Chapter 1

Preliminaries: Set theory and categories

1 Naive set theory

Exercises

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

Solution. There are many available options. I first read about Russell's paradox in Section 3.2 of [1]. □

1.2. ▷ Prove that if $\sim$ is a relation on a set S, then the corresponding family $\mathscr{P}_\sim$ 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 $[a]_\sim \in \mathscr{P}_\sim$ for some $a \in S$. Then $[a]_\sim$ is nonempty since it contains a, by reflexivity.

Let $[b]_\sim$ be another equivalence class, where $b \in S$. Suppose $c \in [a]_\sim \cap [b]_\sim$, that is $c \sim a$ and $c \sim b$. By symmetry we have $a \sim c$ and $c \sim b$. By transitivity this implies $a \sim b$. From this, it is not hard to show that $[a]_\sim = [b]_\sim$. In conclusion, equivalence classes are either equal or disjoint.

Clearly $\bigcup_{s\in S}[s]_\sim \subseteq S$ since we are taking the union of subsets of S. Conversely, $S \subseteq \bigcup_{s\in S}[s]_\sim$ since $s \in [s]_\sim$ for all $s \in S$ by reflexivity. □

1.3. ▷ Given a partition $\mathscr{P}$ on a set S, show how to define an equivalence relation $\sim$ on S such that $\mathscr{P}$ is the corresponding partition. [§1.5]

Solution. For $a, b \in S$ we say $a \sim b$ iff there exists some $X \in \mathscr{P}$ such that $a, b \in X$. □

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

Solution. This is equivalent to finding all partitions of $\{1,2,3\}$.

$$\{\{1\},\{2\},\{3\}\} \quad \{\{1\},\{2,3\}\} \quad \{\{1,3\},\{2\}\}$$

$$\{\{1,2\},\{3\}\} \quad \{\{1,2,3\}\}.$$ □

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. Consider the relation in the set $\mathbb{R}$, defined by the following rule. Let $a, b \in \mathbb{R}$. We say $a \sim b$ iff $|a-b| \leq 1$. This relation is clearly reflexive and symmetric, but it is not transitive (why?).

A reflexive, symmetric, non-transitive relation will result in a "partition" in which the classes are no longer disjoint. □

1.6. ▷ Define a relation $\sim$ on the set $\mathbb{R}$ of real numbers 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 $(a_1,a_2) \approx (b_1,b_2) \iff b_1 - a_1 \in \mathbb{Z}$ and $b_2 - a_2 \in \mathbb{Z}$. [§II.8.1, II.8.10]

Solution. Let $a, b, c \in \mathbb{R}$. We have that $a - a = 0 \in \mathbb{Z}$, so $a \sim a$ and the relation is reflexive. If $a \sim b$ then $b - a \in \mathbb{Z}$ and so $-(b-a) = a - b \in \mathbb{Z}$, which means $b \sim a$; hence the relation is symmetric. Finally, if $a \sim b$ and $b \sim c$ then $b - a$ and $c - b$ are integers and so $(b-a)+(c-b) = c - a \in \mathbb{Z}$, which means $a \sim c$ and the relation is transitive. We have shown that this is an equivalence relation. Notice that we are identifying real numbers that differ by an integer. In particular, we are identifying each (positive) real number with its fractional part (a similar thing is true for negative real numbers). So we can think of the quotient $\mathbb{R}/\sim$ as the interval $[0,1)$ since every number in this interval is a representative of a unique equivalence class, and these are all the equivalence classes.

For $\approx$ a similar discussion applies: it is analogously showed it is an equivalence relation, and one can think of the quotient as the unit square $[0,1)\times[0,1)$. This result also follows from Exercise 5.11. □

2 Functions between sets

Exercises

2.1. ▷ How many different bijections are there between a set S with n elements and itself? [§II.2.1]

Solution. $n!$. □

2.2. $\triangleright$ 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, V.3.3]

Solution. First we prove that if $f\colon A \to B$ has a right inverse then it is a surjection. Let $g\colon B \to A$ the the right inverse of f. Let $b \in B$. Then clearly $f(g(b)) = b$, so f is surjective.

Conversely, assume f is surjective. Then, if $b \in B$, we have that $f^{-1}(\{b\})$ is nonempty. For $b \in B$ we pick some $a_b \in f^{-1}(\{b\})$ and define $g\colon B \to A$ by $g(b) \coloneqq a_b$. By construction, $f \circ g = \mathrm{id}_B$. □

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

Solution. Let $f\colon A \to B$ and $g\colon B \to C$ be two bijections. Then f^{-1} is also a bijection since it has a two-sided inverse, namely f. Also, $g \circ f$ is a bijection since $f^{-1} \circ g^{-1}$ is a two-sided inverse. □

2.4. $\triangleright$ Prove that 'isomorphism' is an equivalence relation (on any set of sets). [§4.1]

Solution. See Exercise 2.3 for some necessary results. Clearly for any set A we have that A is isomorphic to A since $\mathrm{id}_A\colon A \to A$ is a bijection. If A is isomorphic to B then there is some bijection $f\colon A \to B$. But then $f^{-1}\colon B \to A$ is also a bijection and hence B is isomorphic to A. Now suppose A is isomorphic to B and B is isomorphic to C, where $f\colon A \to B$ and $g\colon B \to C$ are bijections. Then $g \circ f\colon A \to C$ is also a bijection and so A is isomorphic to C. □

2.5. $\triangleright$ 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. [§2.6, §4.2]

Solution. We say a function $f\colon A \to B$ is an *epimorphism* (or *epic*) if the following holds:

$$\textit{for all sets } Z \textit{ and all functions } \beta', \beta''\colon B \to Z$$

$$\beta' \circ f = \beta'' \circ f \implies \beta' = \beta''.$$

Now we claim that a function is an epimorphism iff it is a surjection. Indeed, if $f\colon A \to B$ is a surjection then it has a right inverse $g\colon B \to A$. Suppose Z is a set and let $\beta', \beta''\colon B \to Z$ be functions with $\beta' \circ f = \beta'' \circ f$. Then $(\beta' \circ f) \circ g = (\beta'' \circ f) \circ g$ which implies $\beta' \circ (f \circ g) = \beta'' \circ (f \circ g)$, and this in turn implies $\beta' \circ \mathrm{id}_B = \beta'' \circ \mathrm{id}_B$, and so $\beta = \beta''$ as desired.

Now suppose $f\colon A \to B$ is an epimorphism. For the sake of contradiction, suppose there is some $b_0 \in B$ such that $f(a) \neq b_0$ for all $a \in A$. Let $Z = \{0, 1\}$ and define $\beta', \beta'' \colon B \to Z$ by

$$\beta'(b) := 0 \text{ and } \beta''(b) := \begin{cases} 0 & \text{if } b \neq b_0 \\ 1 & \text{if } b = b_0 \end{cases},$$

for all $b \in B$. Clearly $\beta' \circ f = \beta'' \circ f$ but $\beta' \neq \beta''$, a contradiction. So f must be a surjection. □

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

Solution. Define $\pi_A^* \colon A \to A \times B$ by the rule $\pi_A^*(a) := (a, f(a))$. This is manifestly a section of π_A. □

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

Solution. Define $f^* \colon A \to \Gamma_f$ by the rule $f^*(a) := (a, f(a))$. We claim that f^* is a bijection. Indeed, we will see that the natural projection restricted to Γ_f, written as $\pi_A\big|_{\Gamma_f}$, is a two-sided inverse. Let $a \in A$ and consider

$$\begin{aligned} (\pi_A\big|_{\Gamma_f} \circ f^*)(a) &= \pi_A\big|_{\Gamma_f}(a, f(a)) \\ &= a = \mathrm{id}_A(a). \end{aligned}$$

Similarly, let $(a, f(a))$ be an arbitrary element of Γ_f. Then

$$\begin{aligned} (f^* \circ \pi_A\big|_{\Gamma_f})(a, f(a)) &= f^*(a) \\ &= (a, f(a)) = \mathrm{id}_{\Gamma_f}(a, f(a)). \end{aligned}$$

Thus f^* is a bijection. □

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

Solution. Let $f \colon \mathbb{R} \to \mathbb{C}$ be defined by $f(r) := e^{2\pi i r}$. We define an equivalence relation on $\mathbb{R}$ by $a \sim a' \iff f(a') = f(a'')$. This is easily seen to be the same as the equivalence relation defined in Exercise 1.6. In that exercise we saw that the quotient can be identified with the interval $[0, 1)$ and the projection $\pi \colon \mathbb{R} \to \mathbb{R}/\sim$ is assigning to each real number its (positive) fractional part. Then the canonical decomposition gives a bijection from the quotient, i.e. $[0, 1)$, to the image of f, i.e. the unit circle in the complex plane, by assigning to each $x \in [0, 1)$ the point $e^{2\pi i x}$. Finally, this unit circle is included in the whole complex plane, in the obvious sense. □

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 $A \sqcup B$ (as described in §1.4) is well-defined up to *isomorphism* (cf. §2.9). [§2.9, 5.7]

Solution. Let $f\colon A' \to A''$ and $g\colon B \to B'$ be bijections. Let us define $f \oplus g\colon A' \cup B' \to A'' \cup B''$ by the rule

$$f \oplus g(x) \coloneqq \begin{cases} f(x) & \text{if } x \in A' \\ g(x) & \text{if } x \in B' \end{cases}.$$

This is well defined since if $x \in A' \cup B'$ then $x \in A'$ or $x \in B'$ but not both, since $A' \cap B' = \emptyset$.

Now we prove $f \oplus g$ is a bijection. Define $f^{-1} \oplus g^{-1}\colon A'' \cup B'' \to A' \cup B'$ by

$$f^{-1} \oplus g^{-1}(y) \coloneqq \begin{cases} f^{-1}(y) & \text{if } y \in A'' \\ g^{-1}(y) & \text{if } y \in B'' \end{cases}.$$

This is well defined since if $y \in A'' \cup B''$ then $y \in A''$ or $y \in B''$ but not both, since $A'' \cap B'' = \emptyset$. It is immediately verified that $f \oplus g$ and $f^{-1} \oplus g^{-1}$ are inverses of each other and hence they are bijections.

In conclusion, no matter how we make disjoint copies of A and B, the resulting disjoint unions will be isomorphic. Hence, it makes some sense to talk about *the* disjoint union of A and B. □

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

Solution. Let $|A| = n$. We use induction on n. If $n = 0$ then $A = \emptyset$ and there is only one function $\emptyset \to B$, and further $1 = |B|^0$. This closes the base case.

Suppose the claim is true for some natural number n. Defining a function from a set of $n + 1$ elements to B is the same as first defining it for n elements, for which there are $|B|^n$ choices by inductive hypothesis, and then figuring out where the last element goes, for which there are $|B|$ choices. Overall, there must be $|B|^n|B| = |B|^{n+1}$ ways of defining the function when $|A| = n + 1$. This closes the induction. □

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. Define $F\colon 2^A \to \mathscr{P}(A)$ by the rule

$$F(f) \coloneqq f^{-1}(\{1\}), \text{ for all } f\colon A \to \{0, 1\}.$$

Now define $G\colon \mathscr{P}(A) \to 2^A$ by saying that, for all $S \subseteq A$ we have

$$G(S) \coloneqq \mathbf{1}_S,$$

where $\mathbf{1}_S$ is the indicator function of S, defined on A. It is readily seen that F and G are inverses of each other and hence bijections. □

3 Categories

Exercises

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

- $\mathrm{Obj}(\mathsf{C}^{op}) := \mathrm{Obj}(\mathsf{C})$;
- for A, B objects of C^{op} (hence objects of C), $\mathrm{Hom}_{\mathsf{C}^{op}}(A, B) := \mathrm{Hom}_{\mathsf{C}}(B, A)$.

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

Intuitively, the 'opposite' category C^{op} is simply obtained by 'reversing all the arrows' in C. [5.1, §VIII.1.1, §IX.1.2, IX.1.10]

Solution. Let A, B, C be objects of C^{op} and let $f \in \mathrm{Hom}_{\mathsf{C}^{op}}(A, B)$ and let $g \in \mathrm{Hom}_{\mathsf{C}^{op}}(B, C)$. Then $f \in \mathrm{Hom}_{\mathsf{C}}(B, A)$ and $g \in \mathrm{Hom}_{\mathsf{C}}(C, B)$. As C is a category, let us write the composition of g and f as $f \circ_{\mathsf{C}} g \in \mathrm{Hom}_{\mathsf{C}}(C, A)$. Then we can define

$$g \circ_{\mathsf{C}^{op}} f := f \circ_{\mathsf{C}} g \in \mathrm{Hom}_{\mathsf{C}}(C, A) = \mathrm{Hom}_{\mathsf{C}^{op}}(A, C).$$

For simplicity, we omit the symbol $\circ_{\mathsf{C}}$ from now on. This law of composition is associative since, if we let D be an object of C^{op} and $h \in \mathrm{Hom}_{\mathsf{C}^{op}}(C, D)$, then

$$h \circ_{\mathsf{C}^{op}} (g \circ_{\mathsf{C}^{op}} f) = h \circ_{\mathsf{C}^{op}} (fg) = (fg)h \overset{!}{=} f(gh) = f(h \circ_{\mathsf{C}^{op}} g) = (h \circ_{\mathsf{C}^{op}} g) \circ_{\mathsf{C}^{op}} f.$$

Notice we used the associativity in C at $\overset{!}{=}$.

If A is an object of C^{op} then it is an object of C and hence we must have an identity in C, denoted $1_A \in \mathrm{Hom}_{\mathsf{C}}(A, A)$. But then $1_A \in \mathrm{Hom}_{\mathsf{C}^{op}}(A, A)$ and thus it works as an identity in C^{op} as well. Indeed, if B is an object of C^{op} then $1_B \in \mathrm{Hom}_{\mathsf{C}^{op}}(B, B)$ and we have, for all $f \in \mathrm{Hom}_{\mathsf{C}^{op}}(A, B)$,

$$\begin{aligned} f \circ_{\mathsf{C}^{op}} 1_A &= 1_A f = f, \\ 1_B \circ_{\mathsf{C}^{op}} f &= f 1_B = f. \end{aligned} \qquad \square$$

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

Solution. $|A|^{|A|}$. □

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. Let $a, b \in S$, and let $f \in \mathrm{Hom}(a, b)$. Then $f = (a, b)$ by necessity. Furthermore, $1_a = (a, a)$ and $1_b = (b, b)$. Thus

$$\begin{aligned} 1_a f &= (a, a)(a, b) = (a, b) = f, \\ f 1_b &= (a, b)(b, b) = (a, b) = f. \end{aligned} \qquad \square$$

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

Solution. No because $<$ is not reflexive; hence the resulting "category" would not have identities. □

3.5. $\triangleright$ Explain in what sense Example 3.4 is an instance of the categories considered in Example 3.3. [§3.2]

Solution. In the power set of a set (or more generally in any set of sets), the relation $\subseteq$ is reflexive and transitive. □

3.6. $\triangleright$ (Assuming some familiarity with linear algebra.) Define a category V by taking $\text{Obj}(\mathsf{V}) = \mathbb{N}$ and letting $\text{Hom}_{\mathsf{V}}(n, m) =$ the set of $n \times m$ matrices with real entries, for all $n, m \in \mathbb{N}$ (We will leave the reader the task of making sense of a matrix with 0 rows or columns.) Use product of matrices to define composition. Does this category 'feel' familiar? [§VI.2.1, §VIII.1.3]

Solution. In this category the product of matrices is associative, hence they form a valid composition law. Furthermore, identity matrices clearly behave like identities with respect to this composition.

Note Having thought about it, I'm not sure what he means by that last question. □

3.7. $\triangleright$ Define carefully objects and morphisms in Example 3.7, and draw the diagram corresponding to composition. [§3.2]

Solution. Objects of C^A are morphisms from A to Z for some object Z of C, i.e. $A \to Z$. Then if we have some $A \xrightarrow{f} Z_1$ and some $A \xrightarrow{g} Z_2$ then a morphism from the former to the latter is a commutative diagram

$$\begin{tikzcd}
& Z_1 \arrow[dd, "\sigma"] \\
A \arrow[ur, "f"] \arrow[dr, "g"'] & \\
& Z_2
\end{tikzcd}$$

where $\sigma \in \text{Hom}_{\mathsf{C}}(Z_1, Z_2)$. □

3.8. $\triangleright$ A *subcategory* C' of a category C consists of a collection of objects of C, with morphisms $\text{Hom}_{\mathsf{C}'}(A, B) \subseteq \text{Hom}_{\mathsf{C}}(A, B)$ for all objects A, B in $\text{Obj}(\mathsf{C}')$, such that identities and compositions in C make C' into a category. A subcategory C' is *full* if $\text{Hom}_{\mathsf{C}'}(A, B) = \text{Hom}_{\mathsf{C}}(A, B)$ for all A, B in $\text{Obj}(\mathsf{C}')$. Construct a category of *infinite sets* and explain how it may be viewed as a full subcategory of Set. [4.4, §VI.1.1, §VIII.1.3]

Solution. Define $\mathrm{Obj}(\mathsf{C}')$ to be all infinite sets, and define $\mathrm{Hom}_{\mathsf{C}'}(A,B) := B^A = \mathrm{Hom}_{\mathsf{Set}}(A,B)$. Under these definitions, it is clear that C' is a full subcategory of Set. □

3.9. ▷ An alternative to the notion of *multiset* introduced in §2.2 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. (There may be more than one reasonable way to do this! This is intentionally an open-ended exercise.) 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. (There are several natural notions of morphisms of multisets. Try to define morphisms in MSet so that the notion you obtain for ordinary multisets captures your intuitive understanding of these objects.) [§2.2, §3.2, 4.5]

Solution. If $(A,\sim_A)$ and $(B,\sim_B)$ are multisets as described in the question, then morphisms from $(A,\sim_A)$ to $(B,\sim_B)$ are functions $f\colon A\to B$ such that

$$a' \sim_A a'' \implies f(a') \sim_B f(a'') \text{ for all } a', a'' \in A.$$

It is trivial to check the axioms of a category. An isomorphism between to multisets would be a bijection between the underlying sets that preserves the equivalence classes.

Set is a full subcategory of MSet in the sense that it is the same as the full subcategory consisting of multisets of the form $(S,=)$.

The objects of MSet that are multisets in the sense of §2.2 are the ones in which the equivalence classes contain finitely many elements. □

3.10. Since the objects of a category C are not (necessarily) 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 $A\to\Omega$ for a fixed, special object Ω of C, called a *subobject classifier.* Show that Set has a subobject classifier.

Solution. Indeed, $\{0,1\}$ is such a subobject classifier; this is the content of Exercise 2.11. □

3.11. ▷ Draw the relevant diagrams and define composition and identities for the category $\mathsf{C}^{A,B}$ mentioned in Example 3.9. Do the same for the category $\mathsf{C}^{\alpha,\beta}$ mentioned in Example 3.10. [§5.5, 5.12]

Solution. Objects in $\mathsf{C}^{A,B}$ are diagrams of the form

$$\begin{tikzcd}
A \arrow[dr] & \\
& Z \\
B \arrow[ur] &
\end{tikzcd},$$

where Z is an object of C and arrows correspond to morphisms in C in the obvious way.

Given two objects of $\mathsf{C}^{A,B}$

$$\begin{tikzcd}
A \arrow[dr, "f_1"] & & & A \arrow[dr, "f_2"] & \\
& Z_1 & & & Z_2 \\
B \arrow[ur, "g_1"'] & & & B \arrow[ur, "g_2"'] &
\end{tikzcd}$$

A morphism from the leftmost one to the other one is given by a commutative diagram of the form

$$\begin{tikzcd}
A \arrow[dr, "f_1"] \arrow[drr, bend left, "f_2"] & & \\
& Z_1 \arrow[r, "\sigma"] & Z_2 \\
B \arrow[ur, "g_1"'] \arrow[urr, bend right, "g_2"'] & &
\end{tikzcd},$$

for some $\sigma \in \mathrm{Hom}_{\mathsf{C}}(Z_1, Z_2)$. Given two morphisms

$$\begin{tikzcd}
A \arrow[dr, "f_1"] \arrow[drr, bend left, "f_2"] & & & A \arrow[dr, "f_2"] \arrow[drr, bend left, "f_3"] & & \\
& Z_1 \arrow[r, "\sigma"] & Z_2 & & Z_2 \arrow[r, "\tau"] & Z_3 \\
B \arrow[ur, "g_1"'] \arrow[urr, bend right, "g_2"'] & & & B \arrow[ur, "g_2"'] \arrow[urr, bend right, "g_3"'] & &
\end{tikzcd},$$

we can compose them as follows. First, combine them to form one big commutative diagram.

$$\begin{tikzcd}
A \arrow[dr, "f_1"] \arrow[drr, bend left, "f_2"] \arrow[drrr, bend left, "f_3"] & & & \\
& Z_1 \arrow[r, "\sigma"] & Z_2 \arrow[r, "\tau"] & Z_3 \\
B \arrow[ur, "g_1"'] \arrow[urr, bend right, "g_2"'] \arrow[urrr, bend right, "g_3"'] & & &
\end{tikzcd}.$$

It is immediate that the diagram obtained by removing the middle object is commutative; that is to say that the diagram

$$\begin{tikzcd}
A \arrow[dr, "f_1"] \arrow[drr, bend left, "f_3"] & & \\
& Z_1 \arrow[r, "\tau\sigma"] & Z_2 \\
B \arrow[ur, "g_1"'] \arrow[urr, bend right, "g_3"'] & &
\end{tikzcd}$$

commutes. Identities in $\mathsf{C}^{A,B}$ are just diagrams of the form

$$\begin{tikzcd}
A \arrow[dr, "f"] \arrow[drr, bend left, "f"] & & \\
& Z \arrow[r, "1_Z"] & Z . \\
B \arrow[ur, "g"'] \arrow[urr, bend right, "g"'] & &
\end{tikzcd}$$

Again, it is immediate that this diagram commutes and it behaves like an identity with respect to composition.

For the category $\mathsf{C}^{\alpha,\beta}$ we are given some fixed objects of C, call them A, B, C, and fixed morphisms $\alpha\colon C \to A$ and $\beta\colon C \to B$. An object in $\mathsf{C}^{\alpha,\beta}$ is a commutative diagram of the form

$$\begin{tikzcd}
& A \arrow[dr] & \\
C \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & Z , \\
& B \arrow[ur] &
\end{tikzcd}$$

where Z is an object of C and arrows correspond to morphisms in C in the obvious way.

Given two objects

$$\begin{tikzcd}
& A \arrow[dr, "f_1"] & & & & A \arrow[dr, "f_2"] & \\
C \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & Z_1 & & C \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & Z_2 , \\
& B \arrow[ur, "g_1"'] & & & & B \arrow[ur, "g_2"'] &
\end{tikzcd}$$

a morphism between from the leftmost one to the other one is a commutative diagram of the form

$$\begin{tikzcd}
& A \arrow[dr, "f_1"] \arrow[drr, bend left, "f_2"] & & \\
C \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & Z_1 \arrow[r, "\sigma"] & Z_2 , \\
& B \arrow[ur, "g_1"'] \arrow[urr, bend right, "g_2"'] & &
\end{tikzcd}$$

where $\sigma \in \mathrm{Hom}_{\mathsf{C}}(Z_1, Z_2)$. Given two morphisms

$$\begin{tikzcd}
& A \arrow[dr, "f_1"] \arrow[drr, bend left, "f_2"] & & & & & A \arrow[dr, "f_2"] \arrow[drr, bend left, "f_3"] & & \\
C \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & Z_1 \arrow[r, "\sigma"] & Z_2 & & C \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & Z_2 \arrow[r, "\tau"] & Z_3 , \\
& B \arrow[ur, "g_1"'] \arrow[urr, bend right, "g_2"'] & & & & & B \arrow[ur, "g_2"'] \arrow[urr, bend right, "g_3"'] & &
\end{tikzcd}$$

we can compose them as follows. First, combine them as depicted below.

$$\begin{tikzcd}
& A \arrow[dr, "f_1"] \arrow[drr, bend left, "f_2"] \arrow[drrr, bend left, "f_3"] & & & \\
C \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & Z_1 \arrow[r, "\sigma"] & Z_2 \arrow[r, "\tau"] & Z_3 \\
& B \arrow[ur, "g_1"'] \arrow[urr, bend right, "g_2"'] \arrow[urrr, bend right, "g_3"'] & & &
\end{tikzcd}$$

The resulting diagram is seen to be commutative. In particular, it is commutative when we remove the middle object, Z_2.

$$\begin{tikzcd}
& A \arrow[dr, "f_1"] \arrow[drr, bend left, "f_3"] & & \\
C \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & Z_1 \arrow[r, "\tau\sigma"] & Z_3 . \\
& B \arrow[ur, "g_1"'] \arrow[urr, bend right, "g_2"'] & &
\end{tikzcd}$$

Identities in this category are morphisms of the form

$$\begin{tikzcd}
& A \arrow[dr, "f"] \arrow[drr, bend left, "f"] & & \\
C \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & Z \arrow[r, "1_Z"] & Z . \\
& B \arrow[ur, "g"'] \arrow[urr, bend right, "g"'] & &
\end{tikzcd}$$

□

4 Morphisms

Exercises

4.1. ▷ Composition is defined for *two* morphisms. If more than two morphisms are given, e.g.,

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \xrightarrow{i} E$$

then one may compose them in several ways, for example:

$$(ih)(gf), \quad (i(hg))f, \quad i((hg)f), \quad \text{etc.}$$

so that at every step one is only composing two morphisms. Prove that the result of any such nested composition is independent of the placement of the parentheses. (Hint: Use induction on n to show that any such choice for $f_n f_{n-1} \dots f_1$ equals

$$((\dots((f_n f_{n-1}) f_{n-2}) \dots) f_1).$$

Carefully working out the case $n = 5$ is helpful.) [§4.1, §II.1.3]

Solution. We use strong induction on the number of morphisms, call it n, to prove that, if the morphisms to be composed are $f_n f_{n-1} \dots f_1$, then all nested compositions equal $((\dots((f_n f_{n-1}) f_{n-2}) \dots) f_1)$. For $n = 1$ the proposition is clear. Suppose inductively that if we have k morphisms to compose, say $f_k f_{k-1} \dots f_1$, for some $k < n$ then all nested compositions equal $((\dots((f_k f_{k-1}) f_{k-2}) \dots) f_1)$. Then, if we are composing n morphisms we have a product of two maps

$$(\dots)(\dots),$$

where each of the parenthesis contain the composition of fewer than n maps. Hence, by the inductive hypothesis, this is equal to

$$((\dots((g_s g_{s-1}) g_{s-2}) \dots) g_1)((\dots((h_t h_{t-1}) h_{t-2}) \dots) h_1) \tag{1.1}$$

for some $s, t < n$ with $s + t = n$. We want the above to equal

$$((\dots((((\dots((g_s g_{s-1}) g_{s-2}) \dots) g_1) h_t) h_{t-1}) \dots) h_1), \tag{1.2}$$

and if we can show this then we are done. Thus, we use induction on t to prove that (1.1) equals (1.2). If $t = 1$ this is obvious. Assume the result is true when we have $t - 1$ morphisms; this is our new inductive hypothesis. Then, we can write (1.1) as follows, by associativity

$$(\underbrace{(((\dots((g_s g_{s-1}) g_{s-2}) \dots) g_1)((\dots((h_t h_{t-1}) h_{t-2}) \dots) h_2))}_{\text{Apply new inductive hypothesis}} \ h_1).$$

Then, applying our new inductive hypothesis on the middle expression we get exactly (1.2). This closes both induction arguments, so we are done.

Note While this proof is not as bad a I'd imagined, I wonder whether there is a simpler proof of such an intuitive fact. □

4.2. ▷ 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 (cf. Example 4.6)? [§4.1]

Solution. When the relation is, in addition, symmetric, i.e. when it is an equivalence relation. □

4.3. Let A, B be objects of a category C, and let $f \in \mathrm{Hom}_C(A, B)$ 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.

Solution.

- Let g be a right inverse. Let Z be an object of C and let $\beta', \beta'' \colon B \to Z$ be morphisms. If we have $\beta' \circ f = \beta'' \circ f$ then apply g on the right as follows.

$$\begin{aligned} & (\beta' \circ f) \circ g = (\beta'' \circ f) \circ g \\ \Longrightarrow \quad & \beta' \circ (f \circ g) = \beta'' \circ (f \circ g) \\ \Longrightarrow \quad & \beta' \circ 1_B = \beta'' \circ 1_B \\ \Longrightarrow \quad & \beta' = \beta''. \end{aligned}$$

Thus f is an epimorphism.

- The category $\leq$ on $\mathbb{Z}$, take any non-identity morphism. □

4.4. Prove that the composition of two monomorphisms is a monomorphism. Deduce that one can define a subcategory $\mathsf{C}_{\mathsf{mono}}$ of a category C by taking the same objects as in C and defining $\mathrm{Hom}_{\mathsf{C}_{\mathsf{mono}}}(A, B)$ to be the subset of $\mathrm{Hom}_{\mathsf{C}}(A, B)$ consisting of monomorphisms, for all objects A, B. (Cf. Exercise 3.8; of course, in general $\mathsf{C}_{\mathsf{mono}}$ is not full in C.) Do the same for epimorphisms. Can you define a subcategory $\mathsf{C}_{\mathsf{nonmono}}$ of C by restricting to morphisms that are *not* monomorphisms?

Solution. Let $f\colon A \to B$ and $g\colon B \to C$ be monomorphisms. We need to prove that $g \circ f\colon A \to C$ is a monomorphism. Let Z be an object of C and let $\alpha', \alpha''\colon Z \to A$ be morphisms. Furthermore, suppose that $(g \circ f) \circ \alpha' = (g \circ f)\alpha''$. By associativity we have $g \circ (f \circ \alpha') = g \circ (f \circ \alpha'')$. Since g is monic this implies that $f \circ \alpha' = f \circ \alpha''$, and since f is monic this implies that $\alpha' = \alpha''$. So, $g \circ f$ is indeed a monomorphism. Clearly identity morphisms are monomorphisms; this is all that is really needed to check the axioms of a subcategory.

Now, let $f\colon A \to B$ and $g\colon B \to C$ be epimorphisms. We need to prove that $g \circ f\colon A \to C$ is an epimorphism. Let Z be an object of C and let $\beta', \beta''\colon C \to Z$ be morphisms. Furthermore, suppose that $\beta' \circ (g \circ f) = \beta'' \circ (g \circ f)$. By associativity we have $(\beta' \circ g) \circ f = (\beta'' \circ g) \circ f$. Since f is monic this implies that $\beta' \circ g = \beta'' \circ g$, and since g is monic this implies that $\beta' = \beta''$. So, $g \circ f$ is indeed an epimorphism. Clearly identity morphisms are epimorphisms; and again, this is all that is really needed to check the axioms of a subcategory.

A "subcategory" $\mathsf{C}_{\mathsf{nonmono}}$ would lack identities, hence it would not be a subcategory. □

4.5. Give a concrete description of monomorphisms and epimorphisms in the category MSet you constructed in Exercise 3.9. (Your answer will depend on the notion of morphism you defined in that exercise!)

Solution. Recall that a morphism $f\colon (A, \sim_A) \to (B, \sim_B)$ is a function $f\colon A \to B$ that respects the equivalence relations. Note that we identify the morphism of multisets with its underlying set-function. This morphism is a *monomorphism* if and only if its underlying set-function is injective, and it an *epimorphism* if and only if the underlying set-function is surjective. The proofs are pretty much the same as in Set, but we go through them anyway.

Suppose f is injective. Let $(Z, \sim_Z)$ be a multiset and let $\alpha', \alpha''\colon Z \to A$ be morphisms of multisets. Furthermore, suppose that $f \circ \alpha' = f \circ \alpha''$. Forget for a moment that we are dealing with multisets and regard these morphisms as set-functions, i.e. morphisms in Set. Then, since f is injective, f is a monomorphism in Set and thus $\alpha' = \alpha''$ as set-functions, which of course implies they are the same morphism of multisets; this shows that f is a monomorphism. We have that "injective $\implies$ monomorphism" in MSet, and essentially the same argument proves that "surjective $\implies$ epimorphism".

Now assume that f is a monomorphism (in MSet). For the sake of contradiction, suppose there are some $x, y \in A$ such that $x \neq y$ but $f(x) = f(y)$. Consider the singleton multiset $(\{*\}, =)$ and let $\alpha'\alpha'' \colon \{*\} \to A$ be functions defined by $\alpha'(*) = x$ and $\alpha''(*) = y$. Clearly these respects equivalence relations so they are morphisms of multisets, and further $f \circ \alpha' = f \circ \alpha''$. As f is a monomorphism, $\alpha' = \alpha''$, but this is clearly not the case, so we have a contradiction. Thus, f is injective and we have shown "monomorphism $\implies$ injective" in MSet.

Finally, assume f is an epimorphism (in MSet). For the sake of contradiction, suppose there is some $b_0 \in B$ such that $f(a) \neq b$ for all $a \in A$. Consider the multiset $(\{0,1\}, \sim)$, where $\sim$ is the relation dictating that all elements of the set are equivalent (in particular $0 \sim 1$). Let $\beta', \beta'' \colon B \to \{0,1\}$ be morphisms of multisets defined by

$$\beta'(b) \coloneqq 0 \text{ and } \beta''(b) \coloneqq \begin{cases} 0 & \text{if } b \neq b_0 \\ 1 & \text{if } b = b_0 \end{cases},$$

for all $b \in B$. Notice that our definition of $\sim$ ensures that these maps respect equivalence. Then $\beta' \circ f = \beta'' \circ f$ but $\beta' \neq \beta''$, contradicting the fact that f is epic. Hence we must conclude that f was surjective in the first place. This shows that "epimorphism $\implies$ surjective" and we are done.

Note Characterizing morphisms with left inverses and morphisms with right inverses would have resulted in a much more interesting exercise. □

5 Universal properties

Exercises

5.1. Prove that a final object in a category C is initial in the opposite category C^{op} (cf. Exercise 3.1).

Solution. Let A be a final object in C. This means that for all objects X of C we have that $|\operatorname{Hom}_{\mathsf{C}}(X, A)| = 1$. But then for all objects X of C^{op} (recall that $\operatorname{Obj}(\mathsf{C}^{op}) = \operatorname{Obj}(\mathsf{C})$) we have that $|\operatorname{Hom}_{\mathsf{C}^{op}}(A, X)| = |\operatorname{Hom}_{\mathsf{C}}(X, A)| = 1$, which shows A is initial in C^{op}. □

5.2. ▷ Prove that $\emptyset$ is the *unique* initial object in Set. [§5.1]

Solution. Indeed, for any set X there is exactly one function $\emptyset \to X$ (the empty function). Further, only the empty set has this property since any other initial object has to be isomorphic to $\emptyset$ which would force it to have cardinality 0, and only the empty set has cardinality 0. □

5.3. ▷ Prove that final objects are unique up to isomorphism. [§5.1]

Solution. Two final objects A, B are initial in the opposite category by Exercise 5.1, and hence they are isomorphic in C^{op}. It is readily verified that an isomorphism $A \to B$ in C^{op} is an isomorphism $B \to A$ in C. Hence, A and B are isomorphic in C. □

5.4. What are initial and final objects in the category of 'pointed sets' (Example 3.8)? Are they unique?

Solution. Let $(\{p\}, p)$ be a singleton pointed set. Then $(\{p\}, p)$ is both initial and final in the category Set^*. Let (A, a) be a pointed set with $a \in A$. There is only one function $A \to \{p\}$ (recall $\{p\}$ is final in Set), and this function happens to preserve the distinguished element. Therefore $(\{p\}, p)$ is final in Set^*.

But more is true! There are, in principle, many functions $\{p\} \to A$ but only one that preserves the distinguished element, namely the function $p \mapsto a$. Hence $(\{p\}, p)$ is initial in Set^*.

Since p was arbitrary, terminal objects are not unique (but they are unique up to isomorphism). □

5.5. ▷ What are the final objects in the category considered in §5.3? [§5.3]

Solution. It is the singleton set (again). To spell this out, for any p, recall that $\{p\}$ is final in Set. Hence there is a unique set-function $\xi\colon A \to \{p\}$, and it happens to send equivalent elements to the same image, so that $(\xi, \{p\})$ gives an object of our category. If (φ, Z) is any other object then there exists a unique $\sigma\colon Z \to \{p\}$ such that the following diagram commutes.

$$\begin{tikzcd}
Z \arrow[rr, "\sigma"] & & \{p\} \\
& A \arrow[ul, "\varphi"] \arrow[ur, "\xi"'] &
\end{tikzcd}$$

Indeed, σ exists as a set-function and is unique because $\{p\}$ is final in Set, and $\xi = \sigma\varphi$ since any two functions $A \to \{p\}$ must be equal (again, because $\{p\}$ is final in Set). □

5.6. ▷ Consider the category corresponding to endowing (as in Example 3.3) the set $\mathbb{Z}^+$ of positive integers with the *divisibility* relation. Thus there is exactly one morphism $d \to m$ in this category if and only if d divides m without remainder; there is no morphism between d and m otherwise. Show that this category has products and coproducts. What are their 'conventional' names? [§VII.5.1]

Solution. In this category, the product of a and b is $\gcd(a, b)$, while their coproduct is $\operatorname{lcm}(a, b)$.

Clearly $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$, so there are "projection" maps $\gcd(a, b) \to a$ and $\gcd(a, b) \to b$. Suppose there is some z that divides both a and b, depicted below.

$$\begin{tikzcd}
& & a \\
z \arrow[r, dashed] \arrow[urr, bend left] \arrow[drr, bend right] & \gcd(a,b) \arrow[ur] \arrow[dr] & \\
& & b
\end{tikzcd}$$

Then we can deduce that z divides $\gcd(a,b)$, producing a morphism making the diagram commute (because all diagrams commute in this category). Further, the morphism is unique since there is at most one morphism $z \to \gcd(a,b)$. This all shows that $\gcd(a,b)$ is a product in this category.

Similarly, we note that $a \mid \operatorname{lcm}(a,b)$ and $b \mid \operatorname{lcm}(a,b)$, so there are "inclusion" maps $a \to \operatorname{lcm}(a,b)$ and $b \to \operatorname{lcm}(a,b)$. Further, if there is some z such that $a \mid z$ and $b \mid z$ then $\operatorname{lcm}(a,b)$ divides z.

$$\begin{tikzcd}
a \arrow[dr] \arrow[drr, bend left] & & \\
& \operatorname{lcm}(a,b) \arrow[r, dashed] & z \\
b \arrow[ur] \arrow[urr, bend right] & &
\end{tikzcd}$$

After some routine checks (diagram commutes, morphism is unique, etc.), this proves that $\operatorname{lcm}(a,b)$ is a coproduct in this category. □

5.7. Redo Exercise 2.9, this time using Proposition 5.4.

Solution. Let $A \cong A' \cong A''$ and $B \cong B' \cong B''$ with $A' \cap B' = \emptyset$ and $A'' \cap B'' = \emptyset$. Then clearly $A' \cup B'$ and $A'' \cup B''$ both satisfy the categorical definition of the coproduct $A \amalg B$, as in Proposition 5.6 (with essentially the same proof). Therefore $A' \cup B' \cong A'' \cup B''$ by Proposition 5.4. □

5.8. Show that in every category C the products $A \times B$ and $B \times A$ are isomorphic, if they exist. (Hint: Observe that they both satisfy the universal property for the product of A and B; then use Proposition 5.4.)

Solution. Note that $\mathsf{C}^{A,B}$ and $\mathsf{C}^{B,A}$ are the same category. Hence both $A \times B$ and $B \times A$ are final objects of the same category, and thus they are isomorphic by Proposition 5.4. □

5.9. Let C be a category with products. Find a reasonable candidate for the universal property that the product $A \times B \times C$ of three objects of C ought to satisfy, and prove that both $(A \times B) \times C$ and $A \times (B \times C)$ satisfy this universal property. Deduce that $(A \times B) \times C$ and $A \times (B \times C)$ are necessarily isomorphic.

Solution. For objects A, B, C the triple product $A \times B \times C$ must satisfy the following. There must be three morphisms π_1, π_2, π_3 such that for any object Z and morphisms f_A, f_B, f_C there exists a unique morphism σ such that the following diagram commutes.

$$\begin{tikzcd}
 & & A \\
Z \arrow[r, "\sigma"] \arrow[urr, bend left, "f_A"] \arrow[rr, bend right, "f_B"'] \arrow[drr, bend right, "f_C"'] & A \times B \times C \arrow[ur, "\pi_1"] \arrow[r, "\pi_2"] \arrow[dr, "\pi_3"'] & B \\
 & & C
\end{tikzcd}$$

We show that $(A \times B) \times C$ satisfies this property. Since $A \times B$ is a product, there are two associated projection morphisms π_A and π_B, to this product. Similarly since $(A \times B) \times C$ is a product, there are two associated projection morphisms, $\pi_{A\times B}$ and π_C, to this product. We claim that there is a unique σ such that the following diagram commutes.

$$\begin{tikzcd}
 & & & A \\
 & & A \times B \arrow[ur, "\pi_A"] \arrow[dr, "\pi_B"] & \\
Z \arrow[r, "\sigma"] \arrow[uurrr, bend left, "f_A"] \arrow[drr, bend right, "f_C"'] \arrow[rrr, bend right=60, "f_B"'] & A \times B \times C \arrow[ur, "\pi_{A\times B}"] \arrow[dr, "\pi_C"'] & & B \\
 & & C &
\end{tikzcd}$$

If we can show this, then we have shown $(A \times B) \times C$ is a triple product, since we can take $\pi_1 \coloneqq \pi_A \circ \pi_{A\times B}$, and $\pi_2 \coloneqq \pi_B \circ \pi_{A\times B}$, and $\pi_3 \coloneqq \pi_C$ in the first diagram.

As $A \times B$ is a product, there is a unique morphism τ from Z to $A \times B$ such that $\pi_A \circ \tau = f_A$ and $\pi_B \circ \tau = f_B$. In addition, we have the following sub-diagram.

$$\begin{tikzcd}
 & & A \times B \\
Z \arrow[r, "\sigma"] \arrow[urr, bend left, "\tau"] \arrow[drr, bend right, "f_C"'] & (A \times B) \times C \arrow[ur, "\pi_{A\times B}"] \arrow[dr, "\pi_C"'] & \\
 & & C
\end{tikzcd}$$

Which commutes for a unique σ since $(A \times B) \times C$ is a product. For completeness, we can check that this σ indeed makes the whole diagram commute. We have three equalities to check, one of which is already given by the sub-diagram, namely $\pi_C \circ \sigma = f_C$. Next, consider $\pi_A \circ \pi_{A\times B} \circ \sigma$, which equals $\pi_A \circ \tau$ by commutativity of the sub-diagram, and this in turn equals f_A (we remarked this when we defined τ). Similarly, one can check that $\pi_B \circ \pi_{A\times B} \circ \sigma = f_B$. So, we have shown the existence of a σ that makes the diagram commute, but we haven't yet shown that it is the unique morphism with this property. Let σ' be a morphism that also makes the diagram commute. Then

$$\begin{aligned} f_A &= \pi_A \circ (\pi_{A\times B} \circ \sigma') \\ f_B &= \pi_B \circ (\pi_{A\times B} \circ \sigma'). \end{aligned}$$

We conclude that $\pi_{A\times B} \circ \sigma' = \tau$ since τ is the unique morphism that satisfies the above identities. Then we have

$$\begin{aligned} \tau &= \pi_{A\times B} \circ \sigma' \\ f_C &= \pi_C \circ \sigma. \end{aligned}$$

Hence $\sigma' = \sigma$ since σ is the only morphism that makes the sub-diagram commute. We have shown that $(A \times B) \times C$ is a triple product, and in a similar fashion one can prove that $A \times (B \times C)$ is a triple product. One can define a category $\mathsf{C}^{A,B,C}$ such that the triple products are terminal in that category; hence all triple products are isomorphic.

Note This is a more personal note; I just don't want to forget how proud of myself I was when I first came up with this argument (ages ago). It must've been my first arrow-theoretic proof. I LaTeX'ed it for an online course I was doing (eventually dropped out). Showed up late for class, whilst they were going through the homework, and bam! the whole class was reading my proof. I was ecstatic as I explained to everyone what I had done. Few months later this grad student at my uni wanted to go over this proof (or was it me, who wanted to?). I spent 2-3 hours with them, late at night in the library, defining all the morphisms and checking the commutativity of the diagrams. And uniqueness, oh uniqueness. I lost the original LaTeX file, but I was able to find the pdf of it, so I rewrote it to the best of my abilities. □

5.10. Push the envelope a little further still, and define products and coproducts for *families* (i.e., indexed sets) of objects of a category.

Do these exist in Set?

It is common to denote the product $\underbrace{A \times \cdots \times A}_{n \text{ times}}$ by A^n.

Solution. Let $(A_i)_{i\in I}$ be a family of objects of a category C, where I is a set. Then a product of this family is an object $\prod_{i\in I} A_i$ with maps $\pi_j \colon \prod_{i\in I} A_i \to A_j$ for all $j \in I$. This product must satisfy the property that, given any object Z with maps $f_j \colon Z \to A_j$ for all $j \in I$, there is a unique map $\sigma \colon Z \to \prod_{i\in I} A_i$ such that, for all $j \in I$, the following diagram commutes.

$$\begin{tikzcd} Z \arrow[r, "\sigma"] \arrow[rr, bend left, "f_j"] & \prod_{i\in I} A_i \arrow[r, "\pi_j"] & A_j \end{tikzcd} .$$

Similarly, a coproduct of the family $(A_i)_{i \in I}$ is an object $\coprod_{i \in I} A_i$ together with a collection of morphisms $\iota_j \colon A_j \to \coprod_{i \in I}$ for each $j \in I$. This coproduct must satisfy the property that, given any object Z with maps $f_j \colon A_j \to Z$ for all $j \in I$, there exists a unique $\sigma \colon \coprod_{i \in I} \to Z$ such that the following diagram commutes for all $j \in I$.

$$\begin{tikzcd}
A_j \arrow[r, "\iota_j"] \arrow[rr, bend left, "f_j"] & \coprod_{i \in I} A_i \arrow[r, "\sigma"] & Z
\end{tikzcd}$$

Products exist in Set, but their construction is a bit tricky. If the index set I is finite then we already know what products look like. If I is infinite, it's not as clear how we are going to define "infinite ordered tuples" of elements of our sets to make up the product. It is better to think of them (the tuples) as functions taking an element $i \in I$ and returning an element of A_i; you should convince yourself that this is essentially the same as an ordinary ordered tuple when I is finite. We now proceed to the construction.

If A_i is a set for all $i \in I$ then so is $\bigcup_{i \in I} A_i$. As I is also a set then so is $\left(\bigcup_{i \in I} A_i\right)^I$. Then define

$$\prod_{i \in I} A_i := \left\{ f \in \left(\bigcup_{i \in I} A_i \right)^I \,\middle|\, f(j) \in A_j \text{ for all } j \in I \right\}.$$

A projection $\pi_j \colon \prod_{i \in I} A_i \to A_j$ would be defined by the rule $f \mapsto f(j)$. And if there was some set Z with maps $f_j \colon Z \to A_j$ for all $j \in I$ then we define $\sigma \colon Z \to \prod_{i \in I} A_i$ by saying that $\sigma(z)$ is the function $I \to \bigcup_{i \in I} A_i$ mapping $j \mapsto f_j(z)$. Commutativity of the relevant diagram is immediately verified and one will notice that the definition of σ was forced unto us, i.e. σ is unique.

Coproducts also exist in Set. We define

$$\coprod_{i \in I} A_i := \bigcup \{\{i\} \times A_i \mid i \in I\}.$$

It is clear that we are producing disjoint copies of our sets and then taking their union. We do not bother to spell out the rest of the details, since they are essentially the same as in the finite case. □

5.11. Let A, resp. B be a set, endowed with an equivalence relation $\sim_A$, resp. $\sim_B$. Define a relation $\sim$ on $A \times B$ by setting

$$(a_1, b_1) \sim (a_2, b_2) \iff a_1 \sim_A a_2 \text{ and } b_1 \sim_B b_2.$$

(This is immediately seen to be an equivalence relation.)

- Use the universal property for quotients (§5.3) to establish that there are functions $(A \times B)/{\sim} \to A/{\sim_A}$, $(A \times B)/{\sim} \to B/{\sim_B}$.

- Prove that $(A\times B)/\sim$, with these two functions, satisfies the universal property for the product of $A/\sim_A$ and $B/\sim_B$.
- Conclude (without further work) that $(A\times B)/\sim \,\cong (A/\sim_A)\times(B/\sim_B)$.

Solution. First, we need to setup our notation. Let $\pi_A\colon A\times B\to A$ and $\pi_B\colon A\times B\to B$ be the projections. Let $p_A\colon A\to A/\sim_A$, $p_B\colon B\to B/\sim_B$, and $p_{A\times B}\colon A\times B\to(A\times B)/\sim$ be the canonical surjections.

$$\begin{tikzcd}
 & A \arrow[r, "p_A"] & A/\sim_A \\
A\times B \arrow[ur, "\pi_A"] \arrow[r, "p_{A\times B}"] \arrow[dr, "\pi_B"'] & (A\times B)/\sim \arrow[ur, dashed, "\exists!\, q_A"] \arrow[dr, dashed, "\exists!\, q_B"] & \\
 & B \arrow[r, "p_B"'] & B/\sim_B
\end{tikzcd}$$

- Notice that there is a map $A\times B\to A/\sim$ given by $p_A\circ\pi_A$. To spell things out, $p_A\circ\pi_A(a,b)=[a]_{\sim_A}$. Furthermore, if $(a_1,b_1)\sim(a_2,b_2)$ then

  $$p_A\circ\pi_A(a_1,b_1)=[a_1]_{\sim_A}=[a_2]_{\sim_A}=p_A\circ\pi_A(a_2,b_2),$$

  by virtue of the fact that $a_1\sim_A a_2$. Thus equivalent elements in $A\times B$ have the same image under $p_A\circ\pi_A$. By the universal property of quotients there is a unique map $q_A\colon(A\times B)/\sim\to A/\sim_A$ such that the top parallelogram in the diagram above commutes. The same argument gives a unique $q_B\colon(A\times B)/\sim\to B/\sim_B$ so that the whole diagram commutes.
- Let Z be a set with maps $f_A\colon Z\to A/\sim_A$ and $f_B\colon Z\to B/\sim_B$.

  $$\begin{tikzcd}
   & & A/\sim_A \\
  Z \arrow[urr, bend left, "f_A"] \arrow[r, dashed, "\exists!\,\sigma"] \arrow[drr, bend right, "f_B"'] & (A\times B)/\sim \arrow[ur, "q_A"] \arrow[dr, "q_B"'] & \\
   & & B/\sim_B
  \end{tikzcd}$$

  We claim that there is a unique $\sigma\colon Z\to(A\times B)/\sim$ such that the above diagram commutes. Said differently, there is a unique $\sigma\colon Z\to(A\times B)/\sim$ such that

  $$\begin{aligned} q_A\circ\sigma&=f_A\\ q_B\circ\sigma&=f_B.\end{aligned}\tag{1.3}$$

  Existence of σ

  Let $p'_A\colon A/\sim_A\to A$ be a right inverse of p_A, and let $p'_B\colon B/\sim_B\to B$ be a right inverse of p_B; these exist because p_A and p_B are surjections. We draw these grey in the diagram below.

$$\begin{tikzcd}
 & & A \arrow[r, "p_A"] & A/{\sim_A} \arrow[l, bend right, gray, "p'_A"'] \\
Z \arrow[r, dashed, "\exists!\,\tau"] \arrow[urrr, bend left, "f_A"] \arrow[drrr, bend right, "f_B"'] & A \times B \arrow[r, "p_{A\times B}"] \arrow[ur, "\pi_A"] \arrow[dr, "\pi_B"'] & (A \times B)/{\sim} \arrow[ur, "q_A"] \arrow[dr, "q_B"'] & \\
 & & B \arrow[r, "p_B"'] & B/{\sim_B} \arrow[l, bend left, gray, "p'_B"]
\end{tikzcd}$$

Notice that we have maps $p'_A \circ f_A \colon Z \to A$ and $p'_B \circ f_B \colon Z \to B$. By the universal property of products there exists a unique map $\tau \colon Z \to A \times B$ such that the following equalities are satisfied.

$$\begin{aligned}
\pi_A \circ \tau &= p'_A \circ f_A \\
\pi_B \circ \tau &= p'_B \circ f_B.
\end{aligned}$$

We claim that $\sigma \coloneqq p_{A\times B} \circ \tau$ has the required properties. We need to check that the equations in (1.3) hold. Indeed,

$$\begin{aligned}
q_A \circ \sigma &= q_A \circ (p_{A\times B} \circ \tau) \\
&= (q_A \circ p_{A\times B}) \circ \tau \\
&= (p_A \circ \pi_A) \circ \tau \\
&= p_A \circ (\pi_A \circ \tau) \\
&= p_A \circ (p'_A \circ f_A) \\
&= (p_A \circ p'_A) \circ f_A \\
&= f_A.
\end{aligned}$$

Notice that we used the defining properties of q_A, p'_A, and τ. A similar computation shows that $q_B \circ \sigma = f_B$.

Uniqueness of σ

Suppose that there are two maps $\sigma', \sigma'' \colon Z \to (A \times B)/{\sim}$ that satisfy the equations in (1.3). We will show that $\sigma' = \sigma''$.

$$\begin{tikzcd}
 & & A \arrow[r, "p_A"] & A/{\sim_A} \\
Z \arrow[urrr, bend left=50, "f_A"] \arrow[rr, bend left, red, "\sigma'"] \arrow[rr, bend right, red, "\sigma''"'] \arrow[drrr, bend right=50, "f_B"'] & A \times B \arrow[ur, "\pi_A"] \arrow[dr, "\pi_B"'] \arrow[r, shift left, "p_{A\times B}"] & (A \times B)/{\sim} \arrow[l, shift left, gray, "p'_{A\times B}"] \arrow[ur, "q_A"] \arrow[dr, "q_B"'] & \\
 & & B \arrow[r, "p_B"'] & B/{\sim_B}
\end{tikzcd}$$

Let $p'_{A\times B} \colon (A \times B)/{\sim} \to A \times B$ be a right inverse of $p_{A\times B}$. Notice the following.

$$\begin{aligned}
p_A \circ \pi_A \circ p'_{A\times B} \circ \sigma' &= (p_A \circ \pi_A) \circ p'_{A\times B} \circ \sigma' \\
&= (q_A \circ p_{A\times B}) \circ p'_{A\times B} \circ \sigma' \\
&= q_A \circ (p_{A\times B} \circ p'_{A\times B}) \circ \sigma' \\
&= q_A \circ \sigma' \\
&= f_A.
\end{aligned}$$

The last equality used the fact that σ' satisfies (1.3). Doing the same calculation for σ'' yields $p_A \circ \pi_A \circ p'_{A\times B} \circ \sigma'' = f_A$. In particular,

$$p_A \circ \pi_A \circ (p'_{A\times B} \circ \sigma') = p_A \circ \pi_A \circ (p'_{A\times B} \circ \sigma''). \tag{1.4}$$

The same calculation on the bottom part of the diagram will give

$$p_B \circ \pi_B \circ (p'_{A\times B} \circ \sigma') = p_B \circ \pi_B \circ (p'_{A\times B} \circ \sigma''). \tag{1.5}$$

Let $z \in Z$ be arbitrary. Suppose $p'_{A\times B} \circ \sigma'(z) = (a', b')$ and also that $p'_{A\times B} \circ \sigma''(z) = (a'', b'')$. Then if we apply (1.4) to z we have that

$$p_A \circ \pi_A(a', b') = p_A \circ \pi_A(a'', b'') \implies [a']_{\sim_A} = [a'']_{\sim_A} \implies a' \sim_A a''.$$

Similarly, (1.5) when applied to z says that

$$p_B \circ \pi_B(a', b') = p_B \circ \pi_B(a'', b'') \implies [b']_{\sim_B} = [b'']_{\sim_B} \implies b' \sim_B b''.$$

As $a' \sim_A a''$ and $b' \sim_B b''$ we conclude that $(a', b') \sim (a'', b'')$; in other words $[(a', b')]_\sim = [(a'', b'')]_\sim$. But then we have these two chains of equalities.

$$\sigma'(z) = p_{A\times B} \circ (p'_{A\times B} \circ \sigma')(z) = p_{A\times B}(a', b') = [(a', b')]_\sim$$

$$\sigma''(z) = p_{A\times B} \circ (p'_{A\times B} \circ \sigma'')(z) = p_{A\times B}(a'', b'') = [(a'', b'')]_\sim$$

In conclusion, $\sigma'(z) = \sigma''(z)$. As $z \in Z$ was arbitrary, $\sigma' = \sigma''$.

- We showed that $(A \times B)/\sim$ is a (categorical) product of $A/\sim_A$ and $B/\sim_B$. By definition, $(A/\sim_A) \times (B/\sim_B)$ is also their product. Products are unique up to isomorphism, so the result follows.

Note I spent a whole day coming up with this proof. I am sure there are easier ways to do this exercise, but, in my very biased opinion, this should be the most elegant proof, or at least it is much closer to the philosophy of category theory. It hints at the fact that similar results should be true in categories other than Set, but I'm too tired to pursue this further. □

5.12. ¬ Define the notions of *fibered products* and *fibered coproducts*, as terminal objects of the categories $\mathsf{C}_{\alpha,\beta}$, $\mathsf{C}^{\alpha,\beta}$ considered in Example 3.10 (cf. also Exercise 3.11), by stating carefully the corresponding universal properties.

As it happens, Set has both fibered products and coproducts. Define these objects 'concretely', in terms of naive set theory. [II.3.9, III.6.10, III.6.11]

Solution. Let A, B, C be objects of a category C. Let $\alpha\colon A \to C$ and $\beta\colon B \to C$ be morphisms. A *fibered product* of α and β (also called *pullback*) is an object $A \times_C B$ together with morphisms $p_A\colon A \times_C B \to A$ and $p_B\colon A \times_C B \to B$ such that $\alpha \circ p_A = \beta \circ p_B$ and furthermore it is universal with that property; this means that for any object Z with morphisms $f\colon Z \to A$ and $g\colon Z \to B$ such that $\alpha \circ f = \beta \circ g$, then there exists a unique morphism $\sigma\colon Z \to A \times_C B$ such that the following diagram commutes.

$$\begin{tikzcd}
 & & A \arrow[rd, "\alpha"] & \\
Z \arrow[r, dashed, "\exists!\,\sigma"] \arrow[rru, bend left, "f"] \arrow[rrd, bend right, "g"'] & A \times_C B \arrow[ru, "p_A"] \arrow[rd, "p_B"'] & & C \\
 & & B \arrow[ru, "\beta"'] &
\end{tikzcd}$$

If we are working in Set then we can explicitly define the fibered product.

$$A \times_C B \coloneqq \{(a, b) \mid \alpha(a) = \beta(b)\}.$$

The maps are defined by $p_A(a, b) \coloneqq a$ and $p_B(a, b) \coloneqq b$. By definition, $\alpha \circ p_A = \beta \circ p_B$. If Z is a set with f and g as above then we can define σ by saying that $\sigma(z) \coloneqq (f(z), g(z))$ for all z. This definition is forced, so σ is unique, but we do need to check that $(f(z), g(z)) \in A \times_C B$ in the first place. This is saying that $\alpha(f(z)) = \beta(g(z))$ and this holds precisely by the conditions we imposed on f and g.

Now suppose we are working with maps out of C, that is $\alpha\colon C \to A$ and $\beta\colon C \to B$. A *fibered coproduct* of α and β (also called *pushout*) is an object $A \amalg_C B$ together with morphisms $i_A\colon A \to A \amalg_C B$ and $i_B\colon B \to A \amalg_C B$ such that $i_A \circ \alpha = i_B \circ \beta$ and furthermore it is universal with that property; this means that for any object Z with morphisms $f\colon A \to Z$ and $g\colon B \to Z$ such that $f \circ \alpha = g \circ \beta$, then there exists a unique morphism $\sigma\colon A \amalg_C B \to Z$ such that the following diagram commutes.

$$\begin{tikzcd}
 & A \arrow[dr, "i_A"] \arrow[drr, bend left, "f"] & & \\
C \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & A \amalg_C B \arrow[r, dashed, "\exists!\,\sigma"] & Z \\
 & B \arrow[ur, "i_B"'] \arrow[urr, bend right, "g"'] & &
\end{tikzcd}$$

Fibered coproducts exist in Set but their construction is more complicated (and more fun). Let $A \amalg B$ be the disjoint union (coproduct) of A, B, equipped with the canonical inclusions, $\iota_A\colon A \to A \amalg B$ and $\iota_B\colon B \to A \amalg B$. Of course this does not work as the fibered coproduct because $\iota_A \circ \alpha(c) \neq \iota_B \circ \beta(c)$ for all $c \in C$, given that the images of ι_A and ι_B are disjoint. The idea is to force this to be true by quotienting out by a suitable equivalence relation.

Define a relation in $A \amalg B$ by saying that for all $x, y \in A \amalg B$

$$x \sim y \iff \begin{cases} x = y & ;\text{ or} \\ x = \iota_A \circ \alpha(c) \text{ and } y = \iota_B \circ \beta(c) \text{ for some } c \in C & ;\text{ or} \\ x = \iota_B \circ \beta(c) \text{ and } y = \iota_A \circ \alpha(c) \text{ for some } c \in C. \end{cases}$$

This relation is clearly reflexive and symmetric. Unfortunately it is not necessarily transitive (why? Try proving it is and see what goes wrong). We will define a new relation "generated" by $\sim$ and this will be an equivalence relation. Don't get too bogged down in the details; the definition of $\sim$ is all that really matters.

Let $x, y \in A \amalg B$. We define a new relation $\approx$ on $A \amalg B$ as follows.

$$x \approx y \quad \iff \quad \begin{array}{l} \text{There exists } s_0, \dots, s_n \in A \amalg B \\ \text{such that } x = s_0, s_n = y \text{ and} \\ s_i \sim s_{i+1} \text{ for all } i. \end{array}$$

This is the most natural way to "force" transitivity. This relation is easily seen to be reflexive and symmetric (because $\sim$ is). Transitivity holds because if we have

$$\begin{gathered} x = s_1 \sim s_2 \sim \ldots \sim s_n = y \\ y = s_1' \sim s_2' \sim \ldots \sim s_n' = z, \end{gathered}$$

then it follows that

$$x = s_1 \sim s_2 \sim \ldots \sim s_n \sim s_1' \sim s_2' \ldots \sim s_n' = z.$$

Thus $\approx$ is an equivalence relation.

We can then talk about the quotient $(A \amalg B)/{\approx}$ together with the canonical surjection $\pi\colon A \amalg B \to (A \amalg B)/{\approx}$. We claim that $A \amalg_C B \coloneqq (A \amalg B)/{\approx}$ is the fibered coproduct of α and β, together with the maps $i_A \coloneqq \pi \circ \iota_A$ and $i_B \coloneqq \pi \circ \iota_B$.

First, we need to check that $i_A \circ \alpha = i_B \circ \beta$. Let $c \in C$ be arbitrary. Then $\iota_A \circ \alpha(c) \sim \iota_B \circ \beta(c)$ by definition, and this implies $\iota_A \circ \alpha(c) \approx \iota_B \circ \beta(c)$, which means $\pi \circ \iota_A \circ \alpha(c) = \pi \circ \iota_B \circ \beta(c)$, that is to say $i_A \circ \alpha = i_B \circ \beta$, which is what we were after.

Next, we need to check that $(A \amalg B)/{\approx}$ indeed satisfies the universal property. This is the fun part. After this strenuous abstract setup comes our reward: all of the other universal properties will come to our aid, in harmonious choreography, and give us our σ in a silver platter.

$$\begin{tikzcd}
 & A \arrow[dr, "\iota_A"] \arrow[rrrd, bend left, "f"] & & & \\
C \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & A \amalg B \arrow[r, two heads, "\pi"'] \arrow[rr, dashed, bend left, "\exists! \tau"] & (A \amalg B)/{\approx} \arrow[r, dashed, "\exists!\, \sigma"'] & Z \\
 & B \arrow[ur, "\iota_B"'] \arrow[rrru, bend right, "g"'] & & &
\end{tikzcd}$$

Recall that Z and f, g are arbitrary, with the only restriction that $f \circ \alpha = g \circ \beta$. We are looking for a unique $\sigma\colon (A \amalg B)/{\approx} \to Z$ such that

$$\begin{aligned} \sigma \circ \pi \circ \iota_A &= f \\ \sigma \circ \pi \circ \iota_B &= g. \end{aligned} \tag{1.6}$$

Notice that f and g are maps out of A and B respectively, and going into a common target Z. By the universal property of coproducts, there is some $\tau\colon A \amalg B \to Z$, which is the unique function such that

$$\begin{aligned} \tau \circ \iota_A &= f \\ \tau \circ \iota_B &= g. \end{aligned} \tag{1.7}$$

Further (and this is the key) τ sends equivalent elements to the same image. Indeed, from (1.7) we deduce

$$\begin{aligned} \tau \circ \iota_A \circ \alpha &= f \circ \alpha \\ \tau \circ \iota_B \circ \beta &= g \circ \beta. \end{aligned}$$

But we said $f \circ \alpha = g \circ \beta$. Hence,

$$\tau \circ \iota_A \circ \alpha = \tau \circ \iota_B \circ \beta \tag{1.8}$$

Let $x, y \in A \amalg B$. So, if $x \sim y$ then either $x = y$, in which case $\tau(x) = \tau(y)$, or else there is some $c \in C$ such that $x = \iota_A \circ \alpha(c)$ and $y = \iota_B \circ \beta(c)$ (or vice versa). Then (1.8) says $\tau(x) = \tau(y)$. In conclusion, $x \sim y \implies \tau(x) = \tau(y)$.

What about $\approx$, the equivalence relation? Well, if $x \approx y$ then we have

$$x = s_1 \sim s_2 \sim \ldots \sim s_n = y.$$

But then, by what we said in the previous paragraph, we deduce $\tau(x) = \tau(s_2)$ and then $\tau(s_2) = \tau(s_3)$, and so on (use induction). Hence in this case we also have $x \approx y \implies \tau(x) = \tau(y)$.

We have gone through the work of showing this because now we can apply the universal property of quotients (!) to deduce that there is a map $\sigma\colon (A \amalg B)/{\approx} \to Z$, which is unique in satisfying

$$\tau = \sigma \circ \pi. \tag{1.9}$$

Applying (1.9) to (1.7) yields the equations in (1.6), so this is indeed the σ we are looking for. We can work backwards to deduce uniqueness as well (!!): if σ' satisfies the equations in (1.6) then $\tau = \sigma' \circ \pi$ by universality of τ, and then $\sigma' = \sigma$ by universality of σ.

Note I spent half a day on this one. As you can probably tell by the way I wrote it, I am very fond of this proof, and I'm proud I figured out what the fibered coproduct is in Set. Hopefully I was able to lay it out in a more or less intuitive manner; I did my best to emphasize that all steps are fairly natural, and we are only doing "the next obvious thing" (even when this is not true, it's important to convince the reader and ourselves that there is some narrative going on: we humans understand things better when they are told as a story).

The idea of defining two relations was tricky and took most of my time. It clearly generalizes as a way to turn any reflexive and symmetric relation into an equivalence relation. There are other ways to phrase this process, as I'm now learning, such as the "intersection of all equivalence relations containing $\sim$" when we view relations on a set S as subsets of $S \times S$. (It'd be interesting to show that this and my definition result in the same equivalence relation, but I'm too tired to pursue this further).

There's a more interesting question lurking in the background. There is (is there?) a category Rel whose objects are sets equipped with a relation, and its morphisms are relation-preserving functions. There is also a category Equiv of equivalence relations defined in a similar way (alternatively one could view an equivalence relation as a small groupoid category, per Exercise 4.2, and we could think of Equiv as the category whose objects are these categories and whose morphisms are functors..., but nevermind). Quite obviously, there is a forgetful functor Equiv → Rel. Does this functor have an adjoint? If so, does it coincide with the processes we've been describing above? I'll try to come back to this later, when I know enough about adjoints. □

Chapter 2

Groups, first encounter

1 Definition of group

Exercises

1.1. ▷ Write a careful proof that every group is the group of isomorphisms of a groupoid. In particular, every group is the group of automorphisms of some object in some category. [§2.1]

Solution. content... □

1.2. ▷ Consider the 'sets of numbers' listed in §1.1, and decide which are made into groups by conventional operations such as $+$ and $\cdot$. Even if the answer is negative (for example, $(\mathbb{R}, \cdot)$ is not a group), see if variations on the definitions of these sets lead to groups (for example, $(\mathbb{R}^*, \cdot)$ *is* a group; cf. §1.4). [§1.2]

Solution. content... □

1.3. Prove that $(gh)^{-1} = h^{-1}g^{-1}$ for all elements g, h of a group G.

Solution. content... □

1.4. Suppose that $g^2 = e$ for all elements g of a group G; prove that G is commutative.

Solution. content... □

1.5. The 'multiplication table' of a group is an array compiling the results of all multiplications $g \bullet h$:

$\bullet$	e	$\cdots$	h	$\cdots$
e	e	$\cdots$	h	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
g	g	$\cdots$	$g \bullet h$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

(Here e is the identity element. Of course the table depends on the order in which the elements are listed in the top row and leftmost column.) Prove that every row and every column of the multiplication table of a group contains all elements of the group exactly once (like Sudoku diagrams!).

Solution. content... □

1.6. ¬ Prove that there is only *one* possible multiplication table for G if G has exactly $1, 2$, or 3 elements. Analyze the possible multiplication tables for groups with exactly 4 elements, and show that there are *two* distinct tables, up to reordering of the elements of G. Use these tables to prove that all groups with ≤ 4 elements are commutative.

(You are welcome to analyze groups with 5 elements using the same technique, but you will soon know enough about groups to be able to avoid such brute-force approaches.) [2.19]

Solution. content... □

1.7. Prove Corollary 1.11.

Solution. content... □

1.8. ¬ Let G be a finite abelian group with exactly one element f of order 2. Prove that $\prod_{g \in G} g = f$. [4.16]

Solution. content... □

1.9. Let G be a finite group, of order n, and let m be the number of elements $g \in G$ of order exactly 2. Prove that $n - m$ is odd. Deduce that if n is even, then G necessarily contains elements of order 2.

Solution. content... □

1.10. Suppose the order of g is odd. What can you say about the order of g^2?

Solution. content... □

1.11. Prove that for all g, h in a group G, $|gh| = |hg|$. (Hint: Prove that $|aga^{-1}| = |g|$ for all a, g in G.)

Solution. content... □

1.12. ▷ In the group of invertible 2×2 matrices, consider

$$g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad h = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Verify that $|g| = 4$, $|h| = 3$, and $|gh| = \infty$. [§1.6]

Solution. content... □

1.13. ▷ Give an example showing that $|gh|$ is not necessarily equal to $\operatorname{lcm}(|g|, |h|)$, even if g and h commute. [§1.6, 1.14]

Solution. content... □

1.14. ▷ As a counterpoint to Exercise 1.13, prove that if g and h commute *and* $\gcd(|g|, |h|) = 1$, then $|gh| = |g||h|$. (Hint: Let $N = |gh|$; then $g^N = (h^{-1})^N$. What can you say about this element?) [§1.6, 1.15, IV.2.5]

Solution. content... □

1.15. ¬ Let G be a commutative group, and let $g \in G$ be an element of maximal *finite* order, that is, such that if $h \in G$ has finite order, then $|h| \leq |g|$. Prove that in fact if h has finite order in G, then h *divides* g. (Hint: Argue by contradiction. If h is finite but does not divide g, then there is a prime integer p such that $|g| = p^m r$, $|h| = p^n s$, with r and s relatively prime to p and $m < n$. Use Exercise 1.14 to compute the order of $g^{p^m} h^s$.) [§2.1, 4.11, IV.6.15]

2 Examples of groups

Exercises

3 The category **Grp**

Exercises

4 Group homomorphisms

5 Free groups

6 Subgroups

7 Quotient groups

8 Canonical decomposition and Lagrange's theorem

9 Group actions

10 Group objects in categories

Bibliography

[1] Terence Tao. *Analysis*. Third edition. Vol. I. Hindustan Book Agency, 2014. 368 pp. ISBN: 81-85931-62-3.