

Exercises

from Aluffi, *Algebra: Chapter 0*

I am self-studying this alongside Riehl, *Category Theory in Context*, so there is a bit of mixed notation.

Chapter I

Preliminaries

I.1 Naive set theory

2

Exercise I.1.1. Prove that if \sim is an equivalence relation on a set S , then the corresponding family \mathcal{P}_\sim is indeed a partition of S : that is, its elements are nonempty, disjoint, and their union is S .

Proof. An equivalence class $[a]_\sim$ is defined as $\{b \in S : b \sim a\}$ where $a \in S$.

Since $a \sim a$ by reflexivity, $a \in [a]_\sim$ and $[a]_\sim$ is nonempty.

Suppose $a \in [a]_\sim$ and $a \in [b]_\sim$, i.e., the classes are not disjoint. Then, by definition, $a \sim b$ and $b \sim a$ by symmetry. But for all $c \in [b]_\sim$, i.e., $c \sim b$, we have $c \sim a$ by transitivity. That is, $[b]_\sim \subseteq [a]_\sim$. Likewise, for all $d \in [a]_\sim$, we have $d \sim a \sim b \implies d \sim b$, so $[a]_\sim \subseteq [b]_\sim$ and in fact $[a]_\sim = [b]_\sim$.

Finally, notice that $[a]_\sim \subseteq S$ by definition. Then, $\bigcup \mathcal{P} \subseteq S$ since all elements of equivalence classes come from S . But $S \subseteq \bigcup \mathcal{P}$, since for all $a \in S$, there exists $[a]_\sim \in \mathcal{P}$ which contains a . Therefore, the union is exactly S . \square

Exercise I.1.2. Given a partition \mathcal{P} on a set S , show how to define a relation \sim on S such that \mathcal{P} is the corresponding partition.

Solution. Let $a, b \in S$ and $A, B \in \mathcal{P}$ be the sets containing a and b , respectively. Define $a \sim b \iff A = B$. \square

Exercise I.1.3. How many different equivalence relations may be defined on the set $\{1, 2, 3\}$?

Solution. Tackle the problem in general for a finite set S of n elements: for every pair of elements $a, b \in S$, $a \neq b$, either $a \sim b$ or $a \not\sim b$. The number of pairs of distinct elements of S is $\binom{n}{2} = \frac{n(n-1)}{2}$.

Therefore, there are $\frac{3(2)}{2} = 3$ possible equivalence relations on $\{1, 2, 3\}$. \square

Exercise I.1.4. Give an example of a relation that is reflexive and symmetric but not transitive. What happens if you attempt to use this relation to define a partition on the set?

Solution. Let $S = \mathbb{N}$ and define $n \sim m \iff n \mid m \vee m \mid n$. Since $n \mid n$, \sim is reflexive and symmetry is built-in. Then, $2 \sim 6$ and $6 \sim 3$, but $2 \not\sim 3$. That is, \sim is not transitive.

If we try to define a partition, notice that $2 \in [6]_{\sim}$ and $3 \in [6]_{\sim}$, but $[6]_{\sim} \neq [2]_{\sim}, [3]_{\sim}$. The “partition” is no longer disjoint. \square

Exercise I.1.5. Define a relation \sim on \mathbb{R} by setting $a \sim b \iff b - a \in \mathbb{Z}$. Prove that this is an equivalence relation, and find a “compelling” description for \mathbb{R}/\sim . Do the same for the relation \approx on the plane $\mathbb{R} \times \mathbb{R}$ defined by declaring $(a_1, a_2) \approx (b_1, b_2) \iff b_1 - a_1, b_2 - a_2 \in \mathbb{Z}$.

Solution. First, $a \sim a$ since $a - a = 0 \in \mathbb{Z}$. Since negation of an integer is an integer, we also have $a \sim b \iff b - a \in \mathbb{Z} \iff -(b - a) \in \mathbb{Z} \iff a - b \in \mathbb{Z} \iff b \sim a$. Finally, if $b - a \in \mathbb{Z}$ and $c - b \in \mathbb{Z}$, then $(c - b) + (b - a) = c - a \in \mathbb{Z}$. That is, \sim is an equivalence relation.

Consider \mathbb{R}/\sim . The difference $b - a$ is an integer if and only if b and a have the same fractional part (e.g., $3.4 - 1.4 = 2$). Therefore, \mathbb{R}/\sim is the set of fractional parts, i.e., the interval $[0, 1)$.

It follows for \approx that $\mathbb{R}/\approx = [0, 1)^2$. \square

I.2 Functions between sets

Exercise I.2.1. How many different bijections are there between a set S with n elements and itself?

Solution. If we give elements of S an arbitrary ordering from 1 to n , consider assigning another order to S (and then matching elements in the same spot). The number of ways to permute n elements is $n!$. \square

Exercise I.2.2. Prove that f has a right-inverse if and only if it is surjective.

Solution. (\Rightarrow) Suppose $f : A \rightarrow B$ has a right-inverse $g : B \rightarrow A$. Let $b \in B$. Then, $f(g(b)) =_B (b) = b$. That is, an element $a := g(b) \in A$ exists such that $f(a) = b$, i.e., f is surjective.

(\Leftarrow) Suppose f is surjective and let $b \in B$. There exists some a (which we pick arbitrarily) such that $f(a) = b$. Define $g(b) := a$. We can do this for all b , so $g : B \rightarrow A$ is a function. Then, $f(g(b)) = f(a) = b$, so $f \circ g =_B$, and we are done. \square

Exercise I.2.3. Prove that the inverse of a bijection is a bijection and that the composition of two bijections is a bijection.

Solution. Let $f : A \rightarrow B$ be a bijection. Then, there exists a two-sided inverse $g : B \rightarrow A$ such that $g \circ f =_A$ and $f \circ g =_B$. But this is exactly what it means for f to be the two-sided inverse of g , so g is a bijection.

Now, let $f : A \rightarrow B$ and $g : B \rightarrow C$ be bijections with inverses f^{-1} and g^{-1} .

Consider the composition $h := g \circ f : A \rightarrow C$. We have $(f^{-1} \circ g^{-1}) \circ h =_A$ since $f^{-1}(g^{-1}(g(f(a)))) = f^{-1}(f(a)) = a$. Likewise, $h \circ (f^{-1} \circ g^{-1}) =_B$ since $g(f(f^{-1}(g^{-1}(b)))) = g(g^{-1}(b)) = b$. Therefore, $(f^{-1} \circ g^{-1}) = h^{-1}$ and h is a bijection. \square

Exercise I.2.4. Prove that “isomorphism” is an equivalence relation (on any set of sets).

Solution. Let A , B , and C be sets of sets. Notice that (any) identity function is its own two-sided inverse since $((a)) = a$. Therefore, $A \cong A$.

Suppose $A \cong B$. Then, there exists a bijection $f : A \rightarrow B$. But the inverse $f^{-1} : B \rightarrow A$ is a bijection (Exercise 3), so $B \cong A$.

Finally, suppose $A \cong B$ and $B \cong C$. That is, there exist bijections $f : A \rightarrow B$ and $g : B \rightarrow C$. The composition $h := g \circ f : A \rightarrow C$ is a bijection (Exercise 3), so $A \cong C$. \square

Exercise I.2.5. Formulate a notion of epimorphism, in the style of the notion of monomorphism, and prove that a function is surjective if and only if it is an epimorphism.

Solution. Define an epimorphism as a function $f : A \rightarrow B$ such that for all sets Z and functions $\zeta, \zeta' : B \rightarrow Z$, $\zeta \circ f = \zeta' \circ f \implies \zeta = \zeta'$.

(\Leftarrow) Suppose that f is surjective and $\zeta \circ f = \zeta' \circ f$. Then, f has a right-inverse g , such that

$$\begin{aligned}\zeta \circ f \circ g &= \zeta' \circ f \circ g \\ \zeta \circ_B &= \zeta' \circ_B \\ \zeta &= \zeta'\end{aligned}$$

as desired.

(\Rightarrow) Suppose that f is epic, i.e., $\zeta \circ f = \zeta' \circ f \implies \zeta = \zeta'$. Then, whenever $b = f(a)$ is in the image of f , we must have $\zeta(f(a)) = \zeta(b) = \zeta'(b) = \zeta'(f(a))$. If f is not surjective, then we could pick ζ and ζ' such that they disagree on a b not in the image of f . Therefore, f must be surjective. \square

7

Exercise I.2.6. Let $f : A \rightarrow B$ be any function. Prove that the graph Γ_f of f is isomorphic to A .

Proof. Recall that $\Gamma_f := \{(a, b) \in A \times B \mid b = f(a)\}$.

We can apply the natural projection $\pi_A : \Gamma_f \rightarrow A$ by picking the first element from the pair. Then, notice that we can define an inverse $\pi_A^{-1}(a) = (a, f(a)) = (a, b)$. This is a bijection.

Therefore, $\Gamma_f \cong A$. \square

Exercise I.2.7. Describe as explicitly as you can all terms in the canonical decomposition of the function $f : \mathbb{R} \rightarrow \mathbb{C} : r \mapsto e^{2\pi ir}$.

Solution. Let \sim be the equivalence relation defined by f . Notice that $f(r)$ is cyclic and is the complex number $2\pi r$ radians along the unit circle, i.e., r rotations.

The canonical projection $\mathbb{R} \rightarrow \mathbb{R}/\sim$ sends each r to its fractional part in $[0, 1)$. Then, the bijection $\tilde{f}([r]_{\sim}) = e^{2\pi ir}$ where $r \in [0, 1)$. Finally, there is a natural injection from the unit circle to \mathbb{C} . \square

Exercise I.2.8. Show that if $A' \cong A''$ and $B' \cong B''$, and further $A' \cap B' = \emptyset$ and $A'' \cap B'' = \emptyset$, then $A' \cup B' \cong A'' \cup B''$. Conclude that the operation $A \coprod B$ is well-defined up to isomorphism.

Proof. Let $f : A' \rightarrow A''$ and $g : B' \rightarrow B''$ be bijections. Since A' and B' are disjoint, every $c \in A' \cup B'$ is either in A' or B' . Give the bijection explicitly:

$$h : A' \cup B' \rightarrow A'' \cup B'' : c \mapsto \begin{cases} f(c) & c \in A' \\ g(c) & c \in B' \end{cases}$$

which is well-defined since the cases are mutually exclusive and both $f(c)$ and $g(c)$ are present in $A'' \cup B''$.

Likewise, since A'' and B'' are disjoint, every $d \in A'' \cup B''$ is either in A'' or B'' . That is, we can write

$$h^{-1} : A'' \cup B'' \rightarrow A' \cup B' : d \mapsto \begin{cases} f^{-1}(d) & d \in A'' \\ g^{-1}(d) & d \in B'' \end{cases}$$

with the same results. This is trivially the inverse of h .

Since there is a bijection, $A' \cup B' \cong A'' \cup B''$. Therefore, since we define the operation $A \coprod B$ by the union of disjoint “copies” of sets, these are all equal up to isomorphism. \square

Exercise I.2.9. Show that if A and B are finite sets, then $|B^A| = |B|^{|A|}$.

Proof. A function $f : A \rightarrow B$ is fully defined by its graph, which associates with every element of A an element of B . That is, it makes $|A|$ choices between $|B|$ elements, of which there are $|B|^{|A|}$ ways to do so. \square

Exercise I.2.10. In view of Exercise 10, it is not unreasonable to use 2^A to denote the set of functions from an arbitrary set A to a set with two elements (say $0, 1$). Prove that there is a bijection between 2^A and the power set of A .

Proof. We can define a subset of A , i.e., an element of its power set, by whether it includes or excludes each element of A . That is, we have the bijection

$$\begin{aligned} f : 2^A &\rightarrow \mathcal{P}(A) : b \mapsto \{a \in A \mid b(a) = 1\} \\ f^{-1} : \mathcal{P}(A) &\rightarrow 2^A : S \mapsto b(a) = \begin{cases} 1 & a \in S \\ 0 & a \notin S \end{cases} \end{aligned}$$

as desired. \square

I.3 Categories

Solution. Let $f \in [C][X](A, B)$ and $g \in [C][X](B, C)$. That is, arrows f' from B to A and g' from C to B exist in C . Then, gf is an arrow in $[C][X](A, C)$ because the arrow $g'f'$ exists in $[C](C, A)$.

Identities from C transfer to C

: the endomorphisms remain unchanged since $[C][X](A, A) := [C](A, A)$ and associativity also trivially transfers. \square

Exercise I.3.2. If A is a finite set, how large is $[Set](A)$?

Solution. This is the number of set functions from A to itself, which we already calculated earlier to be $|A|^{|A|}$. \square

Exercise I.3.3. Formulate precisely what it means to say that 1_a is an identity with respect to composition in Example 3.3 (given by a reflexive and transitive \sim over S), and prove this assertion.

Solution. The morphism $1_a \in (a, a)$ must have the property that $1_a f = f$ and $g 1_a = g$ for all $f \in (b, a)$ and $g \in (a, c)$.

If such morphisms exist, then $f = (b, a)$ and $g = (a, c)$. Then, $1_a f = (b, a) = f$ as well, since $1_a f$ must be in (b, a) , which contains only one element f . Likewise, $g 1_a = (a, c) = g$. \square

Exercise I.3.4. Can we define a category in the style of Example 3.3 (using \leq) using the relation $<$ on the set \mathbb{Z} ?

Solution. No, since we do not get an identity 1_n in (n, n) (since $n \not< n$). \square

Exercise I.3.5. Explain in what sense Example 3.4 (using \subseteq) is an instance of the categories considered in Example 3.3 (using \sim).

Solution. The category \hat{S} is just the category from Example 3.3 defined over the set $\mathcal{P}(S)$ with the equivalence relation $A \sim B \iff A \subseteq B$. \square

Exercise I.3.6. Define a category V by taking $(V) = \mathbb{N}$ and letting $[V](n, m) =$ the set of $m \times n$ matrices with real entries, for all $n, m \in \mathbb{N}$. (I will leave the reader the task of making sense of a matrix with 0 rows or columns.) Use the product of matrices to define composition. Does this category “feel” familiar?

Solution. This “feels” like a category of linear transformations between dimensions. A 0-dimensional vector space is a singleton, so we will say that a $0 \times n$ matrix is like the zero matrix, and an $m \times 0$ matrix is like an m -dimensional vector. Verify the axioms.

The square identity matrices I_n fall into $[V](n, n)$ and have the property that $AI_n = A$ and $I_n B = B$ for all $m \times n$ matrices A and $n \times m$ matrices B . Associativity follows from matrix multiplication. Composition also follows, since the multiplication of any real-valued $m \times n$ matrix by an $n \times p$ matrix is a well-defined $m \times p$ matrix. \square

Exercise I.3.7. Define carefully objects and morphisms in Example 3.7 (coslice categories), and draw the diagram corresponding to composition.

Solution. This is the opposite of the slice category, so we will call it $C|X|A$. Like in Example 3.5, everything inherits from C .

The objects are morphisms from $[C](A, Z)$ for any Z . The morphisms are morphisms from $[C]$ between the other two non- A endpoints of the object.

For $f : A \rightarrow Z$ in $C|X|A$, the identity 1_f is

$$\begin{array}{ccc} & A & \\ f \swarrow & & \searrow f \\ Z & \xrightarrow{1_Z} & Z \end{array}$$

Commutativity is

$$\begin{array}{ccccc} & & A & & \\ & \swarrow f_1 & \downarrow f_2 & \searrow f_3 & \\ Z_1 & \xrightarrow{\sigma} & Z_2 & \xrightarrow{\tau} & Z_3 \end{array} \quad \text{becoming} \quad \begin{array}{ccc} & A & \\ \swarrow f_1 & & \searrow f_3 \\ Z_1 & \xrightarrow{\sigma\tau} & Z_3 \end{array} \quad \text{as desired.} \quad \square$$

Exercise I.3.8. A subcategory C' of a category C consists of a collection of objects of C with sets of morphisms $[C'](A, B) \subseteq [C](A, B)$ for all objects A, B in (C') , such that identities and compositions in C make C' into a category. A subcategory C' is full if $[C'](A, B) = [C](A, B)$ for all A, B in (C') .

Construct a category of infinite sets and explain how it may be viewed as a full subcategory of Set .

Solution. Let $InfSet$ be the category such that the objects are infinite sets and morphisms are set functions between them. Then, since infinite sets are sets, $(InfSet) \subseteq (Set)$. We are also taking all set functions between infinite sets, so $[InfSet](A, B) = [Set](A, B)$.

Now, the identities on infinite sets $1_A : A \rightarrow A$ exist and are included in $InfSet$.

Also, the composition of set functions $f : A \rightarrow B$ and $g : B \rightarrow C$ is a set function $gf : A \rightarrow C$. Since A and C are infinite sets, we include the composition in $[InfSet](A, C)$.

Therefore, $InfSet$ is a full subcategory of Set . \square

Exercise I.3.9. An alternative to the notion of a multiset is obtained by considering sets endowed with equivalence relations; equivalent elements are taken to be multiple instances of elements “of the same kind”.

Define a notion of morphism between such enhanced sets, obtaining a category $MSet$ containing (a “copy” of) Set as a full subcategory.

Which objects in $MSet$ determine ordinary multisets as defined in §2.2 and how? Spell out what a morphism of multisets would be from this point of view.

Solution. A morphism $f : (A, \sim) \rightarrow (B, \approx)$ between two multisets is a set function $f' : A \rightarrow B$ such that for all x and y in A , $x \sim y \implies f'(x) \approx f'(y)$.

We can define the subcategory Set' with objects as all the multisets $(A, =)$ where $=$ is “true” (set) equality. Then, every morphism between these “sets” must respect equality, i.e., this is a full subcategory.

In §2.2, multisets are defined as functions from sets to \mathbb{N}^* which return the multiplicity of a given element. For $(A, \sim) \in (MSet)$, we can construct the set function $m : A/\sim \rightarrow \mathbb{N}^* : [a]_\sim \mapsto |[a]_\sim|$. Then, a morphism $(A, \sim) \rightarrow (B, \approx)$ is a function $A/\sim \rightarrow B/\approx$ between the sets of equivalence classes. \square

Exercise I.3.10. Since the objects of a category C are not (necessarily interpreted as) sets, it is not clear how to make sense of a notion of “subobject” in general. In some situations it does make sense to talk about subobjects, and the subobjects of any given object A in C are in one-to-one correspondence with the morphisms $A \rightarrow \Omega$ for a fixed, special object Ω of C , called a subobject classifier.

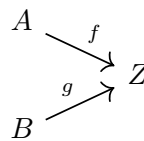
Show that Set has a subobject classifier.

Proof. Let $\Omega = \{\text{true}, \text{false}\}$. We then have a one-to-one correspondence between subsets of an object (set) A and morphisms (set functions) $A \rightarrow \Omega$.

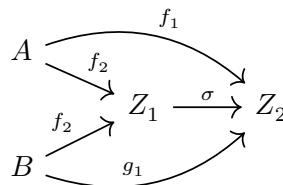
For $B \subseteq A$, let $b : A \rightarrow \Omega : b(a) = (a \in B)$. Likewise, for $f : A \rightarrow \Omega$, let $F = \{a \in A : f(a) = \text{true}\}$. Since a set is uniquely defined by its elements, this is a one-to-one correspondence, as desired. \square

Exercise I.3.11. Draw the relevant diagrams and define composition and identities for the category $C^{A,B}$ mentioned in Example 3.9. Do the same for the category $C^{\alpha,\beta}$ mentioned in Example 3.10.

Solution. We define the objects of $C^{A,B}$ to be tuples (Z, f, g) in C such that the diagram

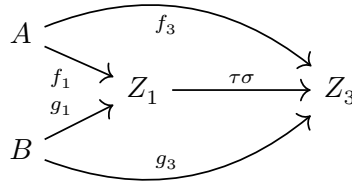


commutes and a morphism $(Z_1, f_1, g_1) \rightarrow (Z_2, f_2, g_2)$ to be a morphism $\sigma : Z_1 \rightarrow Z_2$ such that the diagram

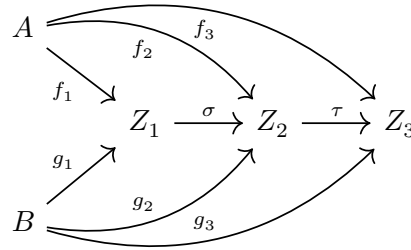


commutes.

To compose $\sigma : Z_1 \rightarrow Z_2$ with $\tau : Z_2 \rightarrow Z_3$, we can show that the diagram

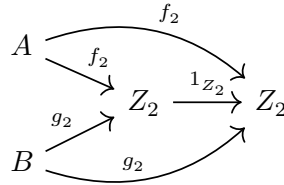


commutes, which follows from the fact that based on the definitions of σ and τ ,

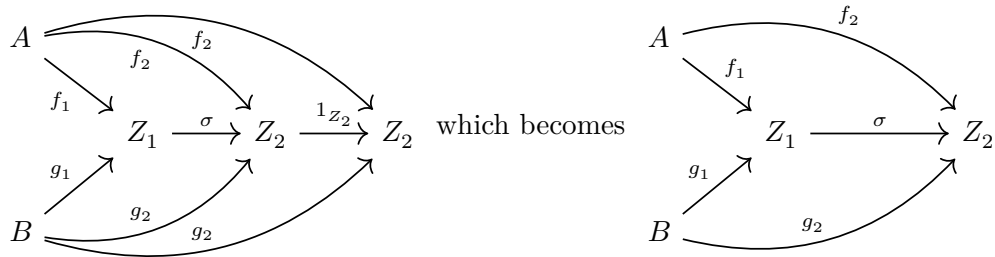


must commute.

The identities in $C^{A,B}$ are the same from C , e.g., $1_{Z_2} : Z_2 \rightarrow Z_2$, representing the diagram

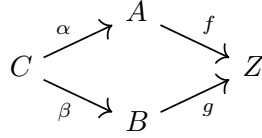


since if we compose on the left with the morphism σ we get the diagram

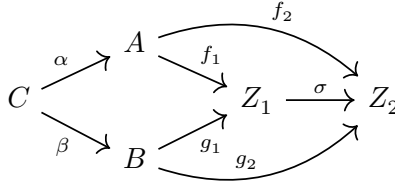


which is the original diagram for σ (and likewise if we compose on the right with 1_{Z_1}).

Now, consider $C^{\alpha,\beta}$ for fixed morphisms $\alpha : C \rightarrow A$ and $\beta : C \rightarrow B$ with the same source. The objects are tuples (Z, f, g) such that the diagram

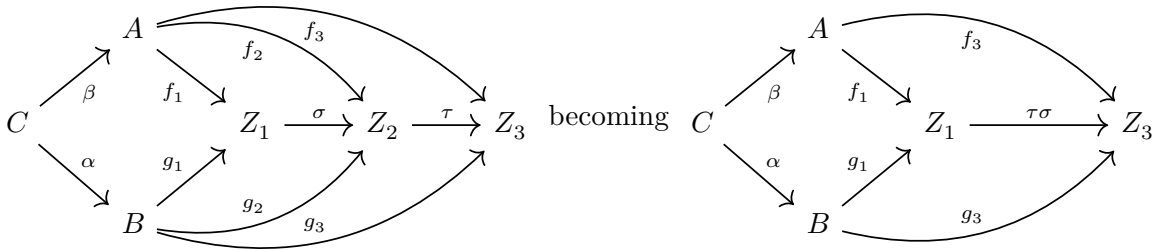


commutes in C (i.e., $f\alpha = g\beta$). A morphism $(Z_1, f_1, g_1) \rightarrow (Z_2, f_2, g_2)$ is a morphism $\sigma : Z_1 \rightarrow Z_2$ such the diagram



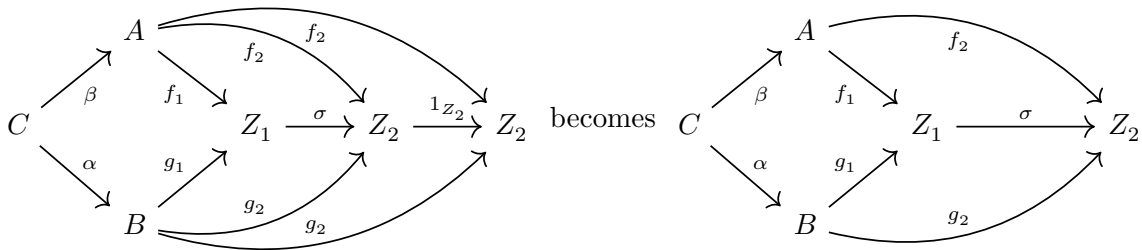
commutes (i.e., $f_2\alpha = \sigma f_1\alpha = \sigma g_1\beta = g_2\beta$).

Composition of $\sigma : Z_1 \rightarrow Z_2$ with $\tau : Z_2 \rightarrow Z_3$ gives us



just as above.

Finally, the identity for (Z, f, g) is again simply 1_Z since



which is just σ . □

I.4 Morphisms

Exercise I.4.1. In Example 3.3 we have seen how to construct a category from a set endowed with a relation, provided this latter is reflexive and transitive. For what types of relations is the corresponding category a groupoid?

Solution. Let (S, \sim) be a category defined as in Example 3.3. A groupoid is a category where all morphisms have inverses. That is, for $a, b \in S$, if there is a relation $a \sim b$, there must also be a relation $b \sim a$. Therefore, (S, \sim) is a groupoid whenever \sim is symmetric, i.e., \sim is an equivalence relation. \square

Exercise I.4.2. Let A, B be objects of a category C , and let $f \in [C](A, B)$ be a morphism.

Prove that if f has a right-inverse, then f is an epimorphism. Show that the converse does not hold, by giving an explicit example of a category and an epimorphism without a right-inverse.

Proof. Let $g : B \rightarrow A$ be the right-inverse of f , so $fg = 1_B$. Now, let $h, k : BC$ and suppose $hf = kf$. Composing on the right by g , we have

$$h = h1_B = h(fg) = (hf)g = (kf)g = k(fg) = k1_B = k.$$

That is, f is epic.

Now, consider the category (\mathbb{Z}, \leq) as defined in Example 3.3 and Exercise 4.2. If we let $h, k : 12$, we *must* have $h = k$ since there is only one relation $1 \leq 2$ in $[\mathbb{Z}](1, 2)$. But $2 \leq 1$ is not a morphism, so there is no inverse. That is, all morphisms are epic, but none have inverses. \square

Exercise I.4.3. Prove that the composition of two monomorphisms is a monomorphism. Deduce that one can define a subcategory C_{mono} of a category C by taking the same objects as in C and defining $[C_{\text{mono}}](A, B)$ to be the subset of $[C](A, B)$ consisting of monomorphisms, for all objects A, B . Do the same for epimorphisms.

Can you define a subcategory C_{nonmono} of C by restricting to morphisms that are not monomorphisms?

Proof. See Riehl, Exercise 1.2.iii for existence of C_{mono} and C_{epi} .

The subcategory C_{nonmono} cannot exist because identity morphisms are monic, i.e., for all $h, k : AB$, $1_B h = 1_B k \implies h = k$. Since we must have the identity morphisms in a subcategory, this subcategory does not exist. \square

Exercise I.4.4. Give a concrete description of monomorphisms and epimorphisms in the category $MSet$ you constructed in ??.

Solution. A monomorphism $f : (A, \sim)(B, \approx)$ in $MSet$ is a set function $f' : A \rightarrow B$ that is injective with respect to equivalence. That is, if $f'(a_1) \approx f'(a_2)$, then $a_1 \sim a_2$.

Likewise, an epimorphism $g : (A, \sim)(B, \approx)$ is a set function $g' : A \rightarrow B$ that is surjective with respect to equivalence. That is, for all b , there exists an a such that $g'(a) \approx b$. \square

I.5 Universal properties

Exercise I.5.1.