# Category Theory exercise sheet 2

September 14, 2022

## 1 Category theory

**Question 1.0.1.** Consider the category $\mathscr{C}$ induced by the following diagram.

$$\bullet \xrightarrow{t} * \tag{1}$$

We define:

$$
\begin{aligned}
F(\bullet) &= F(*) = \mathbb{N} \\
F(\mathrm{id}_\bullet) &= F(\mathrm{id}_*) = \mathrm{id}_\mathbb{N} \\
F(t) &= \mathrm{Succ} : \mathbb{N} \longrightarrow \mathbb{N}
\end{aligned}
$$

where Succ is the **successor function** defined by $\mathrm{Succ}(n) = n + 1$ for all $n \in \mathbb{N}$.

1. Prove that $F : \mathscr{C} \longrightarrow \underline{\mathrm{Set}}$ is a functor.
2. Prove that the image of $F$ is *not* a category.

## 2 Mathematics

**Question 2.0.1.** Introducing: monoids and rings.

**Definition 2.0.2.** A **monoid** consists of a set $M$ along with a **multiplication** function

$$
\begin{aligned}
\cdot : M \times M &\longrightarrow M \\
(m_1, m_2) &\longmapsto m_1 \cdot m_2
\end{aligned}
$$

and an identity element $e \in M$, subject to the following conditions:

- $\forall m_1, m_2, m_3 \in M, (m_1 \cdot m_2) \cdot m_3 = m_1 \cdot (m_2 \cdot m_3)$.
- $\forall m \in M, m \cdot e = e \cdot m = m$.

**Remark 2.0.3.** Notice that if we also required the following axiom

$$\forall m \exists m, m \cdot m' = m' \cdot m = e \tag{2}$$

then we would obtain exactly the definition of a *group*. This will help you think about monoids.

The canonical example of a monoid is the set $\mathbb{N}$ of natural numbers (including 0) with multiplication given by addition, and identity element given by 0.

**Definition 2.0.4.** A **ring** consists of an abelian group $(R, +, 0)$ along with a **multiplication** function

$$\begin{aligned} \cdot : R \times R &\longrightarrow R \\ (r_1, r_2) &\longmapsto r_1 \cdot r_2 \end{aligned}$$

and an identity element $1 \in R$ satisfying the following properties:

- $\forall r_1, r_2, r_3 \in R, (r_1 \cdot r_2) \cdot r_3 = r_1 \cdot (r_2 \cdot r_3)$.
- $\forall r \in R, 1 \cdot r = r \cdot 1 = r$.
- $\forall r_1, r_2, r_3 \in R, r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_2$.
- $\forall r_1, r_2, r_3 \in R, (r_1 + r_2) \cdot r_3 = r_1 \cdot r_3 + r_2 \cdot r_3$.

1. Guess the definitions of *morphisms of monoids* and *morphisms of rings.*
2. Let $\mathscr{C}$ be a category consisting of a single object $\mathrm{Obj}(\mathscr{C}) = \{\bullet\}$. Prove that $\mathrm{Hom}(\bullet, \bullet)$ is a monoid with multiplication given by composition, and identity element given by $\mathrm{id}_\bullet$.
3. Consider the inclusion morphism of the integers into the rational numbers.

   $$\iota : \mathbb{Z} \rightarrowtail \mathbb{Q} \tag{3}$$

   This is both a morphism of rings, and a morphism of groups, when $\mathbb{Z}, \mathbb{Q}$ are appropriately interpreted. Prove that:

- $\iota$ is a monomorphism in the category of rings and in the category of groups.
- $\iota$ is an epimorphism in the category of rings but *not* in the category of groups.

This exercise shows you that the *ambient category matters*. The map $\iota$ did not change, but the ambient category did, and we ended up with a new property about it. These kinds of situations are where the power of category theory shines.

Also, notice that $\iota$ is clearly not an isomoprhism (it is not surjective), yet in the category of groups we have that $\iota$ is a monomorphism and an epimorphism. Thus, it is *not* the case that a morphism is an isomorphism if if it is a monomorphism and an epimorphism. However, the converse *does* hold, that is, any isomorphism *is* a monomorphism and an epimorphism (prove this).

# 3 Computer Science

The computer science question for this week is to read and appreciate the following.

Assume we have a countably infinite collection of **variable types** $X, Y, Z, \dots$ (just formal symbols). We consider the following type construction rules:

- If $A, B$ are types then so is $A \times B$.
- If $A$ is a type then so is $A^*$.
- If $A, B$ are types then so is $A \longrightarrow B$.
- If $A(X)$ is a type depending on a variable $X$ then $\forall X.A(X)$ is a type.

In case the last dotpoint is confusing, we provide an example.

**Example 3.0.1.** Consider $\forall X.B \times X$ where $B$ is an arbitrary type and $X$ is a variable type. Spelling this out: we let $A(X)$ denote $B \times X$ (which is a type depending on a variable), and so $\forall X.A(X) = \forall X.B \times X$.

We define an interpretation $[\![\cdot]\!]$ of these types as relations.

- We interpret each variable type $X$ as the identity relation on some choice of set $\hat{X}$
$$[\![X]\!] := \mathrm{id}_{\hat{X}} \subseteq \hat{X} \times \hat{X} \tag{4}$$
That is, for each variable $X$ we choose a set $\hat{X}$ and interpret $X$ as the identity relation $[\![X]\!] = \mathrm{id}_{\hat{X}}$.

- Given interpretations $[\![A]\!], [\![B]\!]$ of types $A, B$ respectively, define $[\![A \times B]\!] \subseteq [\![A]\!] \times [\![B]\!]$ to be the relation defined by
$$\big((x, y), (x', y')\big) \in [\![A \times B]\!]$$
if and only if
$$(x, x') \in [\![A]\!] \text{ and } (y, y') \in [\![B]\!]$$

- Given an interpretation $[\![A]\!]$ define $[\![A^*]\!] \subseteq \bigcup_{i=1}^{\infty} \prod_{j=1}^{i} [\![A]\!]$ to be the relation:
$$\big([x_1, \ldots, x_n], [x'_1, \ldots, x'_n]\big) \in [\![A^*]\!]$$
if and only if for all $i = 1, \ldots, n$:
$$(x_i, x'_i) \in [\![A]\!]$$

- Given interpretations $[\![A]\!], [\![B]\!]$ the relation $[\![A \longrightarrow B]\!] \subseteq [\![A]\!] \times [\![B]\!]$ consists of pairs $(f, f')$ of functions from $[\![A]\!]$ to $[\![B]\!]$ given by
$$(f, f') \in [\![A \longrightarrow B]\!]$$
if and only if
$$(x, x') \in [\![A]\!] \text{ implies } (fx, f'x) \in [\![B]\!]$$

- If $X = \mathrm{id}_{\hat{X}}$ is a variable and $A(X)$ is a type depending on $X$ then $[\![\forall X.A(X)]\!]$ is the relation on the set of functions $r$ which take a type $B$ and return a relation $r_B \in [\![A(B)]\!]$ where $A(B)$ is such that $[\![A(B)]\!] \subseteq [\![C_1]\!] \times [\![C_2]\!]$ given by:
$$(r, r') \in [\![\forall X.A(X)]\!]$$
if and only if
$$(r_C, r'_{C'}) \in [\![A(B)]\!]$$

Now we make the *assumption of parametricity*.

**Proposition 3.0.2.** *If $t$ is a closed term of type $T$ then $(t,t) \in [\![T]\!]$.*

*Proof.* This is difficult (and outside the scope of the course), but the interested reader can look at [1] $\square$

We now show an example of how a theorem about a closed terms can be derived from knowledge of their type alone.

Let $r$ be a closed term of type

$$r : \forall X.X^* \longrightarrow X^* \tag{5}$$

By Parametricity, we have

$$(r,r) \in [\![\forall X.X^* \longrightarrow X^*]\!] \tag{6}$$

That is, for any relation $[\![A]\!] \subseteq [\![C_1]\!] \times [\![C_2]\!]$ we have

$$(r_{C_1}, r_{C_2}) \in [\![A^* \longrightarrow A^*]\!] \tag{7}$$

This in turn means that for any pair of lists $([x_1,\ldots,x_n],[x'_1,\ldots,x'_n]) \in [\![A^*]\!]$ we have

$$\big(r_{C_1}[x_1,\ldots,x_n], r_{C_2}[x'_1,\ldots,x'_n]\big) \in [\![A^*]\!] \tag{8}$$

Now we consider the case when the relation $[\![A]\!]$ is a function $\gamma : [\![C_1]\!] \longrightarrow [\![C_2]\!]$. In this setting we have

$$\gamma^*\big(r_{C_1}[x_1,\ldots,x_n]\big) = r_{C_2}[x'_1,\ldots,x'_n] \tag{9}$$

where $\gamma^*$ is the extension of $\gamma$ to lists. Noticing that $\gamma(x_i) = x'_i$ for each $i = 1,\ldots,n$ we now have

$$\gamma^*(r_{C_1})[x_1,\ldots,x_n] = r_{C_2}\gamma^*\big([x_1,\ldots,x_n]\big) \tag{10}$$

That is, we have the following equality of functions.

$$\gamma^* \circ r_{C_1} = r_{C_2} \circ \gamma^* \tag{11}$$

This is non-trivial and was derived purely from knowledge of the type of $r$.

As an example of this, take $r$ to be the function $\texttt{reverse} : \forall X. X^* \longrightarrow X^*$ that reverses a list, and $\gamma$ might be the function $\texttt{code} : \texttt{Char} \longrightarrow \texttt{Int}$ that converts a character to its ASCII code. Then we have

$$\begin{aligned}
\texttt{code}^*(\texttt{reverse}_{\texttt{Char}}[a,b,c]) &= \texttt{code}^*[c,b,a] \\
&= [99, 98, 97] \\
&= \texttt{reverse}_{\texttt{Int}}([97, 98, 99]) \\
&= \texttt{reverse}_{\texttt{Int}}(\texttt{code}^*[a,b,c])
\end{aligned}$$

that is,

$$\texttt{code}^* \circ \texttt{reverse}_{\texttt{Char}} = \texttt{reverse}_{\texttt{Int}} \circ \texttt{code}^* \tag{12}$$

as predicted by the theorem.

The above is an analysis of a simple typing system using set theoretic semantics. Taking formal systems (be them logical or computational) and interpretting them inside abstract categories (such as the category of sets, as done above) is a very active area of current research, and involves a lot of category theory. The interested reader can learn more by consulting [2], [3], [4].

# References


[1] P. Wadler *Theorems for free*. University of Glasgow. June 1989

[2] J.Y. Girard, *Geometry of Interaction, Interpretation of System F*, Studies in logic and the foundations of mathematics, 1989.

[3] D. Scott, *Toward a mathematical theory semantics for computer lanuages* Oxford University Computing Laboratory, 1971

[4] G. Manzonetto, *Models and theories of lambda-calculus* `https://tel.archives-ouvertes.fr/tel-00715207/document`