Mathematical structures explained in categorical language

Mariusz Wodzicki

September 9, 2023

Contents

1 The concept of a category

1.1 Oriented graphs

1.1.1

An *oriented graph* $\mathscr{C}$ consists of two sets, $\mathscr{C}_0$ (the set of *vertices*) and $\mathscr{C}_1$ (the set of *arrows*) which are related by a pair of correspondences:

$$\mathscr{C}_0 \underset{s}{\overset{t}{\longleftarrow\!\!\longleftarrow}} \mathscr{C}_1 \tag{1}$$

1.1.2

For any arrow γ we shall refer to $s(\gamma)$ as its *source*, and to $t(\gamma)$ as its *target*.

1.1.3

We shall denote by

$$\mathrm{Arr}_{\mathscr{C}}(c, c') \tag{2}$$

the set of arrows with source c and target c'.

1.1.4 A binary relation canonically associated with an oriented graph

Given an oriented graph $\mathscr{C}$, consider the binary relation on the set of vertices

$$\rho_{\mathscr{C}} : \mathscr{C}_0, \mathscr{C}_0 \longrightarrow \text{Statements}, \qquad c, c' \longmapsto \text{“ } \mathrm{Arr}_{\mathscr{C}}(c, c') \neq \emptyset \text{ ”}. \tag{3}$$

1.1.5 An oriented graph canonically associated with binary relation

Given a binary relation on a set X,

$$\rho : X, X \longrightarrow \text{Statements}, \tag{4}$$

consider the set of ordered pairs (x, x') for which statement $\rho(x, x')$ holds,

$$\Gamma_\rho := \{(x, x') \in X^2 \mid \rho(x, x')\}. \tag{5}$$

Set (5) is called the *graph* of relation ρ for a good reason: the composition of the canonical inclusion function $\iota : \Gamma_\rho \hookrightarrow X^2$ with two canonical projections π_0 and π_1 onto each of the two factors X of the Cartesian product $X^2 = X \times X$ defines an oriented graph

$$\mathscr{C}_\rho := \left(X \underset{\pi_1 \circ \iota}{\overset{\pi_0 \circ \iota}{\longleftarrow\!\!\longleftarrow}} \Gamma_\rho \right) \tag{6}$$

that is canonically associated with relation ρ.

Exercise 1 *Show that relations $\rho_{\mathscr{C}_\rho}$ and ρ are* equipotent.

1.1.6

Later, when we define the concept of a morphism between oriented graphs, we shall see that the oriented graphs $\mathscr{C}_{p_{\mathscr{C}}}$ and $\mathscr{C}$ are *isomorphic* precisely when no two different arrows in $\mathscr{C}$ have the same source and target.

1.2 Categories

1.2.1 The set of composable pairs of arrows

Consider the set $\mathscr{C}_2$ of pairs γ_0, γ_1 of arrows such that the source of γ_0 is the target of γ_1. We shall refer to $\mathscr{C}_2$ as the *set of composable pairs of arrrows.*

1.2.2

A graph equipped with a correspondence

$$\mathscr{C}_1 \xleftarrow{\;\circ\;} \mathscr{C}_2 \tag{7}$$

is said to be a *category* if (7) is *associative*, i.e., if

$$(\gamma_0 \circ \gamma_1) \circ \gamma_2 = \gamma_0 \circ (\gamma_1 \circ \gamma_2) \tag{8}$$

for any *composable* triple of arrows

$$\bullet \xleftarrow{\gamma_0} \bullet \xleftarrow{\gamma_1} \bullet \xleftarrow{\gamma_2} \bullet \;.$$

The latter means that

$$s(\gamma_0) = t(\gamma_1) \qquad \text{and} \qquad s(\gamma_1) = t(\gamma_2). \tag{9}$$

1.2.3

If we denote by $\mathscr{C}_3$ the set of composable triples of arrows, then the associativity identity (8) can be expressed as commutativity of the diagram

$$\begin{tikzcd}
\mathscr{C}_2 \arrow[d, "\circ"'] & \mathscr{C}_3 \arrow[l, "\circ_{01}"'] \arrow[d, "\circ_{12}"] \arrow[dl, phantom, "\circlearrowleft"] \\
\mathscr{C}_1 & \mathscr{C}_2 \arrow[l, "\circ"]
\end{tikzcd}$$

where $\circ_{01}$ replaces a list

$$\gamma_0, \gamma_1, \gamma_2 \tag{10}$$

by the list

$$\gamma_0 \circ \gamma_1, \gamma_2$$

while $\circ_{12}$ replaces (10) by

$$\gamma_0, \gamma_1 \circ \gamma_2 \,.$$

1.2.4 Objects and morphisms

Members of $\mathscr{C}_0$ are referred to as *objects* of category $\mathscr{C}$ while members of $\mathscr{C}_1$ are referred to as its *morphisms*.

1.2.5 $\mathrm{Hom}_{\mathscr{C}}(c, c')$

The set of arrows with source c and target c' is usually denoted $\mathrm{Hom}_{\mathscr{C}}(c, c')$. Its elements are referred as morphisms *from* c *to* c'.

1.2.6 Endomorphisms of an object

Given an object c, morphisms from c to c are referred to as *endomorphisms* of c. The set $\mathrm{Hom}_{\mathscr{C}}(c, c)$ is often denoted $\mathrm{End}_{\mathscr{C}}\, c$.

1.2.7

Note that $\mathrm{End}_{\mathscr{C}}\, c$ endowed with the composition operation is a *semigroup*. Semigroups of endomorphisms of objects of various categories are, perhaps, the most important class of semigroups.

1.2.8 Semigrouos viewed as categories with a single object

Given a semigroup $(S, \circ)$, the diagram

$$S^0 \underset{s}{\overset{t}{\leftleftarrows}} S^1 \xleftarrow{\;\circ\;} S^2$$

defines a category with a single object. Here S^n, $n = 0, 1, 2$, denote the Cartesian powers of S,

Vice-versa, morphisms of a category $\mathscr{C}$ with a single object form a semigroup, the semigroup of endomorphisms of that single object. The source and the target maps coincide with the unique function from $\mathscr{C}_1$ to the singleton set $\mathscr{C}_0$.

In other words, semigroups are all purposes the same as categories with a single object.

1.2.9 Transitive binary relations viewed as skeletal categories

On the other end of the realm of categories are situated categories where no two arrows have the same source and target. Such categories as referred to as *skeletal categories*. Skeletal categories correspond to *transitive* binary relations on the sets of objects, via the correspondence described in Sections 1.1.4 and 1.1.5.

1.2.10 The identity morphisms

A morphism ι is said to be an *identity* morphism if

$$\gamma \circ \iota = \gamma \qquad \text{and} \qquad \iota \circ \gamma' = \gamma'$$

for any arrows γ and γ' pre- and post-composable with ι.

Exercise 2 *Show that $s(\iota) = t(\iota)$ if there exists at least one arrow with target $s(\iota)$ or with source $t(\iota)$.*

1.2.11

The concept of an identity morphism is obviously of interest only if there exist arrows pre- or post-composable with ι. An identity morphism with source and target being c is referred to as *the identity morphism* of object c. The use of the definite article is due to the fact that such a morphism is necessarily unique if it exists.

Exercise 3 *Show that two identity morphisms ι and ι' with source and target c are equal.*

1.2.12

The identity morphism of c is denoted id_c.

1.2.13 Left and right inverses

Given a composable pair γ, γ' whose composition is an identity morphism, we say that γ' is a *right* inverse of γ while γ is a *left* inverse of γ'.

Exercise 4 *Suppose that γ' is a right inverse of γ and γ'' is a left inverse of γ. Show that $\gamma' = \gamma''$.*

1.2.14 Isomorphisms

The common right and left inverse is simply referred to as *the inverse* of γ and γ in this case is said to be *invertible*. If its source is c and its target is c', we say that γ supplies an *isomorphism* between objects c and c'.

1.2.15 Caveat

An arrow may have many different left inverses and not a single right inverse, and vice-versa.

1.2.16 Automorphisms of an object

Isomorphisms of c with itself are referred to as *automorphisms* of c. The set of automorphisms is denoted $\mathrm{Aut}_{\mathscr{C}}\, c$.

1.2.17 Unital categories

If every object of a category possesses the identity morphism, the category is said to be unital. Unital categories are equipped with a correspondence

$$\mathscr{C}_0 \xrightarrow{\mathrm{id}} \mathscr{C}_1 \,, \qquad c \longmapsto \mathrm{id}_c\,. \tag{11}$$

1.2.18

Note that

$$s \circ \mathrm{id} \;=\; \mathrm{id}_{\mathscr{C}_0} \;=\; t \circ \mathrm{id}\,.$$

Here $\circ$ denotes composition of *mappings* and $\mathrm{id}_{\mathscr{C}_0}$ denotes the identity *mapping* of set $\mathscr{C}_0$.

1.2.19

Although there are very good reasons not to require presence of the identity morphisms in general, the tradition going back to Eilenberg and Mac Lane was to incorporate existence of the identity morphisms into the definition of a category. We shall not do that and will use the term "category" not assuming the presence of the identity morphisms.

1.2.20

In a unital category the semigroups of endomorphisms of object become monoids.

1.2.21 Monoids viewed as unital categories with a single object

Exactly like in the case of semigroups, cf. Section 1.2.8, arbitrary monoids can be viewed as unital categories with a single object, and vice-versa.

1.2.22 Preordered sets

A *reflexive* and *transitive* binary relation is usually referred to as *preorder*, or *quasiorder* relation. Sets equipped with a preorder relation are referred to as *preordered sets*. We shall use generic notation

$$(X, \precsim) . \tag{12}$$

1.2.23 Preordered sets viewed as skeletal unital categories

Unital skeletal categories correspond to preordered sets cf. Section 1.2.9.

1.2.24 Order relations

A preorder relation which is *weakly antisymmetric*, i..e, it satisfies the following condition

$$\textit{if} \;\; x \precsim y \;\; \textit{and} \;\; y \precsim x \, , \;\; \textit{then} \;\; x = y \, , \tag{13}$$

is called an *order relation*. We shall be using the generic notation

$$(X, \preccurlyeq) . \tag{14}$$

Notice a subtle but significant difference between (14) and (12).

1.2.25 "Partially ordered sets"

To emphasise the fact that arbitrary elements of ordered sets are not necessarily *comparable*, such structures are often referred to as *partially ordered sets*. This is, however, not necessary, we will be calling them *ordered sets*.

It folloows that theories of semigroups, of monoids, of sets equipped with a transitive relation, of preordered, as well of oredered sets, form parts of a single theory: Category Theory.

1.2.26 Small categories

What we have discussed so far is referred to as *small* categories. This concept is sufficient to describe a great variety of structures encountered in Mathematics and its applications to Physics, Engineering, Statistics, Economics and so on. As a matter of convenience rather than necessity, it has been a practice from the outset to relax the requirement that $\mathscr{C}_0$ and $\mathscr{C}_1$ are sets. This allows one to consider the category of *all* sets, *all* groups, *all* real vector spaces, etc, while none of the respective classes of sets, groups, or vector spaces, forms a set itself.

Thus, the standard definition of a category assumes that $\mathscr{C}_0$ and $\mathscr{C}_1$ are *classes* rather than sets while it is still expected that $\mathrm{Hom}_{\mathscr{C}}(c, c')$ are *sets*.

If one exercise caution, one still can use certain set theoretic concepts like membership, mapping, relation, in the context of classes. Experts in Foundations of Mathematics have been addressing the axiomatic basis of theory of classes that includes and extends theory of sets.

1.2.27 Symmetries

Before the categorical language was proposed and developed as means to describe and study underlying structure of numerous areas of Mathematics, automorphisms of various objects: geometric, physical systems, etc—were often called *symmetries*.

1.2.28 Subcategories

For a category $\mathscr{C}$, suppose that, a pair of subclasses $\mathscr{C}'_0 \subseteq \mathscr{C}_0$ and $\mathscr{C}'_1 \subseteq \mathscr{C}_1$ is given such that the source and the target of any morphism in $\mathscr{C}'_1$ is a member of $\mathscr{C}'_0$ and the composition of any two such morphisms is a member of $\mathscr{C}'_1$.

If one equips those subclasses with the source, target, and multiplication correspondences induced from category $\mathscr{C}$, one obtains a category on its own. We shall denote it $\mathscr{C}'$ and say that $\mathscr{C}'$ is a *subcategory* of $\mathscr{C}$.

1.2.29 Full subcategories

If

$$\mathrm{Hom}_{\mathscr{C}'}(c', d') = \mathrm{Hom}_{\mathscr{C}}(c', d') \qquad (c', d' \in \mathscr{C}'_0),$$

then we say that $\mathscr{C}'$ is a *full* subcategory of category $\mathscr{C}$.

2 Various categories of sets

2.1 The category of sets

2.1.1

The class of all sets and the class of all mappings between arbitrary sets form naturally a unital category.

2.1.2

The source and the target correspondences ascribe to a mappping $f\colon X \longrightarrow Y$ its *domain* X and, respectively, its *antidomain* Y.

2.1.3

Composition of mappings plays the role of composition of arrows, the identity mappings id_X serve as the identity morphisms.

2.1.4

The category of sets will be denoted **Set**, one often denotes $\mathrm{Hom}_{\mathbf{Set}}(X,Y)$ by Y^X.

2.1.5 Bijections

Isomorphisms in the category of sets are called *bijections*.

2.1.6 Permutations

Automorphisms of a set X are called *permutations* (of elements of X). They form a group denoted Σ_X or S_X.

2.2 The category of sets and multimaps

2.2.1 Multivalued mappings

A *multivalued* map, $\phi\colon X \multimap Y$, from a set X to a set Y, is, by definition, a mapping $\phi\colon X \to \mathscr{P}(Y)$ from X to the set $\mathscr{P}(Y)$ of all subsets of Y. Multivalued mappings will be also called *multimaps*.

2.2.2 Mappings versus multimaps

Every mapping $f\colon X \to Y$ defines the multimap

$$x \longmapsto \phi_f(x) := \{f(x)\} \qquad (x \in X).$$

The correspondence

$$f \longmapsto \phi_f$$

identifies mappings $f\colon X \to Y$ with multimaps $\phi\colon X \multimap Y$ satisfying the property

$$|\phi(x)| = 1 \qquad (x \in X). \tag{15}$$

2.2.3 The image mapping associated with a multimap

Every multimap $\phi\colon X \multimap Y$ naturally extends to a mapping from $\mathscr{P}(X)$ to $\mathscr{P}(Y)$,

$$A \longmapsto \phi(A) := \bigcup_{x\in A} \phi(x) \qquad (A \subseteq X). \tag{16}$$

We will denote it ϕ_* and will call it the *image mapping* associated with the multimap.

2.2.4

Any mapping $\varphi\colon \mathscr{P}(X) \longrightarrow \mathscr{P}(Y)$ defines a multimap

$$\phi\colon X \multimap Y, \qquad \phi(x) := \varphi(\{x\}),$$

and this sets up a natural one-to-one correspondence between multimaps $X \multimap Y$ and mappings $\mathscr{P}(X) \longrightarrow \mathscr{P}(Y)$.

2.2.5 The reverse of a multimap

Every multimap $\phi\colon X \multimap Y$ also defines a multimap $Y \multimap X$

$$\phi^{\mathrm{rev}}(y) := \{x \in X \mid \phi(x) \ni y\}. \tag{17}$$

We shall refer to it as the *reverse* of ϕ. When $\phi = \phi_f$ for a mapping $f\colon X \to Y$, then

$$\phi^{\mathrm{rev}}(x) \;=\; \{x \in X \mid f(x) = y\}$$

is called the *fiber* of f at $y \in Y$.

2.2.6 The preimage mapping associated with a multimap

The image mapping associated with the reverse multimap, ϕ^{rev}, will be called the *preimage mapping* associated with ϕ and denoted ϕ^*.

Exercise 5 *Show that*

$$\phi^{\mathrm{rev}}(B) = \{x \in X \mid \phi(x) \cap B \neq \emptyset\} \qquad (B \subseteq Y). \tag{18}$$

2.2.7 Composition of multimaps

Given multimaps $\phi\colon X \multimap Y$ and $\chi\colon Y \multimap Z$, their *composition*,

$$\chi \circ \phi\colon x \longmapsto \chi_*(\phi(x)) \qquad (x \in X), \tag{19}$$

is a multimap $X \multimap Z$.

Exercise 6 *Show that*

$$\left(\chi \circ \phi\right)_* = \chi_* \circ \phi_*.$$

Exercise 7 *Given mappings $f\colon X \to Y$ and $g\colon Y \to Z$, show that*

$$\phi_g \circ \phi_f = \phi_{g\circ f}. \tag{20}$$

Exercise 8 *Show that composition of multimaps is associative, i.e.,*

$$(\chi \circ \phi) \circ \upsilon = \chi \circ (\phi \circ \upsilon),$$

for any $\upsilon\colon W \multimap X$, $\phi\colon X \multimap Y$, and $\chi\colon Y \multimap Z$.

2.2.8 $\mathbf{Set}_{\text{mult}}$

Thus, the class of sets equipped with multimaps as morphisms forms a category. We shall denote it $\mathbf{Set}_{\text{mult}}$.

Exercise 9 *Show that the canonical embedding* $\iota_X \colon X \hookrightarrow \mathscr{P}(X)$,

$$\iota_X \colon x \longmapsto \{x\} \qquad (x \in X)$$

is the identity endomorphism of set X *in* $\mathbf{Set}_{\text{mult}}$.

Exercise 10 *Show that a multimap* ϕ *is invertible if and only if* $\phi = \phi_f$ *and* $\phi^{\text{rev}} = \phi_g$ *for some mappings* f *and* g.

2.3 The category of sets and submaps

2.3.1 Submaps

A multimap $\phi \colon X \multimap Y$, such that $\phi(x)$ has *at most* one element,

$$|\phi(x)| \leq 1 \qquad (x \in X), \tag{21}$$

will be called a *submap* (compare it with (15)).

While multimaps satisfying (15) corespond to mappings $f \colon X \to Y$, then submaps correspond to *partially defined* mappings from X to Y, i.e., to mappings $f \colon X' \to Y$ whose domain is a subset of X.

Exercise 11 *Show that* $\chi \circ \phi$ *is a submap if both* ϕ *and* χ *are submaps.*

2.3.2 $\mathbf{Set}_{\text{sub}}$

The class of sets with submaps as morphisms defines another category whose objects are sets. We shall denote it $\mathbf{Set}_{\text{sub}}$.

2.4 The category of sets and finitely-valued mappings

2.4.1 $\mathbf{Set}_{\text{fin}}$

More generally, we shall say that $\phi \colon X \multimap Y$ is a *finitely-valued mapping*, if

$$|\phi(x)| < \infty \qquad (x \in X). \tag{22}$$

Exercise 12 *Show that* $\chi \circ \phi$ *is finitely-valued if both* ϕ *and* χ *are finitely-valued.*

In particular, sets with finitely-valued mappings as morphisms form a category. We shall denote it $\mathbf{Set}_{\text{fin}}$.

2.4.2 $\mathbf{Set}_{\text{count}}$

Another possibility is to consider *countably-valued mappings* as morphisms,

$$\phi(x) \quad \text{countable for all } x \in X. \tag{23}$$

Let us denote denote the corresponding category by $\mathbf{Set}_{\text{count}}$.

2.4.3

The above categories form an increasing chain of unital subcategories of the category of sets and multimaps

$$\mathbf{Set} \subseteq \mathbf{Set}_{\text{sub}} \subseteq \mathbf{Set}_{\text{fin}} \subseteq \mathbf{Set}_{\text{count}} \subseteq \mathbf{Set}_{\text{mult}}.$$

Note that they share the same class of objects. They differ only in their morphisms.

2.5 The category of sets and relations

2.5.1 Composition of binary relations

A different approach to defining morphisms from a set X to a set Y is to consider binary relations $R \subseteq X \times Y$. For $R \subseteq X \times Y$ and $S \subseteq Y \times Z$,

$$R \circ S := \{(x,z) \in X \times Z \mid \text{there exists } y \in Y \text{ such that } (x,y) \in R \text{ and } (y,z) \in S\}. \tag{24}$$

is a binary relation between elements of X and Z. If we use notation $x \sim_R y$ (*"element $x \in X$ is in relation R with element $y \in Y$"*) to express the fact that $(x,y) \in R$, then we can rewrite Definition (24) as follows

$$R \circ S := \{(x,z) \in X \times Z \mid \text{there exists } y \in Y \text{ such that } x \sim_R y \text{ and } y \sim_S z\}. \tag{25}$$

Exercise 13 *Show that composition of binary relations is associative, i.e.,*

$$(Q \circ R) \circ S = Q \circ (R \circ S)$$

for any $Q \subseteq W \times X$, $R \subseteq X \times Y$, and $S \subseteq Y \times Z$.

2.5.2 The identity relation

For any set X we shall call the binary relation

$$\Delta_X := \{(x,x') \in X \times X \mid x = x'\} \tag{26}$$

the *identity* relation on X.

Exercise 14 *Show that*

$$\Delta_X \circ R = R = R \circ \Delta_Y$$

for any $R \subseteq X \times Y$.

2.5.3

Denote the category whose objects are sets and relations $R \subseteq X \times Y$ are morphisms $X \to Y$ by $\mathbf{Set}_{\text{rel}}$.

3 Categories of binary structures

3.1 Bin

3.1.1 Binary structures

A binary structure consists of a set G equipped with a binary operation

$$G, G \xrightarrow{\mu} G \quad .$$

3.1.2 Multiplicative notation

The result of applying the binary operation to elements $g, h \in G$ is often denoted gh.

3.1.3 Homomorphisms

A mapping $f\colon G \longrightarrow G'$, satisfying the identity,

$$f\big(\mu(g,h)\big) \;=\; \mu'(f(g), f(h)), \qquad (g, h \in G),$$

is called a *homomorphism* of binary structures. In multiplicative notation, the above identity reads

$$f(gh) = f(g)f(h), \qquad (g, h \in G).$$

3.1.4

The class of all binary structures with homomorphisms as arrows forms a category that will be denoted Bin.

3.1.5 Sgr

Associative binary structures are referred to as *semigrups*. They form a full subcategory of the category of all binary structures.

3.2 The category of monoids

3.2.1 Idempotents

An element $e \in G$ is said to be an idempotent of a binary structure if $e^2 := eei$ equals e. Homomorphisms preserve the property of being an idempotent:

$$f(e)^2 = f\big(e^2\big) = f(e).$$

3.2.2 Identity elements

An element $e \in G$ is said to be a *left* identity of a binary structure if

$$eg = g \qquad (g \in G).$$

Right identities are defined similarly.

3.2.3

There may be many different left identities and no right identity, and vice-versa. For example, for any set X, the operation that removes the first argument from the list of arguments,

$$x_1, x_2 \longmapsto x_2 \qquad (x_1, x_2 \in X),$$

is associative and every element of X is a left identity while a right identity exists precisely when X has one element.

3.2.4

On the other hand, if e is a left identity and e' is a right identity, then they coincide. A semigroup with identity is called a *monoid*.

3.2.5

Since any one-sided identity is an *idempotent*, homomorphisms of binary structures send one-sided identities to idempotents. They do not preserve the property of being an identity, however, as the following example shows.

3.2.6 Example

Let $G = \mathbf{Z}$ and $G' = M_2(\mathbf{Z})$ be the sets of integers and, respectively, of 2 by 2 matrices with integral coefficients, equipped with the corresponding operations of multiplication. Then

$$n \longmapsto \begin{pmatrix} n & \\ & 0 \end{pmatrix}, \qquad (n \in \mathbf{Z}),$$

is a homomorphism that sends 1 to an element in $M_2(\mathbf{Z})$,

$$\begin{pmatrix} 1 & \\ & 0 \end{pmatrix}$$

that is not an identity in $M_2(\mathbf{Z})$.

3.2.7 Mon

Homomorphisms between monoids that preserve the identity elements are said to be *unital*. The class of all monoids with unital homomorphisms as arrows forms a non-full subcategory of the categories of semigroupsi and of binary structures. It will be denoted **Mon**.

3.3 The category of groups

3.3.1 Left and right inverses

Given a pair of element $\gamma, \gamma' \in G$ whose product is the identity element e, we say that γ' is a *right* inverse of γ while γ is a *left* inverse of γ'.

3.3.2

If γ' is a right inverse of γ and γ'' is a left inverse of γ, and multiplication is associative, then $\gamma' = \gamma''$.

3.3.3

In particular, if an element g of a monoid admits both a left and a right inverse, that inverse is necessarily two-sided and unique. In multiplicative notation it is denoted g^{-1}.

3.3.4

A monoid in which every element has inverse is called a *group*.

Exercise 15 *Show that in a group, the identity element is the only idempotent.*

Exercise 16 *Show that any homomorphism from a monoid to a group is unital.*

3.3.5 Grp

The class of all groups with homomorphisms as arrows forms a full subcategory of the categories of monoids, of semigroups, and of binary structures. It will be denoted **Grp**.

3.4 Comutative binary structures

3.4.1

A binary operation is said to be *commutative*, if

$$gh = hg \qquad (g, h \in G).$$

3.4.2

Commutative binary structures form a full subcategory $\mathbf{Bin}_{\mathrm{co}}$ of the category of all binary structures, commutative semigroups form a full subcategory $\mathbf{Sgr}_{\mathrm{co}}$ of the category of all semigroups, commutative monoids form a full subcategory $\mathbf{Mon}_{\mathrm{co}}$ of the category of all monoids.

3.5 The category of abelian groups

3.5.1 Terminology

The tradition to refer to commutative groups as *abelian* predates most of the terminology used in theory of algebraic structures. Abelian groups form a full subcategory **Ab** of the category of groups.

3.5.2 Additive notation

In theory of abelian groups, the result of performing the operation is often written

$$g + h,$$

the identity element is denoted 0 and referred to as the *zero* element, finally, the inverse of an element g is denoted $-g$. The operation itself is referred to as *addition*.

4 Categories of rings

4.1 Binary rings

4.1.1

A set R equipped with two binary operations,

$$r, s \longmapsto r + s, \qquad r, s \longmapsto rs \qquad (r, s \in R),$$

is said to be a *binary ring* if $(R, +)$ is an abelian group and $(R, \cdot)$ is a binary structure whose multiplication is *biadditive*, i.e., it satisfies the following distributivity identities

$$(r + r')s = rs + r's \qquad (r, r', s \in R), \tag{27}$$

and

$$r(s + s') = rs + rs' \qquad (r, s, s' \in R). \tag{28}$$

4.1.2 $\mathbf{Rng}_{\mathrm{bin}}$

Binary rings with morphisms being homomorphisms for both addition and multiplication, form a category denoted $\mathbf{Rng}_{\mathrm{bin}}$.

4.1.3 Terminology

In the context or rings, such terms as *associative*, *unital*, *commutative*, always refer to the multiplicative binary structure $(R, \cdot)$.

4.1.4 Domains

Rings for which the set of nonzero elements $R \setminus \{0\}$ is closed under multiplication are called *domains*.

4.1.5 Zero divisors

Given a pair r, r' of nonzero elements whose product iz zero,

$$rr' = 0,$$

we say that r is a *left zero divisor* and r' is a *right zero divisor*.

4.1.6

A ring is a domain precisely when it has no zero divisors.

4.1.7 The commutator operation

The binary operation

$$r, s \longmapsto [r, s] := rs - sr \qquad (r, s \in R),$$

is called the *commutator operation*.

4.1.8 $*$-rings

A ring equipped with an *antiinvolution*, i.e., an antiisomorphism

$$r \longmapsto r^*, \qquad (r \in R),$$

such that $r^{**} = r$, is called a $*$*-ring*. Such structures play an important role in Analysis and Mathematical Physics.

4.1.9 The associator operation

The ternary operation

$$r, s, t \;\longmapsto\; [r, s, t] := (rs)t - r(st) \qquad (r, s, t \in R),$$

is called the *associator operation*.

Exercise 17 *Show the so called Jacobi Identity*

$$[[r_0, r_1], r_2] + [[r_1, r_2], r_0] + [[r_2, r_0], r_1] = \sum_{\sigma \in S_3} \pm [r_{\sigma(0)}, r_{\sigma(1)}, r_{\sigma(2)}], \tag{29}$$

for any $r_0, r_1, r_2 \in R$, where summation is over all 6 permutations of the set $\{0, 1, 2\}$, and the sign is '$-$' for 3 transpositions ('odd' permutations) and '$+$' for the remaining 3 permutations ('even' permutations).

Exercise 18 *Prove the following commutator-associator identity*

$$r[s, t] - [rs, t] + [r, t]s \;=\; [r, t, s] - [r, s, t] - [t, r, s]\,. \tag{30}$$

Exercise 19 *Prove the following associator identity*

$$r[s, t, u] - [rs, t, u] + [r, st, u] - [r, s, tu] + [r, s, t]u \;=\; 0\,. \tag{31}$$

4.1.10

For associative rings the associator operation is identically zero, for commutative rings—the commutator operation.

4.2 Alternating rings

4.2.1

Rings satisfying the pair of identities

$$[r, r, s] = 0 = [r, s, s] \qquad (r, s \in R) \tag{32}$$

are said to be *alternating*.

Exercise 20 *Show that in an alternating ring the associator operation alternates, i.e., for any permutation $\sigma \in S_3$, one has*

$$[r_{\sigma(0)}, r_{\sigma(1)}, r_{\sigma(2)}] \;=\; \pm[r_0, r_1, r_2] \qquad (r_0, r_1, r_2 \in R) \tag{33}$$

with the sign determined by the parity *of the permutation.*

Exercise 21 *Show that a binary ring satisfying identity (33) satisfies also the identities*

$$2[r, r, s] \;=\; 0 \;=\; 2[r, s, s] \qquad (r, s \in R).$$

4.3 Unital rings

4.3.1 The characteristic of a unital ring

For any unital ring R, the correspondence

$$1 \longmapsto 1_R$$

extends uniquely to a homomorphism of unital rings $\mathbf{Z} \longrightarrow R$,

$$n \longmapsto \begin{cases} 1 + \cdots + 1 & (n \text{ times}) \;\; \text{if } n > 0 \\ 0_R & \text{if } n = 0 \\ -(1 + \cdots + 1) & (-n \text{ times}) \;\; \text{if } n < 0 \end{cases}.$$

The image of the ring of integers in R is either infinite—in this case we say that R is a ring of *characteristic zero*, or is a finite ring with n elements. In the latter case we say that R is a ring of characteristic n.

Exercise 22 *Show that the characteristic of a domain is either zero or a prime number.*

4.4 Associative rings

4.4.1 Rng

Associative rings form a full subcategory **Rng** of the category of binary rings.

4.4.2 $\mathbf{Rng}_{\mathrm{un}}$

Unital associative rings form a non-full subcategory $\mathbf{Rng}_{\mathrm{un}}$ of the category of associative rings.

4.4.3 Division rings

An associative domain is said to be a *division ring* if $(R\setminus\{0\}, \cdot)$ is a group, i.e., if any R is unital and any nonzero element of R has a multiplicative inverse.

4.4.4 Fields

Commutative division rings are called *fields*.

4.4.5 Rational numbers

Any field of characteristic zero, i.e., a field containing the ring of inteegers $\mathbf{Z}$, contains the field of rational numbers $\mathbf{Q}$.

Exercise 23 *Show that any automorphism α of $\mathbf{Q}$ fixes every element, i.e.,*

$$\alpha\left(\frac{m}{n}\right) = \frac{m}{n}$$

for all $m \in \mathbf{Z}$ and $n \in \mathbf{Z} \setminus \{0\}$. In particular, the field of rational numbers admits no nontrivial automorphisms.

Exercise 24 *Show that any automorphism α of the field of real numbers $\mathbf{R}$ preserves the property of being a positive number. Deduce from it that any automorphism of $\mathbf{R}$ preserves order.*

Exercise 25 *Show that any automorphism α of the field of real numbers $\mathbf{R}$ preserves the property of being a rational number. Deduce from this and the previous exercise that any automorphism of $\mathbf{R}$ fixes every element of $\mathbf{R}$. In particular, the field or real numbers admits no nontrivial automorphisms.*

4.4.6 Complex numbers

A *complex number* is a formal expresion $z = a + bi$ with $a, b \in \mathbf{R}$ and i being a reserved symbol. The multiplication of such expressions is dictated by the desire that multiplication by i is a linear transformation of the corresponding 2-dimensional real vector space with basis consisting of 1 and i, subject to the requirement that i supplies the missing square root of -1, i.e., $i^2 = 1$. The real numbers a and b are called the *real* and, respectively, the *imaginary* parts of z.

4.4.7

The ring of complex numbers is denoted $\mathbf{C}$ and is equipped with a structure of a $*$-ring via the complex conjugate operation

$$z \longmapsto \bar{z} := a - bi.$$

The number $\bar{z}$ is called the *conjugate* of z.

4.4.8

Since $z\bar{z} = a^2 + b^2$ is a nonnegative real number and

$$z\bar{z} = 0 \qquad \text{if and only if} \qquad z = 0,$$

any nonzero complex number is invertible with

$$z^{-1} = \frac{1}{z\bar{z}}\bar{z}.$$

In particular, $\mathbf{C}$ is a field.

4.4.9 The matrix realization of complex numbers

The field of complex numbers is isomorphic with the subring

$$\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right\}.$$

of the ring $M_2(\mathbf{R})$ of 2 by 2 real matrices. Transposition of matrices,

$$M \longmapsto {}^tM,$$

corresponds to complex conjugation of complex numbers.

Exercise 26 *Show that for any automorphism α of $\mathbf{C}$ one has*

$$\alpha(i) = \pm i.$$

Deduce from this that an automorphism of $\mathbf{C}$ that fixes every real number is either $\mathrm{id}_{\mathbf{C}}$ or the operation of complex conjugation.

4.4.10 Quaternions

A *quaternion* is a formal expression $\zeta = \alpha + \beta j$ with the "real" and "imaginary" parts being *complex numbers* and j being again an "imaginary unit", i.e., a square root of -1. Multiplication by j is again expected be a linear transformation of the corresponding $2 \cdot 2 = 4$ dimensional real vector space with basis $\{1, i, j, ij\}$, and ij is expected to be an imaginary unit itself, i.e., $(ij)^2 = -1$. The latter condition implies that symbols i and j *anticommute*.

Exercise 27 *Assuming that the multiplication is associative, show that the equality $(ij)^2 = -1$ is equivalent to the condition*

$$ij = -ji.$$

4.4.11

The product ij is denoted k. The resulting ring of quaternions is denoted $\mathbf{H}$.

Exercise 28 *Show that*

$$\zeta \longmapsto \bar{\zeta} := \bar{\alpha} - j\bar{\beta}$$

is an antiinvolution of $\mathbf{H}$.

4.4.12

Since $\zeta\bar{\zeta} = a^2 + (a')^2 + b^2 + (b')^2$ is a nonnegative real number and

$$\zeta\bar{\zeta} = 0 \qquad \text{if and only if} \qquad \zeta = 0,$$

any nonzero quaternion is invertible with

$$\zeta^{-1} = \frac{1}{\zeta\bar{\zeta}}\bar{\zeta}.$$

In particular, $\mathbf{H}$ is a noncommutative $*$-division ring.

4.4.13 The matrix realization of quaternions

The division ring of quaternions is isomorphic with the subring

$$\left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \right\}.$$

of the ring $M_2(\mathbf{C})$ of 2 by 2 complex matrices. Passing to the *adjoint* matrix

$$M \longmapsto {}^t\bar{M},$$

corresponds to conjugation of quaternions.

Exercise 29 *For a real number r, show that the set of quaternions satisfying equality*

$$\zeta^2 = r$$

consists of the real numbers $\pm\sqrt{r}$, when $r \geq 0$, and with the set of points of the 2-dimensional sphere of radius $\sqrt{-r}$ in the real vector space V with basis $\{i, j, k\}$, when $r < 0$.

4.4.14

It follows that subfields of $\mathbf{H}$ isomorphic to $\mathbf{C}$ that contain $\mathbf{R}$ are in one-to-one correspondence with 1-dimensional subspaces of V. The space of 1-dimensional subspaces of any vector space is called the *projectivization* of V and denoted $\mathbf{P}(V)$. Its dimension is one less than the dimension of V. In our case, its dimension is 2. Thus, complex number subfields of the ring of quaternions form naturally a real projective plane.

4.4.15 The quaternion group

The set

$$\{\pm 1, \pm i, \pm j, \pm k\} \tag{34}$$

is closed under the multiplication and forms a group which is usually referred to as the *quaternion group* (of order 8). It is denoted either Q or Q_8.

4.5 Lie rings

4.5.1

A binary ring satisfying the following two identities

$$(rs)t + (st)r + (tr)s \;=\; 0 \qquad (r, s, t \in R) \tag{35}$$

and

$$r^2 = 0 \qquad (r \in R)$$

is called a *Lie ring*.

4.5.2 $\mathrm{Rng}_{\mathrm{Lie}}$

Lie rings form a full subcategory of the category of binary rings.

4.5.3 The Lie ring associated with an associative ring

According to Exercise 17, the binary ring

$$(R, +, [\ ,\ ])$$

is a Lie ring if $(R, +, \cdot)$ is associative. We shall denote it R_{Lie}.

4.5.4 Terminology and notation

In view of the above relation between associative and Lie rings, the result of multiplication in a Lie ring performed on elements r, s is traditionally denoted $[r, s]$ rather than rs and the operation is often referred to as the *bracket* operation.

5 Actions of various structures on objects

5.1 Action of a set on an object

5.1.1

Let A be a set. A family of endomorphisms $(\lambda_a)_{a \in A}$ of an object $c \in \mathscr{C}_0$, i.e., a function

$$\lambda : A \longrightarrow \mathrm{End}_{\mathscr{C}}\, c\,, \tag{36}$$

represents *action of* A on c.

5.1.2 The category of A-objects

An object equipped with an action of A,

$$(c, \lambda)\,,$$

is referred to as an A*-object*.

5.1.3 Morphisms between A-objects

A morphism $\gamma : c \to c'$ is said to be a morphism of A-sets,

$$\gamma : (c, \lambda) \to (c', \lambda')\,, \tag{37}$$

if, for every $a \in A$, the following square

$$\begin{tikzcd} c' \arrow[r, "\lambda'_a"] & c' \\ c \arrow[u, "\gamma"] \arrow[r, "\lambda_a"'] \arrow[ur, phantom, "\circlearrowright"] & c \arrow[u, "\gamma"'] \end{tikzcd} \tag{38}$$

is commutative.

We shall often refer to morphisms of category $\mathscr{C}$ as A*-morphisms*.

Exercise 30 *Show that composition of A-morphisms produces an A-morphism.*

5.2 Action of a semigroup on an object

5.2.1

When A is equipped with a binary operation $\cdot$, then we say that $(A, \cdot)$ acts on an object c when a *homomorphism* of binary structures (36) is given, which means that

$$\forall_{a,b \in A}\ \lambda_{ab} = \lambda_a \circ \lambda_b\,.$$

5.2.2

Since composition of morphisms in category $\mathscr{C}$ is associative, actions of arbitrary binary structures $A, \cdot)$ always reduce to actions of semigroups.

5.3 Action of a monoid on an object with the identity morphism

5.3.1

When A is equipped with a structure of a monoid $(A, e, \cdot)$, then we say that $(A, \cdot)$ acts on an object c when a *homomorphism* of *monoids* (36) is given, which means that

$$\lambda_e = \mathrm{id}_c \qquad \text{and} \qquad \forall_{a,b\in A}\, \lambda_{ab} = \lambda_a \circ \lambda_b\,.$$