

I. Chapter 1

1. Preliminaries: Set theory and categories

1.1. Locate a discussion of Russel's paradox, and understand it.

Solution. Recall that, in naive set theory, any collection of objects that satisfy some property can be called a set. Russel's paradox can be illustrated as follows. Let R be the set of all sets that do not contain themselves. Then, if $R \notin R$, then by definition it must be the case that $R \in R$; similarly, if $R \in R$ then it must be the case that $R \notin R$.

1.2. ▷ Prove that if \sim is an equivalence relation on a set S , then the corresponding family \mathcal{P}_\sim defined in §1.5 is indeed a partition of S ; that is, its elements are nonempty, disjoint, and their union is S . [§1.5]

Solution. Let S be a set with an equivalence relation \sim . Consider the family of equivalence classes w.r.t. \sim over S :

$$\mathcal{P}_\sim = \{ [a]_\sim \mid a \in S \}$$

Let $[a]_\sim \in \mathcal{P}_\sim$. Since \sim is an equivalence relation, by reflexivity we have $a \sim a$, so $[a]_\sim$ is nonempty. Now, suppose a and b are arbitrary elements in S such that $a \not\sim b$. For contradiction, suppose that there is an $x \in [a]_\sim \cap [b]_\sim$. This means that $x \sim a$ and $x \sim b$. By transitivity, we get that $a \sim b$; this is a contradiction. Hence the $[a]_\sim$ are disjoint. Finally, let $x \in S$. Then $x \in [x]_\sim \in \mathcal{P}_\sim$. This means that

$$\bigcup_{[a]_\sim \in \mathcal{P}_\sim} [a]_\sim = S,$$

that is, the union of the elements of \mathcal{P}_\sim is S . ■

1.3. ▷ Given a partition \mathcal{P} on a set S , show how to define a relation \sim such that $\mathcal{P} = \mathcal{P}_\sim$. [§1.5]

Solution. Define, for $a, b \in S$, $a \sim b$ if and only if there exists an $X \in \mathcal{P}$ such that $a \in X$ and $b \in X$. We will show that $\mathcal{P} = \mathcal{P}_\sim$.

1. ($\mathcal{P} \subseteq \mathcal{P}_\sim$). Let $X \in \mathcal{P}$; we want to show that $X \in \mathcal{P}_\sim$. We know that X is nonempty, so choose $a \in X$ and consider $[a]_\sim \in \mathcal{P}_\sim$. We need to show that $X = [a]_\sim$. Suppose $a' \in X$ (it may be that $a' = a$.) Since $a, a' \in X$, $a \sim a'$, so $a' \in [a]_\sim$. Now, suppose $a' \in [a]_\sim$. We have $a' \sim a$, so $a' \in X$. Hence $X = [a]_\sim \in \mathcal{P}_\sim$, so $\mathcal{P} \subseteq \mathcal{P}_\sim$.

2. ($\mathcal{P}_\sim \subseteq \mathcal{P}$). Let $[a]_\sim \in \mathcal{P}_\sim$. From exercise I.1.1 we know that $[a]_\sim$ is nonempty. Suppose $a' \in [a]_\sim$. By definition, since $a' \sim a$, there exists a set X such that

$a, a' \in X$. Hence $[a]_{\sim} \subseteq X$. Also, if $a, a' \in X$ (not necessarily distinct) then $a \sim a'$. Therefore, $\mathcal{P}_{\sim} \subseteq \mathcal{P}$, and with 1. we get that the sets \mathcal{P} and \mathcal{P}_{\sim} are equal. ■

1.4. How many different equivalence relations can be defined on the set $\{1, 2, 3\}$?

Solution. From the definition of an equivalence relation and the solution to problem I.1.3, we can see that an equivalence relation on S is equivalent to a partition of S . Thus the number of equivalence relations on S is equal to the number of partitions of S . Since $\{1, 2, 3\}$ is small we can determine this by hand:

$$\begin{aligned}\mathcal{P}_0 &= \{ \{1, 2, 3\} \} \\ \mathcal{P}_1 &= \{ \{1\}, \{2\}, \{3\} \} \\ \mathcal{P}_2 &= \{ \{1, 2\}, \{3\} \} \\ \mathcal{P}_3 &= \{ \{1\}, \{2, 3\} \} \\ \mathcal{P}_4 &= \{ \{1, 3\}, \{2\} \}\end{aligned}$$

Thus there can be only 5 equivalence relations defined on $\{1, 2, 3\}$. ■

1.5. 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? (Hint: Thinking about the second question will help you answer the first one.)

Solution. For $a, b \in \mathbf{Z}$, define $a \diamond b$ to be true if and only if $|a - b| \leq 1$. It is reflexive, since $a \diamond a = |a - a| = 0 \leq 1$ for any $a \in \mathbf{Z}$, and it is symmetric since $a \diamond b = |a - b| = |b - a| = b \diamond a$ for any $a, b \in \mathbf{Z}$. However, it is not transitive. Take for example $a = 0, b = 1, c = 2$. Then we have $|a - b| = 1 \leq 1$, and $|b - c| = 1 \leq 1$, but $|a - c| = 2 > 1$; so $a \diamond b$ and $b \diamond c$, but not $a \diamond c$.

When we try to build a partition of \mathbf{Z} using \diamond , we get "equivalence classes" that are not disjoint. For example, $[2]_{\diamond} = \{1, 2, 3\}$, but $[3]_{\diamond} = \{2, 3, 4\}$. Hence \mathcal{P}_{\diamond} is not a partition of \mathbf{Z} . ■

1.6. Define a relation \sim on the set \mathbf{R} of real numbers by setting $a \sim b \iff b - a \in \mathbf{Z}$. Prove that this is an equivalence relation, and find a 'compelling' description for \mathbf{R}/\sim . Do the same for the relation \approx on the plane $\mathbf{R} \times \mathbf{R}$ by declaring $(a_1, b_1) \approx (a_2, b_2) \iff b_1 - a_1 \in \mathbf{Z}$ and $b_2 - a_2 \in \mathbf{Z}$. [§II.8.1, II.8.10]

Solution. Suppose $a, b, c \in \mathbf{R}$. We have that $a - a = 0 \in \mathbf{Z}$, so \sim is reflexive. If $a \sim b$, then $b - a = k$ for some $k \in \mathbf{Z}$, so $a - b = -k \in \mathbf{Z}$, hence $b \sim a$. So \sim is symmetric. Now, suppose that $a \sim b$ and $b \sim c$, in particular that $b - a = k \in \mathbf{Z}$ and $c - b = l \in \mathbf{Z}$. Then $c - a = (c - b) + (b - a) = l + k \in \mathbf{Z}$, so $a \sim c$. So \sim is transitive.

An equivalence class $[a]_{\sim} \in \mathbf{R}/\sim$ is the set of integers \mathbf{Z} transposed by some real number $\epsilon \in [0, 1)$. That is, for every set $X \in \mathbf{R}/\sim$, there is a real number $\epsilon \in [0, 1)$ such that every $x \in X$ is of the form $k + \epsilon$ for some integer k .

Now we will show that \approx is an equivalence relation over $\mathbf{R} \times \mathbf{R}$. Supposing $a_1, a_2 \in \mathbf{R} \times \mathbf{R}$, we have $a_1 - a_1 = a_2 - a_2 = 0 \in \mathbf{Z}$, so $(a_1, a_2) \approx (a_1, a_2)$. If we also suppose that $b_1, b_2, c_1, c_2 \in \mathbf{R} \times \mathbf{R}$, then symmetry and transitivity can be shown as well: $(a_1, a_2) \approx (b_1, b_2) \implies b_1 - a_1 = k$ for some integer k and $b_2 - a_2 = l$ for some integer l , hence $a_1 - b_1 = -k \in \mathbf{Z}$ and $a_2 - b_2 = -l \in \mathbf{Z}$, so $(b_1, b_2) \approx (a_1, a_2)$; also if $(a_1, a_2) \approx (b_1, b_2)$ and $(b_1, b_2) \approx (c_1, c_2)$, then $(b_1, b_2) - (a_1, a_2) = (k_1, k_2) \in \mathbf{Z} \times \mathbf{Z}$ as well as $(c_1, c_2) - (b_1, b_2) = (l_1, l_2) \in \mathbf{Z} \times \mathbf{Z}$, so $(c_1, c_2) - (a_1, a_2) = (c_1, c_2) - (b_1, b_2) + (b_1, b_2) - (a_1, a_2) = (k_1 + l_1, k_2 + l_2) \in \mathbf{Z} \times \mathbf{Z}$. Thus \approx is an equivalence relation.

The interpretation of \approx is similar to \sim . An equivalence class $X \in \mathbf{R} \times \mathbf{R}/\approx$ is just the 2-dimensional integer lattice $\mathbf{Z} \times \mathbf{Z}$ transposed by some pair of values $(\epsilon_1, \epsilon_2) \in [0, 1) \times [0, 1)$. ■

2. Functions between sets

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

Solution. A function $f : S \rightarrow S$ is a graph $\Gamma_f \subseteq S \times S$. Since f is bijective, then for all $y \in S$ there exists a unique $x \in S$ such that $(x, y) \in \Gamma_f$. We can see that $|\Gamma_f| = n$. Since each x must be unique, all the elements $x \in S$ must be present in the first component of exactly one pair in Γ_f . Furthermore, if we order the elements (x, y) in Γ_f by the first component, we can see that Γ_f is just a permutation on the n elements in S . For example, for $S = \{1, 2, 3\}$ one such Γ_f is:

$$\{(1, 3), (2, 2), (3, 1)\}$$

Since $|S| = n$, the number of permutations of S is $n!$. Hence there can be $n!$ different bijections between S and itself. ■

2.2. ▷ Prove statement (2) in Proposition 2.1. You may assume that given a family of disjoint subsets of a set, there is a way to choose one element in each member of the family. [§2.5, V3.3]

Proposition 2.1. Assume $A \neq \emptyset$, and let $f : A \rightarrow B$ be a function. Then

- (1) f has a left-inverse if and only if f is injective; and
- (2) f has a right-inverse if and only if f is surjective.

Solution. Let $A \neq \emptyset$ and suppose $f : A \rightarrow B$ is a function.

(\implies) Suppose there exists a function g that is a right-inverse of f . Then $f \circ g = \text{id}_A$. Let $b \in B$. We have that $f(g(b)) = b$, so there exists an $a = g(b)$ such that $f(a) = b$. Hence f is surjective.

(\impliedby) Suppose that f is surjective. We want to construct a function $g : B \rightarrow A$ such that $f(g(a)) = a$ for all $a \in A$. Since f is surjective, for all $b \in B$ there is an $a \in A$ such that $f(a) = b$. For each $b \in B$ construct a set Λ_b of such pairs:

$$\Lambda_b = \{ (a, b) \mid a \in A, f(a) = b \}$$

Note that Λ_b is non-empty for all $b \in B$. So that we can choose one pair (a, b) (a not necessarily unique) from each set in $\Lambda = \{ \Lambda_b \mid b \in B \}$ to define $g : B \rightarrow A$:

$$g(b) = a, \text{ where } a \text{ is in some } (a, b) \in \Lambda_b$$

Now, g is a right-inverse of f . To show this, let $b \in B$. Since f is surjective, g has been defined such that when $a = g(b)$, $f(a) = b$, so we get that $f(g(b)) = (f \circ g)(b) = b$, thus g is a right-inverse of f . ■

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

Solution. (1) Suppose $f : A \rightarrow B$ is a bijection, and that $f^{-1} : B \rightarrow A$ is its inverse. We have that $f \circ f^{-1} = \text{id}_B$ and $f^{-1} \circ f = \text{id}_A$. Hence f is the left- and right-inverse of f^{-1} , so f^{-1} must be a bijection. ■

(2) Let $f : B \rightarrow C$ and $g : A \rightarrow B$ be bijections, and consider $f \circ g$. To show that $f \circ g$ is injective, let $a, a' \in A$ such that $(f \circ g)(a) = (f \circ g)(a')$. Since f is a bijection, $f(g(a)) = f(g(a')) \implies g(a) = g(a')$. Also, since g is a bijection, $g(a) = g(a') \implies a = a'$. Hence $f \circ g$ is injective. Now, let $c \in C$. Since f is surjective, there is a $b \in B$ such that $f(b) = c$. Also, since g is surjective, there is an $a \in A$ such that $g(a) = b$; this means that there is an $a \in A$ such that $(f \circ g)(a) = c$. So $f \circ g$ is bijective.

2.4. ▷ Prove that ‘isomorphism’ is an equivalence relation (on any set of sets.) [§4.1]

Solution. Let S be a set. Then id_S is a bijection from S to itself, so $S \cong S$. Let T be another set with $S \cong T$, i.e. that there exists a bijection $f : S \rightarrow T$. Since f is a bijection, it has an inverse $f^{-1} : T \rightarrow S$, so $T \cong S$. Finally, let U also be a set, and assume that there exists bijections $f : S \rightarrow T$ and $g : T \rightarrow U$, i.e. that $S \cong T$ and $T \cong U$. From exercise I.2.3 we know that the composition of bijections is itself a bijection. This means that $g \circ f : S \rightarrow U$ is a bijection, so $S \cong U$. Hence \cong is an equivalence relation. ■

2.5. ▷ Formulate a notion of *epimorphism*, in the style of the notion of *monomorphism* seen in §2.6, and prove a result analogous to Proposition 2.3, for epimorphisms and surjections.

Solution. A function $f : A \rightarrow B$ is an *epimorphism* if and only if for all sets Z and all functions $b' : Z \rightarrow B$, there is a function $a' : Z \rightarrow A$ such that $f \circ a' = b'$. Now we will show that f is a surjection if and only if it is an epimorphism.

(\implies) Suppose that $f : A \rightarrow B$ is surjective. Let Z be a set and $b' : Z \rightarrow B$ a function. We need to construct a function $a' : Z \rightarrow A$ such that $f \circ a' = b'$. Fix $z \in Z$. Suppose $b = b'(z) \in B$. Since $b \in B$ and f is surjective, there exists an $a \in A$ such $f(a) = b$. Now, define $a'(z) = a$ this way for each $z \in Z$. Then $f \circ a'(z) = b'(z)$ for all $z \in Z$, so $f \circ a' = b'$. Hence f is an epimorphism.

(\impliedby) Suppose that f is an epimorphism. Let $b' : B \rightarrow B$ be a bijection. Since f is an epimorphism, there is a function $a' : B \rightarrow A$ such that $f \circ a' = b'$. Let $b \in B$. Since b' is a bijection, there is a unique element $y \in B$ such that $b'(y) = b$. Furthermore, we have that $(f \circ a')(y) = b$. In other words, $a = a'(y)$ is an element in A such that $f(a) = b$. Hence f is surjective, as required. ■

2.6. With notation as in Example 2.4, explain how any function $f : A \rightarrow B$ determines a section of π_A .

Solution. Let $f : A \rightarrow B$ and let $\pi_A : A \times B \rightarrow A$ be such that $\pi_A(a, b) = a$ for all $(a, b) \in A \times B$. Construct $g : A \rightarrow A \times B$ defined as $g(a) = (a, f(a))$ for all $a \in A$. The function g can be thought of as ‘determined by’ f . Now, since $(\pi_A \circ g)(a) = \pi_A(g(a)) = \pi_A(a, f(a)) = a$ for all $a \in A$, g is a right inverse of π_A , i.e. g is a section of π_A as required. ■

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

Solution. Recall that sets Γ_A and A are *isomorphic*, written $\Gamma_A \cong A$, if and only if there exists a bijection $g : \Gamma_A \rightarrow A$. Let’s construct such a function g , defined to be $g(a, b) = a$. Keep in mind that here $(a, b) \in \Gamma_f \subseteq A \times B$.

Let $(a', b'), (a'', b'') \in \Gamma_f$ such that $f(a', b') = f(a'', b'')$. For contradiction, suppose that $(a', b') \neq (a'', b'')$. Since $f(a', b') = a' = a'' = f(a'', b'')$, it must be that $b' \neq b''$. However, this would mean that both (a', b') and (a', b'') are in Γ_f ; this would mean that $f(a') = b' \neq b'' = f(a')$, which is impossible since f is a function. Hence g is injective.

Let $a' \in A$. Since f is a well-defined function with A as its domain, there must exist a pair $(a', b') \in \Gamma_f$ for some $b' \in B$, in particular that $g(a', b') = a'$; thus g is surjective, so it is a bijection. ■

2.8. Describe as explicitly as you can all terms in the canonical decomposition (cf. §2.8) of the function $\mathbf{R} \rightarrow \mathbf{C}$ defined by $r \mapsto e^{2\pi i r}$. (This exercise matches one

previously. Which one?)

Solution. Let $f : \mathbf{R} \rightarrow \mathbf{C}$ be as above. The first piece in the canonical decomposition is the equivalence relation \sim defined as $x \sim x' \iff f(x) = f(x')$, i.e. $[x]_{\sim}$ is the set of all elements in \mathbf{R} that get mapped to the same element in \mathbf{C} by f as x .

The second piece is the set \mathcal{P}_{\sim} . This set is the set of all equivalence classes of \mathbf{R} over equality up to f . Note that, since $f(x) = e^{2\pi i x} = \cos(2\pi x) + i \sin(2\pi x)$, f is periodic with period 1. That is, $f(x) = e^{2\pi i x} = e^{2\pi i x + 2\pi i} = e^{2\pi i(x+1)} = f(x+1)$. In other words, we can write \mathcal{P}_{\sim} as,

$$\mathcal{P}_{\sim} = \{ \{ r + k \mid k \in \mathbf{Z} \} \mid r \in [0, 1) \subseteq \mathbf{R} \},$$

and it is here when we notice uncanny similarities to exercise 1.6 where $x \sim y$, for $x, y \in \mathbf{R}$, if and only if $x - y \in \mathbf{Z}$, in which we could have written \mathcal{P}_{\sim} in the same way.

Now we will explain the mysterious $\tilde{f} : \mathcal{P}_{\sim} \rightarrow \text{im} f$. This function is taking each *equivalence class* $[x]_{\sim}$ over the reals w.r.t. \sim and mapping it to the element in \mathbf{C} that f maps each element $x' \in [x]_{\sim}$ to; indeed, since $x \sim x'$ is true for $x, x' \in \mathbf{R}$ if and only if $f(x) = f(x')$, we can see that for any $x \in \mathbf{R}$, for all $x' \in [x]_{\sim}$, there exists a $c \in \mathbf{C}$ such that $f(x') = c$. To illustrate with the equivalence class over \mathbf{R} w.r.t. \sim corresponding to the element $0 \in \mathbf{R}$, we have $[0]_{\sim} = \{ \dots, -2, -1, 0, 1, 2, \dots \}$. We can see that $e^{-4\pi i} = e^{-2\pi i} = e^{0\pi i} = 1 = e^{2\pi i} = e^{4\pi i}$, etc; so the function would map $[0]_{\sim} \mapsto 1 \in \mathbf{C}$, and so on. Furthermore, we can see that \tilde{f} is surjective, since for y to be in $\text{im} f$ is to say that there is an $x \in \mathbf{R}$ such that $f(x) = y$; so there must be an equivalence class $[x]_{\sim}$ which is mapped to y by \tilde{f} .

Finally, the simple map from $\text{im} f \rightarrow \mathbf{C}$ that simply takes $c \mapsto c$. This can be thought of as a potential “expansion” of the domain of \tilde{f} . It is obviously injective, since (trivially) $c \neq c' \implies c \neq c'$. However, it may not be surjective: for example, $2 \in \mathbf{C}$ is not in $\text{im} f$ as it is defined above.

2.9. ▷ 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 $A \sqcup B$ is well-defined up to *isomorphism* (cf. §2.9) [§2.9, 5.7]

Solution. Let A', A'', B', B'' be sets as described above. Since $A' \cong A''$ and $B' \cong B''$, we know there exists respective bijections $f : A' \rightarrow A''$ and $g : B' \rightarrow B''$. Now, we wish to show that $A' \cup B' \cong A'' \cup B''$. Define a function $h : A' \cup B' \rightarrow A'' \cup B''$ such that $h(x) = f(x)$ if $x \in A'$ and $g(x)$ if $x \in B'$.

We will now show that h is a bijection. Let $y \in A'' \cup B''$. Then, since $A'' \cap B'' = \emptyset$, either $y \in A''$ or $y \in B''$. Without loss of generality suppose that $y \in A''$. Then, since $f : A' \rightarrow A''$ is a bijection, it is *surjective*, so there exists an $x \in A' \subseteq A' \cup B'$ such that

$h(x) = f(x) = y$. So h is surjective. Now, suppose that $x \neq x'$, for $x, x' \in A' \cup B'$. If $x, x' \in A'$, then since f is injective and $h(x) = f(x)$ for all $x \in A'$, then $h(x) \neq h(x')$. Similarly for if $x, x' \in B'$. Now, without loss of generality if $x \in A'$ and $x' \in B'$, then $h(x) = f(x) \neq g(x') = h(x')$ since $A'' \cap B'' = \emptyset$. Hence h is a bijection, so $A' \cup B' \cong A'' \cup B''$.

Since these constructions of A', A'', B', B'' correspond to creating “copies” of sets A and B for use in the disjoint union operation, we have that disjoint union is a well-defined function *up to isomorphism*. In particular, since \cong is an equivalence relation, we can consider \sqcup to be well-defined from \mathcal{P}_{\cong} to $A' \cup B'$. ■

2.10. ▷ Show that if A and B are finite sets, then $|B^A| = |B|^{|A|}$. [§2.1, 2.11, I.4.1]

Solution. Let A and B be sets with $|A| = n$ and $|B| = m$, with n, m being non-negative integers. Recall that B^A denotes the set of functions $f : A \rightarrow B$. Now, if $A = B = \emptyset$ or $A = \emptyset$ and $|B| = 1$, we get one function, the empty function $\Gamma_f = \emptyset$, and $0^0 = 1^0 = 1$. If $|A| = |B| = 1$, then we get the singleton function $\Gamma_f = \{(a, b)\}$, and $1^1 = 1$. If $A \neq \emptyset$ and $B = \emptyset$, then no well-defined function can exist from A to B since there will be no value for the elements in A to take; this explains $|B^A| = |B|^{|A|} = 0^{|A|} = 0$.

Suppose that $B \neq \emptyset$ and B is finite. We will show inductively that $|B^A| = |B|^{|A|}$. First, suppose that $|A| = 1$. Then there are exactly $|B|$ functions from A to B : if $B = \{b_1, b_2, \dots, b_m\}$, then the functions are $\{(a, b_1)\}, \{(a, b_2)\}$, etc. Hence $|B^A| = |B|^{|A|} = |B|$. Now, fix $k \geq 2$, and assume that $|B^A| = |B|^{|A|}$ for all sets A such that $|A| = k - 1$. Suppose that $|A| = k$. Let $a \in A$. (We can do this since $|A| = k \geq 2$.) Then, by the inductive hypothesis, since $|A \setminus \{a\}| = k - 1$, $|B^{(A \setminus \{a\})}| = |B|^{|A|-1}$. Let F be the set of functions from $A \setminus \{a\}$ to B . Then, for each of those functions $f \in F$, there is $|B|$ “choices” of where to assign a : one choice for each element in B . Hence, $|B^A| = |B| |B|^{|A|-1} = |B|^{|A|}$ as required. ■

2.11. ▷ In view of Exercise 2.10, it is not unreasonable to use 2^A to denote the set of functions from an arbitrary set A to a set with 2 elements (say $\{0, 1\}$). Prove that there is a bijection between 2^A and the *power set* of A (cf. §1.2). [§1.2, III.2.3]

Solution. Let $S = \{0, 1\}$, and consider $f : \mathcal{P}(A) \rightarrow 2^A$, defined as

$$f(X) = \{(a, 1) \text{ if } a \in X, \text{ and } (a, 0) \text{ otherwise}\}$$

We will show that f is bijective. Let $g \in 2^A$. Then f is a function from A to S . Let $A_1 = \{a \in A \mid g(a) = 1\}$. Then A_1 is a set such that $A_1 \in \mathcal{P}(A)$, and $f(A_1) = g$. Hence f is surjective. Now, suppose that $X, Y \subseteq A$ and $f(X) = f(Y)$. Then, for all $a \in A$, $a \in X \iff f(X)(a) = 1 \iff f(Y)(a) = 1 \iff a \in Y$. Hence f is injective, so $2^A \cong \mathcal{P}(A)$. ■

3. Category theory

3.1. \triangleright Let \mathbf{C} be a category. Consider a structure \mathbf{C}^{op} with

1. $\text{Obj}(\mathbf{C}^{op}) = \text{Obj}(\mathbf{C})$
2. For A, B objects of \mathbf{C}^{op} (hence objects of \mathbf{C}), $\text{Hom}_{\mathbf{C}^{op}}(A, B) := \text{Hom}_{\mathbf{C}}(B, A)$.

Show how to make this into a category (that is, define composition of morphisms in \mathbf{C}^{op} and verify the properties listed in §3.1).

Intuitively, the ‘opposite’ category \mathbf{C}^{op} is simply obtained by ‘reversing all the arrows’ in \mathbf{C} . [5.1, §III.1.1, §IX.1.2, IX.1.10]

Solution. For objects $A, B, C \in \text{Obj}(\mathbf{C}^{op})$, the set of morphisms between A and B in \mathbf{C}^{op} , $\text{Hom}_{\mathbf{C}^{op}}(A, B)$, is defined as $\text{Hom}_{\mathbf{C}}(B, A)$. Similarly for the morphisms between B and C . So for morphisms $f \in \text{Hom}_{\mathbf{C}^{op}}(A, B)$ and $g \in \text{Hom}_{\mathbf{C}^{op}}(B, C)$, to define composition we recall the set-function $\circ_{\mathbf{C}} : \text{Hom}_{\mathbf{C}}(C, B) \times \text{Hom}_{\mathbf{C}}(B, A) \rightarrow \text{Hom}_{\mathbf{C}}(C, A)$ that is defined for the objects $A, B, C \in \text{Obj}(\mathbf{C}) = \text{Obj}(\mathbf{C}^{op})$; we shall define the composition of morphisms $f : A \rightarrow B$ and $g : B \rightarrow C$ in \mathbf{C}^{op} with this function. Precisely, we define

$$\circ_{\mathbf{C}^{op}} : \text{Hom}_{\mathbf{C}^{op}}(A, B) \times \text{Hom}_{\mathbf{C}^{op}}(B, C) \rightarrow \text{Hom}_{\mathbf{C}^{op}}(A, C)$$

to be

$$\circ_{\mathbf{C}^{op}}(f, g) = \circ_{\mathbf{C}}(g, f)$$

for all $f \in \text{Hom}_{\mathbf{C}^{op}}(A, B)$ and $f \in \text{Hom}_{\mathbf{C}^{op}}(B, C)$. The domain and codomain of $\circ_{\mathbf{C}}$ and $\circ_{\mathbf{C}^{op}}$ match (up to transposing the coordinates in the domain) due to the equality of $\text{Hom}_{\mathbf{C}}(A, B)$ with $\text{Hom}_{\mathbf{C}^{op}}(B, A)$.

To show that this composition makes \mathbf{C}^{op} a category, first we note that the fact that \mathbf{C} is a category implies the existence of a morphism 1_A taking A to itself where $A \in \text{Obj}(\mathbf{C})$; this morphism is thus also present in $\text{Hom}_{\mathbf{C}^{op}}(A, A) = \text{Hom}_{\mathbf{C}}(A, A)$. Secondly, for objects $A, B, C, D \in \text{Obj}(\mathbf{C})$, any morphisms $f \in \text{Hom}_{\mathbf{C}^{op}}(A, B)$, $g \in \text{Hom}_{\mathbf{C}^{op}}(B, C)$, and $h \in \text{Hom}_{\mathbf{C}^{op}}(C, D)$ are associative, since

$$(h \circ_{\mathbf{C}^{op}} g) \circ_{\mathbf{C}^{op}} f = f \circ_{\mathbf{C}} (g \circ_{\mathbf{C}} h) = (f \circ_{\mathbf{C}} g) \circ_{\mathbf{C}} h = h \circ_{\mathbf{C}^{op}} (g \circ_{\mathbf{C}^{op}} f).$$

Finally, for any morphism $f \in \text{Hom}_{\mathbf{C}^{op}}(A, B)$ we have,

$$f \circ_{\mathbf{C}^{op}} 1_A = 1_A \circ_{\mathbf{C}} f = f \text{ and } 1_B \circ_{\mathbf{C}^{op}} f = f \circ_{\mathbf{C}} 1_B = f;$$

hence the identities are “identities with respect to composition”. Last, for objects $A, B, C, D \in \text{Obj}(\mathbf{C})$ where $A \neq C$ and $B \neq D$, clearly $\text{Hom}_{\mathbf{C}}(B, A) \cap \text{Hom}_{\mathbf{C}}(D, C) = \emptyset$ is true iff $\text{Hom}_{\mathbf{C}^{op}}(A, B) \cap \text{Hom}_{\mathbf{C}^{op}}(C, D) = \emptyset$. Hence \mathbf{C}^{op} is a category.

3.2. If A is a finite set, how large is $\text{End}_{\text{Set}}(A)$?

Solution. The set $\text{End}_{\text{Set}}(A)$ is the set of functions $f : A \rightarrow A$. Since A is finite, write $|A| = n$ for some $n \in \mathbf{Z}$. By exercise 2.10, we know that $|A^A| = |A|^{|A|} = n^n$. So the set $\text{End}_{\text{Set}}(A)$ has size n^n .

3.3. \triangleright Formulate precisely what it means to say that 1_a is an identity with respect to composition in Example 3.3, and prove this assertion. [§3.2]

Solution.