Solutions to Exercises from 'Algebra: Chapter 0'

Abstract. Solutions to exercises from the book 'Algebra: Chapter 0' by Paolo Aluffi.

Contents

Preface

This document contains my attempt at writing (hopefully correct!) solutions to exercises from Aluffi's book, while engaging in some self-study of modern abstract algebra with the ultimate aim of teaching myself some modern algebraic geometry.

CHAPTER 1

Preliminaries: Set theory and categories

1. Naive set theory

EXERCISE 1.1. Let $U = \{x \mid x \notin x\}$. Then, $U \notin U \iff U \in U$, a contradiction. This is Russell's paradox. Either we assume the *set of all sets* doesn't exist, or we need to give up the axiom of *unrestricted comprehension* in set theory.

EXERCISE 1.2. Suppose $\sim$ is an equivalence relation on a set S. For every element $a \in S$, define the *equivalence class* of a (with respect to $\sim$) by

$$[a]_\sim := \{b \in S \mid b \sim a\}.$$

Then, we note that due to *reflexivity*, the equivalence class $[a]_\sim$ of every element $a \in S$ contains a, and hence, is nonempty. Also, $[a]_\sim \subset S$, and therefore, $\bigcup_{a\in S}[a]_\sim = S$. Finally, we show the equivalence classes are mutually disjoint. Indeed, for any two elements $a, b \in S$, if $[a]_\sim$ and $[b]_\sim$ are disjoint, then there is nothing to prove. So, suppose $[a]_\sim \cap [b]_\sim$ is nonempty. Then, there exists some $c \in S$ that belongs to such an intersection. Thus, $c \sim a$ and $c \sim b$. By symmetry, $a \sim c$, and thus, by transitivity, $a \sim b$, which by symmetry again, implies $b \sim a$. Therefore, for all $x \in [a]_\sim$, we have $x \sim a$, and since $a \sim b$, by transitivity, $x \sim b$, which implies $x \in [b]_\sim$, from which we conclude $[a]_\sim \subset [b]_\sim$. We can similarly show $[b]_\sim \subset [a]_\sim$. Hence, $[a]_\sim = [b]_\sim$. This establishes equivalence classes are mutually disjoint. Hence, the set $\mathscr{P}_\sim$ of equivalence classes of S is indeed a partition of S.

EXERCISE 1.3. Suppose $\mathscr{P}$ is a partition on a set S. Define a relation $\sim$ on S as follows: For any two elements $a, b \in S$, $a \sim b$ iff a and b belong to the same set in the partition. Then, it is easy to check $\sim$ is indeed an equivalence relation on S. $\mathscr{P}$ is, therefore, the corresponding partition of the aforesaid equivalence relation, and we are done.

EXERCISE 1.4. Note the set of equivalence relations on a set S are in a one-to-one correspondence with the set of partitions of S. Thus, the number of different equivalence relations that may be defined on $S = \{1, 2, 3\}$ equals the number of partitions of S, and this number equals 5, since the partitions of S are

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

The above partitions are also written as $1|2|3, 12|3, 13|2, 23|1, 123$.

EXERCISE 1.5. An example of a relation R (defined on a set S) that is reflexive and symmetric but not transitive is the following:

$$R = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (2, 3), (3, 2)\}, \text{ where } S = \{1, 2, 3\}.$$

EXERCISE 1.6. Define a relation $\sim$ on the set $\mathbb{R}$ of real numbers by setting

$$a \sim b \iff b - a \in \mathbb{Z}.$$

We claim $\sim$ is an equivalence relation. To that end, note, for all $a \in \mathbb{R}$, we have $a \sim a$, since $a - a = 0 \in \mathbb{Z}$. Therefore, $\sim$ is reflexive. Also, if $a \sim b$, then $b - a \in \mathbb{Z}$, which implies $a - b \in \mathbb{Z}$, and thus, $b \sim a$. Therefore, $\sim$ is symmetric. Finally, suppose $a \sim b$ and $b \sim c$. Then, $b-a, c-b \in \mathbb{Z}$, and thus, $c-a = (c-b)+(b-a) \in \mathbb{Z}$. Thus, $\sim$ is transitive. Therefore, $\sim$ is an equivalence relation on $\mathbb{R}$.

(Description of $\sim$) Note all reals that have the same decimal expansion belong to the same equivalence class under $\sim$. Thus, $[0]_\sim = \mathbb{Z}$, and for any $0 < \alpha < 1, [\alpha]_\sim = \{n+\alpha \mid n \in \mathbb{Z}\}$. This takes care of all the reals, since each real can always be written as $n + \alpha$, for some $n \in \mathbb{Z}$ and $0 < \alpha < 1$. Therefore, a 'compelling' description for $\mathbb{R}/\sim$ is the unit interval $[0, 1]$, such that the endpoints, 0 and 1, are 'glued' together. In other words, it is a 'loop' or a 1-sphere.

Define a relation $\approx$ on the plane $\mathbb{R} \times \mathbb{R}$ as follows:

$$(a_1, a_2) \approx (b_1, b_2) \iff b_1 - a_1 \in \mathbb{Z} \text{ and } b_2 - a_2 \in \mathbb{Z}.$$

Then, just as above, it is easy to show $\approx$ defines an equivalence relation on $\mathbb{R} \times \mathbb{R}$. We note $[(0, 0)]_\sim = \{(m, n) \mid m, n \in \mathbb{Z}\}$, and for any $0 < \alpha, \beta < 1, [(\alpha, \beta)]_\sim = \{(m + \alpha, n + \beta) \mid m, n \in \mathbb{Z}\}$. Thus, a 'compelling' description of $\mathbb{R} \times \mathbb{R}/\approx$ is the unit square $[0, 1] \times [0, 1]$ with the four corners joined together, so that it forms a 2-sphere.

2. Functions between sets

Exercise 2.1. We claim the number of bijections from a set S with n elements to itself is $n!$. To begin with, any element in S can be mapped to any of the n possible elements in S. Then, the next element in S can be mapped to any of the remaining $n - 1$ elements in S, and so on, with the last element in S being mapped to the last remaining element in S. Thus, the number of bijections equals $n \cdot (n - 1) \cdot \ldots \cdot 1 = n!$, which proves our claim.

Exercise 2.2. Assume $A \neq \varnothing$, and let $f : A \to B$ be a function. We claim f has a right inverse iff it is surjective.

($\Longleftarrow$) Suppose f has a right inverse, $g : B \to A$, say. Then, $f \circ g = 1_B$. Thus, for all $b \in B$, $b = 1_B(b) = (f \circ g)(b) = f(g(b)) = f(a)$, where $g(b) = a \in A$. This shows f is surjective.

($\Longrightarrow$) Suppose f is surjective. Then, for any $b \in B$, the fiber of f over b is nonempty. Thus, $\{f^{-1}(b)\}_{b \in B}$ is a family of nonempty sets, and therefore, using the *axiom of choice*, we can construct a function $g : B \to A$ as follows: For all $b \in B$, $g(b) = a$ for some $a \in f^{-1}(b)$. Hence, for all $b \in B, (f \circ g)(b) = f(g(b)) = f(a) = b = 1_B(b)$, and so, $f \circ g = 1_B$. This establishes g is the right inverse of f, and we are done.

Exercise 2.3. Suppose $f : A \to B$ is a bijection. Then, f has an inverse $f^{-1} : B \to A$ such that $f^{-1} \circ f = 1_A$ and $f \circ f^{-1} = 1_B$. Clearly, f is an inverse of f^{-1}, showing f^{-1} is also a bijection.

Suppose $f : A \to B$ and $g : B \to C$ are bijections. We claim $g \circ f : A \to C$ is also a bijection. To that end, we show $f^{-1} \circ g^{-1} : C \to A$ is the inverse of $g \circ f$. Indeed, $(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ 1_B \circ g^{-1} = g \circ g^{-1} = 1_C$. And, $(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ 1_B \circ f = f^{-1} \circ f = 1_A$, and we are done.

EXERCISE 2.4. We show 'isomorphism' is an equivalence relation on any set of sets.
(Reflexivity) For all sets $A, 1_A : A \to A$ is a natural bijection, and thus, $A \cong A$.
(Symmetry) Suppose $A \cong B$ for any two sets A, B. Then, there exists a bijection $f : A \to B$, such that its inverse $f^{-1} : B \to A$ is also a bijection (as shown in the above exercise.) Thus, $B \cong A$.
(Transitivity) Finally, suppose for any three sets, A, B and C, $A \cong B$ and $B \cong C$, with $f : A \to B$ and $g : B \to C$ as bijections. Then, from the previous exercise, $g \circ f : A \to C$ is also a bijection, and thus $A \cong C$.
Thus, our original claim is established.

EXERCISE 2.5. (***Epimorphism***) A function $f : A \to B$ is an *epimorphism* (or *epi*) if the following holds: For all sets Z and all functions $\alpha', \alpha'' : B \to Z$,

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

In other words, an epimorphism f is *right cancellative*.

Proposition: A function is surjective iff it is an epimorphism.

Proof. ($\implies$) Suppose $f : A \to B$ is an epimorphism. Assume, for the sake of contradiction, f is *not* surjective. Then, there exists an element $b_0 \in B$, such that, for all $a \in A$, $f(a) \neq b_0$. We now construct two distinct functions $\alpha', \alpha'' : B \to \{0, 1\}$ as follows:

$$\alpha'(b) = 0$$

$$\alpha''(b) = \begin{cases} 0 & \text{if } b \neq b_0 \\ 1 & \text{if } b = b_0 \end{cases}$$

Then, it is easy to check that, for all $a \in A$, $(\alpha'' \circ f)(a) = \alpha''(f(a)) = 0 = \alpha'(f(a)) = (\alpha' \circ f)(a)$, which implies $\alpha' \circ f = \alpha'' \circ f$. However, $\alpha' \neq \alpha''$, which contradicts our assumption that f is an epimorphism. Hence, we conclude f is surjective.

($\impliedby$) Suppose $f : A \to B$ is surjective. Then, it has a right inverse $g : B \to A$ such that $f \circ g = 1_B$. Now, assume, for any set Z and any two functions $\alpha', \alpha'' : B \to Z$, $\alpha' \circ f = \alpha'' \circ f$. Then, $\alpha' = \alpha' \circ 1_B = \alpha' \circ (f \circ g) = (\alpha' \circ f) \circ g = (\alpha'' \circ f) \circ g = \alpha'' \circ (f \circ g) = \alpha'' \circ 1_B = \alpha''$, thus proving f is an epimorphism.

EXERCISE 2.6. Any function $f : A \to B$ determines a section $g : A \to A \times B$ of $\pi_A : A \times B \to A$ by defining g as follows:

$$a \mapsto (a, f(a))$$

Then, for all $a \in A$, $(\pi_A \circ g)(a) = \pi_A(g(a)) = \pi_A(a, f(a)) = a = 1_A(a)$, which implies $\pi_A \circ g = 1_A$, thereby showing g as defined above is indeed a section of π_A.

EXERCISE 2.7. Let $f : A \to B$ by any function. We show the graph Γ_f of f is isomorphic to A. First, recall the definition of Γ_f:

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

We define a function $g : A \to \Gamma_f$ by

$$a \mapsto (a, f(a)).$$

Then, for any $(a, b) \in \Gamma_f$, we have $b = f(a)$, which implies $g(a) = (a, f(a)) = (a, b)$, proving g is surjective. Next, for any $a', a'' \in A$, suppose $g(a') = g(a'')$. This implies $(a', f(a')) = (a'', f(a''))$, which implies $a' = a''$, thus proving g is injective. Hence, g is an isomorphism, and so, $A \cong \Gamma_f$.

EXERCISE 2.8. We describe below explicitly all the terms in the canonical decomposition of the function $f : \mathbb{R} \to \mathbb{C}$ defined by

$$r \mapsto e^{2\pi i r}.$$

Note f determines an equivalence relation $\sim$ on $\mathbb{R}$ as follows: For all $r', r'' \in \mathbb{R}$,

$$r' \sim r'' \iff f(r') = f(r'').$$

Now, $f(r') = f(r'')$ whenever $e^{i2\pi r'} = e^{i2\pi r''}$, *i.e.* $e^{i2\pi(r'-r'')} = e^0$; that is, $2\pi(r' - r'') = 2\pi k$, where $k \in \mathbb{Z}$. In other words, $f(r') = f(r'')$ iff $r' - r'' = k$, where $k \in \mathbb{Z}$. This implies

$$r' \sim r'' \iff r' - r'' \in \mathbb{Z}.$$

The above equivalence relation matches the one stated in Exercise 1.6 of Chapter 1. And, from the solution to the aforesaid exercise, we note that all equivalence classes are of the form $[\alpha]_\sim$, where $\alpha \in [0, 1)$. Therefore, the isomorphism $\tilde{f} : \mathbb{R}/\sim \xrightarrow{\sim} \operatorname{im} f$ is defined by

$$\tilde{f}(\alpha) = e^{2\pi i \alpha},\ \alpha \in [0, 1).$$

Also, note $\operatorname{im} f$ is the unit circle on the complex plane. So, the entire decomposition of $f : \mathbb{R} \to \mathbb{C}$ is as shown below:

$$\mathbb{R} \twoheadrightarrow \mathbb{R}/\sim \xrightarrow[\tilde{f}]{\sim} \operatorname{im} f \hookrightarrow \mathbb{C}\ ,$$

where $\mathbb{R}/\sim$ is a 'loop' (1-sphere.)

EXERCISE 2.9. Suppose $A' \cong A''$ and $B' \cong B''$, and further $A' \cap B' = \varnothing$ and $A'' \cap B'' = \varnothing$. Then, there exist isomorphisms $f : A' \to A''$ and $g : B' \to B''$. Define a piecewise function $h : A' \cup B' \to A'' \cup B''$ as follows:

$$h(x) = \begin{cases} f(x) & \text{if } x \in A' \\ g(x) & \text{if } x \in B' \end{cases}$$

We claim h is an isomorphism. Indeed, let $y \in A'' \cup B''$. Since A'' and B'' are disjoint, there are two cases to consider. Either, $y \in A''$, in which case, since f is surjective there exists some $x_1 \in A'$ such that $f(x_1) = y$, which implies $h(x_1) = y$. Or, $y \in B''$, in which case, since g is surjective there exists some $x_2 \in B'$ such that $g(x_2) = y$, which implies $h(x_2) = y$. Thus, in either case, h maps some $x \in A' \cup B'$ to $y \in A'' \cup B''$, thus showing h is surjective.
Now, suppose $h(x_1) = h(x_2)$ for any $x_1, x_2 \in A' \cup B'$. There are three cases to consider. First, if both $x_1, x_2 \in A'$, then $f(x_1) = f(x_2)$, and since f is injective, $x_1 = x_2$. Second, if both $x_1, x_2 \in B'$, then $g(x_1) = g(x_2)$, and since g is injective, $x_1 = x_2$. Finally, without loss of generality, we can assume $x_1 \in A'$ and $x_2 \in B'$, which implies $f(x_1) = g(x_2)$, but this is impossible, since $f(x_1) \in A''$ and $f(x_2) \in B''$, but A'', B'' are disjoint. Thus, we conclude h is injective.
Hence, h is an isomorphism.

The above demonstrates the *disjoint union* operation $A \amalg B$ for any two sets A and B is, indeed, well-defined *up to isomorphism*.

EXERCISE 2.10. Suppose A and B are finite sets. Then, any one of the $|A|$ elements in A can be mapped to any one of the $|B|$ elements in B. Thus, there are exactly $|B|^{|A|}$ ways of constructing a function $A \to B$. Hence, $|B^A| = |B|^{|A|}$.

EXERCISE 2.11. Let A be a set, and let 2^A denote the set of functions from A to $2 = \{0, 1\}$. Then, define a mapping $f : 2^A \to \mathcal{P}A$, where $\mathcal{P}A$ is the powerset of A, as follows: Any function $A \to 2$ is mapped to the subset consisting of all those elements of A that are mapped to 1 under such a function. Then, it is easy to check f is both surjective and injective, and hence, a bijection.

3. Categories

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

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

We can make $\mathcal{C}^{op}$ into a category as follows.

- For every object A of $\mathcal{C}^{op}$, its identity morphism in $\mathcal{C}^{op}$ is defined as the identity morphism 1_A in $\mathcal{C}$.
- For any two morphisms $f \in \mathrm{Hom}_{\mathcal{C}^{op}}(A, B)$ and $g \in \mathrm{Hom}_{\mathcal{C}^{op}}(B, C)$, the composite $g \circ f \in \mathrm{Hom}_{\mathcal{C}^{op}}(A, C)$ is defined as the composite $f \circ g$ in $\mathcal{C}$.
- The associativity of composition in $\mathcal{C}^{op}$ is a direct consequence of associativity of composition in $\mathcal{C}$.
- The fact that identity morphisms in $\mathcal{C}^{op}$ are identities with respect to composition is a direct consequence of identity morphisms in $\mathcal{C}$ being identities with respect to composition.

The above construction, thus, shows $\mathcal{C}^{op}$ is a category. This ***opposite category*** is simply obtained by 'reversing all the arrows' in $\mathcal{C}$.

EXERCISE 3.2. If A is a finite set, then $|\mathrm{End}_{\mathbf{Set}}(A)| = |A^A| = |A|^{|A|}$.

EXERCISE 3.3. In Example 3.3, to say $1_a = (a, a)$ is the identity of element $a \in S$ with respect to composition means that any $f = (a, b) \in \mathrm{Hom}(a, b)$ remains unchanged when composed with 1_a or 1_b in the appropriate manner. In the first case, we have $a \sim a$ and $a \sim b$, and thus, by transitivity, $a \sim b$, from which we conclude $f1_a = (a, b) = f$. Similarly, in the second case, we conclude $1_b f = f$.

EXERCISE 3.4. Suppose we can define a category in the style of Example 3.3 using the relation $<$ on the set $\mathbb{Z}$. Then, any element (object) $n \in \mathbb{Z}$ will have an identity morphism $1_n = (n, n)$ that would imply $n < n$, which is impossible. Hence, we can't define such a category using the relation $<$ on the set $\mathbb{Z}$.

EXERCISE 3.5. Example 3.4 is an instance of the categories considered in Example 3.3 in the sense that set inclusion $\subseteq$ (morphisms) between subsets of S (objects) satisfies the reflexivity and transitivity axioms for $\sim$.

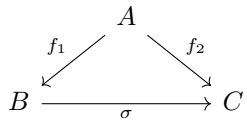
EXERCISE 3.6. (Assuming some familiarity with linear algebra.) Define a category V by taking $\mathrm{Obj}(\mathsf{V}) = \mathbb{N}$ and letting $\mathrm{Hom}_{\mathsf{V}}(n, m) =$ the set of $m \times n$ matrices with real entries, for all $n, m \in \mathbb{N}$. Composition is defined as products of matrices. Note, for all $n \in \mathbb{N}$,

$$\mathrm{Hom}_{\mathsf{V}}(n, 0) = \varnothing = \mathrm{Hom}_{\mathsf{V}}(0, n).$$

This category does *not* 'feel' familiar, since it is quite unlike any of the other categories we have seen before. Objects of V are not like the usual sets or elements we have encountered so far, and its morphisms are matrices which are not the typical set-theoretic functions.

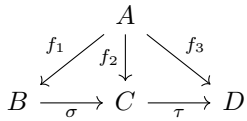
EXERCISE 3.7. Let $\mathcal{C}$ be a category, and A an object of $\mathcal{C}$. We define a category $\mathcal{C}^A$ as follows:

- $\mathrm{Obj}(\mathcal{C}^A) :=$ collection of all morphisms from A to any object of $\mathcal{C}$; that is, an object of $\mathcal{C}^A$ is a morphism $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ for some object B of $\mathcal{C}$.
- For any two objects $f_1 : A \to B$ and $f_2 : A \to C$ of $\mathcal{C}^A$, morphisms $f_1 \to f_2$ are defined to be commutative diagrams

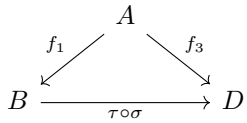


  in the 'ambient' category $\mathcal{C}$. That is, morphisms $f_1 \to f_2$ correspond precisely to those morphisms $\sigma : B \to C$ in $\mathcal{C}$ such that $\sigma \circ f_1 = f_2$.

(Composition) Two morphisms $f_1 \to f_2$ and $f_2 \to f_3$ in $\mathcal{C}^A$ correspond to putting two commutative diagrams side-by-side:



Then, the diagram obtained by removing the central arrow, *i.e.*



also commutes, since $\mathcal{C}$ is a category.

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

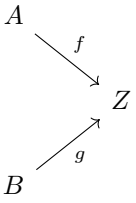
We can construct a category of *infinite sets* as follows. The objects of this category are all infinite sets from **Set**, and morphisms from an infinite set A to another infinite set B are just the usual set-functions. Then, it is clear that this category is indeed a full subcategory of **Set**.

EXERCISE 3.9.

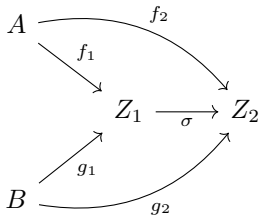
EXERCISE 3.10. Given any set A in **Set**, the subsets (subobjects) of A are in a one-to-one correspondence with functions $A \to \{0, 1\}$. Thus, $\Omega = \{0, 1\}$ is a *subobject classifier* of **Set**.

EXERCISE 3.11. The category $\mathcal{C}^{A,B}$ consists of the following pieces of data:

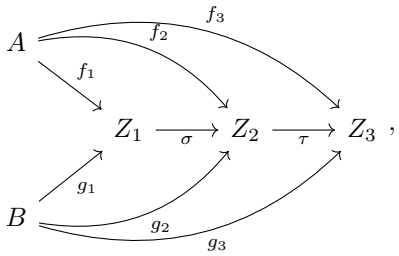
- $\mathrm{Obj}(\mathcal{C}^{A,B})$ = diagrams



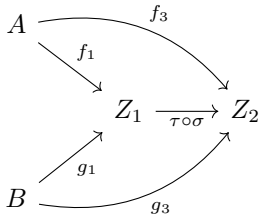
- morphisms $(f_1 : A \to Z_1, g_1 : B \to Z_1) \to (f_2 : A \to Z_2, g_2 : B \to Z_2)$ are commutative diagrams



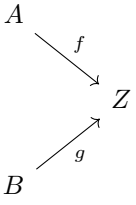
- (Composition) Given commutative diagrams



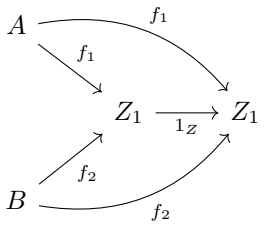
the following diagram commutes:



- (Identities) The identity morphism of

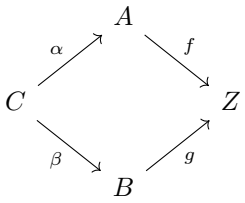


is $Z \xrightarrow{1_Z} Z$, thus making the following diagram commute:

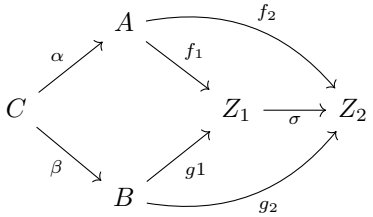


Given a category $\mathcal{C}$ and two fixed morphisms $\alpha : C \to A$ and $\beta : C \to B$, the category $\mathcal{C}^{\alpha,\beta}$ consists of the following pieces of data:

- $\mathrm{Obj}(\mathcal{C}^{\alpha,\beta})$ = commutative diagrams



  in $\mathcal{C}$.
- Morphisms correspond to commutative diagrams



- Composition and identities are defined in the obvious way.
- The usual composition and identity laws for $\mathcal{C}^{\alpha,\beta}$ follow from the composition and identity laws in $\mathcal{C}$.

4. Morphisms

EXERCISE 4.1. Suppose $A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \xrightarrow{f_3} \ldots \xrightarrow{f_n} A_n$ is a sequence of $n > 0$ morphisms in a category $\mathcal{C}$. We claim any choice of placement of parentheses for $f_n f_{n-1} \ldots f_1$ equals

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

We use induction on n to prove our claim.

(Base cases) We note $f_1 = (f_1)$. And, also $f_2 f_1 = (f_2)f_1$. So the statement holds for $n = 1, 2$.

(Inductive case) Suppose the statement holds for some $n > 1$. Now, consider the placement of parentheses for the expression $E = f_{n+1} f_n f_{n-1} \ldots f_1$. Any such choice will correspond to a representation of E in the form ee', where both e and e' contain at least one term. This also implies both e and e' contain at most n

terms. So, assume e contains the terms $f_{n+1}, f_n, \ldots, f_i$ and e' contains the terms $f_{i-1}, \ldots, f_1$ for some $1 < i \leq n+1$. Then, by the inductive hypothesis,

$$e = (((f_{n+1}f_n)\ldots)f_i)$$
$$e' = (f_{i-1}(\ldots(f_2f_1)))$$

Then, through repeated use of the associativity of morphisms under composition, we have E
$= ee'$
$= e(f_{i-1}(\ldots(f_2f_1)))$
$= ((((ef_{i-1})f_{i-2})f_{i-3})\ldots)f_1$
$= (\ldots((f_{n+1}f_n)f_{n-1})\ldots)f_1$

So, the statement holds for $n+1$ as well, and hence, by induction, the statement holds for all naturals $n > 0$. And, we are done.

EXERCISE 4.2. We claim if a set S is endowed with an equivalence relation $\sim$, then the corresponding category $\mathcal{C}$ is a groupoid. Indeed, if $a \to b$ is a morphism in $\mathcal{C}$, then $a \sim b$, which (by symmetry) implies $b \sim a$. Thus, $b \to a$, and since there is at most one morphism from any object (element) to another, we must have

$$a \to b \to a = 1_a$$
$$b \to a \to b = 1_b$$

Hence, $a \to b$ is an isomorphism, for all elements $a, b \in S$, and thus, $\mathcal{C}$ is a groupoid.

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

- Suppose f has a right inverse, $g : B \to A$, say. Then, $f \circ g = 1_B$. Assume Z is an object of $\mathcal{C}$ and $\beta, \beta' : B \to Z$ morphisms such that $\beta \circ f = \beta' \circ f$. Then, $\beta = \beta \circ 1_B = \beta \circ (f \circ g) = (\beta \circ f) \circ g = (\beta' \circ f) \circ g = \beta' \circ (f \circ g) = \beta' \circ 1_B = \beta'$, thus showing f is an epimorphism.
- In $(\mathbb{Z}, \leq)$, considered as a category, any morphism is an epimorphism, but the same does not have a right inverse. For example, $1 \leq 2$, *i.e.* $1 \to 2$. But, if the latter were to have a right inverse, then we would have $2 \to 1$, which would then imply $2 \leq 1$, clearly a contradiction.

EXERCISE 4.4. Suppose $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$ are both monomorphisms in a category $\mathcal{C}$. Let Z be any object of $\mathcal{C}$, and let $\alpha', \alpha'' : Z \to A$ be morphisms such that

$$(g \circ f) \circ \alpha' = (g \circ f) \circ \alpha''.$$

Then, $g \circ (f \circ \alpha') = g \circ (f \circ \alpha'')$, which implies $f \circ \alpha' = f \circ \alpha''$, which implies $\alpha' = \alpha''$. Hence, $g \circ f$ is a monomorphism. This demonstrates the composition of two monomorphisms is a monomorphism.

Now, it is easy to check identity morphisms in $\mathcal{C}$ are monomorphisms. Thus, one can define a subcategory $\mathcal{C}_{\text{mono}}$ of a category $\mathcal{C}$ by taking the same objects as in $\mathcal{C}$ and defining $\mathrm{Hom}_{\mathcal{C}_{\text{mono}}}$ to be the subset of $\mathrm{Hom}_{\mathcal{C}}(A, B)$ consisting of monomorphisms, for all objects A, B of $\mathcal{C}$.

(Epimorphisms) Suppose $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$ are both epimorphisms in a category $\mathcal{C}$. Let Z be any object of $\mathcal{C}$, and let $\beta', \beta'' : C \to Z$ be morphisms such that

$$\beta' \circ (g \circ f) = \beta'' \circ (g \circ f).$$

Then, $(\beta' \circ g) \circ f = (\beta'' \circ g) \circ f$, which implies $\beta' \circ g = \beta'' \circ g$, which implies $\beta' = \beta''$, thus showing $g \circ f$ is an epimorphism. In a manner similar to the one shown above, one can define a subcategory $\mathcal{C}_{\text{epi}}$ of a category $\mathcal{C}$.

EXERCISE 4.5.

5. Universal properties

EXERCISE 5.1. Suppose F is a final object in a category $\mathcal{C}$. Then, for all objects A of $\mathcal{C}$, there exists a unique morphism $A \to F$ in C, which implies for all objects A of $\mathcal{C}^{op}$, there exists a unique morphism $F \to A$ in $\mathcal{C}^{op}$. We thus conclude F is initial in the opposite category $\mathcal{C}^{op}$.

EXERCISE 5.2. For any set A, the function

$$\varnothing \xrightarrow{(\varnothing, A, \varnothing)} A$$

is the unique function from $\varnothing$ to A. Thus, $\varnothing$ is initial in **Set**. Now, suppose I is a set that's also initial in **Set**. Then, $\varnothing \cong I$. Therefore, $|I| = |\varnothing| = 0$, which implies $I = \varnothing$. Hence, $\varnothing$ is the unique initial object in **Set**.

EXERCISE 5.3. Suppose F_1 and F_2 are final objects in a category $\mathcal{C}$. Then, there are unique morphisms $F_1 \to F_2$ and $F_2 \to F_1$. So, we must have

$$F_1 \to F_2 \to F_1 = 1_{F_1}$$
$$F_2 \to F_1 \to F_2 = 1_{F_2}$$

Thus, $F_1 \cong F_2$, and hence, we conclude final objects are unique up to isomorphism.

EXERCISE 5.4. In the category $\mathbf{Set}^*$ of pointed sets, any object $(\{*\}, *)$ is both an initial and a final object.

EXERCISE 5.5. The final objects considered in the category considered in §5.3 are $A \to \{\bullet\}$.

EXERCISE 5.6. Consider the category corresponding to endowing the set $\mathbb{Z}^+$ of positive integers with the *divisibility* relation. Then, for any two positive integers m, n, if their product $m \times n$ exists, then $m \times n$ divides both m and n, and further, if some positive integer d divides both m and n, then d divides $m \times n$. $\gcd(m, n)$ satisfies the aforesaid condition, and hence, it is the product of m and n. Similarly, it is easy to check $\operatorname{lcm}(m, n)$ is the coproduct of any two positive integers m and n.

EXERCISE 5.7. Suppose $A' \cong A''$ and $B' \cong B''$, and further, $A' \cap B' = \varnothing$ and $A'' \cap B'' = \varnothing$. Then, there exist isomorphisms $k : A' \to B'$ and $l : B' \to B''$, say. We claim

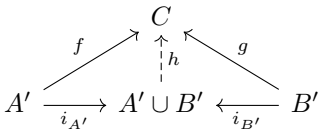
$$A' \xrightarrow{i_{A'}} A' \cup B' \xleftarrow{i_{B'}} B',$$

where $i_{A'}, i_{B'}$ are inclusion functions, is the coproduct of A' and B'.

Toward that end, for any set C and functions $A' \xrightarrow{f} C \xleftarrow{g} B'$, we define a function $h : A' \cup B' \to C$ by

$$h(x) = \begin{cases} f(x) & \text{if } x \in A' \\ g(x) & \text{if } x \in B' \end{cases}$$

Then, it is easy to check the following diagram commutes:



Also, h is necessarily the unique function $A' \cup B' \to C$ that makes the above diagram commute.

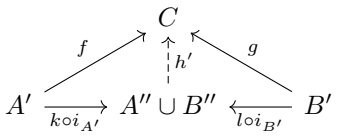
We next verify

$$A' \xrightarrow{k \circ i_{A'}} A'' \cup B'' \xleftarrow{l \circ i_{B'}} B'$$

is also a coproduct of A' and B'. Indeed, for any set C and functions $A' \xrightarrow{f} C \xleftarrow{g} B'$, we define a function $h' : A'' \cup B'' \to C$ by

$$h'(x) = \begin{cases} f \circ k^{-1}(x) & \text{if } x \in A'' \\ g \circ l^{-1}(x) & \text{if } x \in B'' \end{cases}$$

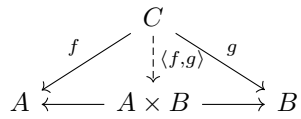
It is, again, easy to check the following diagram commutes:



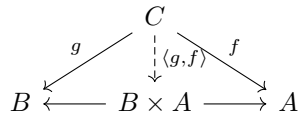
Also, h'' is necessarily the unique function $A'' \cup B'' \to C$ that makes the above diagram commute.

Thus, we see both $A' \cup B'$ and $A'' \cup B''$ along with their associated functions are coproducts of A' and B', and hence, we conclude they are isomorphic to each other.

EXERCISE 5.8. Suppose $\mathcal{C}$ is a category and A, B are objects of $\mathcal{C}$. Assume the products $A \leftarrow A \times B \to B$ and $B \leftarrow B \times A \to A$ exist. Then, for all sets C and functions $A \xleftarrow{f} C \xrightarrow{g} B$, there exists a unique function $\langle f, g \rangle : C \to A \times B$ such that the following diagram commutes:



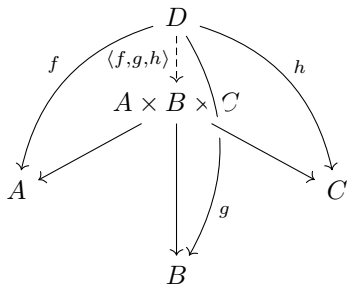
This implies there is a unique function $\langle g, f \rangle : C \to B \times A$ such that the following diagram commutes:



We thus see both $A \leftarrow A \times B \to B$ and $B \leftarrow B \times A \to A$ satisfy the universal property for the product of A and B. That is, they are both final objects in the corresponding category, and hence, by Proposition 5.4, they are isomorphic.

EXERCISE 5.9. Let $\mathcal{C}$ be a category with products. For any three objects A, B, C of $\mathcal{C}$, their product $A \times B \times C$ satisfies the following property:
The product is equipped with morphisms $A \times B \times C \to A$, $A \times B \times C \to B$ and

$A \times B \times C \to C$ such that, for all objects D and morphisms $f : D \to A$, $g : D \to B$ and $h : C \to C$, there is a unique morphism $\langle f, g, h\rangle : D \to A \times B \times C$, making the following diagram commute:



A routine check can verify $\langle f, \langle g, h\rangle\rangle : D \to A \times (B \times C)$ satisfies the aforesaid universal property, and so does $\langle\langle f, g\rangle, h\rangle : D \to (A \times B) \times C$. Hence, $A \times (B \times C)$ and $(A \times B) \times C$ are isomorphic.

EXERCISE 5.10. (Product) Let $\mathcal{C}$ be a category, and let $\{A_i\}_{i\in I}$ be a family of objects A_i of $\mathcal{C}$ indexed by some set I. The product of the family of objects A_i $(i \in I)$ is an object

$$\prod_{i\in I} A_i$$

of $\mathcal{C}$ equipped with a family of morphisms

$$p_j : \prod_{i\in I} A_i \to A_j \quad (j \in I)$$

such that, for all objects Z and morphisms $q_j : Z \to A_j$ $(j \in I)$, there exists a unique morphism $h : Z \to \prod_{i\in I} A_i$ such that

$$p_j \circ h = q_j \quad (j \in I)$$

(Coproduct) The coproduct of the family of objects A_i $(i \in I)$ is an object

$$\coprod_{i\in I} A_i$$

of $\mathcal{C}$ equipped with a family of morphisms

$$p_j : A_j \to \coprod_{i\in I} A_i \quad (j \in I)$$

such that, for all objects Z and morphisms $q_j : A_j \to Z$ $(j \in I)$, there exists a unique morphism $h : \coprod_{i\in I} A_i \to Z$ such that

$$h \circ p_j = q_j \quad (j \in I)$$

These exist in **Set** if we assume the *axiom of choice*.

EXERCISE 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

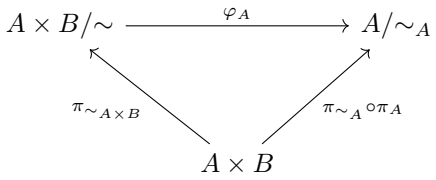
$$(a_1, b_1) \sim (a_2, b_2) \iff a_1 \sim_A a_2 \text{ and } b_1 \sim_B b_2$$

We can easily check $\sim$ is an equivalence relation on $A \times B$.

- The composite of the first projection function $\pi_A : A \times B \to A$ and the natural surjection $\pi_{\sim_A} : A \to A/\!\sim_A$ is a function $A \times B \xrightarrow{\pi_{\sim_A} \circ \pi_A} A/\!\sim_A$. Note, if $(a_1, b_1) \sim (a_2, b_2)$, then $a_1 \sim_A a_2$, and thus, $\pi_{\sim_A} \circ \pi_A(a_1, b_1) = \pi_{\sim_A}(a_1) = [a_1]_{\sim_A} = [a_2]_{\sim_A} = \pi_{\sim_A} \circ \pi_A(a_2, b_2)$. That is, equivalent elements in $A \times B$ have the same image in $A/\!\sim_A$ under the map $\pi_{\sim_A} \circ \pi_A$. Therefore, by the universal property of quotients, there exists a unique function $\varphi_A : A \times B/\!\sim \to A/\!\sim_A$, given by

$$\varphi_A([(a, b)]_\sim) = \pi_{\sim_A} \circ \pi_A(a, b)$$

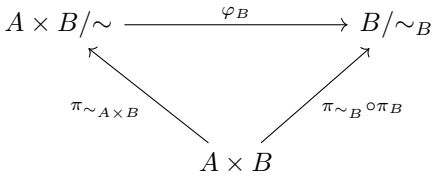
such that the following diagram commutes:



Similarly, by the universal property of quotients, there exists a unique function $\varphi_B : A \times B/\!\sim \to B/\!\sim_B$, given by

$$\varphi_B([(a, b)]_\sim) = \pi_{\sim_B} \circ \pi_B(a, b)$$

such that the following diagram commutes:



The above, thus, demonstrates there are functions $A \times B/\!\sim \to A/\!\sim_A$ and $A \times B/\!\sim \to B/\!\sim_B$.

- We now claim $A/\!\sim_A \xleftarrow{\varphi_A} A \times B/\!\sim \xrightarrow{\varphi_B} B/\!\sim_B$ is the product of $A/\!\sim_A$ and $B/\!\sim_B$.

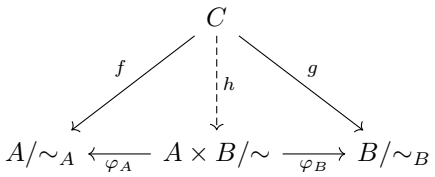
  To that end, suppose C is any set, endowed with an equivalence relation $\sim_C$. Let $A/\!\sim_A \xleftarrow{f} C \xrightarrow{g} B/\!\sim_B$ be functions, such that, for all $c_1, c_2 \in C$,

$$c_1 \sim_C c_2 \implies f(c_1) = f(c_2) \text{ and } g(c_1) = g(c_2).$$

  Now, define a function $h : C \to A \times B/\!\sim$ by

$$\begin{aligned} &h(c) = [(a, b)]_\sim, \text{ where} \\ &f(c) = [a]_{\sim_A} \text{ for some } a \in A, \text{ and} \\ &g(c) = [b]_{\sim_B} \text{ for some } b \in B. \end{aligned}$$

Then, h is the unique function $C \to A \times B/\sim$ that makes the following diagram commute:



We can easily verify, for all $c \in C$,

$$\begin{aligned}\varphi_A \circ h(c) &= \varphi_A([(a,b)]_\sim) \\ &= \pi_{\sim_A} \circ \pi_A(a,b) \\ &= \pi_{\sim_A}(a) \\ &= [a]_{\sim_A} \\ &= f(c)\end{aligned}$$

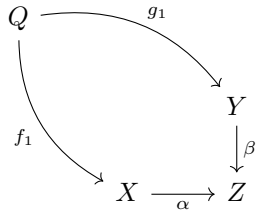
That is, $\varphi_A \circ h = f$. Similarly, it is easy to check $\varphi_B \circ h = g$. Also, it is necessarily the case that h as defined is unique. Hence, our claim is proved.

- From the previous proof, it immediately follows

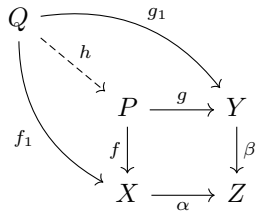
$$A \times B/\sim \cong (A/\sim_A) \times (B/\sim_B).$$

EXERCISE 5.12. Let $\mathcal{C}$ be a category, and let $X \xrightarrow{\alpha} Z \xleftarrow{\beta} Y$ be two fixed morphisms in $\mathcal{C}$.

Then, the *fibered product* of α and β is a final object $X \xleftarrow{f} P \xrightarrow{g} Y$ in the category $\mathcal{C}_{\alpha,\beta}$. That is, for all objects $X \xleftarrow{f_1} Q \xrightarrow{g_1} Y$ that makes the following diagram commute



there exists a unique morphism $h : Q \to P$ that makes the following diagram commute



In **Set**, the fibered product of two functions $X \xrightarrow{\alpha} Z \xleftarrow{\beta} Y$ is the object

$$X \xleftarrow{\pi_X} X \times_Z Y \xrightarrow{\pi_Y} Y,$$

where $X \times_Z Y := \{(x, y) \in X \times Y \mid \alpha(x) = \beta(y)\}$, and π_X and π_Y are the canonical projection functions.

Let $\mathcal{C}$ be a category, and let $X \xleftarrow{\alpha} Z \xrightarrow{\beta} Y$ be two fixed morphisms in $\mathcal{C}$. Then, the *fibered coproduct* of α and β is an initial object $X \xrightarrow{f} P \xleftarrow{g} Y$ in the category $\mathcal{C}^{\alpha,\beta}$.

CHAPTER 2

Groups, first encounter

1. Definition of group

EXERCISE 1.1. Let $(G, \bullet)$ be a group with e denoting the identity element of G. We construct a category $\mathcal{C}$ as follows:

- $\mathrm{Obj}(\mathcal{C}) := \{*\}$.
- $\mathrm{Hom}_{\mathcal{C}}(*, *) := G$.
- $1_* = e$.

Then, it is easy to check $\mathcal{C}$ is indeed a category. Also, since every element $g \in G$ has an inverse, every morphism $* \to *$ has an inverse. That is, every morphism $* \to *$ is an isomorphism. Thus, $\mathcal{C}$ is a groupoid. Hence, we conclude every group is the group of isomorphisms of a groupoid (with a single object.)

In particular, we note every group is the group of automorphisms of some object in some category.

EXERCISE 1.2. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are all groups with (additive) identity 0.

$(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot)$, and $(\mathbb{C}^*, \cdot)$ are all groups, with (multiplicative) identity 1.

EXERCISE 1.3. For all elements g, h of a group G, we note $(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = g1_Gg^{-1} = gg^{-1} = 1_G$, and $(h^{-1}g^{-1})(gh) = h^{-1}(g^{-1}g)h = h^{-1}1_Gh = h^{-1}h = 1_G$. Therefore, we conclude $(gh)^{-1} = h^{-1}g^{-1}$.

EXERCISE 1.4. Suppose $g^2 = e$ for all elements g of a group G. Then, $g^{-1} = g^{-1}e = g^{-1}(g^2) = (g^{-1}g)g = eg = g$. That is, every element g of G is its own inverse. Therefore, for all $g, h \in G$, $gh = g^{-1}h^{-1} = (hg)^{-1} = hg$, thereby implying G is commutative.

EXERCISE 1.5. Suppose the row corresponding to an element g in the multiplication table of a group contains the same element in two different columns that correspond to (distinct) elements, h_1 and h_2, say. Then, $gh_1 = gh_2$, which, by cancellation on the left, implies $h_1 = h_2$, a contradiction.
The argument is similar for any column of the multiplication table of the group.

Hence, we conclude every row and column of the multiplication table of a group contains all elements of the group exactly once.

The above statements can also be recast in the following form:
Let g be an element of a group G. Then, the mappings given by

$$h \mapsto gh$$

and

$$h \mapsto hg,$$

for all elements $h \in G$, are bijective.

EXERCISE 1.6. (G has one element) This element must be the identity 1_G. And, thus, there can be only one multiplication table for G: $1_G 1_G = 1_G$.

(G has two elements) Let these elements be 1_G and a. Now, if $aa = a$, then by the cancellation property, $a = 1_G$, a contradiction. Thus, we must have $aa = 1_G$. Therefore, there is only one multiplication table for G: $1_G 1_G = 1_G, aa = 1_G$.

(G has three elements) Let these distinct elements be $1_G, a, b$. Now, $ab \neq a$, for otherwise, by cancellation, $b = 1_G$, a contradiction. Similarly, $ab \neq b$. Thus, we must have $ab = 1_G$. That is, a and b are inverses of each other. Also, $aa \neq 1$, for otherwise, $a = a^{-1}$, which implies $a = b$, a contradiction. Again, $aa \neq a$, for otherwise, by cancellation, $a = 1_G$, a contradiction. Thus, $aa = b$. Similarly, $bb = a$. And, this exhausts all the possible cases for the multiplication table of G. Hence, there is only one multiplication table for G: $ab = 1_G, aa = b, bb = a$.

The above thus shows there is only *one* possible multiplication table for G if G has exactly 1, 2, or 3 elements.

(G has four elements) Let these distinct elements be $1_G, a, b, c$. There are two possible choices for ab: $ab = 1_G$, or $ab = c$. Other choices for ab, *viz.* a, or b, lead to contradictions. The two choices are:

- ($ab = 1_G$) Now, $ac \neq c$, for otherwise, we get $a = 1_G$, a contradiction. So, we must have $ac = b$, and thus, $aa = c$. Once we fill in the (partially-completed) multiplication table with the above data, we can fill in the rest of the multiplication table as follows. We can't have $ba = b$, so we must have $ba = 1_G$, and hence, $ca = b$. Then, $bb = c$, and $cb = a$, which forces $bc = a$, and $cc = 1_G$.

  The completed multiplication table in this case is as follows:

	1	a	b	c
1	1	a	b	c
a	a	c	1	b
b	b	1	c	a
c	c	b	a	1

  A little bit of calculation shows $a^2 = c$, $a^3 = a^2 a = ca = b$, and $a^4 = cc = 1_G$. Therefore, the above multiplication table can be entirely rewritten in terms of 1_G and a as follows:

	1	a	a^2	a^3
1	1	a	a^2	a^3
a	a	a^2	a^3	1
a^2	a^2	a^3	1	a
a^3	a^3	1	a	a^2

  The above table is precisely the one for the *cyclic group* C_4 of order 4.
- ($ab = c$) The elements of the group are $1, a, b$, and ab. There are two possible choices for a^2: 1, or b. If $a^2 = b$, then we have $b = a^2, ab = a^3$, which reduces to the previous case above. So, we are left with the only case to consider: $a^2 = 1$. Then, this forces $a(ab) = b$. Now, if $b^2 = a$, then this again reduces to the previous case above (up to isomorphism.) So, we are left with only one case to consider: $b^2 = 1$. Therefore, $b(ab) = a$. Filling up the rest of the multiplication table, we finally obtain $(ab)a = b, (ab)b = a$, and $(ab)^2 = 1$.

So, the completed multiplication table looks as follows:

	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	b
b	b	ab	1	a
ab	ab	b	a	1

Hence, we conclude there are *two* distinct tables, up to reordering the elements of G, if G has exactly four elements.

Using the tables above, it is also easy to verify all groups with ≤ 4 elements are commutative.

EXERCISE 1.7. (Prove Corollary 1.11) Let g be an element of finite order, and let $N \in \mathbb{Z}$. We claim

$$g^N = e \iff N \text{ is a multiple of } |g|.$$

Note, if $N = 0$, then the statement

$$g^0 = e \iff 0 \text{ is a multiple of } |g|$$

holds, since both sides of the double implication are trivially true. Hence, the statement holds for $N = 0$.

We now need prove our claim only for all $N \neq 0$.

($\Longrightarrow$) Suppose $g^N = e$, where $N \neq 0$. If $N > 0$, then by Lemma 1.10, N is a multiple of $|g|$. And, if $N < 0$, then $g^{-N} = g^{-N}e = g^{-N}g^N = g^{-N+N} = g^0 = e$, and since $-N > 0$, again, by Lemma 1.10, $-N$ is a multiple of $|g|$. Hence, for all $N \neq 0$, N is a multiple of $|g|$.

($\Longleftarrow$) Suppose N is a multiple of $|g|$, where $N \neq 0$. Then, $N = n|g|$, for some $0 \neq n \in \mathbb{Z}$. Therefore, $g^N = g^{n|g|} = (g^{|g|})^n = e^n = e$.

Hence, our original claim is proved.

EXERCISE 1.8. Suppose G is a finite abelian group with exactly one element f of order 2. That is, $f^2 = 1_G$. Then, $f^{-1} = f$, which means f is its own inverse. Therefore, every element, other than f, of G, necessarily has an inverse that is not f. And, since the elements of the group commute, every (non-identity) term in $\prod_{g \in G} g$ can be placed next to its inverse, and all these pairs reduce to 1_G, except f. Hence, $\prod_{g \in G} g = f$.

EXERCISE 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. We claim $n - m$ is odd.

First, note the identity element is the only element in a group with order 1. Also, it is easy to check, for all non-identity elements $g \in G$,

$$|g| = 2 \iff g = g^{-1}.$$

That is, elements with order 2 are precisely the elements that are their own inverses (not counting the identity element.) This implies elements g with order > 2 have inverses that are distinct from themselves. Thus, these elements come in pairs,

which all have distinct components. So,

$$\begin{aligned}|G| &= \sum_{|g|\in\mathbb{Z}^+} \#\text{ of elements with order } |g| \\ &= \sum_{|g|=1} \bullet + \sum_{|g|=2} \bullet + \sum_{|g|>2} \bullet \\ &= 1 + m + 2k,\end{aligned}$$

for some $k \in \mathbb{N}$. Therefore, $n - m = 2k + 1$, showing $n - m$ is indeed odd.

In addition, if n is even, then using the previous equation, it is easy to see $m = n - 2k + 1$ is odd, and hence G necessarily contains elements of order 2.

EXERCISE 1.10. Suppose the order of g is odd. Then $|g| = 2n + 1$, for some $n \in \mathbb{N}$. Using Proposition 1.13, we have

$$\begin{aligned}|g^2| &= \frac{\text{lcm}(2, |g|)}{2} \\ &= \frac{\text{lcm}(2, 2n+1)}{2} \\ &= \frac{2(2n+1)}{2} \\ &= 2n + 1\end{aligned}$$

We thus conclude $|g^2| = |g|$.

EXERCISE 1.11. We claim for all g, h in a group G, $|gh| = |hg|$.

To that end, we first prove the following ancillary claim:

$$|aga^{-1}| = |g| \text{ for all } a, g \in G.$$

Indeed, suppose a, g are elements of a group G, and let $|g| = n$, where $n \in \mathbb{Z}^+$. Then, $(aga^{-1})^n = \underbrace{(aga^{-1}) \cdots (aga^{-1})}_{n \text{ times}} = ag^n a^{-1} = a1_G a^{-1} = aa^{-1} = 1_G$.

So, $m = |aga^{-1}|$ divides n. Now, suppose $m < n$. Then, $(aga^{-1})^m = 1_G = (aga^{-1})^n$, which implies $ag^m a^{-1} = ag^n a^{-1}$, which by cancellation, $g^m = g^n$, which implies $g^{n-m} = 1_G$, which (since $n - m < n$) contradicts the assumption $|g| = n$. Therefore, $|aga^{-1}| = n = |g|$, which proves our ancillary claim.

Now, using the previous result, we immediately conclude, for all g, h in a group G, $|gh| = |gh1_G| = |gh(gg^{-1})| = |g(hg)g^{-1}| = |hg|$, and we are done.

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

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

We verify below $|g| = 4, |h| = 3$, and $|gh| = \infty$.

It is easy to verify

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

Therefore, $|g| = 4$.

Again, it is easy to verify

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

Therefore, $|h| = 3$.

Now, note

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

Using induction on n, it is easy to show

$$(gh)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},$$

for all $n \in \mathbb{Z}^+$. Therefore, $(gh)^n \neq I_n$ for any positive integer n, where I_n is the $n \times n$ (identity) diagonal matrix. Hence, $|gh| = \infty$.

EXERCISE 1.13. Consider the cyclic group C_4 of order 4, generated by a. Choose elements $g = a$ and $h = a^3$. Then, it is easy to verify $|g| = 4$ and $|h| = 4$. Therefore, $\text{lcm}(|g|, |h|) = \text{lcm}(4, 4) = 4$. And, $|gh| = |aa^3| = |a^4| = |e| = 1$. Also, g and h commute. Thus, we have an example wherein g, h commute but $|gh| = 1 \neq 4 = \text{lcm}(|g|, |h|)$.

EXERCISE 1.14. Suppose g and h commute *and* $\gcd(|g|, |h|) = 1$. We claim $|gh| = |g||h|$.

To that end, let $m = |g|$ and $n = |h|$, so that $\gcd(m, n) = 1$. By Proposition 1.14, $|gh|$ divides $\text{lcm}(|g|, |h|) = \text{lcm}(m, n) = mn/\gcd(m, n) = mn/1 = mn$. Let $N = |gh|$. So, $N \mid mn$.

Now, $(gh)^N = 1$

$$\begin{aligned}
&\implies g^N = (h^{-1})^N \\
&\implies |g^N| = |(h^{-1})^N| \\
&\implies |g^N| = |h^N| \\
&\implies \frac{|g|}{\gcd(N, |g|)} = \frac{|h|}{\gcd(N, |h|)} \\
&\implies \frac{m}{\gcd(N, m)} = \frac{n}{\gcd(N, n)} \\
&\implies m \cdot \gcd(N, n) = n \cdot \gcd(N, m)
\end{aligned}$$

Since $\gcd(m, n) = 1$, it follows $m \mid \gcd(N, m)$ and $n \mid \gcd(N, n)$. And, since $\gcd(N, m) \mid N$ and $\gcd(N, n) \mid N$, it follows $m \mid N$ and $n \mid N$, whence $mn \mid N$. But, $N \mid mn$, and so, $N = mn$. Thus, $|gh| = N = mn = |g||h|$, and this proves our claim.

EXERCISE 1.15.

2. Examples of groups

EXERCISE 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

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in S_3$$

would be

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

We show 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.

First, note $\sigma\tau \in S_n$, and so, $M_{\sigma\tau}$ is an $n \times n$ matrix where the entry at $(i, (i)\sigma\tau)$ is 1 and all other entries is 0. And, $M_\sigma M_\tau$ is an $n \times n$ matrix whose entry at (i, j) equals

$$\sum_{r=1}^{n} (M_\sigma)_{i,r} (M_\tau)_{r,j},$$

which equals 1 (otherwise, 0) iff $(M_\sigma)_{i,r} = 1 = (M_\tau)_{r,j}$ for some $1 \leq r \leq n$ iff $(i)\sigma = r$ and $(r)\tau = j$ for some $1 \leq r \leq n$ iff $((i)\sigma)\tau = j$ iff $(i)(\sigma\tau) = j$ iff the entry at $(i, (i)\sigma\tau)$ of $M_{\sigma\tau}$ equals 1 and all other entries is 0. We thus conclude $M_{\sigma\tau} = M_\sigma M_\tau$, and we are done.

EXERCISE 2.2. Suppose $d \leq n$. Then, consider the permutation $\sigma \in S_n$ given by

$$1 \to 2 \to 3 \to \ldots \to d \to 1$$

and all positive integers $> d$ being mapped to themselves. Then, clearly, $|\sigma| = d$. This shows S_n contains elements of order d.

EXERCISE 2.3. For every positive integer n, an element $\sigma \in S_{\mathbb{N}}$ of order n is given by the mapping

$$1 \to 2 \to 3 \to \ldots \to n \to 1$$

such that $n + i$ is mapped to itself, for all positive integers $i \geq 1$.

EXERCISE 2.4.

EXERCISE 2.5.

EXERCISE 2.6.

EXERCISE 2.7.

EXERCISE 2.8.

EXERCISE 2.9. We verify 'congruence mod n' is an equivalence relation. Indeed, let n be a positive integer.

(Reflexivity) For all $a \in \mathbb{Z}$, $n \mid (a - a)$, and so, $a \equiv a \mod n$.

(Symmetry) For all $a, b \in \mathbb{Z}$, if $a \equiv b \mod n$, then $n \mid (b - a)$, which implies $n \mid (a - b)$, and thus, $b \equiv a \mod n$.

(Transitivity) For all $a, b, c \in \mathbb{Z}$, if $a \equiv b \mod n$ and $b \equiv c \mod n$, then $n \mid (b - a)$ and $n \mid (c - b)$, and since $c - a = (c - b) + (b - a)$, $n \mid (c - a)$, and so, $a \equiv c \mod n$.

And, we are done.

EXERCISE 2.10. We claim $\mathbb{Z}/n\mathbb{Z}$ consists precisely of n elements, for all positive integers n.

Indeed, suppose n is a positive integer. First, note the n equivalence classes

$$[0]_n, [1]_n, \ldots, [n-1]_n$$

are all distinct, for if $[i]_n = [j]_n$ for some $0 \leq i < j < n$, then $n \mid (j - i)$, a contradiction, since $0 < j - i < n$.

Next, note for any $a \in \mathbb{Z}$, by the Euclidean algorithm, $a = qn + r$, for some $q, r \in \mathbb{Z}$, where $0 \leq r < n$. That is, $n \mid (a - r)$, and so, $a \equiv r \mod n$, and thus, $[a]_n = [r]_n$. That is to say, the equivalence class of any integer equals one of the n equivalence classes stated above.

Hence, we conclude $\mathbb{Z}/n\mathbb{Z}$ consists precisely of n elements.

EXERCISE 2.11. We show the square of every odd integer is congruent to 1 modulo 8.

Indeed, consider $\mathbb{Z}/8\mathbb{Z}$. Suppose $a \in \mathbb{Z}$ is an odd integer. Then, $[a]_8$ equals $[1]_8, [3]_8, [5]_8$, or $[7]_8$. But, $[1]_8^2 = [3]_8^2 = [5]_8^2 = [7]_8^2 = [1]_8$, which implies $[a]_8^2 = [1]_8$, and hence, $a^2 \equiv 1 \mod 8$, and we are done.

EXERCISE 2.12. We show there are no *nonzero* integers a, b, c such that $a^2 + b^2 = 3c^2$.

To that end, we study the solutions to the equation $[a]_4^2 + [b]_4^2 = 3[c]_4^2$ in $\mathbb{Z}/4\mathbb{Z}$. First, note $[0]_4^2 = [0]_4, [1]_4^2 = [1]_4, [2]_4^2 = [0]_4$, and $[3]_4^2 = [1]_4$. This implies $3[c]_4^2$ equals $[0]_4$ or $[3]_4$. Thus, any solutions to the equation above exist only when $[a]_4^2 + [b]_4^2 = [0]_4 = 3[c]_4^2$, and this is possible precisely when a, b, c are all even.

Now, assume, for the sake of contradiction, triples (a, b, c) (where a, b, c are all nonzero) exist that are solutions to the original equation $a^2 + b^2 = 3c^2$. Then, from the foregoing argument, a, b, c must all be even. Let us restrict our attention, for the moment, only to positive integer solutions c. Using the well-ordering principle, there must exist a smallest c, such that with the corresponding a and b, the triple (a, b, c) is a solution to the original equation. Now, let $a = 2k, b = 2l$, and $c = 2m$, for some integers k, l, m. Therefore, $(2k)^2 + (2l)^2 = 3(2m)^2$, which implies $k^2 + l^2 = 3m^2$, which is of the same form as the original equation. But, this implies there exists some triple (k, l, m) that is a solution to the original equation, where $m = c/2 < c$, thus contradicting the assumption that c is the smallest positive integer such that (a, b, c) (for some a, b) is a solution to the original equation.

We obtain a similar result if we assume c is a negative integer. Hence, we conclude there do not exist nonzero integers a, b, c, such that $a^2 + b^2 = 3c^2$.

EXERCISE 2.13. Suppose $\gcd(m, n) = 1$. Then, by Corollary 2.5, the class $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$. Therefore, there exists some $a \in \mathbb{Z}$ such that $a[m]_n = [1]_n$, which implies $[am]_n = [1]_n$, and thus, $am \equiv 1 \mod n$, which implies $n \mid am - 1$. Therefore, there exists some integer k such that $am - 1 = kn$, and thus, $am + (-k)n = 1$. We thus conclude there exist integers a and $b = -k$ such that $am + bn = 1$.

Conversely, suppose $am + bn = 1$ for some integers a and b. Then, since $\gcd(m, n)$ divides both m and n, $\gcd(m, n) \mid am + bn = 1$. This forces $\gcd(m, n) = 1$, and we are done.

EXERCISE 2.14. (Analog of Lemma 2.2) If $a \equiv a' \mod n$ and $b \equiv b' \mod n$, then

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

(Proof) Suppose $a \equiv a' \mod n$ and $b \equiv b' \mod n$. Then, $n \mid a' - a$ and $n \mid b' - b$, and since $a'b' - ab = a'(b' - b) + b(a' - a)$, $n \mid a'b - ab$, which implies $ab \equiv a'b' \mod n$. And, this completes our proof.

The above statement shows if $[a]_n = [a']_n$ and $[b]_n = [b']_n$, then $[ab]_n = [a'b']_n$, thus showing the multiplication on $\mathbb{Z}/n\mathbb{Z}$ is a well-defined operation.

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

- We show if $\gcd(m, n) = 1$, then $\gcd(2m + n, 2n) = 1$. We prove the contrapositive of our claim. Indeed, suppose $\gcd(2m + n, 2n) = d \neq 1$. Then, $d \mid 2m + n$ and $d \mid 2n$. Now, since n is an odd integer, $2m + n$ is odd and $2n$ is even. Therefore, d must be an odd integer, and since d and 2 are relatively prime, $d \mid n$. In addition, $d \mid 2m$, which implies $d \mid m$, and since $\gcd(m, n) \geq d$, $\gcd(m, n) \neq 1$, and we are done.
- Suppose $\gcd(r, 2n) = 1$. Then, r must be an odd integer, and hence, $(r - n)$ is an even integer. Furthermore, there exist integers a, b such that $ar + b(2n) = 1$, which implies
$$2a\left(\frac{r-n}{2}\right) + (a + 2b)n = 1.$$
Therefore, $\gcd(\frac{r-n}{2}, n) = 1$, and we are done.
- We now show the function given by
$$[m]_n \mapsto [2m + n]_{2n}$$
is a bijection between $(\mathbb{Z}/n\mathbb{Z})^*$ and $(\mathbb{Z}/2n\mathbb{Z})^*$.

  Indeed, note that since $\gcd(m, n) = 1$ implies $\gcd(2m+n, 2n) = 1$, the above mapping does define a function between $(\mathbb{Z}/n\mathbb{Z})^*$ and $(\mathbb{Z}/2n\mathbb{Z})^*$.

  (Injective) Suppose for any $[m_1]_n, [m_2]_n \in (\mathbb{Z}/n\mathbb{Z})^*$, $[2m_1 + n] = [2m_2 + n]$. Then, $2m_1 + n \equiv 2m_2 + n \mod 2n$, which implies $2n \mid (2m_2 + n) - (2m_1 + n)$, and thus, $2n \mid 2(m_2 - m_1)$, and so, $n \mid (m_2 - m_1)$, from which we conclude $m_1 \equiv m_2 \mod n$, and hence, $[m_1]_n = [m_2]_n$, thereby proving the aforesaid mapping is injective.

  (Surjective) Let $[2m+n]_{2n} \in (\mathbb{Z}/2n\mathbb{Z})^*$, where $m \in \mathbb{Z}$. Then, $\gcd(2m+n, 2n) = 1$, which, by one of the previous results, implies $\gcd(\frac{2m+n-n}{2}, n) = 1$, and thus, $\gcd(m, n) = 1$. Therefore, $[m]_n \in (\mathbb{Z}/n\mathbb{Z})^*$. Hence, $[m]_n$ in $(\mathbb{Z}/n\mathbb{Z})^*$ maps to $[2m + n]_{2n}$ in $(\mathbb{Z}/2n\mathbb{Z})^*$. Thus, the aforesaid function is surjective.

  Thus, from the foregoing arguments, it follows the defined function between $(\mathbb{Z}/n\mathbb{Z})^*$ and $(\mathbb{Z}/2n\mathbb{Z})^*$ is a bijection.

  The number $\phi(n)$ of elements of $(\mathbb{Z}/n\mathbb{Z})^*$ is *Euler's ϕ-function*. We have just proved if n is odd, then $\phi(2n) = \phi(n)$.

EXERCISE 2.16. We show the last digit of $1238237^{18238456}$ is 1. Working in $\mathbb{Z}/10\mathbb{Z}$, we first note $[1238237]_{10} = [1238230 + 7]_{10} = [1238230]_{10} + [7]_{10} = [0]_{10} + [7]_{10} = [0+7]_{10} = [7]_{10}$. Therefore, $[1238237]^4_{10} = [7]^4_{10} = [7^2]^2_{10} = [49]^2_{10} = [-1]^2_{10} = [1]_{10}$. Thus, $[1238237]^{4\cdot 4559614}_{10} = [1]^{4559614}_{10}$. That is, $[1238237]^{18238456}_{10} = [1]_{10}$. Hence, $1238237^{18238456} \equiv 1 \mod 10$, whence the last digit of $1238237^{18238456}$ is 1.