant functor from the category of R-modules to itself.

4.32 Definition. Let $(M, +_M, \cdot_M)$ be an R-module. The *contravariant* Hom-*functor* associated to M is given by

$$\begin{array}{rccc} \mathbf{Hom}(\bullet, M): & (R\text{-Mod}) & \to & (R\text{-Mod}) \\ & N & \mapsto & \mathrm{Hom}_R(N, M) \\ & \alpha : N \to N' & \mapsto & \alpha^* : \mathrm{Hom}_R(N', M) \to \mathrm{Hom}_R(N, M) \end{array}$$

with $\alpha^*(\varphi) := \varphi \circ \alpha$ for all $\alpha \in \mathrm{Hom}_R(N, N')$ and $\varphi \in \mathrm{Hom}_R(N', M)$.

4.33 Remark. Note that the Hom-functor is additive: for any pair of homomorphisms $\alpha, \beta : N \to N'$ of R-modules holds $(\alpha +_{pw} \beta)^* = \alpha^* +_{pw} \beta^*$.

A special case of the Hom-functor is obtained, when one considers in place of the R-module M the module $M := R$ itself.

4.34 Definition. Let $(N, +_N, \cdot_N)$ be an R-module. The *dual module* of $(N, +_N, \cdot_N)$ is the R-module $(\mathrm{Hom}_R(N, R), +_{pw}, \cdot_{pw})$. It is denoted by

$$N^* := \mathrm{Hom}_R(N, R).$$

4.35 Examples. a) Consider $(\mathbb{Z}, +, \cdot)$ as $\mathbb{Z}$-module. Let $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z})$. For any $a \in \mathbb{Z}$ holds $\varphi(a) = a \cdot \varphi(1)$. Hence the homomorphism φ is uniquely determined by its value on 1, which can be any element of $\mathbb{Z}$. We thus obtain an isomorphism of $\mathbb{Z}$-modules

$$\mathbb{Z}^* \cong \mathbb{Z}.$$

b) Let $n \in \mathbb{N}_{>0}$ be fixed, and consider $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ as a $\mathbb{Z}$-module. Let $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$, and let $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ denote the equivalence class of some integer $a \in \mathbb{Z}$ modulo n. Then $0 = \varphi(\overline{0}) = \varphi(n \cdot \overline{a}) = n \cdot \varphi(\overline{a})$, which implies $\varphi(\overline{a}) = 0$. So φ is the constant zero homomorphism, and hence

$$(\mathbb{Z}/n\mathbb{Z})^* = \{0\}.$$

c) Consider $(\mathbb{Q}, +, \cdot)$ as $\mathbb{Z}$-module. We claim that for the dual module holds

$$\mathbb{Q}^* = \{0\}.$$

Indeed, assume that there is a homomorphism $\alpha \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z})$ with $\alpha \neq 0$. Then there exists some $a \in \mathbb{Q}$ such that $b := \alpha(a) \neq 0$. Since $b \in \mathbb{Z} \setminus \{0\}$, we can find an integer $n \in \mathbb{Z}$, such that $\frac{b}{n} \neq \mathbb{Z}$. For the rational number $\frac{a}{n} \in \mathbb{Q}$, we compute $\alpha(\frac{a}{n}) = \frac{n}{n}\alpha(\frac{a}{n}) = \frac{1}{n}\alpha(\frac{na}{n}) = \frac{\alpha(a)}{n} = \frac{b}{n} \notin \mathbb{Z}$, contradicting the definition of α.

4.36 Remark. Dualizing R-modules defines a contravariant functor

$$\begin{array}{rccc} * : & (R\text{-Mod}) & \to & (R\text{-Mod}) \\ & (N, +_N, \cdot_N) & \mapsto & (N^*, +_{N^*}, \cdot_{N^*}) \\ & \alpha : N \to N' & \mapsto & \alpha^* : N'^* \to N^* \end{array}$$

where the homomorphism α^* is given on elements of the dual module $\varphi \in \mathrm{Hom}_R(N', R)$ by $\alpha^*(\varphi) := \varphi \circ \alpha \in \mathrm{Hom}_R(N, R)$. Again, the dualizing functor is additive: for any pair of homomorphisms $\alpha, \beta : N \to N'$ of R-modules holds $(\alpha + \beta)^* = \alpha^* + \beta^*$.

Let us return to the general situation.

4.37 Proposition. *Let $(M, +_M, \cdot_M)$ be an R-module. Let $\alpha : N \to N'$ be a homomorphism of R-modules, which is an epimorphism. Then the dual homomorphism $\alpha^* : \mathrm{Hom}_R(N', M) \to \mathrm{Hom}_R(N, M)$ is a monomorphism.*

Proof. Let $\beta, \beta' : L \to \mathrm{Hom}_R(N, M)$ be two homomorphism of R-modules, such that $\alpha^* \circ \beta = \alpha^* \circ \beta'$. We need to show the identity $\beta = \beta'$.

By assumption, for all $\ell \in L$ holds $\alpha^* \circ \beta(\ell) = \alpha^* \circ \beta'(\ell)$ as an identity of morphisms in $\mathrm{Hom}_R(N, M)$. By the definition of α^*, this is equivalent to $\beta(\ell) \circ \alpha = \beta'(\ell) \circ \alpha$. Since α is an epimorphism, this implies $\beta(\ell) = \beta'(\ell)$ for all $\ell \in L$. Thus $\beta = \beta'$. □

4.38 Remark. Note that in general the dual of proposition 4.37 is not true. For example, consider the inclusion map $\iota : \mathbb{Z} \hookrightarrow \mathbb{Q}$, which is clearly a monomorphism of $\mathbb{Z}$-modules. By 4.35, we have for the dual modules $\mathbb{Z}^* \cong \mathbb{Z}$ and $\mathbb{Q}^* = \{0\}$. Hence the dual homomorphism $\iota^* : \mathbb{Q}^* \to \mathbb{Z}^*$ is not an epimorphism.

In definition 3.28 we called a functor exact, if it maps kernels and cokernels to kernels and cokernels again. In this terminology, proposition 4.37 translates into the following corollary.

4.39 Corollary. *Let $(M, +_M, \cdot_M)$ be an R-module. Then the contravariant Hom-functor* $\mathbf{Hom}(\bullet, M)$ *is left exact.*

Proof. Note that in order to apply the definition of left-exactness, we need to view $\mathbf{Hom}(\bullet, M)$ as a (covariant) functor on the opposite category $(R\text{-Mod})^{op}$. Thus we need to show that kernels in $(R\text{-Mod})^{op}$ (i.e. cokernels in $(R\text{-Mod})$) get mapped to kernels in $(R\text{-Mod})$.

Let $\alpha : N \to N'$ be a homomorphism of R-modules, with cokernel $\gamma : N' \to Q$. Up to isomorphism, the cokernel of α is given by the canonical quotient homomorphism $\pi : N' \to N'/\mathrm{im}(\alpha)$. Since π is an epimorphism, its dual $\pi^* : \mathrm{Hom}_R(N'/\mathrm{im}(\alpha), M) \to \mathrm{Hom}_R(N', M)$ is a monomorphism by proposition 4.37. Hence we may identify $\mathrm{Hom}_R(N'/\mathrm{im}(\alpha), M)$ with its image in $\mathrm{Hom}_R(N', M)$, i.e.

$$\begin{aligned}\mathrm{Hom}_R(N'/\mathrm{im}(\alpha), M) &\cong \mathrm{im}(\pi^*) \\ &= \{\varphi \in \mathrm{Hom}_R(N', M) : \exists \overline{\varphi} \in \mathrm{Hom}_R(N'/\mathrm{im}(\alpha), M) \text{ s.th. } \varphi = \overline{\varphi} \circ \pi\}\end{aligned}$$

as a submodule of $\mathrm{Hom}_R(N', M)$. For any $\varphi \in \mathrm{Hom}_R(N'/\mathrm{im}(\alpha), M)$ we clearly have $\alpha^*\varphi = \overline{\varphi} \circ \pi \circ \alpha = 0$, so $\mathrm{Hom}_R(N'/\mathrm{im}(\alpha), M) \subseteq \ker(\alpha^*)$. Conversely, let $\varphi \in \mathrm{Hom}_R(N', M)$ be such that $\varphi \in \ker(\alpha^*)$. Then $\alpha^*\varphi = 0$ as a homomorphism $N \to M$. Hence for all $n \in N$, we have $\varphi \circ \alpha(n) = 0$, which implies $\mathrm{im}(\alpha) \subseteq \ker(\varphi)$. By the universal property of the quotient, there exists a factorization $\overline{\varphi} : N'/\mathrm{im}(\alpha) \to M$ such that $\varphi = \overline{\varphi} \circ \pi$. Hence $\varphi \in \mathrm{Hom}_R(N'/\mathrm{im}(\alpha), M)$. This establishes the equality $\mathrm{Hom}_R(N'/\mathrm{im}(\alpha), M) = \ker(\alpha^*)$. $\square$

4.40 Definition. The *bi-dual functor* is the (covariant) functor given by

$$\begin{array}{rccc} ** : & (R\text{-Mod}) & \to & (R\text{-Mod}) \\ & M & \mapsto & M^{**} := \mathrm{Hom}_R(\mathrm{Hom}_R(M,R)) \\ & \alpha : M \to N & \mapsto & (\alpha^*)^* : M^{**} \to N^{**} \end{array} .$$

4.41 Remark. For any R-module $(M, +_M, \cdot_M)$, there exists a natural homomorphism of R-modules given by

$$\begin{array}{rccc} e_M : & M & \to & M^{**} \\ & m & \mapsto & e_M(m) \end{array}$$

where for $m \in M$, the homomorphism $e_m \in M^{**}$ is the R-linear evaluation map

$$\begin{array}{rccc} e_M(m) : & M^* = \mathrm{Hom}_R(M,R) & \to & R \\ & f & \mapsto & f(m). \end{array}$$

In general, the homomorphisms e_M are neither injective nor surjective.

It is not hard to verify that for the category $\mathcal{C} := (R\text{-Mod})$ of R-modules, the family $e := \{e_M\}_{M \in \mathrm{Ob}(\mathcal{C})}$ is a natural transformation $e : \mathrm{id}_{\mathcal{C}} \Rightarrow **$.

4.4 Finitely generated and free modules

4.42 Definition. Let $\{M_\lambda\}_{\lambda \in \Lambda}$ be a family of R-modules, indexed by some set $\Lambda \neq \emptyset$. We define a set

$$\prod_{\lambda \in \Lambda} M_\lambda := \Big\{ \{m_\lambda\}_{\lambda \in \Lambda} : \, m_\lambda \in M_\lambda \Big\}.$$

For an element $r \in R$ and a pair of families $\{m_\lambda\}_{\lambda \in \Lambda}$ and $\{n_\lambda\}_{\lambda \in \Lambda}$, we define a composition and an operation by

$$\{m_\lambda\}_{\lambda \in \Lambda} + \{n_\lambda\}_{\lambda \in \Lambda} := \{m_\lambda + n_\lambda\}_{\lambda \in \Lambda} \text{ and } r \cdot \{m_\lambda\}_{\lambda \in \Lambda} := \{r \cdot m_\lambda\}_{\lambda \in \Lambda}.$$

In this way, the triple $(\prod_{\lambda \in \Lambda} M_\lambda, +, \cdot)$ becomes an R-module. It is called the *direct product* of the family $\{M_\lambda\}_{\lambda \in \Lambda}$. Moreover, by defining

$$\bigoplus_{\lambda \in \Lambda} M_\lambda := \Big\{ \{m_\lambda\}_{\lambda \in \Lambda} \in \prod_{\lambda \in \Lambda} M_\lambda : \, m_\lambda \neq 0 \text{ for only finitely many } \lambda \in \Lambda \Big\}$$

one obtains a submodule $(\bigoplus_{\lambda\in\Lambda} M_\lambda, +, \cdot)$, which is called the *direct sum* of the family $\{M_\lambda\}_{\lambda\in\Lambda}$.

4.43 Remark. **a)** Clearly, if the set of indices Λ is finite, the notions of direct product and direct sum coincide. The product of two R-modules M and N is simply denoted by $M \times N$ or $M \oplus N$, and the product of a finite number n of copies of the same R-module M by M^n.

b) For any $\lambda \in \Lambda$, let $i_\lambda := M_\lambda \to \bigoplus_{\lambda\in\Lambda} M_\lambda$ denote the canonical inclusion homomorphism, and $p_\lambda : \prod_{\lambda\in\Lambda} M_\lambda \to M_\lambda$ the canonical projection. Moreover, let $\iota_\lambda : \{0\} \to M_\lambda$ denote the trivial inclusion homomorphism, and $\tau_\lambda : M_\lambda \to \{0\}$ the constant null homomorphism. Then one verifies that $(\prod_{\lambda\in\Lambda} M_\lambda, \{p_\lambda\}_{\lambda\in\Lambda})$ is a product of the family of morphisms $\{\tau_\lambda\}_{\lambda\in\Lambda}$ in the category (R-Mod) of R-modules. Analogously, $(\bigoplus_{\lambda\in\Lambda} M_\lambda, \{i_\lambda\}_{\lambda\in\Lambda})$ is a coproduct of the family $\{\iota_\lambda\}_{\lambda\in\Lambda}$ in (R-Mod). Compare example 1.41 above.

4.44 Definition. Let E be a non-empty set. The *free R-module generated by E* is the direct sum of the constant family $\{R\}_{e\in E}$. We will denote it by

$$R\langle E\rangle := \bigoplus_{e\in E} R.$$

For $E = \emptyset$, we define $R\langle\emptyset\rangle := \{0\}$ as the trivial module.

4.45 Remark. An alternative, and slightly abusive, notation for the free R-module generated by E is

$$R\langle E\rangle = \bigoplus_{e\in E} Re$$

Here, elements of $R\langle E\rangle$ are thought of as so-called *formal sums* in the elements of E. By this one means the following.

Let $\varepsilon \in R\langle E\rangle$. Instead of writing ε as a family $\varepsilon = \{r_e\}_{e\in E}$, one uses the notation $\varepsilon = \sum_{e\in E} r_e \cdot e$. By definition, there exists a number $n \in N$, and elements $e_1, \ldots, e_n \in E$, such that $r_e = 0$ if $e \notin \{e_1, \ldots, e_n\}$. Put $r_i := r_{e_i}$ for $i = 1, \ldots, n$. Then one writes

$$\varepsilon := r_1 e_1 + \ldots + r_n e_n$$

and applies the usual rules for addition and R-module-multiplication to these expressions. For the special case $n = 0$, where ε is constant the zero-family, we write $\varepsilon = 0$. In particular, the elements $e \in E$ are actually thought of as elements $e = 1 \cdot e \in R\langle E\rangle$.

4.46 Exercise. Show that as an R-module, $R\langle E\rangle$ is isomorphic to the submodule of $\mathrm{Map}(E,R)$, which is given by

$$\mathrm{Map}^{\oplus}(E,R) := \{f \in \mathrm{Map}(E,R) :\ f(e) \neq 0 \text{ for only finitely many } e \in E\}.$$

4.47 Example. Let $(K,+,\cdot)$ be a field, and let V be a finite-dimensional vector space over K. Let $E = \{e_1,\ldots,e_n\}$ be a basis of V. The free K-module generated by the set E is $K\langle E\rangle = \bigoplus_{i=1}^n K = K^n$, and the isomorphism $V \cong K^n$ determined by the basis E is usually written as an identification

$$V = \bigoplus_{i=1}^{n} Ke_i.$$

4.48 Notation. Let $(M,+,\cdot)$ be an R-module, and let $E \subseteq M$ be a subset. The map

$$\begin{array}{rccc} \Gamma_E : & R\langle E\rangle & \to & M \\ & \{r_e\}_{e\in E} & \mapsto & \sum_{e\in E} r_e \cdot e \end{array}$$

is well-defined, since the sum in M is actually finite by the definition of the free R-module generated by a set. Moreover, Γ_E is a homomorphism of R-modules.

4.49 Definition. Let $(M,+,\cdot)$ be an R-module. A subset $E \subseteq M$ is called

- **a)** a *generating subset of* M, if Γ_E is surjective;
- **b)** *R-linearly independent*, if Γ_E is injective;
- **c)** a *basis of* M, if Γ_E is bijective.

4.50 Remark. Let $(M,+,\cdot)$ be an R-module with $M \neq \{0\}$.

a) A subset $E \subseteq M$ is a generating subset of M if and only if for all $m \in M$ there exists a natural number $n \in \mathbb{N}_{>0}$, elements $r_1,\ldots,r_n \in R$ and elements $e_1,\ldots,e_n \in E$, such that $m = r_1e_1 + \ldots + r_ne_n$.

b) A subset $E \subseteq M$ is R-linearly independent if and only if for any natural number $n \in \mathbb{N}_{>0}$, any pairwise distinct elements $e_1,\ldots,e_n \in E$, and all elements $r_1,\ldots,r_n \in R$, the equality $r_1e_1 + \ldots + r_ne_n = 0_M$ implies $r_1 = \ldots = r_n = 0_R$.

c) A subset $E \subseteq M$ is a basis of M if and only if for all $0 \neq m \in M$ there exists a unique natural number $n \in \mathbb{N}$, unique elements $r_1,\ldots,r_n \in R$ and unique pairwise distinct elements $e_1,\ldots,e_n \in E$, such that $m = r_1e_1 + \ldots + r_ne_n$.

4.51 Examples. a) Let $(K, +_K, \cdot_K)$ be a field. Then any K-vector space $(V, +, \cdot)$ has a basis.

b) The set of monomials $E := \{X^i : i \in \mathbb{N}\}$ is a basis of the R-module $(R[X], +, \cdot)$ of polynomials.

c) Consider $(\mathbb{Q}, +, \cdot)$ as a $\mathbb{Z}$-module. Clearly, the set $E := \{\frac{1}{n} : n \in \mathbb{N}_{>0}\}$ is a generating set. However, there exists no basis of $(\mathbb{Q}, +, \cdot)$.

Indeed, assume that there exists a basis E. It is easy to see that E must contain more then one element to be a generating subset. So let $p, q \in E$ be two different elements. Let $a, b, c, d \in \mathbb{Z}$ be such that $p = \frac{a}{b}$ and $q = \frac{c}{d}$. Then $(-cb) \cdot q + (ad) \cdot q = 0_{\mathbb{Q}}$ is a non-trivial $\mathbb{Z}$-linear combination, contradicting the injectivity of Γ_E.

4.52 Definition. Let $(M, +, \cdot)$ be an R-module. It is called

a) *finitely generated*, if there exists a generating set, which is finite.

b) *free*, if there exists a basis of $(M, +, \cdot)$.

4.53 Lemma. *Let $(R, +_R, \cdot_R)$ be a commutative ring with multiplicative identity element $1_R \neq 0_R$. Let $(M, +, \cdot)$ be an R-module, which is finitely generated and free. Then there exists a basis of $(M, +, \cdot)$ which is finite. Any two bases of $(M, +, \cdot)$ have the same cardinality.*

Proof. Using some elements from ring theory the proof reduces the claims of the lemma to the case of a vector space over a field, where the statements are well-known. See for example [Lang] for details. □

4.54 Definition. Let $(R, +_R, \cdot_R)$ be a commutative ring with multiplicative identity element $1_R \neq 0_R$. Let $(M, +, \cdot)$ be an R-module, which is finitely generated and free. Then the *rank* of $(M, +, \cdot)$ over R is

$$\operatorname{rank}_R(M) := d,$$

where d is the cardinality of a basis of $(M, +, \cdot)$. By some authors, this is also called the *dimension* of $(M, +, \cdot)$.

4.55 Examples. a) Any vector space $(V, +, \cdot)$ over a field $(K, +, \cdot)$ has a basis. So any K-vector space is a free K-module. If V is finite dimensional, then

$$\dim_K(V) = \operatorname{rank}_K(V).$$

b) The ring of polynomials $R[X_1, \ldots, X_n]$ has a basis $E = \{1, X, X^2, \ldots\}$. It is a free R-module, but not finitely generated.

c) Consider the ring $(\mathbb{Z}, +, \cdot)$ as module over itself. Obviously, it is free and of rank 1. The only possible bases are $\{1\}$ and $\{-1\}$.

Let $n \in \mathbb{N}_{>0}$. The ideal $(n) = n\mathbb{Z} \subseteq \mathbb{Z}$ is a submodule, which is again free and of rank 1.

By remark 4.26, the quotient $\mathbb{Z}/n\mathbb{Z}$ is a $\mathbb{Z}$-module, too. It is obviously finitely generated, since $|\mathbb{Z}/n\mathbb{Z}| = n < \infty$. However, $\mathbb{Z}/n\mathbb{Z}$ is not a free module. Indeed, suppose that $E \subseteq \mathbb{Z}/n\mathbb{Z}$ is a basis. Since E is a generating set, there must exist an element $\overline{0} \neq \overline{e} \in E$, with a representative $e \in \mathbb{Z}$. We compute

$$n \cdot \overline{e} = \overline{ne} = \overline{0} = 0 \cdot \overline{e},$$

contradicting the uniqueness of the representation of $\overline{0}$.

4.56 Exercise. Let $A \subseteq M$ be a subset of an R-module $(M, +, \cdot)$. We define the *span of A* by

$$\operatorname{span}_R(A) := \bigcap_{U \subseteq M \text{ submodule with } A \subseteq U} U.$$

It is the smallest submodule of M, which contains A. Let $(N, +, \cdot)$ be a submodule of $(M, +, \cdot)$. Show that A is a generating subset of N if and only if $N = \operatorname{span}_R(A)$.

4.57 Proposition. *Let $(M, +, \cdot)$ be an R-module. Then M is finitely generated, if and only if there exists a natural number $n \in \mathbb{N}_{>0}$ and a submodule $U \subseteq R^n$, such that*

$$M \cong R^n/U.$$

Proof. The reverse implication is trivial. Let us assume that M is finitely generated by a finite generating set $E = \{e_1, \ldots, e_n\} \subseteq M$, with $|E| = n > 0$. By definition, the homomorphism Γ_E is surjective. Put $U := \ker(\Gamma_E)$. For the underlying groups, we have an isomorphism of groups

$$M = \operatorname{im}(\Gamma_E) \cong R^n/\ker(\Gamma_E) = R^n/U.$$

The isomorphism $\gamma : R^n/U \to M$ is given on $\overline{v} \in R^n/U$ by $\gamma(\overline{v}) = \Gamma_E(v)$. In particular, γ is a homomorphism of R-modules.

Let $r \in R$. We compute

$$\gamma^{-1}(r \cdot \overline{v}) = \gamma^{-1}(r \cdot \gamma(\gamma^{-1}(\overline{v}))) = \gamma^{-1}(\gamma(r \cdot \gamma^{-1}(\overline{v}))) = r \cdot \gamma^{-1}(\overline{v}).$$

This shows that γ^{-1} is a homomorphism of R-modules, too. Therefore γ is an isomorphism of R-modules. $\square$

References

[Bou] Bourbaki N., *Algebra I, Chapters 1-3*, Springer (1989)

[Eis] Eisenbud D., *Commutative Algebra with a View Toward Algebraic Geometry*, Springer (1995)

[Gre] Greub W., *Multilinear Algebra*, Springer Universitext (1978)

[Lang] Lang S., *Algebra*, Addison-Wesley (1984)

[Mac] MacLane S., *Categories for the Working Mathematician*, Springer GTM 5 (1971)

[Sch] Schubert, H., *Kategorien, Vol. I+II*, Heidelberger Taschenbücher 65, Springer (1970)