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

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

$$\{\{1, 2\}, \{3\}\} \quad \{\{1, 2, 3\}\}. \qquad \square$$

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. $\square$

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. $\square$

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. $n!$. $\square$

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, 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. ▷ 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. ▷ 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

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

for all $b \in B$. 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 $\pi_A^*(a) \coloneqq (a, f(a))$. 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 $f^*(a) \coloneqq (a, f(a))$. 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 $f(r) \coloneqq e^{2\pi i r}$. 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. ▷ 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), $\mathrm{Hom}_{\mathsf{C}^{op}}(A, B) \coloneqq \mathrm{Hom}_{\mathsf{C}}(B, A)$.

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

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

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 $f \in \mathrm{Hom}_{\mathsf{C}^{op}}(A, B)$,

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

□

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

Solution. $|A|^{|A|}$. □

3.3. ▷ 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

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

□

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. ▷ 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. □

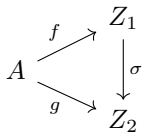
3.6. ▷ (Assuming some familiarity with linear algebra.) Define a category V by taking $\mathrm{Obj}(\mathsf{V}) = \mathbb{N}$ and letting $\mathrm{Hom}_{\mathsf{V}}(n, m) =$ the set of $n \times m$ matrices with real entries, for all $n, m \in \mathbb{N}$ (We will leave the reader the task of making 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. ▷ 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



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

3.8. ▷ A *subcategory* C' of a category C consists of a collection of objects of C, with morphisms $\mathrm{Hom}_{\mathsf{C}'}(A, B) \subseteq \mathrm{Hom}_{\mathsf{C}}(A, B)$ for all objects A, B in $\mathrm{Obj}(\mathsf{C}')$, such that identities and compositions in C make C' into a category. A subcategory C' is *full* if $\mathrm{Hom}_{\mathsf{C}'}(A, B) = \mathrm{Hom}_{\mathsf{C}}(A, B)$ for all A, B in $\mathrm{Obj}(\mathsf{C}')$. 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 $\mathrm{Hom}_{\mathsf{C}'}(A,B) \coloneqq B^A = \mathrm{Hom}_{\mathsf{Set}}(A,B)$. 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 $(S, =)$.

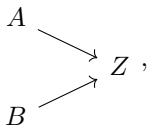
The objects of MSet that are multisets in the sense of §2.2 are the ones in which the equivalence classes contain finitely many elements. □

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]

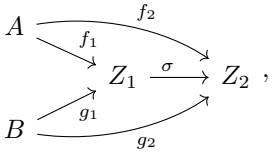
Solution. Objects in $\mathsf{C}^{A,B}$ are diagrams of the form



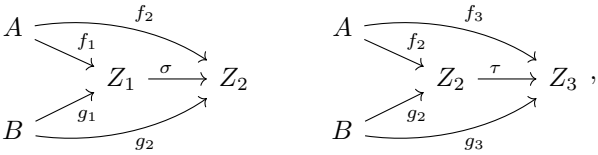
where Z is an object of C and arrows correspond to morphisms in C in the obvious way.

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

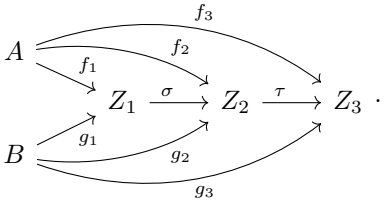
A morphism from the leftmost one to the other one is given by a commutative diagram of the form



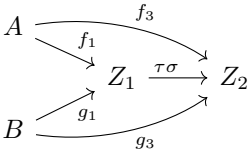
for some $\sigma \in \mathrm{Hom}_{\mathsf{C}}(Z_1, Z_2)$. Given two morphisms



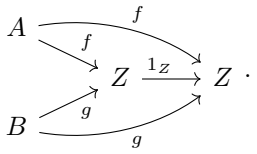
we can compose them as follows. First, combine them to form one big commutative diagram.



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

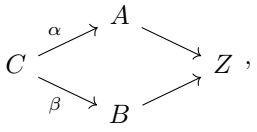


commutes. Identities in $\mathsf{C}^{A,B}$ are just diagrams of the form



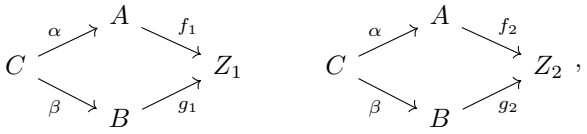
Again, it is immediate that this diagram commutes and it behaves like an identity with respect to composition.

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

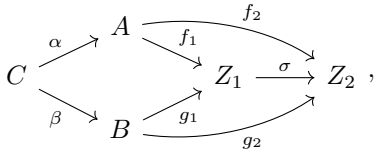


where Z is an object of C and arrows correspond to morphisms in C in the obvious way.

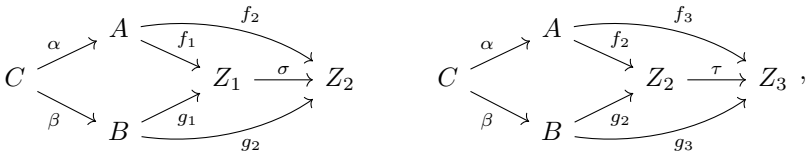
Given two objects



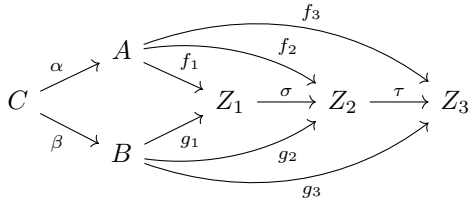
a morphism between from the leftmost one to the other one is a commutative diagram of the form



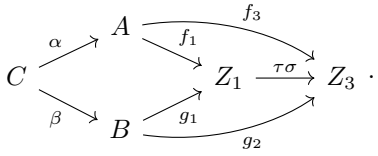
where $\sigma \in \mathrm{Hom}_{\mathsf{C}}(Z_1, Z_2)$. Given two morphisms



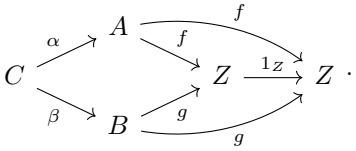
we can compose them as follows. First, combine them as depicted below.



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



Identities in this category are morphisms of the form



□

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.

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

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?

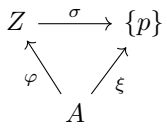
Solution. Let $(\{p\}, p)$ be a singleton pointed set. Then $(\{p\}, p)$ is both initial and final in the category Set^*. Let (A, a) be a pointed set with $a \in A$. There is only one function $A \to \{p\}$ (recall $\{p\}$ is final in Set), and this function happens to preserve the distinguished element.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



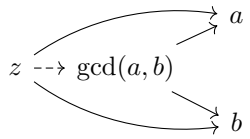
Indeed, σ exists as a set-function and is unique because $\{p\}$ is final in Set, and $\xi = \sigma\varphi$ since any two functions $A \to \{p\}$ must be equal (again, because $\{p\}$ is final in Set). □

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 $\operatorname{lcm}(a, b)$.

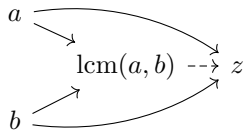
Clearly $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$, so there are "projection" maps $\gcd(a, b) \to a$ and $\gcd(a, b) \to b$. Suppose there is some z that divides both a and b, depicted

below.



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.



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. □

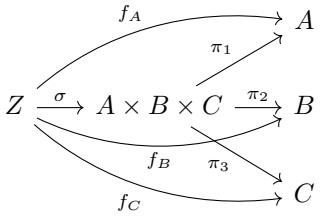
5.8. Show that in every category C the products $A \times B$ and $B \times A$ are isomorphic, if they exist. (Hint: Observe that they both satisfy the universal property for the product of A and B; then use Proposition 5.4.)

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. □

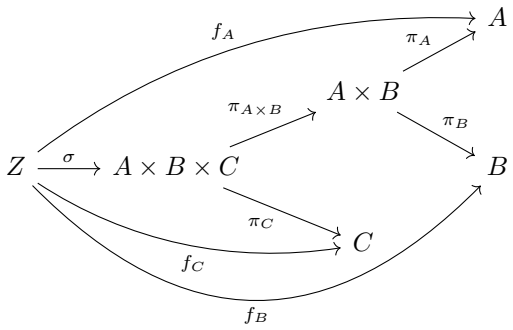
5.9. Let C be a category with products. Find a reasonable candidate for the universal property that the product $A \times B \times C$ of three objects of C ought to satisfy, and prove that both $(A \times B) \times C$ and $A \times (B \times C)$ satisfy this universal property. Deduce that $(A \times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

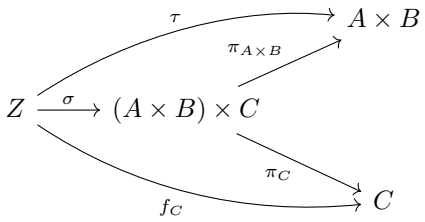


We show that $(A \times B) \times C$ satisfies this property. Since $A \times B$ is a product, there are two associated projection morphisms π_A and π_B, to this product. Similarly since $(A \times B) \times C$ is a product, there are two associated projection morphisms, $\pi_{A \times B}$ and π_C, to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



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.



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

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

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

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

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.

$$Z \xrightarrow{\sigma} \prod_{i\in I} A_i \xrightarrow{\pi_j} A_j \quad , \qquad Z \xrightarrow{f_j} A_j$$

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 $j \in I$.

$$\begin{array}{ccccc} & & f_j & & \\ & \overset{\iota_j}{\nearrow} & & \overset{\sigma}{\searrow} & \\ A_j & \longrightarrow & \coprod_{i\in I} A_i & \longrightarrow & Z \end{array}$$

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

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

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

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

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

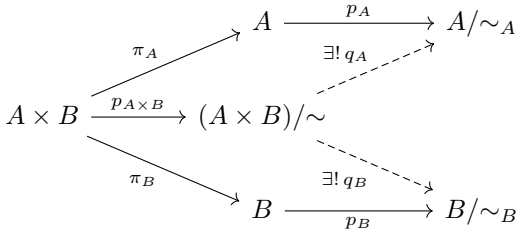
$$(a_1, b_1) \sim (a_2, b_2) \iff a_1 \sim_A a_2 \text{ and } b_1 \sim_B b_2.$$

(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.

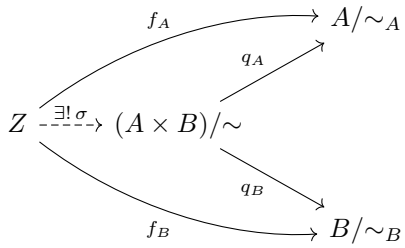


- Notice that there is a map $A \times B \to A/\sim$ given by $p_A \circ \pi_A$. To spell things out, $p_A \circ \pi_A(a, b) = [a]_{\sim_A}$. Furthermore, if $(a_1, b_1) \sim (a_2, b_2)$ then

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

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 $f_B \colon Z \to B/\sim_B$.



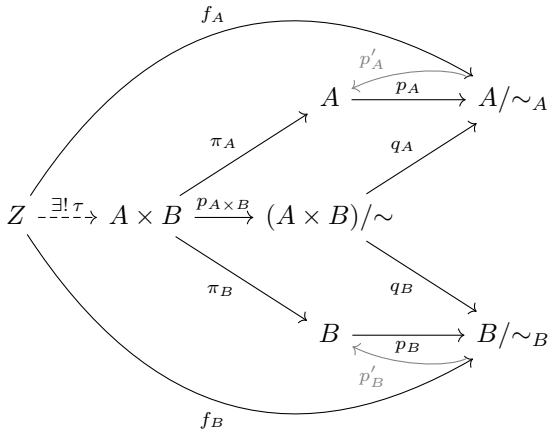
We claim that there is a unique $\sigma \colon Z \to (A \times B)/\sim$ such that the above diagram commutes. Said differently, there is a unique $\sigma \colon Z \to (A \times B)/\sim$ such that

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

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.



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.

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

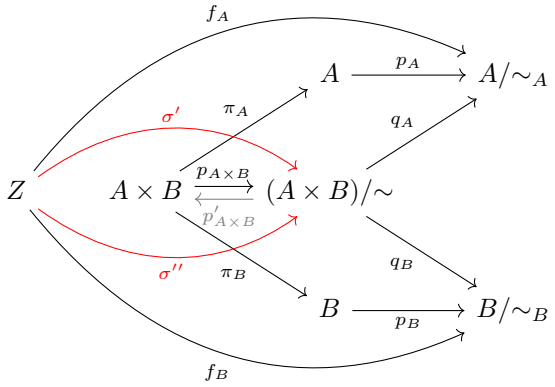
We claim that $\sigma \coloneqq p_{A\times B} \circ \tau$ has the required properties. We need to check that the equations in (1.3) hold. Indeed,

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

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 $\sigma' = \sigma''$.



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, $\sigma' = \sigma''$.

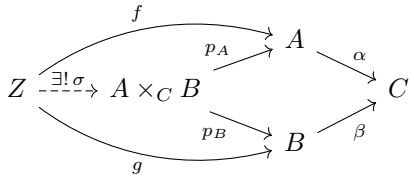
- We showed that $(A \times B)/\sim$ is a (categorical) product of $A/\sim_A$ and $B/\sim_B$. By definition, $(A/\sim_A) \times (B/\sim_B)$ is also their product. Products are unique up to isomorphism, so the result follows.

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.

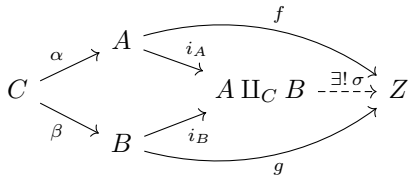


If we are working in Set then we can explicitly define the fibered product.

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

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.



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.

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

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

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

then it follows that

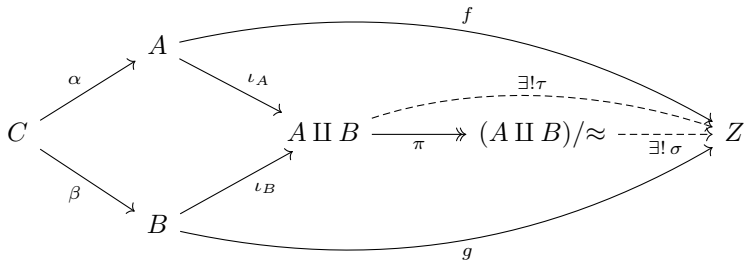
$$x = s_1 \sim s_2 \sim \ldots \sim s_n \sim s_1' \sim s_2' \ldots \sim s_n' = z.$$

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.



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 $\mathsf{Equiv} \to \mathsf{Rel}$. 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. $\square$

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. Let $(G, \cdot)$ be a group. Define a category G with one object $*$, and morphisms $\mathrm{Hom}_{\mathsf{G}}(*,*) = G$. Composition is given by the multiplication $\cdot$. By definition of a group, this composition is associative, has an identity element, and in fact all morphisms are isomorphisms, so this defines a groupoid. □

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. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are all groups. This amounts to saying that addition is associative, that there is an additive identity 0, and that every element has an additive inverse (its negation).

$(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, and $(\mathbb{C}^*, \cdot)$ are all groups. This amounts to saying that multiplication is associative, that there is a multiplicative identity 1, and that every nonzero element has a multiplicative inverse (its reciprocal). □

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

Solution. Indeed,

$$(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = geg^{-1} = gg^{-1} = e,$$

and similarly,

$$(h^{-1}g^{-1})(gh) = h^{-1}(g^{-1}g)h = h^{-1}eh = h^{-1}h = e,$$

so $h^{-1}g^{-1}$ is *the* inverse of gh. □

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

Solution. Multiply the given equation by g^{-1} to see that this implies $g = g^{-1}$ for all $g \in G$. Let g and h be elements of G, and consider the following chain of reasoning

$$gh(hg)^{-1} = ghhg = gh^2g = geg = g^2 = e.$$

Multiply this equation by hg to conclude that $gh = hg$. As g, h were arbitrary, the group is commutative. □

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. Let G be the group in question. First, we show that left- and right-multiplication are bijective. For all $g \in G$ define $l_g \colon G \to G$ by $h \mapsto g \bullet h$ for all $h \in G$; this map is always a bijection since a two-sided inverse is given by $l_{g^{-1}}$. Similarly, define a bijection $r_g \colon G \to G$ by $h \mapsto h \bullet g$ for all $h \in G$.

Look at any row corresponding to some element of the group, say g. A little thought reveals that the row is really what you get when applying l_g to all the elements in G. As l_g is a bijection of the underlying set of G to itself, every element of G appears exactly once in the row. Similarly, by considering r_g, one sees that the same is true for columns. □

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 re-ordering 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. Suppose G has one element, say e. Then the only possible multiplication is $e \bullet e = e$. This is trivially a group, and it is the only one (up to isomorphism) of order 1.

Suppose G has two elements, e and f, where e is the identity. Then multiplication where one of the factors is e is uniquely determined by the fact that e is an identity, as shown.

$\bullet$	e	f
e	e	f
f	f	f^2

By Exercise 1.5, f^2 cannot be f, hence $f^2 = e$.

Suppose G has three elements, e, f, and g, where e is the identity.

$\bullet$	e	f	g
e	e	f	g
f	f	f^2	$f \bullet g$
g	g	$g \bullet f$	g^2

By Exercise 1.5, $f \bullet g$ and $g \bullet f$ are neither f nor g, so $f \bullet g = g \bullet f = e$. Therefore, again by Exercise 1.5, f^2 cannot be f nor e, and g^2 cannot g nor e. Thus $f^2 = g$ and $g^2 = f$.

Suppose G has four elements, e, f, g, and h.

$\bullet$	e	f	g	h
e	e	f	g	h
f	f	f^2	$f \bullet g$	$f \bullet h$
g	g	$g \bullet f$	g^2	$g \bullet h$
h	h	$h \bullet f$	$h \bullet g$	h^2

By the same reasoning as in the previous paragraph, $f \bullet g \neq f$and $f \bullet g \neq g$. Here we have two cases.

Case I: $f \bullet g = e$

We have the following Sudoku puzzle.

$\bullet$	e	f	g	h
e	e	f	g	h
f	f		e	
g	g			
h	h			

Note that $f \bullet h$ cannot be h, e, nor f; therefore it must be g. Then we can fill the remaining entry in the second row $f^2 = h$.

$\bullet$	e	f	g	h
e	e	f	g	h
f	f	h	e	g
g	g			
h	h			

Here we find that $g \bullet f$ cannot be g, h, nor f, so we have $g \bullet h = e$. This implies that $g \bullet h$ is not g, h, nor e; hence $g \bullet h = f$. At this point the puzzle solves itself and we are left with the following multiplication table.

$\bullet$	e	f	g	h
e	e	f	g	h
f	f	h	e	g
g	g	e	h	f
h	h	g	f	e

Case II: $f \bullet g = h$

Here is our starting point.

$\bullet$	e	f	g	h
e	e	f	g	h
f	f		h	
g	g			
h	h			

However, we soon realize that more information is needed to solve this one. Indeed, there is more than one multiplication table with $f \bullet g = h$. For instance, note that f^2 cannot be h nor f. Thus, we can further subdivide into two cases.

Case IIa: $f \bullet g = h$ **and** $f^2 = g$

Here is the puzzle.

$\bullet$	e	f	g	h
e	e	f	g	h
f	f	g	h	
g	g			
h	h			

Immediately we deduce that $f \bullet h = e$. With this information, $g \bullet h$ is also uniquely determined: it must be f. Then the last entry in the last column must read $h^2 = g$, and at this point the rest is straightforward. We just reveal the answer below.

$\bullet$	e	f	g	h
e	e	f	g	h
f	f	g	h	e
g	g	h	e	f
h	h	e	f	g

Case IIb: $f \bullet g = h$ **and** $f^2 = e$

We have the following.

$\bullet$	e	f	g	h
e	e	f	g	h
f	f	e	h	
g	g			
h	h			

The second row is solved immediately. Then, $g \bullet f$ is forced to be h and hence

$h \bullet f = g$.

$\bullet$	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	h		
h	h	g		

Yet, there are two options for the multiplication table at this point. Notice that g^2 is either f or e. We get two more cases, which are easily seen to be

$\bullet$	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	h	f	e
h	h	g	e	f

and,

$\bullet$	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	h	e	f
h	h	g	f	e

To recap, we have four tables allowed by Exercise 1.5.

$\bullet$	e	f	g	h
e	e	f	g	h
f	f	h	e	g
g	g	e	h	f
h	h	g	f	e

$\bullet$	e	f	g	h
e	e	f	g	h
f	f	g	h	e
g	g	h	e	f
h	h	e	f	g

$\bullet$	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	h	f	e
h	h	g	e	f

$\bullet$	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	h	e	f
h	h	g	f	e

However, the first three tables are seen to be essentially the same. Start with the first table; swap the roles of h and g to get the second table. Similarly, swapping h and f will get you the third table. But the fourth table is really different from the other ones, since no relabelling is going to change the fact that in the fourth table all elements square to the identity, whereas this isn't true in the first three tables. Therefore, for groups of order four, there are two tables up to reordering of the elements.

Notice that all the tables we have found so far are symmetric with respect to the main diagonal (the one with all the squares). This implies all groups with order 4 or less are commutative. □

1.7. Prove Corollary 1.11.

Solution. Firstly, notice that g^{-N}, as defined in §1.3, is the inverse of g^N (just multiply out). Therefore $g^{-N} = (g^N)^{-1}$. We will also use the identity $g^{nm} = (g^n)^m$ for integers n, m; this is immediate to verify.

Suppose $g^N = e$, for N an integer. If $N = 0$ then clearly N is a multiple of $|g|$. If N is positive, apply Lemma 1.10 directly to conclude that N is a multiple of N.

If N is negative, notice that $g^{-N} = (g^N)^{-1} = e^{-1} = e$. Then, apply Lemma 1.10 to the positive integer $-N$ to conclude that $-N$ is a multiple of $|g|$, which implies that N is a multiple of $|g|$.

Conversely, now suppose that N is a multiple of $|g|$, and write $N = k|g|$, for some integer k. Then $g^N = g^{k|g|} = (g^{|g|})^k = e^k = e$. □

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. Define an relation on G by saying $x \sim y$ iff $x = y$ or $x = y^{-1}$. This relation is clearly reflexive and symmetric (because $y = (y^{-1})^{-1}$). We will show it is transitive. Suppose $x \sim y$ and $y \sim z$ for x, y, z in G. If either $x = y$ or $y = z$ then $x \sim z$ is clear, so suppose $x = y^{-1}$ and $y = z^{-1}$. Then it follows that $x = (z^{-1})^{-1} = z$, i.e. $x \sim z$. Thus $\sim$ is an equivalence relation.

In fact, each equivalence class can have at most two elements. This is because if x, y, and z are distinct and they belong to the same class, we have $x \sim y$ and $y \sim z$ and the argument above shows $x = z$, a contradiction.

It is clear that an element is in a singleton equivalence class iff that element satisfies $x = x^{-1}$, which happens iff $x^2 = e$. From this we deduce either $|x| = 1$, in which case $x = e$, or $|x| = 2$, in which case $x = f$. Thus we see the only singleton equivalence classes are $\{e\}$ and $\{f\}$; all other classes are of the form $\{y, y^{-1}\}$.

As the group is abelian, the order in which we multiply does not matter. Let $y_1, y_2, \ldots, y_k$ be representatives of each equivalence class of size 2. Then, as the classes partition the group, we have

$$\begin{aligned}\prod_{g\in G} g &= (y_1 y^{-1})(y_2 y_2^{-1}) \ldots (y_k y_k^{-1})(e)(f) \\ &= (e)(e) \ldots (e)(e) f \\ &= f.\end{aligned}$$

□

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. Recall the equivalence relation defined in the solution of Exercise 1.8. We showed that all equivalence classes are of the form $\{y, y^{-1}\}$, $\{f\}$, or $\{e\}$, where $|y| \neq 2$, $|f| = 2$ and e is the identity. Therefore, removing all equivalence classes of the form $\{f\}$ leaves us with an odd number of elements: the identity $\{e\}$ along with elements that come in pairs $\{y, y^{-1}\}$.

Then if n is even then $n - m$ is odd, which implies m is odd, which implies $m > 0$. □

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

Solution. If $|g|$ is odd, then, by Proposition 1.13, we have

$$|g^2| = \frac{|g|}{\gcd(2, |g|)} = |g|.$$

□

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. First we show that if $a, g \in G$ we have $|aga^{-1}| = |g|$. Notice that, for any integer N, we have

$$\begin{aligned}(aga^{-1})^N &= \underbrace{(aga^{-1})(aga^{-1})\cdots(aga^{-1})}_{N \text{ times}} \\ &= ag(a^{-1}a)g(a^{-1}a)\cdots(a^{-1}a)ga^{-1}) \\ &= agg\cdots ga^{-1} \\ &= ag^N a^{-1}.\end{aligned}$$

This easily implies that $g^N = e$ if and only if $ag^N a^{-1} = e$. Therefore it must be the case that $|aga^{-1}| = |g|$.

Now, let $g, h \in G$. By our above remarks $|gh| = |h(gh)h^{-1}| = |hg|$. □

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. We see that g is a counter-clockwise rotation of 90°, so it makes sense that $|g| = 4$. Indeed,

$$g^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad g^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad g^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Analogously,

$$h^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad h^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Now, we have

$$gh = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

We claim that

$$(gh)^s = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}.$$

for all natural numbers s, and we prove so by induction. For $s = 0$ this is evident. Suppose the above equation holds for a particular value of s. Then,

$$(gh)^{s+1} = (gh)^s(gh) = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & s+1 \\ 0 & 1 \end{pmatrix}.$$

This closes the induction. Now it is clear that no positive value of s will yield the identity; thus $|gh| = \infty$. □

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. Consider the group with 3 elements; we derived its multiplication table in Exercise 1.6. The two non-identity elements commute (because the group is commutative), they both have order 3, so that the least common multiple of their order is also 3. However, they multiply to give the identity, which has order 1; a counterexample.

Formally, we need to prove that this is in fact a group. This will be done in the next section. (Can the reader prove this before then?) □

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. Let $N = |gh|$. We wish to show that $N = |g||h|$. We will be using the identity $(a^M)^{-1} = (a^{-1})^M$, valid for all $a \in G$ and for all positive integers M; this is proved by verifying that $(a^{-1})^N$ is the inverse of a^N. From this identity it easily follows that $|a| = |a^{-1}|$, for all $a \in G$.

As g and h commute, we have that $(gh)^N = g^N h^N$. But $(gh)^N = e$ by definition of N. Hence, $g^N h^N = e$, which implies $g^N = (h^N)^{-1}$.

This means that $|g^N| = |(h^N)^{-1}| = |h^N|$. By Proposition 1.13, we have that $|g^N|$ divides $|g|$ and $|h^N|$ divides $|h|$. Thus, $|g^N| = |h^N|$ is a common divisor of $|g|$ and $|h|$, hence $|g^N| = |h^N| = 1$, that is, $g^N = h^N = e$. By Lemma 1.10, $|g|$ divides N and $|h|$ divides N. *As* $|g|$ *and* $|h|$ *are coprime* we can deduce $|g||h| \mid N$, by basic number theory.

We also have $N \mid |g||h|$ by Proposition 1.14. Therefore $N = |g||h|$ as desired. □

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]

Solution. Consider the prime factorization of $|h|$, say $|h| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, such that all p_i's are distinct primes, and all n_i's are positive. We wish to show that each of these factors, that each $p_i^{n_i}$ divides $|g|$, so, for the sake of contradiction, suppose there is some i for which $p_i^{n_i}$ does not divide $|g|$ and write $p \coloneqq p_i$ and $n \coloneqq n_i$. Then clearly we can write $|h| = p^n s$ for some integer s relatively prime to p. Furthermore, if m is the largest nonnegative integer (possibly zero) such that $p^m \mid |g|$ then we must have $m < n$ and we can write $|g| = p^m r$ where r is relatively prime to p.

By Proposition 1.13,

$$|g^{p^m}| = \frac{|g|}{\gcd(p^m, |g|)} = \frac{|g|}{p^m} = r,$$

and,

$$|h^s| = \frac{|h|}{\gcd(s, |h|)} = \frac{|h|}{s} = p^n.$$

Therefore $\gcd(|g^{p^m}|, |h^s|) = \gcd(r, p^n) = 1$. Then we can apply Exercise 1.14 to conclude that $|g^{p^m} h^s| = |g^{p^m}||h^s| = p^n r$. But this is nonsense since $p^n r > p^m r = |g|$ but $|g|$ was supposed to have maximal order; this is our contradiction. □

2 Examples of groups

Exercises

2.1. ¬ One can associate an $n \times n$ matrix M_σ with a permutation $\sigma \in S_n$ by letting the entry at $(i, (i)\sigma)$ be 1 and letting all other entries be 0. For example, the matrix corresponding to the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in S_n$$

would be

$$M_\sigma = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Prove that, with this notation,

$$M_{\sigma\tau} = M_\sigma M_\tau$$

for all $\sigma, \tau \in S_n$, where the product on the right is the ordinary product of matrices. [IV.4.13]

Solution. Let $\mathbf{e}_1, \ldots, \mathbf{e}_n$ be the standard basis, but expressed as *row vectors*. Note that if we have an $n \times n$ matrix A, then $\mathbf{e}_i A$ is the i-th row of A.

By definition, we see that the i-th row of M_σ is just $\mathbf{e}_{(i)\sigma}$. That is, we have the identity

$$\mathbf{e}_i M_\sigma = \mathbf{e}_{(i)\sigma}.$$

Therefore we have the following chain of reasoning,

$$\begin{aligned}\mathbf{e}_i(M_\sigma M_\tau) &= \mathbf{e}_{(i)\sigma} M\tau \\ &= \mathbf{e}_{((i)\sigma)\tau} \\ &\overset{!}{=} \mathbf{e}_{(i)(\sigma\tau)} \\ &= \mathbf{e}_i M_{\sigma\tau}.\end{aligned}$$

At the first equality we used the fact that matrix multiplication is associative. At $\overset{!}{=}$ we used the fact that S_n *acts* on the set $\{1, \ldots, n\}$, that is, we assumed $((i)\sigma)\tau = (i)(\sigma\tau)$, which is evident from the definition of multiplication in S_n. We have deduced from the above that the i-th row of $M_{\sigma\tau}$ is the same as the i-th row of $M_\sigma M_\tau$. As i was arbitrary, we must conclude that $M_{\sigma\tau} = M_\sigma M\tau$. □

2.2. ▷ Prove that if $d \leq n$, then S_n contains elements of order d. [§2.1]

Solution. The "cycle" of length d:

$$\begin{pmatrix} 1 & 2 & \cdots & d-1 & d & d+1 & \cdots & n \\ 2 & 3 & \cdots & d & 1 & d+1 & \cdots & n \end{pmatrix}.$$

□

2.3. For every positive integer n, find an element of order n in $S_{\mathbb{N}}$.

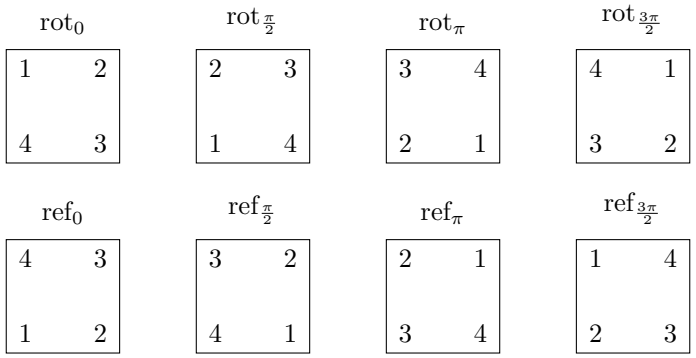
Solution. If $n = 1$ then the identity function works, so assume $n > 1$. Using the same idea as in Exercise 2.2, we construct a "cycle" of length n. Let $f\colon \mathbb{N} \to \mathbb{N}$ be given by

$$f(x) \coloneqq \begin{cases} x+1 & \text{if } x < n-1, \\ 0 & \text{if } x = n-1, \\ x & \text{otherwise.} \end{cases}$$

It can easily be checked that this function is bijective, hence an element of $S_{\mathbb{N}}$. □

2.4. Define a homomorphism $D_8 \to S_4$ by labeling vertices of a square, as we did for a triangle in §2.2. List the 8 permutations in the image of this homomorphism.

Solution. Let rot_θ represent a counterclockwise rotation by an angle of θ radians, and let ref_θ represent a reflection with respect to a line, passing through the origin, at an angle $\frac{\theta}{2}$ from the x-axis (measured counterclockwise). Label the vertices of a square as in rot_0 below. With this notation, we can see the resulting permutations of D_8.



From the diagram above, one can read all the permutations of S_4. For example, the permutation corresponding to ref$_\pi$ is

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

□

2.5. ▷ Describe the generators and relations for all dihedral groups D_{2n}. (Hint: Let x be the reflection about a line through the center of a regular n-gon and a vertex, and let y be the counterclockwise rotation by $2\pi/n$. The group D_{2n} will be generated by x and y subject to three relations. To see that these relations really determine D_{2n}, use them to show that any product $x^{i_1}y^{i_2}x^{i_3}y^{i_4}\cdots$ equals x^iy^j for some i, j with $0 \le i \le 1$, $0 \le j < n$.)[8.4, IV.2.5]

Solution. Let x be the reflection about a line through the center of a regular n-gon and a vertex, and let y be the counterclockwise rotation by $2\pi/n$. Then $x^2 = e$ and $y^n = e$. Also, it is true that $yxyx = (yx)^2 = e$; perhaps the easiest way to see this is to notice that yx must be a reflection along some line (since the n-gon is "flipped" as a result) and hence it must be its own inverse.

Suppose we have an arbitrary element of the form $x^{i_1}y^{j_1}x^{i_2}y^{j_2}\cdots x^{i_n}y^{j_n}$ for integers i_k, j_k. Actually we can assume all i_k and j_k are natural numbers, since if some were negative we can use the identities $x^{-1} = x$ and $y^{-1} = y^{n-1}$ to turn them positive. We will prove, using induction on n, that this product equals x^iy^j for some i, j with $0 \le i \le 1$, $0 \le j < n$.

Let $n = 1$. Then we have the product $x^{i_1}y^{j_1}$. Divide i_1 by 2 with remainder such that $i_1 = 2q_i + r_i$ for $0 \le r_i \le 1$ and $q_i \in \mathbb{N}$. Similarly, divide j_1 by n with remainder such that $j_1 = nq_j + r_j$ for $0 \le r_j < n$ and $q_j \in \mathbb{N}$. Then

$$x^{i_1}y^{j_1} = x^{2q_i+r_i}y^{nq_j+r_j} = (x^2)^{q_i}x_i^r(y^n)^{q_j}y^{r_j} = x^{r_i}y^{r_j},$$

as desired; this closes the base case. Assume inductively that the result is true for a positive integer n. Now, consider the product $x^{i_1}y^{j_1}\cdots x^{i_n}y^{j_n}x^{i_{n+1}}y^{j_{n+1}}$. By

inductive hypothesis, this is equal to $x^i y^j x^{i_{n+1}} y^{j_{n+1}}$ for some i, j with $0 \leq i \leq 1$, $0 \leq j < n$.

Note that we can assume i_{n+1} is either 0 or 1 using division with remainder, as in the base case. If $i_{n+1} = 0$ then we have that the product is $x^i y^{j+j_n}$ and then we can use division with remainder again to reduce $j + j_n$ to be in the desired range. So if $i_{n+1} = 0$ we can close the induction.

If $i_{n+1} = 1$ then we have $x^i y^j x y^{j_{n+1}}$. Using the relation $yxy = x^{-1} = x$ it is not hard to show (using induction) that $y^k x y^k = x$ for all natural numbers k. Then we have

$$x^i y^j x y^{j_{n+1}} = x^i (y^j x y^j) y^{j_{n+1}-j} = x^{i+1} y^{j_{n+1}-j}.$$

We can assume $j_{n+1} - j$ is nonnegative by possibly replacing it with $(n-1)(j - j_{n+1})$(see the paragraph before the induction started). Using division with remainder, this reduces the exponents to the desired range and we are done with the induction.

We have proven that x and y, subject to the relations $x^2 = y^n = (yx)^2 = e$, generate exactly $2n$ elements $x^i y^j$ for some i, j with $0 \leq i \leq 1$, $0 \leq j < n$. As D_{2n} has exactly $2n$ elements, and $x, y \in D_{2n}$, these generators and relations completely characterize D_{2n}. □

2.6. ▷ For every positive integer n construct a group containing elements g, h such that $|g| = 2$, $|h| = 2$, and $|gh| = n$. (Hint: For $n > 1$, D_{2n} will do.) [§1.6]

Solution. For $n = 1$ any group with an element of order 2 will do since, if g is such an element, then $|g| = |g^{-1}| = 2$ and $|gg^{-1}| = |e| = 1$.

For $n > 1$ take the dihedral group D_{2n} and consider two reflections with respect to adjacent reflection lines. They both have order 2 and their product will be a rotation by $2\pi/n$. If you prefer presentations, take $g = x$ and $h = yx$ with notation as in Exercise 2.5. □

2.7. ¬ Find all elements of D_{2n} that commute with every other element. (The parity of n plays a role.) [IV.1.2]

Solution. Let g be an element of D_{2n} commuting with every other element. Using Exercise 2.5 we can assume that $g = x^i y^j$ for some i, j with $0 \leq i \leq 1$, $0 \leq j < n$.

In particular we must have $xg = gx$. That is $x^{i+1} y^j = x^i (y^j x)$. Notice that

$$y^j x = (y^j x y^j) y^{-j} = x y^{-j} = x y^{n-j}$$

using the algorithm described in Exercise 2.5. Therefore we have $x^{i+1} y^j = x^{i+1} y^{n-j}$. As $0 \leq j < n$ we must have $0 < n - j \leq n$.

If $n - j = n$ then $j = 0$ and in that case it is clear that $xg = gx$ holds. If $0 < n - j < n$ then both $x^{i+1} y^j$ and $x^{i+1} y^{n-j}$ are in the canonical form described in Exercise 2.5, and as they are equal this implies $j = n - j$, i.e. $n = 2j$. In conclusion either $j = 0$ or $n = 2j$ and in that case we have $gx = xg$.

If n is odd then the only possibility is $j = 0$ so only elements that could commute with everything are e and x. But $xy \neq yx$; for if we had $xy = yx$ we deduce $x = yxy^{-1} = yxy^{n-1} = (yxy)y^{n-2} = xy^{n-2}$, and by cancellation we get $y^{n-2} = e$ but we know $n > 2$ and $|y| = n$, giving our contradiction. Therefore when n is odd the only element that commutes with every other element is the identity.

If n is even then we have $j = n/2$ and $x^i y^{n/2} x = x^{i+1} y^{n/2}$ for all $i \in \{0, 1\}$. This is only interesting when $i = 1$ so we have $xy^{n/2}x = x^2 y^{n/2}$ which by cancellation implies $y^{n/2}x = xy^{n/2}$ which means that $y^{n/2}$ commutes with x, and as it also commutes with y this shows that it commutes with every element of the group.

We have not discarded the possibility that $xy^{n/2}$ commutes with everything. By the above it clearly commutes with x, so let's check if it commutes with y. If we had $xy^{\frac{n}{2}+1} = yxy^{n/2}$ then we can say $xy^{\frac{n}{2}+1} = (yxy)y^{\frac{n}{2}-1}$ and as $yxy = x$ we get $xy^{\frac{n}{2}+1} = xy^{\frac{n}{2}-1}$ and by cancellation this simplifies to $y^2 = e$. This is absurd since $n > 2$ and $|y| = n$. Thus $xy^{n/2}$ does not commute with everything.

In summary, if n is odd the only element that commutes with everything is the identity, and if n is even we get in addition the element $y^{n/2}$ but nothing else. □

2.8. Find the orders of the groups of symmetries of the five 'platonic solids'.

Solution.

Polyhedron	Order
Tetrahedron	24
Cube	48
Octahedron	48
Dodecahedron	120
Icosahedron	120

□

2.9. Verify carefully that 'congruence mod n' is an equivalence relation.

Solution. Let $a, b, c \in \mathbb{Z}$ and let n be a positive integer. Clearly n divides $a - a = 0$ since $0 = 0n$, so $a \equiv a \mod n$ and the relation is reflexive. If $a \equiv b \mod n$ then $n \mid (b - a)$, that is $b - a = kn$ for some integer k. Then $a - b = (-k)n$ and thus $n \mid (a - b)$ so that $b \equiv a \mod n$; thus the relation is symmetric.

Now suppose $a \equiv b \mod n$ and $b \equiv c \mod n$. Then $n \mid (b - a)$ and $n \mid (c - b)$ so that $b - a = kn$ and $c - b = k'n$ for integers k and k'. But then $c - a = (b - a) + (c - b) = kn + k'n = (k + k')n$, which means $n \mid (c - a)$ and so $a \equiv c \mod n$. Therefore the relation is also transitive. □

2.10. Prove that if $n > 0$, then $\mathbb{Z}/n\mathbb{Z}$ consists of precisely n elements.

Solution. We claim that every integer is equivalent to exactly one of $0, 1, \ldots, n-1$; from this the result follows immediately. Indeed, for every integer m we can perform division by n with remainder so that $m = qn + r$ where q and r are integers such that $0 \leq r \leq n-1$. Then notice that we have $m - r = qn$ and so $n \mid (m - r)$ so that $m \equiv r \mod n$. This proves that every integer is equivalent to one of $0, 1, \ldots, n-1$.

Now let us show that none of $0, 1, \ldots, n-1$ are equivalent to one another. Suppose a, b are distinct integers such that $0 \leq a < b < n$, and for the sake of contradiction suppose that $a \equiv b \mod n$. It immediately follows that $0 < b - a < n$. By definition we have that $n \mid (b - a)$ so that $b - a = kn$ for some integer k. But then we have $0 < \frac{b-a}{n} = k < 1$ which is absurd since k is an integer. This is our contradiction and the claim follows. □

2.11. ▷ Prove that the square of every odd integer is congruent to 1 modulo 8. [VII.5.1]

Solution. Let $n = 2k + 1$ be an odd integer. Then

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1.$$

There are two cases. If k is even then write $k = 2p$ for some integer p so that

$$n^2 = 4(2p)^2 + 4(2p) + 1 = 8(2p^2 + p) + 1,$$

from which it follows that $n^2 \equiv 1 \mod 8$.

If k is odd then write $k = 2p + 1$ so that

$$n^2 = 4(2p+1)^2 + 4(2p+1) + 1 = 16p^2 + 24p + 9 = 8(2p^2 + 3p + 1) + 1,$$

and again it follows that $n^2 \equiv 1 \mod 8$. □

2.12. Prove that there are no nonzero integers a, b, c such that $a^2 + b^2 = 3c^2$. (Hint: By studying the equation $[a]_4^2 + [b]_4^2 = 3[c]_4^2$ in $\mathbb{Z}/4\mathbb{Z}$, show that a, b, c would all have to be even. Letting $a = 2k$, $b = 2l$, $c = 2m$, you would have $k^2 + l^2 = 3m^2$. What's wrong with that?)

Solution. Let us begin by studying squares in $\mathbb{Z}/4\mathbb{Z}$. We have that

$$\begin{aligned} 0^2 &\equiv 0 \mod 4 \\ 1^2 &\equiv 1 \mod 4 \\ 2^2 = 4 &\equiv 0 \mod 4 \\ 3^2 = 9 &\equiv 1 \mod 4. \end{aligned}$$

We do not have to check anything further since if x is an integer and we are interested in knowing x^2 modulo 4 we can perform division by 4 with remainder on x, i.e. writing $x = 4q + r$ for some integers q and r with $0 \leq r \leq 3$, and then noticing

that $x^2 = 4(4q^2 + 2qr) + r^2$ so that $x^2 \equiv r^2 \mod 4$. This shows that every integer squared is congruent to 0 or 1 modulo 4.

So, if $c^2 \equiv 1 \mod 4$ then it is not hard to see that $3c^2 = a^2 + b^2 \equiv 3 \mod 4$. This congruence relation has no solution since a^2 and b^2 are congruent to 0 or 1 modulo 4, which implies that $a^2 + b^2$ is congruent to 0, 1, or 2 modulo 4. Therefore we must have $c^2 \equiv 0 \mod 4$, which implies $a^2 + b^2 \equiv 0 \mod 4$, and this is only satisfied when $a^2 \equiv b^2 \equiv 0 \mod 4$.

We have deduced that in any solution to the equation $a^2 + b^2 = 3c^2$ we must have 4 dividing a^2, b^2, and c^2. For any integer x, if x has no factor of 2, i.e. is odd, then x^2 will not have a factor of 2. It follows that if x^2 does have a factor of 2, as is the case for a^2, b^2, and c^2, then x does as well, i.e. x is even. Hence, a, b, and c are all even.

We have shown that any solution to the equation $a^2 + b^2 = 3c^2$ must have a, b, and c, be even. Assume, for the sake of contradiction, that a, b, c is a solution and further assume $a, b, c > 0$, since we can clearly negate the variables while keeping equality. Write $a = 2k$, $b = 2l$, and $c = 2m$. Plugging these expressions in, we get $k^2 + l^2 = 3m^2$ so that k, l, and m are even. Repeating this process would yield an infinite decreasing sequence of positive integers; but there is no such thing so in fact the equation has no non-zero solutions. □

2.13. ▷ Prove that if $\gcd(m, n) = 1$, then there exist integers a and b such that

$$am + bn = 1.$$

(Use Corollary 2.5.) Conversely, prove that if $am + bn = 1$ for some integers a and b, then $\gcd(m, n) = 1$. [2.15, §V.2.1, V.2.4]

Solution. If $\gcd(m, n) = 1$ then Corollary 2.5 says that $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$. In particular, there is some integer a such that $a \cdot [m]_n = [1]_n$, which implies $[am]_n = [1]_n$, and that is $am \cong 1 \mod n$. Then $n \mid 1 - am$ and there exists some integer b such that $1 - am = bn$, i.e. $am + bn = 1$.

Conversely, suppose $am + bn = 1$ for some integers a and b. If $d > 0$ divides both n and m then it clearly divides $am + bn = 1$, and hence $d = 1$. Then $\gcd(m, n) = 1$. □

2.14. ▷ State and prove an analog of Lemma 2.2, showing that the multiplication on $\mathbb{Z}/n\mathbb{Z}$ is a well-defined operation. [§2.3, §III.1.2]

Solution. The claim is that if $a \equiv a' \mod n$ and $b \equiv b' \mod n$ then

$$ab \equiv a'b' \mod n.$$

The proof is given below.

By hypothesis $n \mid (a' - a)$ and $n \mid (b' - b)$; therefore there exists some integers k and l such that

$$a' - a = kn, \quad b' - b = ln.$$

It follows that $a' = kn + a$ and $b' = b + ln$. Then, $a'b' = (a + kn)(b + ln) = ab + n(al + bk + kln)$. Hence $n \mid (a'b' - ab)$ and the claim follows. □

2.15. ¬ Let $n > 0$ be an odd integer.

- Prove that if $\gcd(m, n) = 1$, then $\gcd(2m + n, 2n) = 1$. (Use Exercise 2.13.)
- Prove that if $\gcd(r, 2n) = 1$, then $\gcd(\frac{r-n}{2}, n) = 1$. (Ditto.)
- Conclude that the function $[m]_n \to [2m+n]_{2n}$ is a bijection between $(\mathbb{Z}/n\mathbb{Z})^*$ and $(\mathbb{Z}/2n\mathbb{Z})^*$.

The number $\phi(n)$ of elements of $(\mathbb{Z}/n\mathbb{Z})^*$ is *Euler's ϕ-function*. The reader has just proved that if n is odd, then $\phi(2n) = \phi(n)$. Much more general formulas will be given later on (cf. Exercise V.6.8). [VII.5.11]

Solution.

- By Exercise 2.13 there are some integers a and b such that

$$am + bn = 1.$$

As n is odd write $n = 2p + 1$ for some integer p. Then

$$\begin{aligned}
&[(2pb - ap - 1)(m + p)](2n) + [1 + 2ap(m + p)](2m + n)\\
&= (m + p)[(2n)(2pb - \cancel{ap} - 1) + 2ap(2m + \cancel{n})] + 2m + n\\
&= 2(m + p)[n(2pb - 1) + ap(2m)] + 2(m + p) + 1\\
&= 2(m + p)[2pnb - n + 2map + 1] + 1\\
&= 2(m + p)[2p(am + bn) + 1 - n] + 1\\
&= 2(m + p)[2p + 1 - n] + 1\\
&= 1.
\end{aligned}$$

This shows, by Exercise 2.13, that $\gcd(2m + n, 2n) = 1$.

- By Exercise 2.13 there are some integers a and b such that

$$ar + b(2n) = 1.$$

We have that r is odd—if it were even the above equation gives a contradiction modulo 2. It follows that $r - n$ is even and that $\frac{r-n}{2}$ is an integer. Then

$$\begin{aligned}
2a\left(\frac{r-n}{2}\right) + (2b + a)n &= a(r - n) + (2b + a)n\\
&= ar + b(2n)\\
&= 1.
\end{aligned}$$

This shows, by Exercise 2.13, that $\gcd\left(\frac{r-n}{2}, n\right) = 1$.

- By the first bullet point the assignment $[m]_n \mapsto [2m+n]_{2n}$ is a well-defined function between $(\mathbb{Z}/n\mathbb{Z})^*$ and $(\mathbb{Z}/2n\mathbb{Z})^*$. By the second bullet point the assignment $[r]_{2n} \mapsto \left[\frac{r-n}{2}\right]_n$ is a well-defined function between $(\mathbb{Z}/2n\mathbb{Z})^*$ and $(\mathbb{Z}/n\mathbb{Z})^*$. These two functions are readily seen to be inverses of each other and the claim follows.

□

2.16. Find the last digit of $1238237^{18238456}$. (Work in $\mathbb{Z}/10\mathbb{Z}$.)

Solution. From Exercise 2.14 it follows that if $a \equiv a' \mod n$ then $a^k \equiv a'^k \mod n$ for all nonnegative integers k. We clearly have $1238237 \equiv 7 \mod 10$, so

$$1238237^{18238456} \equiv 7^{18238456} \mod 10.$$

Now, notice that $7^2 = 49 \equiv 9 \equiv -1 \mod 10$. Then,

$$7^{18238456} = (7^2)^{9119228} \equiv (-1)^9 119228 = 1 \mod 10.$$

Thus, the last digit of $1238237^{18238456}$ is 1. □

2.17. ▷ Show that if $m \equiv m' \bmod n$, then $\gcd(m,n) = 1$ if and only if $\gcd(m',n) = 1$. [§2.3]

Solution. As $m \equiv m' \mod n$ there is some integer k such that $kn = m' - m$. Notice that the statement is symmetrical so it suffices to prove only one direction.

Suppose $\gcd(m,n) = 1$. By Exercise 2.13 there exists some integers a and b such that $am + bn = 1$. Then $am' + (b-ak)n = a(m'-kn) + bn = am + bn = 1$, which shows, by Exercise 2.13, that $\gcd(m',n) = 1$. □

2.18. For $d \leq n$, define an injective function $\mathbb{Z}/d\mathbb{Z} \to S_n$ preserving the operation, that is, such that the sum of equivalence classes in $\mathbb{Z}/d\mathbb{Z}$ corresponds to the product of the corresponding permutations.

Solution. Let $c_d \in S_n$ stand for the permutation defined in Exercise 2.2:

$$\begin{pmatrix} 1 & 2 & \cdots & d-1 & d & d+1 & \cdots & n \\ 2 & 3 & \cdots & d & 1 & d+1 & \cdots & n \end{pmatrix}.$$

Define a function $\mathbb{Z}/d\mathbb{Z} \to S_n$ by the rule $[m]_d \mapsto (c_d)^m$ for $0 \leq m \leq d-1$. □

2.19. ▷ Both $(\mathbb{Z}/5\mathbb{Z})^*$ and $(\mathbb{Z}/12\mathbb{Z})^*$ consist of 4 elements. Write their multiplication tables, and prove that no re-ordering of the elements will make them match. (Cf. Exercise 1.6.) [§4.3]

Solution. For $(\mathbb{Z}/5\mathbb{Z})^*$ we have the following table.

	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

For $(\mathbb{Z}/12\mathbb{Z})^*$ we have the following table.

	$[1]_{12}$	$[5]_{12}$	$[7]_{12}$	$[11]_{12}$
$[1]_{12}$	$[1]_{12}$	$[5]_{12}$	$[7]_{12}$	$[11]_{12}$
$[5]_{12}$	$[5]_{12}$	$[1]_{12}$	$[11]_{12}$	$[7]_{12}$
$[7]_{12}$	$[7]_{12}$	$[11]_{12}$	$[1]_{12}$	$[5]_{12}$
$[11]_{12}$	$[11]_{12}$	$[7]_{12}$	$[5]_{12}$	$[1]_{12}$

Note that reordering the elements will not change the fact that in $(\mathbb{Z}/12\mathbb{Z})^*$ all elements square to the (unique) identity, but this is not the case for $(\mathbb{Z}/5\mathbb{Z})^*$. □

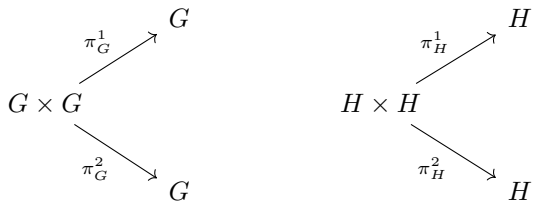
3 The category Grp

Exercises

3.1. ▷ Let $\varphi\colon G \to H$ be a morphism in a category C with products. Explain why there is a unique morphism $(\varphi \times \varphi)\colon G \times G \to H \times H$ compatible in the evident way with the natural projections.

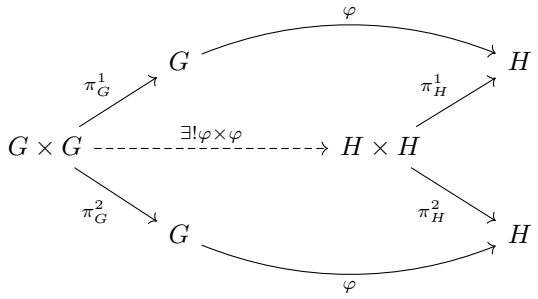
(This morphism is defined explicitly for $\mathsf{C} = \mathsf{Set}$ in §3.1.) [§3.1, 3.2]

Solution. As C has products then the products $G \times G$ and $H \times H$ exist and they are depicted as follows.



Now, there is a map $\varphi\colon G \to H$, that is used to define two maps from $G \times G \to H$ as below. Then, by the universal property of $H \times H$, there exists a unique map

$\varphi \times \varphi$ such that the diagram commutes.



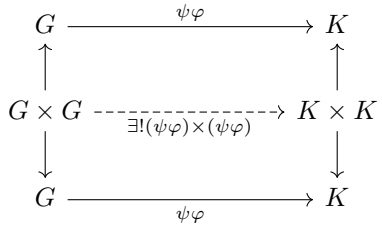
□

3.2. Let $\varphi\colon G \to H$, $\psi\colon H \to K$ be morphisms in a category with products, and consider morphisms between the products $G \times G$, $H \times H$, $K \times K$ as in Exercise 3.1. Prove that

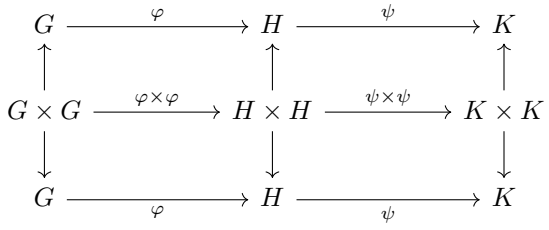
$$(\psi\varphi) \times (\psi\varphi) = (\psi \times \psi)(\varphi \times \varphi).$$

(This is part of the commutativity of the diagram displayed in §3.2.)

Solution. We have the map $\psi\varphi\colon G \to K$. By Exercise 3.1, $(\psi\varphi)\times(\psi\varphi)$ is the unique map $G \times G \to K \times K$ that makes the diagram below commute (I am obviating the names of the projections).



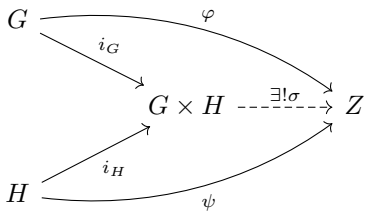
But, by applying Exercise 3.1 twice, we have that the diagram below also commutes and the claim follows.



□

3.3. ▷ Show that if G, H are *abelian* groups, then $G \times H$ satisfies the universal property for coproducts in Ab (cf. §I.5.5). [§3.5, 3.6, §III.6.1]

Solution. Define group homomorphisms $i_G\colon G \to G \times H$ by $g \mapsto (g, e_H)$ and $i_H\colon H \to G \to H$ by $h \mapsto (e_G, h)$; it is immediate to check that these are indeed homomorphisms. Let Z be an arbitrary abelian group and let $\varphi\colon G \to Z$ and $\psi\colon H \to Z$ be homomorphisms.



Then if we define a homomorphism $\sigma\colon G \times H \to Z$ by $\sigma(g, h) = \varphi(g)\psi(h)$. It is a homomorphism by the following chain of reasoning:

$$\begin{aligned}
\sigma((g,h)(g',h')) &= \sigma(gg', hh') \\
&= \varphi(gg')\psi(hh') \\
&= \varphi(g)\varphi(g')\psi(h)\psi(h') \\
&\overset{!}{=} (\varphi(g)\psi(h))(\varphi(g')\psi(h')) \\
&= \sigma(g,h)\sigma(g',h'),
\end{aligned}$$

where at $\overset{!}{=}$ we used the crucial fact that Z is abelian.

Of course σ makes the diagram commute. It is easy to see that this definition is forced by the commutativity of the diagram and the fact that σ is a homomorphism. □

3.4. Let G, H be groups, and assume that $G \cong H \times G$. Can you conclude that H is trivial? (Hint: No. Can you construct a counterexample?)

Solution. No. Let $\mathbb{R}^{\oplus\mathbb{N}}$ be the set of functions $f\colon \mathbb{N} \to \mathbb{R}$, i.e. real-valued sequences. If $f, g \in \mathbb{R}^{\oplus\mathbb{N}}$, then define a function $f+g \in \mathbb{R}^{\oplus\mathbb{N}}$ by the rule $f+g(n) \coloneqq f(n)+g(n)$ for all $n \in \mathbb{N}$. It is easy to check that operation this turns $\mathbb{R}^{\oplus\mathbb{N}}$ into an abelian group. Notice that $\mathbb{R}^{\oplus\mathbb{N}} \cong \mathbb{R} \times \mathbb{R}^{\oplus\mathbb{N}}$ since there is an isomorphism $\varphi\colon \mathbb{R}^{\oplus\mathbb{N}} \to \mathbb{R} \times \mathbb{R}^{\oplus\mathbb{N}}$ defined by $\varphi(f) \coloneqq (f(0), g)$, where $g\colon \mathbb{N} \to \mathbb{R}$ is defined by the rule $g(n)\colon f(n+1)$. □

3.5. Prove that $\mathbb{Q}$ is not the direct product of two nontrivial groups.

Solution. Let G and H be groups such that $G \times H \cong \mathbb{Q}$, and let $\varphi\colon G \times H \to \mathbb{Q}$ be an isomorphism. Define two subsets of $\mathbb{Q}$ by

$$\begin{aligned}
G' &\coloneqq \{q \in \mathbb{Q} \mid q = \varphi(g, e_H) \text{ for some } g \in G\} \\
H' &\coloneqq \{q \in \mathbb{Q} \mid q = \varphi(e_G, h) \text{ for some } h \in H\}.
\end{aligned}$$

Note that $G' \cap H' = \{0\}$. Indeed, it is clear that $\varphi(e_G, e_H) = 0 \in G' \cap H'$; conversely, if there is some $q \in \mathbb{Q}$ such that $q = \varphi(g, e_H) = \varphi(e_G, h)$ for some $g \in G$ and $h \in H$ then $g = e_G$ and $h = e_H$, and hence $q = 0$, since φ is injective.

Furthermore, we claim that both G' and H' are (abelian) groups under addition. We prove this only for G' since the argument for H' is completely analogous. If $q, r \in G'$ such that $q = \varphi(g_1, e_H)$ and $r = \varphi(g_2, e_H)$ then $q + r = \varphi(g_1 g_2, e_H)$ since φ is a homomorphism; thus addition does define a binary operation on G'. This operation is clearly associative, and G' has the identity element 0, as we noted in the previous paragraph. Finally, G' has inverses, for if $q = (g, e_H) \in G'$ then $-q = (g^{-1}, e_H)$ as it is verified by computing $q + (-q)$ and using the fact that φ is a homomorphism.

For the sake of contradiction, suppose both G and H are nontrivial. This easily implies that G' and H' are nontrivial, so let $\frac{a}{b} \in G'$ and $\frac{c}{d} \in H'$ for nonzero integers a, b, c, d. But then $(bc)\frac{a}{b} = ac \in G'$, since G' is a group, and $(ad)\frac{c}{d} = ac \in H'$, since H' is a group. Hence $ac \in G' \cap H' = \{0\}$, which is a contradiction since $a, c \neq 0$. Thus either G or H is trivial.

Note This is the simplest proof I could come up with. It also proves the stronger claim that there are no injective homomorphism $G \times H \to \mathbb{Q}$ unless one of G or H is trivial. □

3.6. ▷ Consider the product of cyclic groups C_2, C_3 (cf. §2.3): $C_2 \times C_3$. By Exercise 3.3, this group is a coproduct of C_2 and C_3 in Ab. Show that it is *not* a coproduct of C_2 and C_3 in Grp, as follows:

- find injective homomorphisms $C_2 \to S_3$, $C_3 \to S_3$;
- arguing by contradiction, assume that $C_2 \times C_3$ is a coproduct of C_2, C_3, and deduce that there would be a group homomorphism $C_2 \times C_3 \to S_3$, with certain properties;
- show that there is no such homomorphism.

[§3.5]

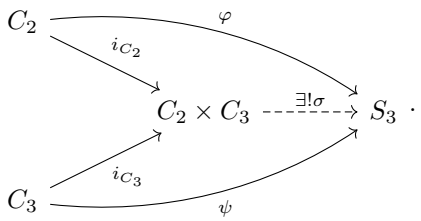
Solution. Before we begin, let us say that we identity C_n with $\mathbb{Z}/n\mathbb{Z}$ during this solution.

- Use the homomorphisms found in Exercise 2.18. Call them $\varphi\colon C_2 \to S_3$ and $\psi\colon C_3 \to S_3$. Use the notation c_2 and c_3 as in Exercise 2.18:

$$c_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad c_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

- For the sake of contradiction, suppose $C_2 \times C_3$ is a coproduct of C_2 and C_3 in Grp. Then, by the universal property of coproducts, there exists a (unique) homomorphism $\sigma\colon C_2 \times C_3 \to S_3$ such that the diagram below commutes.

Here i_{C_2} and i_{C_3} are defined as in Exercise 3.3.



- This implies that $\sigma \circ i_{C_2}([1]_2) = \varphi([1]_2)$, i.e. $\sigma([1]_2, [0]_3) = c_2$. Similarly, we have $\sigma([0]_2, [1]_3) = c_3$. In particular, since σ is a homomorphism,

  $$c_2c_3 = \sigma([1]_2, [0]_3)\sigma([0]_2, [1]_3) = \sigma([1]_2, [1]_3) = \sigma([0]_2, [1]_3)\sigma([1]_2, [0]_3) = c_3c_2.$$

  But this simply is not true, giving our contradiction.

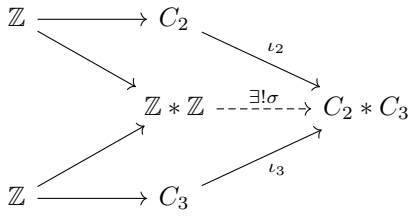
$$c_2c_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad c_3c_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

□

3.7. Show that there is a *surjective* homomorphism $\mathbb{Z} * \mathbb{Z} \to C_2 * C_3$. ($*$ denotes coproduct in Grp; cf. §3.4.)

One can think of $\mathbb{Z} * \mathbb{Z}$ as a group with two generators x, y, subject to no relations whatsoever. (We will study a general version of such groups in §5; see Exercise 5.6.)

Solution. There clearly are surjective homomorphisms $\mathbb{Z} \to C_2$ and $\mathbb{Z} \to C_3$ sending 1 to the generator of C_2 and the generator of C_3 respectively. Then, using notation as in Exercise 3.8, we have the following diagram.



Using the universal property of $\mathbb{Z} * \mathbb{Z}$, we get that there is a unique σ as above, that makes the diagram commute. We will prove that σ is surjective, giving the desired result.

Indeed, we know by Exercise 3.8 that $C_2 * C_3$ is generated by two elements x and y, so we just need to verify that these are in the image of σ and then, since σ is a homomorphism, the claim would follow. But this is clear from the commutativity of the diagrams, since the surjective maps take 1 to the generators and ι_2 and ι_3 take the generators to x and y. □

3.8. ▷ Define a group G with two generators x, y subject (only) to the relations $x^2 = e_G, y^3 = e_G$. Prove that G is a coproduct of C_2 and C_3 *in* Grp. (The reader will obtain an even more concrete description for $C_2 * C_3$ in Exercise 9.14; it is called the *modular group*.) [§3.4, 9.14]

Solution. We define a group G whose elements are "words" in the alphabet

$$\{x, y, x^{-1}, y^{-1}\}$$

but we identify words w and w' whenever one can get from w to w' by "using" the rule

$$xx^{-1} = x^{-1}x = yy^{-1} = y^{-1}y = x^2 = y^3 = e,$$

where e symbolizes the empty word. Multiplication in G is given by concatenation.[1] This gives G a group structure. Then there are natural group homomorphisms $\iota_2 \colon C_2 \to G$ and $\iota_3 \colon C_3 \to G$ given by sending the generator of C_2 to x and the generator of C_3 to y respectively.

Now let Z be a group with group homomorphisms $f \colon C_2 \to Z$ and $g \colon C_3 \to Z$. Then we will define a $\sigma \colon G \to Z$ that makes the relevant diagram commute. In particular, we will require that σ sends x to where f sends the generator of C_2 and that σ sends y to where g sends the generator of C_3. It's easily seen that this uniquely determines σ. □

3.9. Show that *fiber* products and coproducts exist in Ab. (Cf. Exercise I.5.12. For coproducts, you may have to wait until you know about *quotients*.)

Solution. Let G, H, and K be abelian groups and let $\alpha \colon G \to K$ and $\beta \colon H \to K$ be homomorphisms. Then the fibered product of G and H in this case is the set $G \times_K H \coloneqq \{(g, h) \in G \times H \mid \alpha(g) = \beta(h)\}$ viewed as a subgroup of $G \times H$.

First we need to prove that that $G \times_K H$ is indeed an (abelian) subgroup of $G \times H$. Firstly, the binary operation is closed since if (g, h) and (g', h') are elements of $G \times_K H$ then

$$\alpha(gg') = \alpha(g)\alpha(g') = \beta(h)\beta(h') = \beta(hh')$$

as α and β are homomorphisms, hence $(gg', hh') \in G \times_K H$. The identity element is clearly (e_G, e_H), which is in $G \times_K H$ since $\alpha(e_G) = \beta(e_H) = e_K$, as homomorphisms take identities to identities. Similarly, if $(g, h) \in G \times_K H$ then its inverse (g^{-1}, h^{-1}) is in $G \times_K H$. This is because

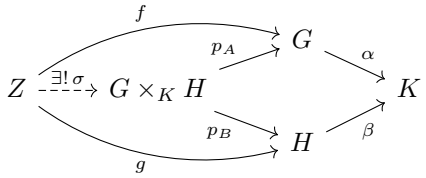
$$\alpha(g^{-1}) = (\alpha(g))^{-1} = (\beta(h))^{-1} = \beta(h^{-1}),$$

since homomorphisms preserve inverses. The operation is clearly associative and commutative. Thus we have proved that $G \times_K H$ is a subgroup of $G \times H$, and in particular it is an abelian group.

[1] This definition is informal, but it will be treated rigorously in section 5.

There are natural homomorphisms $p_G\colon G \times_K H \to G$ and $p_H\colon G \times_K H \to H$ given by projecting the first and second coordinates respectively (it's easy to check these are indeed homomorphisms). It is immediate that $\alpha \circ p_G = \beta \circ p_H$ by definition of $G \times_K H$.

We will show that $G \times_K H$, with these maps, satisfies the universal property of a fibered coproduct. Suppose Z is an abelian group and $f\colon Z \to G$ and $g\colon Z \to H$ are homomorphisms that satisfy $\alpha \circ f = \beta \circ g$. We need to prove that there is a unique homomorphism σ making the diagram below commute



But by Exercise I.5.12, it is clear that there is a unique *set-function* σ, defined by $\sigma(z) :== (f(z), g(z))$ for all $z \in Z$, making the diagram commute. So, the only thing we need to verify is that σ is a group homomorphism. Let $z, z' \in Z$. Then

$$\sigma(zz') = (f(z)f(z'), g(z)g(z')) = (f(z), g(z))(f(z'), g(z')) = \sigma(z)\sigma(z').$$

Now we will describe fibered coproducts. Again we let G, H, K be abelian groups but now we assume $\alpha\colon K \to G$ and $\beta\colon K \to H$. Define a relation on $G \times H$ by the following rule. For $x, y \in G \times H$ we say

$$x \sim y \iff x = \iota_G \circ \alpha(k) \text{ and } y = \iota_H \circ \beta(k) \text{ for some } k \in K,$$

where $\iota_G\colon G \to G \times H$ and $\iota_H\colon H \to G \times H$ are as in Exercise 3.3. Now define a subset of $G \times H$ by

$$S \coloneqq \{xy^{-1} \mid x, y \in G \times H \text{ and } x \sim y\}.$$

Let $\langle S \rangle$ be the smallest subgroup of $G \times H$ generated by S, as in §6.3. As $G \times H$ is abelian, $\langle S \rangle$ is normal and hence we can define

$$G *_K H \coloneqq (G \times H)/\langle S \rangle$$

to be the fibered coproduct of G and H; and we know it to be an abelian group. In particular, there is a natural homomorphism $\pi\colon G \times H \to (G \times H)/\langle S \rangle$ that satisfies the universal property of quotients. Hence we can think of the inclusions of the fibered coproduct as $\pi \circ i_G$ and $\pi \circ i_H$. We need to verify, firstly, that

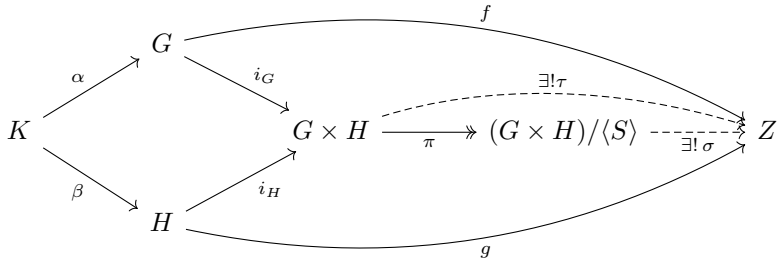
$$\pi \circ \iota_G \circ \alpha = \pi \circ \iota_H \circ \beta.$$

But notice that for all $k \in K$, we have that $\iota_G \circ \alpha(k) \sim \iota_H \circ \beta(k)$ and thus

$$(\iota_G \circ \alpha(k))(\iota_H \circ \beta(k))^{-1} \in S \subseteq \langle S \rangle,$$

which makes the claim obvious.

Now we will verify that $(G \times H)/\langle S \rangle$ satisfies the universal property of fibered coproducts. Let Z be an abelian group with maps $f\colon G \to Z$ and $g\colon H \to Z$ that satisfy $f \circ \alpha = g \circ \beta$. We will show that there exists some unique σ as below such the diagram commutes.



By the universal property of coproducts, there exists a unique $\tau\colon G \times H \to Z$ such that

$$f = \tau \circ \iota_G$$
$$g = \tau \circ \iota_H.$$

We claim that $S \subseteq \ker \tau$. Indeed, if $g \in S$ then, by definition, there is some k such that if we define $x \coloneqq \iota_G \circ \alpha(k)$ and $y \coloneqq \iota_H \circ \beta(k)$ then $g = xy^{-1}$. But then

$$\begin{aligned}
\tau(g) &= \tau(xy^{-1}) \\
&= \tau(x)(\tau(y))^{-1} \\
&= (\tau \circ \iota_G \circ \alpha(k))(\tau \circ \iota_H \circ \beta(k))^{-1} \\
&= (f \circ \alpha(k))(g \circ \beta(k))^{-1} \\
&= e
\end{aligned}$$

since $f \circ \alpha = g \circ \beta$. This shows that $S \subseteq \ker \tau$. As $\langle S \rangle$ is the smallest subgroup containing S, we have $\langle S \rangle \subseteq \ker \tau$. By Proposition 7.12, there exists a unique homomorphism $\sigma\colon (G \times H)/\langle S \rangle \to Z$ such that

$$\tau = \sigma \circ \pi.$$

That the whole diagram commutes is immediate and uniqueness follows from the uniqueness of τ and σ itself. □

4 Group homomorphisms

Exercises

4.1. ▷ Check that the function π_m^n defined in §4.1 is well-defined and makes the diagram commute. Verify that it is a group homomorphism. Why is the hypothesis $m|n$ necessary? [§4.1]

Solution. The commutativity of the diagram simply states that for all integers a we have

$$\pi_m^n([a]_n) = [a]_m,$$

which we can take as our definition of π_m^n. We need to verify this assignment is well-defined, i.e. that if $[a]_n = [a']_n$ then $\pi_m^n([a]_n) = \pi_m^n([a']_n)$. In other words, we need to check that if $n \mid a - a'$ then $m \mid a - a'$; but this is obvious *provided we know* that $m \mid n$. □

4.2. Show that the homomorphism $\pi_2^4 \times \pi_2^4 \colon C_4 \to C_2 \times C_2$ is *not* an isomorphism. In fact, is there *any* isomorphism $C_4 \to C_2 \times C_2$?

Solution. Indeed, $\pi_2^4 \times \pi_2^4$ is not injective since $\pi_2^4 \times \pi_2^4([0]_1) = \pi_2^4 \times \pi_2^4([2]_4) = ([0]_2, [0]_2)$. There is no isomorphism $C_4 \to C_2 \times C_2$ since there is an element of order 4 in C_4 but there is none in $C_2 \times C_2$. □

4.3. ▷ Prove that a group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ if an only if it contains an element of order n. [§4.3]

Solution. If a group G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ then there is an isomorphism $\varphi \colon \mathbb{Z}/n\mathbb{Z} \to G$. By Proposition 4.8, $|\varphi([1]_n)| = n$.

Conversely, suppose there is a group G of order n with an element $g \in G$ such that $|g| = n$. Consider $\varphi \colon \mathbb{Z}/n\mathbb{Z} \to G$ defined by $\varphi([a]_n) \coloneqq g^a$. We need to verify that this function is well-defined, i.e. that if $[a]_n = [a']_n$ then $\varphi([a]_n) = \varphi([a']_n)$. Indeed, if $n \mid a - a'$ then, by Corollary 1.11, $g^{a-a'} = e$ which means

$$\varphi([a]_n) = g^a = g^{a'} = \varphi([a']_n).$$

Therefore φ is well-defined. It is a homomorphism since,

$$\varphi([a]_n + [b]_n) = \varphi([a+b]_n) = g^{a+b} = g^a g^b = \varphi([a]_n)\varphi([b_n]).$$

Now we verify that φ is an isomorphism. Suppose that $\varphi([a]_n) = \varphi([b]_n)$, which means that $g^a = g^b$ and thus $g^{a-b} = e$. Again, by Corollary 1.11, $n \mid a - b$ and so $[a]_n = [b]_n$. This shows φ is injective. As $|\mathbb{Z}/n\mathbb{Z}| = |G| = n$ then φ is surjective. Thus φ is an isomorphism. □

4.4. Prove that no two of the groups $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ are isomorphic to one another. Can you decide whether $(\mathbb{R}, +), (\mathbb{C}, +)$ *are* isomorphic to one another? (Cf. Exercise VI.1.1.)

Solution. Firstly, $(\mathbb{R}, +)$ is isomorphic to neither $(\mathbb{Z}, +)$ nor $(\mathbb{Q}, +)$ since the underlying sets have different cardinalities—$\mathbb{R}$ is uncountable while both $\mathbb{Z}$ and $\mathbb{Q}$ are countable. Also notice that while 1 generates all of $(\mathbb{Z}, +)$ but there is no element in $(\mathbb{Q}, +)$ playing an analogous role. Indeed, if $\frac{a}{b} \in \mathbb{Q}$, where a, b are integers with $b > 0$, then $n\frac{a}{b} = \frac{na}{b}$ for all integers n and notice that, for example $\frac{1}{b+1}$ is not of this form. To prove this assume, for the sake of contradiction, that $\frac{na}{b} = \frac{1}{b+1}$; then

this would imply $na = \frac{b}{b+1}$ and, since na is an integer, we have that $(b+1) \mid b$, which is impossible since both b and $b+1$ are positive yet $b+1 > b$.

The groups $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are isomorphic to each other. For a proof see Exercise VI.1.1. □

4.5. Prove that the groups $(\mathbb{R} \setminus \{0\}, \cdot)$ and $(\mathbb{C} \setminus \{0\}, \cdot)$ are not isomorphic.

Solution. Notice that, in $(\mathbb{C} \setminus \{0\}, \cdot)$, we have that the order of i is 4, yet if $r \in \mathbb{R}/ \setminus \{0\}$ and $r^4 = 1$ then either $r = 1$ or $r = -1$, and neither of these have order 4. □

4.6. We have seen that $(\mathbb{R}, +)$ and $(\mathbb{R}^{>0}, \cdot)$ are isomorphic (Example 4.4). Are the groups $(\mathbb{Q}, +)$ and $(\mathbb{Q}^{>0}, \cdot)$ isomorphic?

Solution. No. For the sake of contradiction, assume there is an isomorphism $\varphi\colon (\mathbb{Q}, +) \to (\mathbb{Q}^{>0}, \cdot)$. We will show that $\varphi(1) = 1$ which will contradict injectivity as $\varphi(0) = 1$ since homomorphisms take identities to identities.

To do this we need a small lemma. We claim that if y is a positive integer such that for all $n \in \mathbb{Z}^+$ there is an $x \in \mathbb{Z}^+$ such that $y = x^n$ then $y = 1$. We prove this as follows. Let y be as above and define

$$S \coloneqq \{x \in \mathbb{Z}^+ \mid y = x^n \text{ for some } n \in \mathbb{Z}^+\}.$$

Clearly $y \in S$, so S is nonempty. By the well-ordering principle, S has a minimal element, so let $x_0 \coloneqq \min S$ such that $y = x_0^{n_0}$ for some positive integer n_0. By the property we assumed of y, there is a positive integer x_1 such that $y = x_1^{n_0+1}$. It is clear that $x_1 \in S$, so $x_0 \leq x_1$. Then it follows that $x_0^{n_0} \leq x_1^{n_0}$, i.e. we have $y \leq x_1^{n_0}$. But $y = x_1^{n_0+1}$ so $x_1^{n_0+1} \leq x_1^{n_0}$, from which we deduce $x_1 \leq 1$. As x_1 is a positive integer we have that $x_1 = 1$, and thus $y = 1^{n_0+1} = 1$, as desired. We have proved the lemma we required.

Now for the solution. Let $\varphi(1) = \frac{a}{b}$ for some positive *coprime* integers a and b. Let n be an arbitrary positive integer and notice that $\varphi(1) = \varphi(n\frac{1}{n}) = (\varphi(\frac{1}{n}))^n$. Then, if $\varphi(\frac{1}{n}) = \frac{c}{d}$ for coprime positive integers c and d, we have

$$\frac{a}{b} = \frac{c^n}{d^n}.$$

As c and d are coprime, it is easy to see that c^n and d^n are also coprime. A positive rational can be *uniquely* represented as a ratio of two positive coprime integers, so the equation above implies $a = c^n$ and $b = d^n$. But n was arbitrary, so the lemma we proved implies that $a = 1$ and $b = 1$. Therefore $\varphi(1) = 1$ and contradiction follows. □

4.7. Let G be a group. Prove that the function $G \to G$ defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian. Prove that $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

Solution. Let $\varphi_1, \varphi_2 \colon G \to G$ be the functions defined by $g \mapsto g^{-1}$ and $g \mapsto g^2$ respectively. If G is abelian then it follows, for all $g, h \in G$, that

$$\varphi_1(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1} = \varphi_1(g)\varphi_1(h),$$

so φ_1 is a homomorphism. Similarly, for all $g, h \in G$ we have

$$\varphi_2(gh) = (gh)^2 = ghgh = gghh = g^2h^2 = \varphi_2(g)\varphi_2(h),$$

so φ_2 is a homomorphism.

Conversely, assume that φ_1 is a homomorphism. Then, for all $g, h \in G$ we have

$$gh = (h^{-1}g^{-1})^{-1} = (\varphi_1(h)\varphi_1(g))^{-1} = (\varphi_1(hg))^{-1} = ((hg)^{-1})^{-1} = hg,$$

so G is abelian. Now assume instead that φ_2 is a homomorphism. Then, for all $g, h \in G$ we have

$$gh = g^{-1}(g^2h^2)h^{-1} = g^{-1}\varphi_2(g)\varphi_2(h)h^{-1} = g^{-1}\varphi_2(gh)h^{-1} = g^{-1}ghghh^{-1} = hg,$$

so G is abelian. □

4.8. ¬ Let G be a group, and let $g \in G$. Prove that the function $\gamma_g \colon G \to G$ defined by $(\forall a \in G) : \gamma_g(a) = gag^{-1}$ is an automorphism of G. (The automorphisms γ_g are called 'inner' automorphisms of G.) Prove that the function $G \to \mathrm{Aut}(G)$ defined by $g \mapsto \gamma_g$ is a homomorphism. Prove that this homomorphism is trivial if and only if G is abelian. [6.7, 7.11, IV.1.5]

Solution. Let $g, a, b \in G$ be arbitrary. Then,

$$\gamma_g(a)\gamma_g(b) = gag^{-1}gbg^{-1} = gabg^{-1} = \gamma_g(ab).$$

So, γ_g is a homomorphism for all $g \in G$. It is an isomorphism since $\gamma_{g^{-1}}$ is clearly its inverse. Therefore it is an automorphism.

Now, consider the function $G \to \mathrm{Aut}(G)$ defined by $g \mapsto \gamma_g$. For $g, h \in G$ we wish to show that $\gamma_g \circ \gamma_h = \gamma_{gh}$. Indeed, for all $x \in G$ we have

$$\gamma_g \circ \gamma_h(x) = \gamma_g(hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = \gamma_{gh}(x).$$

Therefore this function is a homomorphism. Notice that for all $g, h \in G$ we have

$$\gamma_g(h) = ghg^{-1} = h = \mathrm{id}(h) \iff gh = hg,$$

and it is easy to see that the homomorphism is trivial if and only if the group is abelian. □

4.9. ▷ Prove that if m, n are positive integers such that $\gcd(m, n) = 1$, then $C_{mn} \cong C_m \times C_n$. [§4.3, 4.10, §IV.6.1, V.6.8]

Solution. As remarked in the text, we have a homomorphism $\pi_m^{mn} \times \pi_n^{mn}$ going from C_{mn} to $C_m \times C_n$. We will verify this homomorphism is injective, and since we have $|C_{mn}| = |C_m \times C_n|$ this will be enough to show it is in fact an isomorphism.

So, suppose we have $[a]_{mn}$ and $[b]_{mn}$ in C_{mn} such that they have the same image under $\pi_m^{mn} \times \pi_n^{mn}$. This means that $([a]_m, [a]_n) = ([b]_m, [b]_n)$, from which it follows that $m \mid b-a$ and $n \mid b-a$. Now, *as m and n are coprime* we can deduce $mn \mid b-a$ and so $[a]_{mn} = [b]_{mn}$, showing the function is injective. □

4.10. ▷ Let $p \neq q$ be odd prime integers; show that $(\mathbb{Z}/pq\mathbb{Z})^*$ is not cyclic. (Hint: Use Exercise 4.9 to compute the order N of $(\mathbb{Z}/pq\mathbb{Z})^*$, and show that no element can have order N.) [§4.3]

Solution. By Exercise 4.9, we have that $\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ via the isomorphism $\pi_p^{pq} \times \pi_q^{pq}$. We claim that is isomorphism restricts to a bijection (not necessarily a homomorphism) $(\mathbb{Z}/pq\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$.

Firstly we need to check that if $[a]_{pq} \in (\mathbb{Z}/pq\mathbb{Z})^*$ then its image under $\pi_p^{pq} \times \pi_q^{pq}$ is in $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$. This is just saying that if $\gcd(a, pq) = 1$ then $\gcd(a, p) = 1$ and $\gcd(a, q) = 1$; but this is evident (if an integer divided a and p then it would divide $pq \ldots$).

Secondly, we will show that the restriction is in fact a bijection. It is clearly an injection since $\pi_p^{pq} \times \pi_q^{pq}$ was injective before the restriction, so we will only show that it is a surjection $(\mathbb{Z}/pq\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$. Let $([x]_p, [y]_q) \in (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$. Again, as $\pi_p^{pq} \times \pi_q^{pq}$ is a surjection $\mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, there is some $[a]_{pq}$ such that $[a]_p = [x]_p$ and $[a]_q = [y]_q$; so we need to check $[a]_{pq} \in (\mathbb{Z}/pq\mathbb{Z})^*$. As $\gcd(x, p) = 1$ and $\gcd(y, q) = 1$ it follows that $\gcd(a, p) = 1$ and $\gcd(a, q) = 1$; see Exercise 2.17. Thus it follows that $\gcd(a, pq) = 1$ (see the proof of Proposition 2.6) as desired.

All of this shows that there is a bijection $(\mathbb{Z}/pq\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$. In particular,

$$|(\mathbb{Z}/pq\mathbb{Z})^*| = |(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*| = |(\mathbb{Z}/p\mathbb{Z})^*| \cdot |(\mathbb{Z}/q\mathbb{Z})^*| = (p-1)(q-1).$$

Let $[x]_{pq} \in (\mathbb{Z}/pq\mathbb{Z})^*$. Notice that, by assumption, $\gcd(x, pq) = 1$, from which it follows that $p \nmid x$ and $q \nmid x$. Then, by Fermat's little theorem, $x^{p-1} \equiv 1 \mod p$, and so $x^{\frac{(p-1)(q-1)}{2}} \equiv 1 \mod p$, where we have used the crucial fact that $q-1$ is even. Similarly we can get $x^{\frac{(p-1)(q-1)}{2}} \equiv 1 \mod q$, using the fact that $p-1$ is even. We can see then, as p and q are primes, that

$$p \text{ and } q \text{ divide } x^{\frac{(p-1)(q-1)}{2}} - 1 \implies pq \text{ divides } x^{\frac{(p-1)(q-1)}{2}} - 1.$$

So, $x^{\frac{(p-1)(q-1)}{2}} \equiv 1 \mod pq$. This implies that

$$|[x]_{pq}| \leq \frac{(p-1)(q-1)}{2} < (p-1)(q-1).$$

In particular $|[x]_{pq}| \neq (p-1)(q-1)$ for all $[x]_{pq} \in (\mathbb{Z}/pq\mathbb{Z})^*$. By Exercise 4.3, $(\mathbb{Z}/pq\mathbb{Z})^*$ is not cyclic.

Note I failed to come up with a solution not involving Fermat's little theorem, which has not been covered thus far in the book, though it follows easily from the aforementioned—not yet proved—Lagrange's Theorem. It also follows from Wilson's Theorem, if I recall correctly, which is only a few exercises below. There is no circularity, but it does leave the question of what the author had in mind for a valid solution to this problem.

There is an, in my opinion, easier and more natural way to compute the order of $(\mathbb{Z}/pq\mathbb{Z})^*$. This is classic application of the Inclusion-Exclusion principle, though you do not need to know what that is to come up with the following.

We are trying to figure out how many of the integers $1, \dots pq-1$ are coprime to pq. This is a list of $pq-1$ numbers. The ones that are not coprime to pq are either divisible by p or q but not both (why?). These are clearly $p, 2p, \dots (q-1)p$ and $q, 2q, \dots (p-1)q$. In total there are $(q-1)+(p-1)$ of these numbers. Therefore the amount of integers $1, \dots pq-1$ that are coprime to pq is

$$(pq-1) - [(q-1)+(p-1)] = pq - p - q + 1 = (p-1)(q-1). \qquad \square$$

4.11. ▷ In due time we will prove the easy fact that if p is a prime integer, then the equation $x^d = 1$ can have at most d solutions in $\mathbb{Z}/p\mathbb{Z}$. Assume this fact, and prove that the multiplicative group $G = (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. (Hint: Let $g \in G$ be an element of maximal order; use Exercise 1.15 to show that $h^{|g|} = 1$ for all $h \in G$. Therefore....) [§4.3, 4.15, 4.16, §IV.6.3]

Solution. Let $g \in G$ be an element of maximal order; we will show that $|g| = p-1$ and so, by Exercise 4.3, we will be able to deduce that $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. Let $h \in G$ and notice that, by Exercise 1.15, $|h|$ divides $|g|$ and in particular $h^{|g|} = [1]_p$. But by our assumption, this can be true for at most $|g|$ elements h, and we have proven it is true for the $p-1$ elements of $(\mathbb{Z}/p\mathbb{Z})^*$; it follows that $p-1 \leq |g|$. But the order of any element is less than or equal to the order of the group, so $|g| \leq p-1$. The claim follows. $\square$

4.12. ¬

- Compute the order of $[9]_{31}$ in the group $(\mathbb{Z}/31\mathbb{Z})^*$.
- Does the equation $x^3 - 9 = 0$ have solutions in $(\mathbb{Z}/31\mathbb{Z})^*$? (Hint: Plugging in all 31 elements of $(\mathbb{Z}/31\mathbb{Z})^*$ is too laborious and will not teach you much. Instead, use the result of the first part: if c is a solution of the equation, what can you say about $|c|$?) [VII.5.15]

Solution.

- The order of $[9]_{31}$ in the group $(\mathbb{Z}/31\mathbb{Z})^*$ is 15.

- Suppose, for the sake of contradiction, that there is some integer c such that $c^3 - 9 \equiv 0 \mod 31$. This implies $c^3 \equiv 9 \mod 31$. By our previous result, we must have $|[c^3]_{31}| = 15$. On the other hand, using Proposition 1.13, we have

$$15 = |[c^3]_{31}| = |([c]_{31})^3| = \frac{|[c]_{31}|}{\gcd(3, |[c]_{31}|)}.$$

That is,

$$|[c]_{31}| = 15 \gcd(3, |[c]_{31}|).$$

Then the order of $[c]_3 1$ is divisible by 15, and hence it is divisible by 3, so we get that the order of $[c]_3 1$ is actually 45, which is absurd since the order of an element must not exceed the order of the group.

□

4.13. ¬ Prove that $\mathrm{Aut}_{\mathsf{Grp}}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$. [IV.5.14]

Solution. First of all, in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ write $x \coloneqq (1,0)$ and $y \coloneqq (0,1)$. Then it is clear that e, x, y, xy is a complete list of the elements of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and thus x and y generate this group. More abstractly, this group has two generators x and y subject to the rules

$$x^2 = e \quad y^2 = e \quad xy = yx;$$

it is easy to see that these ensure that any product of the generators is equal to either e, x, y or xy.

Furthermore, notice that a homomorphism φ from $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ to a group G is completely determined by the images of x and y under φ since we then would have $\varphi(e) = e$ and $\varphi(xy) = \varphi(x)\varphi(y)$. Conversely, we can try to define an homomorphism from $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ to G by sending $x \mapsto g$ and $y \mapsto g'$ and $e \mapsto e$ and $xy \mapsto gg'$ for some $g, g' \in G$. However, to prove that this is a homomorphism we would need to ensure that any product of generators is mapped to the product of the images of the generators. This is achieved when $g^2 = (g')^2 = e$ and $gg' = g'g$ (why?).

Therefore, to construct an automorphism of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ it suffices to map x, y to $(0,0), (1,0), (0,1)$, or $(1,1)$; notice that all these elements satisfy the identities discussed previously. As isomorphisms preserve order, we cannot map to $(0,0)$ since $|x| = |y| = 2$. And as isomorphisms are injective we cannot map x and y to the same image. This gives us 6 choices, and by our previous remarks these are all homomorphisms.

Now notice that x and y are sent to distinct non-identity elements, and it is easy to see that the product of two such elements is not the identity and is distinct from the first two. Thus xy is not sent to either the identity nor the images of x or y, and it follows that the assignment is injective. As we are mapping the group to itself, it also follows that the assignment is surjective. Thus all of these 6 maps are isomorphisms.

But there are 6 bijections from the set of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ to itself that preserve the identity (the permutations of the three non-identity elements); hence all of

these are our automorphisms. It is clear that the composition here correspond exactly with the operation in S_3, which has 6 elements. It follows that the group of automorphisms of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is isomorphic to S_3. □

4.14. ▷ Prove that the order of the group of automorphisms of a cyclic group C_n is the number of positive integers $r \leq n$ that are relatively prime to n. (This is called *Euler's ϕ-function*; cf. Exercise 6.14.) [§IV.1.4, IV.1.22, §IV.2.5]

Solution. Throughout we assume x is the generator of C_n with $|x| = n$. It is clear that any automorphism of C_n is determined by the image of x, and as automorphisms preserve order, the image of x must have order n. By Proposition 2.3. there are $\phi(n)$ elements of order n, so there are at most $\phi(n)$ automorphisms of C_n, by mapping x a class of positive integers relatively prime to n. We will prove that all of these are indeed automorphisms.

Let $y \in C_n$ be such that $|y| = n$; we need to prove that the assignment $x \mapsto y$ is indeed an automorphism. First of all, it does define a function by mapping $x^j \mapsto y^j$ since we can express any element of C_n as x^j for some j, and it is well defined since if $x^j = x^{j'}$ then $n \mid (j - j')$ and so $y^j = y^{j'}$. It is evidently a homomorphism, and it is surjective since y generates C_n, so it is injective. Then the assignment is an automorphism. □

4.15. ¬ Compute the group of automorphisms of $(\mathbb{Z}, +)$. Prove that if p is prime, then $\mathrm{Aut}_{\mathsf{Grp}}(C_p) \cong C_{p-1}$. (Use Exercise 4.11.) [IV.5.12]

Solution. Let φ be an automorphism of $(\mathbb{Z}, +)$. Then, as φ is surjective, there is some integer n such that $\varphi(n) = 1$. This implies $n\varphi(1) = 1$ and we see that $\varphi(1)$ divides 1. So, it follows that $\varphi(1) = \pm 1$. As $\varphi(n) = n\varphi(1)$ for all n we see that φ is determined by the value of $\varphi(1)$; hence there are at most two automorphisms of $(\mathbb{Z}, +)$. The assignment $1 \mapsto 1$ clearly corresponds to the identity, which is definitely an automorphism. The assignment $1 \mapsto -1$ extends to the function $n \mapsto -n$. This function is clearly bijective and it is a homomorphism because $-(n + m) = -n + (-m)$. Hence both assignments yield an automorphism, and these are all automorphisms. There is only group of order 2 so we have computed the group of automorphisms of $(\mathbb{Z}, +)$.

From Exercise 4.14, it follows that $|\mathrm{Aut}_{\mathsf{Grp}}(C_p)| = p-1$, where p is prime. Then, by Exercise 4.3, it suffices to find an automorphism of order $p - 1$.

Thinking of C_p as $\mathbb{Z}/p\mathbb{Z}$, we notice that, by Exercise 4.11, there is some $[n]_p \in (\mathbb{Z}/p\mathbb{Z})^*$ such that

$$n, n^2, \ldots, n^{p-1}$$

are all distinct modulo p and $n^{p-1} \equiv 1 \mod p$. Also, n generates $\mathbb{Z}/p\mathbb{Z}$ additively since p is prime. So, as we proved in the solution of Exercise 4.14, there is an automorphism of $\mathbb{Z}/p\mathbb{Z}$ mapping $1 \mapsto n$, call it ψ. Then it follows by an easy induction that composing ψ with itself k times maps 1 to n^k, and it is also clear

that ψ maps 1 to 1 if and only if it is the identity map. By our previous remarks it follows that $|\psi| = p - 1$ in $\mathrm{Aut}_{\mathsf{Grp}}(C_p)$. □

4.16. ¬ Prove *Wilson's theorem: an integer $p > 1$ is prime if and only if*

$$(p-1)! \equiv -1 \mod p.$$

(For one direction, use Exercises 1.8 and 4.11. For the other, assume d is a proper divisor of p, and note that d divides $(p-1)!$; therefore....) [IV.4.11]

Solution. For $p = 2$ then the claim is obvious, so assume $p > 2$.

First suppose p is prime. Let n be an integer such that $n^2 \equiv 1 \mod p$. This means that $p \mid (n^2 - 1)$ and so $p \mid (n+1)(n-1)$ so either $n \equiv 1 \mod p$ or $n \equiv -1 \mod p$ since p is prime. As -1 is not congruent to 1 when $p > 2$, we have that $[-1]_p$ is the only element of order 2 in $(\mathbb{Z}/p\mathbb{Z})^*$. Hence, by Exercise 1.11, it follows that $[(p-1)!]_p = [-1]_p$.

Conversely, suppose that $p > 1$ is an integer and that $(p-1)! \equiv -1 \mod p$. For the sake of contradiction, assume there is some integer d with $1 < d \leq p-1$ so that $d \mid p$. Then we see that $d \mid (p-1)!$. We also know that $p \mid (p-1)! + 1$, from which it follows that $d \mid (p-1)! + 1$. But if $d \mid (p-1)!$ and $d \mid (p-1)! + 1$ then d divides $(p-1)! + 1 - (p-1)! = 1$, which is absurd. Therefore p is prime. □

4.17. For a few small (but not too small) primes p, find a generator of $(\mathbb{Z}/p\mathbb{Z})^*$.

Solution. For $p = 2, 3, 5, 11$, we have that $[2]_p$ is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. Also $[3]_7$ is a generator of $(\mathbb{Z}/7\mathbb{Z})^*$. □

4.18. Prove the second part of Proposition 4.8.

Solution. Suppose $\varphi\colon G \to H$ is an isomorphism of groups. Let G be abelian. Let $h, h' \in H$ and, since φ is surjective, there are some g and g' such that $\varphi(g) = h$ and $\varphi(g') = h'$. Then,

$$hh' = \varphi(g)\varphi(g') = \varphi(gg') = \varphi(g'g) = \varphi(g')\varphi(g) = h'h.$$

This proves H is abelian. Conversely, now suppose H is abelian. Then φ^{-1} is an isomorphism $H \to G$ and the same argument proves G is abelian. □

5 Free groups

Exercises

5.1. Does the category $\mathscr{F}^A$ defined in §5.2 have final objects? If so, what are they?

Solution. Yes, trivial groups are final in $\mathscr{F}^A$. Let $j\colon A \to \{e\}$ be the set-function defined by $j(a) \coloneqq e$ for all $a \in A$. Let G be a group and let $f\colon A \to G$ be a set-function. Then there clearly exists a unique group homomorphism $\sigma\colon G \to \{e\}$, and it is evident that $j = \sigma \circ f$. □

5.2. Since trivial groups T are initial in Grp, one may be led to think that (e, T) should be initial in $\mathscr{F}^A$, for every A, e would be defined by sending every element of A to the (only) element in T; and for any other group G, *there is a unique* homomorphism $T \to G$. Explain why (e, T) is *not* initial in $\mathscr{F}^A$ (unless $A = \emptyset$).

Solution. If $A \neq \emptyset$ then let $a \in A$. For any nontrivial group G let $f\colon A \to G$ be a function such that $f(a)$ is not the identity. Then the $f(a)$ is not the same as the image of the homomorphism $T \to G$ composed with e, showing that the relevant diagram is not commutative. □

5.3. ▷ Use the universal property of free groups to prove that the map $j\colon A \to F(A)$ is injective, for all sets A. (Hint: It suffices to show that for every two elements a, b of A there is a group G and a set-function $f\colon A \to G$ such that $f(a) \neq f(b)$. Why? How do you construct f and G?) [§III.6.3]

Solution. Let $G = \{e, g\}$ be a group of order 2 (which is unique up to isomorphism). Let $a, b \in A$ be distinct and let $f\colon A \to G$ be the function defined by

$$f(x) \coloneqq \begin{cases} e & \text{if } x = a \\ g & \text{otherwise.} \end{cases}$$

Then, by the universal property of free groups, there is a unique homomorphism $\sigma\colon F(A) \to G$ such that $\sigma \circ j = f$. As $f(a) \neq f(b)$ we have that $\sigma(j(a)) \neq \sigma(j(b))$ which implies $j(a) \neq j(b)$. As $a, b \in A$ were arbitrary distinct elements, j is injective. □

5.4. In the 'concrete' construction of free groups, one can try to reduce words by performing cancellations in any order; the process of 'elementary reductions' used in the text (that is, from left to right) is only one possibility. Prove that the result of iterating cancellations on a word is independent of the order in which the cancellations are performed. Deduce the associativity of the product in $F(A)$ from this. [§5.3]

Solution. First we fix some notation. For $w, w' \in W(A)$ write $w \to_r w'$ iff w' can be obtained from w by deleting exactly one instance of a pair aa^{-1} or $a^{-1}a$ for some $a \in A$ (not necessarily the leftmost one). So, for example, $w \to_r r(w)$ for any *non-reduced* $w \in W(A)$, but we also have other examples such as

$$a^{-1}a^{-1}aa\underline{aa^{-1}}aa^{-1} \to_r a^{-1}a^{-1}aaaa^{-1},$$

where we "cancel" not from left to right but starting in the middle. Note that $w \to_r w$ is *not* true for any $w \in W(A)$ since we are requiring that at least one

(and at most one) cancellation is performed. Similarly, if w is a reduced word, then $w \to_r v$ is false for all words $v \in W(A)$.

We introduce another piece of notation. For $w, w' \in W(A)$ we write $w \twoheadrightarrow_r w'$ if, for some integer $n \geq 0$ there exists some $w_0, \ldots, w_n \in W(A)$ such that $w = w_0$ and $w' = w_n$ and $w_i \to_r w_{i+1}$ for all $0 \leq i < n$. We usually write this as follows,

$$w = w_0 \to_r w_1 \to_r \cdots \to_r w_n = w'.$$

As we allow for $n = 0$ in this definition, we see that $w \twoheadrightarrow_r w$ for all $w \in W(A)$. Also, $\twoheadrightarrow_r$ is clearly a transitive relation. Now we prove some results.

Claim 1. *Let $w, v, v' \in W(A)$ be such that $w \to_r v$ and $w \to_r v'$. Then either $v = v'$ or there exists some $u \in W(A)$ such that $v \to_r u$ and $v' \to_r u$.*

Proof of Claim 1. Let $w = a_1 a_2 \cdots a_n$ where each a_i is either in A or in A'. Unravelling the definitions, we see that v is the word obtained by deleting from w some pair $a_i a_{i+1}$ where there is some $a \in A$ such that either $a_i = a$ and $a_{i+1} = a^{-1}$ or $a_i = a^{-1}$ and $a_{i+1} = a$. Similarly, there is some j such that v' is the word obtained from w by deleting $a_j a_{j+1}$. Without loss of generality, we can assume $i \leq j$. There are several cases.

- We have $i = j$. In this case, both v and v' are obtained from w by deleting the same letters and so $v = v'$.

- We have that i and j are consecutive integers, i.e. $j = i + 1$. Then, we have the following.

$$w = a_1 \cdots a_i a_{i+1} a_{j+1} \cdots a_n$$

If $a_{i+1} = a_j = a \in A$ then, by our assumptions, $a_i = a_{j+1} = a^{-1}$ and whether we delete $a_i a_{i+1}$ or $a_j a_{j+1}$ the resulting word is the same, so $v = v'$. Similarly, if $a_{i+1} = a_j = a^{-1}$ for some $a \in A$ then it follows that $a_i = a_{j+1} = a$ and it is readily seen that $v = v'$.

- We have that i and j are neither equal nor consecutive. Then w looks as follows.

$$w = a_1 \cdots a_i a_{i+1} \cdots a_j a_{j+1} \cdots a_n$$

Let u be the word obtained by deleting both $a_i a_{i+1}$ and $a_j a_{j+1}$ from w. Then it is clear that $v \to_r u$ and $v' \to_r u$. □

Claim 2. *Let $w, v, v' \in W(A)$ be such that $w \to_r v$ and $w \twoheadrightarrow_r v'$. Then there exists some $u \in W(A)$ such that $v \twoheadrightarrow_r u$ and $v' \twoheadrightarrow_r u$.*

Proof of Claim 2. We will use induction on a slightly stronger statement. Let $w, v \in W(A)$ be fixed words such that $w \to_r v$. For integers $n \geq 0$, let $P(n)$ be the following statement.

For all $v' \in W(A)$, if there exists $w_0, \ldots, w_n \in W(A)$, such that $w = w_0$ and $v' = w_n$ and $w_i \to_r w_{i+1}$ for all i, then there is some $u \in W(A)$ such that $v \twoheadrightarrow_r u$ and either $v' = u$ or $v' \to_r u$.

We will prove that $P(n)$ is true for all n using induction. For $n = 0$ we see that $w = v'$ and so, if we let $u \coloneqq v$, then $v \twoheadrightarrow_r u$ as $v = u$, and $v' = w \to_r v = u$ by assumption. Therefore the base case, $P(0)$, is true.

Now assume inductively that $P(k)$ is true for some $k \geq 0$; we will show that $P(k+1)$ is true. So, let $v' \in W(A)$ be such that there are some $w_0, \dots w_{k+1} \in W(A)$ such that

$$w = w_0 \to_r \cdots \to_r w_k \to_r w_{k+1} = v'.$$

By the inductive hypothesis, there is some $u_0 \in W(A)$ such that $v \twoheadrightarrow_r u_0$ and either $w_k = u_0$ or $w_k \to_r u_0$.

If $u_0 = w_k$ then we have $v \twoheadrightarrow_r w_k$ and then $v \twoheadrightarrow_r w_{k+1} = v'$. Then setting $u \coloneqq v'$ we have $v \twoheadrightarrow_r u$ and $v' = u$, as desired.

On the other hand, suppose $w_k \to_r u_0$, and notice we also had $w_k \to_r v'$. By Claim 1, either $u_0 = v'$ or there exists some $u \in W(A)$ such that $u_0 \to_r u$ and $v' \to_r u$. If $u_0 = v'$ then it suffices to set $u \coloneqq u_0$ since then $v \twoheadrightarrow_r u$ by assumption and $u = v'$. If we instead had a word u such that $u_0 \to_r u$ and $v' \to_r u$ then we only need to verify that $v \twoheadrightarrow_r u$, but this is obvious now since $v \twoheadrightarrow_r u_0$. This closes the induction and $P(n)$ is true for all $n \geq 0$.

Now let $v' \in W(A)$ be a word such that $v' \twoheadrightarrow_r w$. Using the definition of $\twoheadrightarrow_r$ and the fact that $P(n)$ is always true, we can deduce that there is some $u \in W(A)$ such that $v \twoheadrightarrow_r u$ and either $v' = u$ or $v' \to_r u$. But both $v' = u$ and $v' \to_r u$ imply that $v' \twoheadrightarrow_r u$, so the claim follows. □

Claim 3. *Let $w, v, v' \in W(A)$ be such that $w \twoheadrightarrow_r v$ and $w \twoheadrightarrow_r v'$. Then there exists some $u \in W(A)$ such that $v \twoheadrightarrow_r u$ and $v' \twoheadrightarrow_r u$.*

Proof of Claim 3. For $n, m \geq 0$, let $w_0, \dots, w_n \in W(A)$ and $w'_0, \dots, w'_m$ be such that

$$w = w_0 \to_r \cdots \to_r w_n = v.$$
$$w = w'_0 \to_r \cdots \to_r w'_m = v';$$

these exist since $w \twoheadrightarrow_r v$ and $w \twoheadrightarrow_r v'$. We will prove the claim using induction on n. For $n = 0$ we see that $w = v$ and setting $u \coloneqq v'$ makes the statement evident.

Now suppose $n > 0$ and assume inductively that there exists some $u_0 \in W(A)$ such that $w_{n-1} \twoheadrightarrow_r u_0$ and $v' \twoheadrightarrow_r u_0$. Then, as $w_{n-1} \to_r v$, we can apply Claim 2 to deduce that there is a word $u \in W(A)$ such that $u_0 \twoheadrightarrow_r u$ and $v \twoheadrightarrow_r u$. We only need to check that $v' \twoheadrightarrow_r u$, but this is evident since $v' \twoheadrightarrow_r u_0$. This closes the induction. □

Claim 4. *Let $w, v, v' \in W(A)$ be such that $w \twoheadrightarrow_r v$ and $w \twoheadrightarrow_r v'$ and both v and v' are reduced words. Then $v = v'$.*

Proof of Claim 4. Indeed, by Claim 3 there is some $u \in W(A)$ such that $v \twoheadrightarrow_r u$ and $v' \twoheadrightarrow_r u$. As v and v' are reduced, it must be the case that $v = u$ and $v' = u$, and the claim follows. □

With Claim 4 at hand, proving associativity is not difficult. We have to show that, for $u, v, w \in F(A)$ we have

$$u \cdot (v \cdot w) = (u \cdot v) \cdot w.$$

By definition, this is equivalent to proving that

$$R(uR(vw)) = R(R(uv)w).$$

So, it is clear that $vw \twoheadrightarrow_r R(vw)$, from which we can see $uvw \twoheadrightarrow_r uR(vw) \twoheadrightarrow_r R(uR(vw))$, which is reduced. Similarly, we have that $uv \twoheadrightarrow_r R(uv)$ and so $uvw \twoheadrightarrow_r R(uv)w \twoheadrightarrow_r R(R(uv)w)$, which is reduced. By Claim 4, the above equality is true. □

5.5. Verify explicitly that $H^{\oplus A}$ is a group.

Solution. content... □

5.6. ▷ Prove that the group $F(\{x, y\})$ (visualized in Example 5.3) is a coproduct $\mathbb{Z} * \mathbb{Z}$ of $\mathbb{Z}$ by itself in the category Grp. (Hint: With due care, the universal property for one turns into the universal property for the other.) [§3.4, 3.7, 5.7]

Solution. content... □

5.7. ▷ Extend the result of Exercise 5.6 to free groups $F(\{x_1, \ldots, x_n\})$ and to free abelian groups $F^{ab}(\{x_1, \ldots, x_n\})$. [§3.4, §5.4]

Solution. content... □

5.8. Still more generally, prove that $F(A \amalg B) = F(A) * F(B)$ and that $F^{ab}(A \amalg B) = F^{ab}(A) \oplus F^{ab}(B)$ for all sets A, B. (That is, the constructions F, F^{ab} 'preserve coproducts'.)

Solution. content... □

5.9. Let $G = \mathbb{Z}^{\oplus \mathbb{N}}$. Prove that $G \times G \cong G$.

Solution. content... □

5.10. ¬ Let $F = F^{ab}(A)$.

- Define an equivalence relation $\sim$ on F by setting $f' \sim f$ if and only if $f - f' = 2g$ for some $g \in F$. Prove that $F/\!\sim$ is a finite set if and only if A is finite, and in that case $|F/\!\sim = 2^{|A|}$.
- Assume $F^{ab}(B) \cong F^{ab}(A)$. If A is finite, prove that B is also, and that $A \cong B$ as sets. (This results holds for free groups as well, and without any finiteness hypothesis. See Exercises 7.13 and VI.1.20.)

[7.4, 7.13]

6 Subgroups

Exercises

6.1. ¬ (If you know about matrices.) The group of invertible $n \times n$ matrices with entries in $\mathbb{R}$ is denoted $\mathrm{GL}_n(\mathbb{R})$ (Example 1.5). Similarly, $\mathrm{GL}_n(\mathbb{C})$ denotes the group of $n \times n$ invertible matrices with *complex* entries. Consider the following sets of matrices:

- $\mathrm{SL}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) \mid \det(M) = 1\}$;
- $\mathrm{SL}_n(\mathbb{C}) = \{M \in \mathrm{GL}_n(\mathbb{C}) \mid \det(M) = 1\}$;
- $\mathrm{O}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) \mid MM^t = M^tM = I_n\}$;
- $\mathrm{SO}_n(\mathbb{R}) = \{M \in \mathrm{O}_n(\mathbb{R}) \mid \det(M) = 1\}$;
- $\mathrm{U}(n) = \{M \in \mathrm{GL}_n(\mathbb{C}) \mid MM^\dagger = M^\dagger M = I_n\}$;
- $\mathrm{SU}(n) = \{M \in \mathrm{U}(n) \mid \det(M) = 1\}$.

Here I_n stands for the $n \times n$ *identity matrix*, M^t is the *transpose* of M, $M^\dagger$ is the *conjugate transpose* of M, and $\det(M)$ denotes the *determinant* of M. Find all possible inclusions among these sets, and prove that in every case the smaller set is a subgroup of the larger one.

These sets of matrices have compelling geometric interpretations: for example, $\mathrm{SO}_3(\mathbb{R})$ is the group of 'rotations' in $\mathbb{R}^3$. [8.8, 9.1, III.1.4, VI.6.16]

Solution. content... □

6.2. ¬ Prove that the set of 2×2 matrices

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

with a, b, d in $\mathbb{C}$ and $ad \neq 0$ is a subgroup of $\mathrm{GL}_2(\mathbb{C})$. More generally, prove that the set of $n \times n$ complex matrices $(a_{ij})_{1 \leq i,j \leq n}$ with $a_{ij} = 0$ for $i > j$ and $a_{11}, \ldots, a_{nn} \neq 0$ is a subgroup of $\mathrm{GL}_n(\mathbb{C})$. (These matrices are called 'upper triangular', for evident reasons.) [IV.1.20]

Solution. content... □

6.3. ¬ Prove that every matrix in $\mathrm{SU}(2)$ may be written in the form

$$\begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}$$

where $a, b, c, d \in \mathbb{R}$ and $a^2 + b^2 + c^2 + d^2 = 1$. (Thus $\mathrm{SU}(2)$ may be realized as a three-dimensional sphere embedded in $\mathbb{R}^4$; in particular, it is *simply connected*.) [8.9, III.2.5]

Solution. content... □

6.4. ▷ Let G be a group, and let $g \in G$. Verify that the image of the exponential map $\epsilon_g \colon \mathbb{Z} \to G$ is a cyclic group (in the sense of Definition 4.7). [§6.3, §7.5]

Solution. content... □

6.5. Let G be a *commutative* group, and let $n > 0$ be an integer. Prove that $\{g^n \mid g \in G\}$ is a subgroup of G. Prove that this is not necessarily the case if G is not commutative.

Solution. content... □

6.6. Prove that the union of a family of subgroups of a group G is not necessarily a subgroup of G. In fact:

- Let H, H' be subgroups of a group G. Prove that $H \cup H'$ is a subgroup of G only if $H \subseteq H'$ or $H' \subseteq H$.
- On the other hand, let $H_0 \subseteq H_1 \subseteq H_2 \subseteq \dots$ be subgroups of a group G. Prove that $\bigcup_{i \geq 0} H_i$ *is* a subgroup of G.

Solution. content... □

6.7. ¬ Show that *inner* automorphisms (cf. Exercise 4.8) form a subgroup of $\mathrm{Aut}(G)$; this subgroup is denoted $\mathrm{Inn}(G)$. Prove that $\mathrm{Inn}(G)$ is cyclic if and only if $\mathrm{Inn}(G)$ is trivial if and only if G is abelian. (Hint: Assume that $\mathrm{Inn}(G)$ is cyclic; with notation as in Exercise 4.8, this means that there exists an element $a \in G$ such that $\forall g \in G \exists n \in \mathbb{Z} \gamma_g = \gamma_a^n$. In particular, $gag^{-1} = a^n aa^- n = a$. Thus a commutes with every g in G. Therefore....) Deduce that if $\mathrm{Aut}(G)$ is cyclic, then G is abelian. [7.10, IV.1.5]

Solution. content... □

6.8. Prove that an *abelian* group G is finitely generated if and only if there is a surjective homomorphism

$$\mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \twoheadrightarrow G$$

for some n.

Solution. content... □

6.9. Prove that every finitely generated subgroup of $\mathbb{Q}$ is cyclic. Prove that $\mathbb{Q}$ is not finitely generated.

Solution. content... □

6.10. ¬ The set of 2×2 matrices with integer entries and determinant 1 is denoted $\mathrm{SL}_2(\mathbb{Z})$:

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ such that } a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}.$$

Prove that $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices

$$s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

(Hint: This is a little tricky. Let H be the subgroup generated by s and t. Given a matrix $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{SL}_2(\mathbb{Z})$, it suffices to show that you can obtain the identity by multiplying m by suitably chosen elements of H. Prove that $\begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix}$ are in H, and note that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b - qa \\ c & d - qc \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix} = \begin{pmatrix} a - qb & b \\ c - qd & d \end{pmatrix}$$

Note that if c and d are both nonzero, one of these two operations may be used to decrease the absolute value of one of them. Argue that suitable applications of these operations reduce to the case in which $c = 0$ or $d = 0$. Prove directly that $m \in H$ in that case.) [7.5]

Solution. content... □

6.11. Since direct sums are coproducts in Ab, the classification theorem for abelian groups mentioned in the text says that every finitely generated *abelian group* is a coproduct of cyclic groups in Ab. The reader may be tempted to conjecture that every finitely generated *group* is a coproduct in *in* Grp. Show that this is not the case, by proving that S_3 is not a coproduct of cyclic groups.

Solution. content... □

6.12. Let m, n be positive integers, and consider the subgroup $\langle m, n \rangle$ of $\mathbb{Z}$ they generate. By Proposition 6.9,

$$\langle m, n \rangle = d\mathbb{Z}$$

for some positive integer d. What is d, in relation to m, n?

Solution. content... □

6.13. ¬ Draw and compare the lattices of subgroups of $C_2 \times C_2$ and C_4. Draw the lattice of subgroups of S_3, and compare it with the one for C_6. [7.1]

Solution. content... □

6.14. ▷ If m is a positive integer, denote by $\phi(m)$ the number of positive integers $r \leq m$ that are *relatively prime* to m (that is, for which the gcd of r and m is 1); this is called *Euler's ϕ- (or 'totient') function.* For example, $\phi(12) = 4$. In other words, $\phi(m)$ is the order of the group $(\mathbb{Z}/m\mathbb{Z})^*$; cf. Proposition 2.6.

Put together the following observations:

- $\phi(m)$ = the number of generators of C_m,
- every element of C_n generates a subgroup of C_n,
- The discussion following Proposition 6.11 (in particular, every subgroup of C_n is isomorphic to C_m, for some $m \mid n$),

to obtain a proof of the formula

$$\sum_{m>0, m|n} \phi(m) = n.$$

(For example, $\phi(1)+\phi(2)+\phi(3)+\phi(4)+\phi(6)+\phi(12) = 1+1+2+2+2+4 = 12$.) [4.14, §6.4, 8.15, V.6.8, §VII.5.2]

Solution. content... □

6.15. ▷ Prove that if a group homomorphism $\varphi\colon G \to G'$ has a left-inverse, that is, a group homomorphism $\psi\colon G' \to G$ such that $\psi\circ\varphi = \mathrm{id}_G$, then φ is a monomorphism. [§6.5, 6.16]

Solution. content... □

6.16. ▷ Counterpoint to Exercise 6.15: the homomorphism $\varphi\colon \mathbb{Z}/3\mathbb{Z} \to S_3$ given by

$$\varphi([0]) = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \quad \varphi([1]) = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \quad \varphi([2]) = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

is a monomorphism; show that it has *no* left-inverse in Grp. (Knowing about *normal* subgroups will make this problem particularly easy.) [§6.5]

Solution. content... □

7 Quotient groups

Exercises

7.1. ▷ List all subgroups of S_3 (cf. Exercise 6.13) and determine which subgroups are normal and which are not normal. [§7.1]

Solution. content... □

7.2. Is the *image* of a group homomorphism necessarily a *normal* subgroup of the target?

Solution. content... □

7.3. ▷ Verify that the equivalent conditions for normality given in §7.1 are indeed equivalent.

Solution. content... □

7.4. Prove that the relation defined in Exercise 5.10 on a free abelian group $F = F^{ab}(A)$ is compatible with the group structure. Determine the quotient $F/\sim$ as a better known group.

Solution. content... □

7.5. ¬ Define an equivalence relation $\sim$ on $\mathrm{SL}_2(\mathbb{Z})$ by letting $A \sim A' \iff A' = \pm A$. Prove that $\sim$ is compatible with the group structure. The quotient $\mathrm{SL}_2(\mathbb{Z})/\sim$ is denoted $\mathrm{PSL}_2(\mathbb{Z})$ and is called the *modular group*; it would be a serious contender in a contest for 'the most important group in mathematics', due to its role in algebraic geometry and number theory. Prove that $\mathrm{PSL}_2(\mathbb{Z})$ is generated by the (cosets of the) matrices

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

(You will not need to work very hard, if you use the result of Exercise 6.10.) Note that the first has order 2 in $\mathrm{PSL}_2(\mathbb{Z})$, the second one has order 3, and their product has infinite order. [9.14]

Solution. content... □

7.6. Let G be a group, and let n be a positive integer. Consider the relation

$$a \sim b \iff (\exists g \in G) ab^{-1} = g^n.$$

- Show that in general $\sim$ is *not* an equivalence relation.
- Prove that $\sim$ is an equivalence relation if G is commutative, and determine the corresponding subgroup of G.

Solution. content... □

7.7. Let G be a group, n a positive integer, and let $H \subseteq G$ be the subgroup generated by all elements of order n in G. Prove that H is normal.

Solution. content... □

7.8. ▷ Prove Proposition 7.6. [§7.3]

Solution. content... □

7.9. State and prove 'mirror' statements of Proposition 7.4 and 7.6, leading to the description of relations satisfying (††).

Solution. content... □

7.10. ¬ Let G be a group, and $H \subseteq G$ a subgroup. With notation as in Exercise 6.7, show that H is normal in G if and only if $\forall \gamma \in \mathrm{Inn}(G)$, $\gamma(H) \subseteq H$.

Conclude that if H is normal in G, then there is an interesting homomorphism $\mathrm{Inn}(G) \to \mathrm{Aut}(H)$. [8.25]

Solution. content... □

7.11. ▷ Let G be a group, and let $[G, G]$ be the subgroup of G generated by all elements of the form $aba^{-1}b^{-1}$. (This is the *commutator* subgroup of G; we will return to it in §IV.3.3.) Prove that $[G, G]$ is normal in G. (Hint: With notation as in Exercise 4.8, $g \cdot aba^{-1}b^{-1} = \gamma_g(aba^{-1}b^{-1})$.) Prove that $G/[G, G]$ is commutative. [7.12, §IV.3.3]

Solution. content... □

7.12. ▷ Let $F = F(A)$ be a free group, and let $f\colon A \to G$ be a set-function from the set A to a *commutative* group G. Prove that f induces a unique homomorphism $F/[F, F] \to G$, where $[F, F]$ is the commutator subgroup of F defined in Exercise 7.11. (Use Theorem 7.12.) Conclude that $F/[F, F] \cong F^{ab}(A)$. (Use Proposition I.5.4.) [§6.4, 7.13, VI.1.20]

Solution. content... □

7.13. ¬ Let A, B be sets and $F(A)$, $F(B)$ the corresponding free groups. Assume $F(A) \cong F(B)$. If A is finite, prove that B is also and $A \cong B$. (Use Exercise 7.12 to upgrade Exercise 5.10.) [5.10, VI.1.20]

Solution. content... □

7.14. Let G be a group. Prove that $\mathrm{Inn}(G)$ is a *normal* subgroup of $\mathrm{Aut}(G)$.

Solution. content... □

8 Canonical decomposition and Lagrange's theorem

Exercises

8.1. If a group H may be realized as a subgroup of two groups G_1 and G_2 and if

$$\frac{G_1}{H} \cong \frac{G_2}{H},$$

does it follow that $G_1 \cong G_2$? Give a proof or a counterexample.

Solution. content... □

8.2. ¬ Extend Example 8.6 as follows. Suppose G is a group and $H \subseteq G$ is a subgroup of *index* 2, that is, such that there are precisely two (say, left-) cosets of H in G. Prove that H is normal in G. [9.11, IV.1.16]

Solution. content... □

8.3. Prove that every finite group is finitely presented.

Solution. content... □

8.4. Prove that $(a, b|a^2, b^2, (ab)^n)$ is a presentation of the dihedral group D_{2n}. (Hint: With respect to the generators defined in Exercise 2.5, set $a = x$ and $b = xy$; prove you can get the relations given here from the ones you obtained in Exercise 2.5, and conversely.)

Solution. content... □

8.5. Let a, b be distinct elements of order 2 in a group G, and assume that ab has finite order $n \geq 3$. Prove that the subgroup generated by a and b in G is isomorphic to the dihedral group D_{2n}. (Use the previous exercise.)

Solution. content... □

8.6. ¬ Let G be a group, and let A be a set of generators for G; assume A is finite. The corresponding *Cayley graph* is a directed graph whose set of vertices is in one-to-one correspondence with G, and two vertices g_1, g_2 are connected by an edge if $g_2 = g_1 a$ for an $a \in A$; this edge may be labeled a an oriented from g_1 to g_2. For example, the graph drawn in Example 5.3 for the free group $F(\{x, y\})$ on two generators x, y is the corresponding Cayley graph (with the convention that horizontal edges are labeled x and point to the right and vertical edges are labeled y and point up).

Prove that if a Cayley graph of a group is a tree, then the group is free. Conversely, prove that free groups admit Cayley graphs that are trees. [§5.3, 9.15]

Solution. content... □

8.7. ▷ Let $(A|\mathscr{R})$, resp., $(A'|\mathscr{R}')$ be a presentation for a group G, resp., G' (cf. §8.2); we may assume that A, A' are disjoint. Prove that the group $G * G'$ presented by

$$(A \cup A'|\mathscr{R} \cup \mathscr{R}')$$

satisfies the universal property for the *coproduct* of G and G' in Grp. (Use the universal properties of both free groups and quotients to construct natural homomorphisms $G \to G * G'$, $G' \to G * G'$.) [§3.4, §8.2, 9.14]

Solution. content... □

8.8. ¬ (If you know about matrices (cf. Exercise 6.1).) Prove that $\mathrm{SL}_n(\mathbb{R})$ is a *normal subgroup* of $\mathrm{GL}_n(\mathbb{R})$, and 'compute' $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R})$ as a well-known group. [VI.3.3]

Solution. content... □

8.9. ¬ (Ditto.) Prove that $\mathrm{SO}_n(\mathbb{R}) \cong \mathrm{SU}(2)/\pm I_2$, where I_2 is the identity matrix. (Hint: It so happens that every matrix in $\mathrm{SO}_3(\mathbb{R})$ can be written in the form

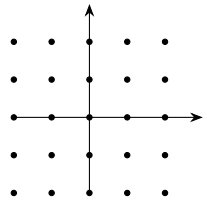
$$\begin{pmatrix} a^2+b^2-c^2-d^2 & 2(bc-ad) & 2(ac+bd) \\ 2(ad+bc) & a^2-b^2+c^2-d^2 & 2(cd-ab) \\ 2(bd-ac) & 2(ab+cd) & a^2-b^2-c^2+d^2 \end{pmatrix}$$

where $a, b, c, d \in \mathbb{R}$ and $a^2+b^2+c^2+d^2 = 1$. Proving this fact is not hard, but at this stage you will probably find it computationally demanding. Feel free to assume this, and use Exercise 6.3 to construct a surjective homomorphism $\mathrm{SU}(2) \to \mathrm{SO}_3(\mathbb{R})$; compute the kernel of this homomorphism.)

If you know a little topology, you can now conclude that the fundamental group of $\mathrm{SO}_3(\mathbb{R})$ is C_2. [9.1, VI.1.3]

Solution. content... □

8.10. View $\mathbb{Z} \times \mathbb{Z}$ as a subgroup of $\mathbb{R} \times \mathbb{R}$:



Describe the quotient

$$\frac{\mathbb{R} \times \mathbb{R}}{\mathbb{Z} \times \mathbb{Z}}$$

in terms analogous to those used in Example 8.7. (Can you 'draw a picture' of this group? Cf. Exercise I.1.6.)

Solution. content... □

8.11. (Notation as in Proposition 8.10.) Prove 'by hand' (that is, without invoking universal properties) that N is normal in G if and only if N/H is normal in G/H.

Solution. content... □

8.12. (Notation as in Proposition 8.11.) Prove 'by hand' (that is, without invoking universal properties) that HK is a subgroup of G if H is normal.

Solution. content... □

8.13. ¬ Let G be a finite group, and assume $|G|$ is odd. Prove that every element of G is a square. [8.14]

Solution. content... □

8.14. Generalize the result of Exercise 8.13: if G is a group of order n and k is an integer relatively prime to n, then the function $G \to G$, $g \mapsto g^k$ is surjective.

Solution. content... □

8.15. Let a, n be positive integers, with $a > 1$. Prove that n divides $\phi(a^n - 1)$, where ϕ is Euler's ϕ-function; see Exercise 6.14. (Hint: Example 8.15.)

Solution. content... □

8.16. Generalize Fermat's little theorem to congruence module arbitrary (that is, possibly nonprime) integers. Note that it is *not* true that $a^n \equiv a \mod n$ for all a and n: for example, 2^4 is not congruent to 2 modulo 4. *What* is true? (This generalization is known as *Euler's theorem*.)

Solution. content... □

8.17. ▷ Assume G is a finite abelian group, and let p be a prime divisor of $|G|$. Prove that there exists an element in G of order p. (Hint: Let $g \neq e$ be an element of G, and consider the subgroup $\langle g \rangle$; use the fact that this subgroup is cyclic to show that there is an element $h \in \langle g \rangle$ in G of *prime* order q. If $q = p$, you are done; otherwise, use the quotient $G/\langle h \rangle$ and induction.) [§8.5, 8.18, 8.20, IV.2.1]

Solution. content... □

8.18. Let G be an abelian group of order $2n$, where n is odd. Prove that G has *exactly one* element of order 2. (It has at least one, for example by Exercise 8.17. Use Lagrange's theorem to establish that it cannot have more than one.) Does the same conclusion hold if G is not necessarily commutative?

Solution. content... □

8.19. Let G be a finite group, and let d be a proper divisor of $|G|$. Is it necessarily true that there exists an element of G of order d? Give a proof or a counterexample.

Solution. content... □

8.20. ▷ Assume G is a finite abelian group, and let d be a divisor of $|G|$. Prove that there exists a *subgroup* $H \subseteq G$ of order d. (Hint: induction; use Exercise 8.17.) [§IV.2.2]

Solution. content... □

8.21. ▷ Let H, K be subgroups of a group G. Construct a bijection between the set of cosets hK with $h \in H$ and the set of left-cosets of $H \cap K$ in H. If H and K are finite, prove that

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Solution. content... □

8.22. ▷ Let $\varphi\colon G \to G'$ be a group homomorphism, and let N be the smallest normal subgroup containing $\operatorname{im}\varphi$. Prove that G'/N satisfies the universal property of $\operatorname{coker}\varphi$ in Grp. [§8.6]

Solution. content... □

8.23. ▷ Consider the subgroup

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

of S_3. Show that the cokernel of the inclusion $H \hookrightarrow S_3$ is trivial, although $H \hookrightarrow S_3$ is not surjective. [§8.6]

Solution. content... □

8.24. ▷ Show that epimorphisms in Grp do not necessarily have right-inverses. [§I.4.2]

Solution. content... □

8.25. Let H be a commutative normal subgroup of G. Construct an interesting homomorphism from G/H to $\operatorname{Aut}(H)$. (Cf. Exercise 7.10.)

Solution. content... □

9 Group actions

Exercises

9.1. (Once more, if you are already familiar with a little linear algebra....) The matrix groups listed in Exercise 6.1 all come with evident actions on a vector space: if M is an $n \times n$ matrix with (say) real entries, multiplication to the right by a column n-vector $\mathbf{v}$ returns a column n-vector $M\mathbf{v}$, and this defines a left-action on $\mathbb{R}^n$ viewed as the space of column n-vectors.

- Prove that, through this action, matrices $M \in \mathrm{O}_n(\mathbb{R})$ preserve lengths and angles in $\mathbb{R}$.

- Find an interesting action of $\mathrm{SU}(2)$ on $\mathbb{R}^3$. (Hint: Exercise 8.9.)

Solution. content... □

9.2. The effect of the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

on the plane is to respectively flip the plane about the y-axis and to rotate it $90°$ clockwise about the origin. With this in mind, construct an action of D_8 on $\mathbb{R}^2$.

Solution. content... □

9.3. If $G = (G, \cdot)$ is a group, we can define an 'opposite' group $G^\circ = (G, \bullet)$ supported on the same set G by prescribing

$$(\forall g, h, \in G): \quad g \bullet h \coloneqq h \cdot g.$$

- Verify that G° is indeed a group.
- Show that the 'identity' $G^\circ \to G$, $g \mapsto g$ is an isomorphism if and only if G is commutative.
- Show that $G^\circ \cong G$ (even if G is not commutative!)
- Show that giving a *right*-action of G on a set A is the same as giving a homomorphism $G^\circ \to S_A$, that is, a *left*-action of G° on A.
- Show that the notions of left- and right-actions coincide 'on the nose' for *commutative* groups. (That is, if $(g, a) \mapsto ag$ defines a right-action of a commutative group G on a set A, then setting $ga = ag$ defines a left-action).
- For any group G, explain how to turn a right-action of G into a left-action of G. (Note that the simple 'flip' $ga = ag$ does *not* work in general if G is not commutative.)

Solution. content... □

9.4. As mentioned in the text, *right*-multiplication defines a right-action of a group on itself. Find *another* natural right-action of a group on itself.

Solution. content... □

9.5. Prove that the action by left-multiplication of a group on itself is free.

Solution. content... □

9.6. Let O be an orbit of an action of a group G on a set. Prove that the induced action of G on O is transitive.

Solution. content... □

9.7. Prove that stabilizers are indeed subgroups.

Solution. content... □

9.8. For a group, verify that G-Set is indeed a category, and verify that the isomorphisms in G-Set are precisely equivariant bijections.

Solution. content... □

9.9. Prove that G-Set has products and coproducts and that every object of G-Set is a coproduct of objects of the type $G/H = \{\text{left-cosets of H}\}$, where H is a subgroup of G and G acts on G/H by left-multiplication.

Solution. content... □

9.10. Let H be an subgroup of a group G. Prove that there is a bijection between the set G/H of *left*-cosets of H and the set $H\backslash G$ of *right*-cosets of H in G. (Hint: G acts on the right on the set of right-cosets; use Exercise 9.3 and Proposition 9.9.)

Solution. content... □

9.11. ¬ Let G be a finite group, and let H be a subgroup of index p, where p is the *smallest prime dividing* $|G|$. Prove that H is normal in G, as follows:

- Interpret the action of G on G/H by left-multiplication as a homomorphism $\sigma\colon G \to S_p$.
- Then $G/\ker\sigma$ is (isomorphic to) a subgroup of S_p. What does this say about the index of $\ker\sigma$ in G?
- Show that $\ker\sigma \subseteq H$.
- Conclude that $H = \ker\sigma$, by index considerations.

Thus H is a kernel, proving that it is normal. (This exercise generalizes the result of Exercise 8.2.) [9.12]

Solution. content... □

9.12. ¬ Generalize the result of Exercise 9.11, as follows. Let G be a group, and let $H \subseteq G$ be a subgroup of index n. Prove that H contains a subgroup K that is normal in G and such that $[G : K]$ divides the gcd of G and $n!$. (In particular, $[G : K] \leq n!$.)

Solution. content... □

9.13. ▷ Prove 'by hand' that for all subgroups H of a group G and $\forall g \in G$, G/H and $G/(gHg^{-1})$ (endowed with the action of G by left-multiplication) are isomorphic in G-Set. [§9.3]

Solution. content... □

9.14. ¬ Prove that the modular group $\mathrm{PSL}_2(\mathbb{Z})$ is isomorphic to the coproduct $C_2 * C_3$. (Recall that the modular group $\mathrm{PSL}_2(\mathbb{Z})$ is generated by $x = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $y = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, satisfying the relations $x^2 = y^3 = e$ in $\mathrm{PSL}_2(\mathbb{Z})$ (Exercise 7.5). The task is to prove that x and y satisfy *no* other relation: this will show that $\mathrm{PSL}_2(\mathbb{Z})$ is presented by $(x, y \mid x^2, y^3)$, and we have agreed that this is a presentation for $C_2 * C_3$ (Exercise 3.8 or 8.7). Reduce this to verifying that no products

$$(y^{\pm 1}x)(y^{\pm 1}x)\cdots(y^{\pm 1}x) \quad \text{or} \quad (y^{\pm 1}x)(y^{\pm 1}x)\cdots(y^{\pm 1}x)y^{\pm 1}$$

with one or more factors can equal the identity. This latter verification is traditionally carried out by cleverly exploiting an action. Let the modular group act on the set of *irrational* real numbers by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(r) = \frac{ar+b}{cr+d}.$$

Check that this does define an action of $\mathrm{PSL}_2(\mathbb{Z})$, and note that

$$y(r) = 1 - \frac{1}{r}, \quad y^{-1}(r) = \frac{1}{1-r}, \quad yx(r) = 1 + r, \quad y^{-1}x(r) = \frac{r}{1+r}.$$

Now complete the verification with a case-by-case analysis. For example, a product $(y^{\pm 1}x)(y^{\pm 1}x)\cdots(y^{\pm 1}x)y^{\pm 1}$ cannot equal the identity in $\mathrm{PSL}_2(\mathbb{Z})$ because if it did, it would act as the identity on $\mathbb{R} \setminus \mathbb{Q}$, while if $r < 0$, then $y(r) > 0$, and both yx and $y^{-1}x$ send positive irrationals to positive irrationals.) [3.8]

Solution. content... □

9.15. ¬ Prove that every (finitely generated) group G acts freely on any corresponding Cayley graph. (Cf. Exercise 8.6. Actions on a directed graphs are defined as actions on the set of vertices preserving incidence: if the vertices v_1, v_2 are connected by an edge, then so must be gv_1, gv_2 for every $g \in G$.) In particular, conclude that every free group acts freely on a tree. [9.16]

Solution. content... □

9.16. ▷ The converse of the last statement in Exercise 9.15 is also true: only free groups can act freely on a tree. Assuming this, prove that every subgroup of a free group (on a finite set) is free. [§6.4]

Solution. content... □

9.17. ▷ Consider G as a G-set, by acting with left-multiplication. Prove that $\mathrm{Aut}_{G-\mathsf{Set}} \cong G$. [§2.1]

Solution. content... □

9.18. Show how to construct a *groupoid* carrying the information of the action of a group G on a set A. (Hint: A will be the set of objects of the groupoid. What will be the morphisms?)

Solution. content... □

10 Group objects in categories

Exercises

10.1. Define all the unnamed maps appearing in the diagrams in the definition of group object, and prove they are indeed isomorphisms when so indicated. (For the projection $1 \times G \to G$, what is left to prove is that the composition

$$1 \times G \to G \to 1 \times G$$

is the identity, as mentioned in the text.)

Solution. content... □

10.2. ▷ Show that *groups*, as defined in §1.2, are 'group objects in the category of sets'. [§10.1]

Solution. content... □

10.3. Let $(G, \cdot)$ be a group, and suppose $\circ\colon G \times G \to G$ is a group homomorphism (w.r.t. $\cdot$) such that $(G, \circ)$ is *also* a group. Prove that $\circ$ and $\cdot$ coincide. (Hint: First prove that the identity with respect to the two operations must be the same.)

Proof. content... □

10.4. Prove that every *abelian* group has exactly one structure of group object *in the category* Ab.

Solution. content... □

10.5. By the previous exercise, a group object in Ab is nothing other than an abelian group. What is a group object in Grp?

Solution. content... □

Bibliography

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