Solutions to *Algebra* by Thomas W. Hungerford

Steven Sabean

December 17, 2025

Contents

Prerequisites and Preliminaries

0.1 Logic

0.2 Sets and Classes

0.3 Functions

0.4 Relations and Partitions

0.5 Products

0.6 The Integers

0.7 The Axiom of Choice, Order, and Zorn's Lemma

Exercise 1. *Let $(A, \leq)$ be a partially ordered set and B a nonempty subset. A* ***lower bound*** *of B is an element $d \in A$ such that $d \leq b$ for* every *$b \in B$. A* ***greatest lower bound (g.l.b.)*** *of B is a lower bound d_0 of B such that $d \leq d_0$ for every other lower bound d of B. A* ***least upper bound (l.u.b.)*** *of B is an upper bound t_0 of B such that $t_0 \leq t$ for every other upper bound t of B. $(A, \leq)$ is a* ***lattice*** *if for all $a, b \in A$ the set $\{a, b\}$ has both a greatest lower bound and a least upper bound.*

(a) If $S \neq \varnothing$, then the power set $P(S)$ ordered by set-theoretic inclusion is a lattice, which has a unique maximal element.

(b) Give an example of a partially ordered set which is not *a lattice.*

(c) Give an example of a lattice with no maximal element and an example of a partially ordered set with two maximal elements.

Solution. (a) For $X, Y \subset S$ the greatest lower bound is

$$X \cap Y.$$

The least upper bound is

$$X \cup Y.$$

Thus every pair X, Y has a g.l.b. and l.u.b., so $(P(S), \subset)$ is a lattice.

A maximal element in $P(S)$ is an element that is not properly contained in any other element. The whole set S is an upper bound for every subset of S and is not contained in any strictly larger subset of S, so S is a maximal element. It is unique because if T is any subset with $U \subset T$ for all $U \subset S$, then in particular $S \subset T$, so $T = S$.

(b) Take the set $A = \{a, b\}$ with the only order relations being reflexivity:

$$a \leq a, \qquad b \leq b,$$

For the pair a, b there is no lower bound other than possibly elements $\leq a$ and $\leq b$; but the only candidates are a and b themselves, and neither is $\leq$ the other. Hence there is no greatest lower bound of a, b. (Similarly there is no least upper bound.) Therefore this poset is not a lattice.

(c) Take the integers $\mathbb{Z}$ with the usual order. For any $m, n \in \mathbb{Z}$ the least upper bound is $\max m, n$ and the greatest lower bound is $\min m, n$; thus $(\mathbb{Z}, \leq)$ is a lattice. But $\mathbb{Z}$ has no maximal element because for every $n \in \mathbb{Z}$ there exists $n + 1 > n$. So $\mathbb{Z}$ is a lattice with no maximal element.

Let $A = \{0, a, b\}$ and define the order by

$$0 \leq a, \qquad 0 \leq b.$$

Exercise 2. *A lattice $(A, \leq)$ (see Exercise 1) is said to be* ***complete*** *if every nonempty subset of A has both a least upper bound and a greatest lower bound. A map of partially ordered sets $f : A \to B$ is said to preserve order if $a \leq a'$ in A implies $f(a) \leq f(a')$ in B. Prove that an order-preserving map f of a complete lattice A into itself has at least one fixed element (that is, an $a \in A$ such that $f(a) = a$).*

Solution. Let $S = \{\, a \in A : f(a) \leq a \,\}$ be the set of all pre-fixed points of f. Since A is complete, it has a greatest element, say 1. Because f preserves order, $f(1) \leq 1$, so $1 \in S$. Thus $S \neq \varnothing$ and, since A is complete, S has a g.l.b; call it

$$m = \inf S.$$

First, we show that $f(m) \leq m$. For every $s \in S$ we have $m \leq s$, hence $f(m) \leq f(s)$ by order preservation. Since $s \in S$, $f(s) \leq s$, and thus $f(m) \leq s$ for all $s \in S$. Hence $f(m)$ is a lower bound of S, and by maximality of m as greatest lower bound, $f(m) \leq m$.

Second, we show that $m \leq f(m)$. Since m is a lower bound of S and f is order-preserving, the argument above shows that $f(m)$ is also a lower bound of S. Therefore $f(m) \leq s$ for all $s \in S$, so $f(m)$ is a lower bound of S. Because m is the greatest lower bound, we must have $m \leq f(m)$.

Combining the inequalities $f(m) \leq m$ and $m \leq f(m)$, we conclude that $f(m) = m$. Thus f has a fixed element.

Exercise 3. *Exhibit a well ordering of the set $\mathbb{Q}$ of rational numbers.*

Solution. Write each rational number in $\mathbb{Q}$ in its unique reduced form a/b with $b > 0$ and $\gcd(a,b) = 1$. (Under this convention the rational 0 is represented uniquely as $0/1$.)

Define a binary relation $\trianglelefteq$ on $\mathbb{Q}$ by declaring

$$\frac{a}{b} \trianglelefteq \frac{c}{d}$$

iff either

1. $|a| + b < |c| + d$, or
2. $|a| + b = |c| + d$ and $a < c$, or
3. $|a| + b = |c| + d$, $a = c$, and $b \leq d$.

Since every rational is written in the unique reduced form specified above, the quantities $|a|+b$, a, and b are well defined for each rational, so $\trianglelefteq$ is well defined.

It is immediate that $\trianglelefteq$ is a total order. To see that it is a well ordering, let $S \subseteq \mathbb{Q}$ be nonempty and for each $x = a/b \in S$ set $N(x) = |a| + b \in \mathbb{N}$. The set $\{N(x) : x \in S\}$ is a nonempty subset of $\mathbb{N}$, hence has a least element n_0. The subset $T = \{x \in S : N(x) = n_0\}$ is therefore nonempty. Among elements of T, the numerators form a finite (hence well-ordered) subset of $\mathbb{Z}$, so there is a least numerator a_0. Finally, among rationals in T with numerator a_0 the denominator is minimal for the $\trianglelefteq$-least element. Thus T (and hence S) has a least element with respect to $\trianglelefteq$. Therefore $\trianglelefteq$ is a well ordering of $\mathbb{Q}$.

Exercise 4. *Let S be a set. A **choice function** for S is a function f from the set of all nonempty subsets of S to S such that $f(A) \in A$ for all $A \neq \varnothing$, $A \subset S$. Show that the Axiom of Choice is equivalent to the statement that every set S has a choice function.*

Solution. We show the two statements are equivalent.

(AC $\Rightarrow$ choice functions exist). Let S be any set and let $\mathcal{I}$ denote the collection of all nonempty subsets of S. If $\mathcal{I} = \varnothing$ then $S = \varnothing$, and the unique function $\varnothing \to \varnothing$ is a choice function for S. Thus assume $\mathcal{I} \neq \varnothing$. Consider the family $\{X_A\}_{A \in \mathcal{I}}$ where $X_A = A$ for each $A \in \mathcal{I}$. Every X_A is nonempty by definition, and the family is indexed by the nonempty set $\mathcal{I}$. By the Axiom of Choice (the product of a family of nonempty sets indexed by a nonempty set is nonempty), the product $\prod_{A \in \mathcal{I}} X_A$ is nonempty. An element of this product is precisely a function $f \colon \mathcal{I} \to S$ with $f(A) \in X_A = A$ for each A; that is exactly a choice function for S. Hence every set S admits a choice function.

(Choice functions exist $\Rightarrow$ AC). Assume every set T admits a choice function c_T defined on the collection of nonempty subsets of T. Let $\{X_i\}_{i \in I}$ be any family of nonempty sets indexed by a nonempty set I. Put $S = \bigcup_{i \in I} X_i$. Then each X_i is a nonempty subset of S, so the hypothesis supplies a choice function c_S for S. Define $g \colon I \to S$ by $g(i) := c_S(X_i)$. By construction $g(i) \in X_i$ for every $i \in I$, so $g \in \prod_{i \in I} X_i$. Hence the product is nonempty. This establishes the Axiom of Choice.

Therefore the two statements are equivalent.

Exercise 5. *Let S be the set of all points (x, y) in the plane with $y \leq 0$. Define an ordering by $(x_1, y_1) \leq (x_2, y_2) \iff x_1 = x_2$ and $y_1 \leq y_2$. Show that this is a partial ordering of S, and that S has infinitely many maximal elements.*

Solution. Let $S = \{(x, y) \in \mathbb{R}^2 : y \leq 0\}$ and define

$$(x_1, y_1) \leq (x_2, y_2) \iff x_1 = x_2 \text{ and } y_1 \leq y_2.$$

(i) This relation is a partial order.

- *Reflexive:* For any $(x, y) \in S$ we have $x = x$ and $y \leq y$, so $(x, y) \leq (x, y)$.
- *Antisymmetric:* If $(x_1, y_1) \leq (x_2, y_2)$ and $(x_2, y_2) \leq (x_1, y_1)$, then $x_1 = x_2$ and $y_1 \leq y_2$, and also $x_2 = x_1$ and $y_2 \leq y_1$. Hence $y_1 = y_2$ and therefore $(x_1, y_1) = (x_2, y_2)$.
- *Transitive:* If $(x_1, y_1) \leq (x_2, y_2)$ and $(x_2, y_2) \leq (x_3, y_3)$, then $x_1 = x_2$ and $x_2 = x_3$, so $x_1 = x_3$, and $y_1 \leq y_2 \leq y_3$, hence $y_1 \leq y_3$. Thus $(x_1, y_1) \leq (x_3, y_3)$.

Therefore the relation is reflexive, antisymmetric, and transitive, i.e. a partial order.

(ii) S has infinitely many maximal elements.

Fix any real number x_0. For that x_0 the point $(x_0, 0) \in S$ satisfies the following: if $(x_0, 0) \leq (x, y)$ then $x = x_0$ and $0 \leq y$. Since every element of S has $y \leq 0$, the only possibility is $y = 0$, so $(x, y) = (x_0, 0)$. Thus there is no element of S strictly greater than $(x_0, 0)$; i.e. $(x_0, 0)$ is maximal.

As x_0 ranges over $\mathbb{R}$ we obtain the family $\{(x, 0) : x \in \mathbb{R}\}$ of maximal elements,which is infinite (indeed uncountable). Hence S has infinitely many maximal elements.

(Observe also that any point (x, y) with $y < 0$ is not maximal because $(x, y) < (x, 0)$.)

Exercise 6. *Prove that if all the sets in the family $\{A_i \mid i \in I \neq \varnothing\}$ are nonempty, then each of the projections $\pi_k \colon \prod_{i \in I} A_i \to A_k$ is surjective.*

Solution. Let $\{A_i\}_{i \in I}$ be a family of sets with $A_i \neq \varnothing$ for each $i \in I$. Fix $k \in I$ and let $\pi_k : \prod_{i \in I} A_i \to A_k$ be the projection onto the k-th coordinate. We must show that π_k is surjective, i.e. that for every $a \in A_k$ there exists $f \in \prod_{i \in I} A_i$ with $\pi_k(f) = f(k) = a$.

For a given $a \in A_k$ we need to define a function $f : I \to \bigcup_{i \in I} A_i$ such that $f(i) \in A_i$ for all $i \in I$ and $f(k) = a$. To do this we must choose, for each $i \in I - \{k\}$, an element $f(i) \in A_i$. The existence of a choice function selecting one element from each A_i (for $i \neq k$) is exactly an instance of the Axiom of Choice. Assuming Choice (or equivalently the hypothesis that the product $\prod_{i \in I} A_i$ is nonempty), pick such elements $f(i)$ for all $i \neq k$, and put $f(k) = a$. Then $f \in \prod_{i \in I} A_i$ and $\pi_k(f) = a$. Since a was arbitrary, π_k is surjective.

Remark. If the index set I is finite, no form of the Axiom of Choice is needed: one can choose elements from the finitely many A_i inductively (or by a finite product of nonempty sets being nonempty). The use of Choice becomes essential only when I is infinite.

Exercise 7. *Let $(A, \leq)$ be a linearly ordered set. The* ***immediate successor*** *of $a \in A$ (if it exists) is the least element in the set $\{x \in A \mid a < x\}$. Prove that if A is well ordered by $\leq$, then at most one element of A has no immediate successor. Give an example of a linearly ordered set in which precisely two elements have no immediate successor.*

Solution. First remark: if $a \in A$ has no immediate successor, that means the set $\{x \in A : x > a\}$ either is empty (so a is maximal) or is nonempty but has no least element.

At most one element has no immediate successor. Suppose for contradiction that a and b are two distinct elements of A with no immediate successor. Since A is linearly ordered, either $a < b$ or $b < a$. Without loss of generality assume $a < b$. Then $b \in \{x \in A : x > a\}$, so this set is nonempty. But A is well ordered, hence every nonempty subset has a least element; therefore $\{x \in A : x > a\}$ has a least element c. By definition c is the immediate successor of a, contradicting the assumption that a has no immediate successor. Thus it is impossible for two distinct elements to both lack immediate successors; at most one element of A can have no immediate successor. □

Example with exactly two elements having no immediate successor. Let

$$B = \{0\} \cup \{1/n : n \in \mathbf{N}^*\} \subset \mathbb{R}$$

equipped with the usual order inherited from $\mathbb{R}$. Every element of B except 0 is of the form $1/n$ for some $n \in \mathbf{N}^*$. For $n \geq 2$, the least element strictly greater than $1/n$ is $1/(n-1)$, so $1/n$ has an immediate successor. The element $1 = 1/1$ is maximal in B (no larger element of B exists), hence it has no immediate successor. The element 0 also has no immediate successor: the set $\{x \in B : x > 0\} = \{1/n : n \in \mathbf{N}^*\}$ has no least element because for each $1/n$ there is $1/(n+1) \in B$ with $0 < 1/(n+1) < 1/n$. Therefore 0 has no immediate successor. No other elements of B lack immediate successors, so exactly two elements of B (namely 0 and 1) have no immediate successor.

0.8 Cardinal Numbers

Exercise 1. *Let $I_0 = \varnothing$ and for each $n \in \mathbf{N}^*$ let $I_n = \{1, 2, 3, \ldots, n\}$.*

*(a) I_n is not equipollent to any of its proper subsets [*Hint*: induction].*

(b) I_m and I_n are equipollent if and only if $m = n$.

(c) I_m is equipollent to a subset of I_n but I_n is not equipollent to any subset of I_m if and only if $m < n$.

Solution. Recall that $I_0 = \varnothing$ and $I_n = \{1, 2, \ldots, n\}$ for $n \geq 1$.

Lemma. For every $n \geq 0$, every injective map $g \colon I_n \to I_n$ is surjective (hence bijective).

Proof. We proceed by strong induction on n.

Base cases. For $n = 0$, the statement is trivial: the only map $\varnothing \to \varnothing$ is bijective. For $n = 1$, any injective map $g : \{1\} \to \{1\}$ must send 1 to 1, so it is surjective.

Inductive step. Fix $n \geq 2$ and assume the claim holds for all $k < n$. Let $g : I_n \to I_n$ be injective. Suppose, for a contradiction, that g is not surjective. Then $g(I_n)$ is a proper subset of I_n, so there exists an element of I_n not in the image of g; choose m to be the largest such element. (A largest element exists since I_n is finite and totally ordered.)

Because $m \notin g(I_n)$, the image of g is contained in $I_n - \{m\}$. Define

$$\phi : I_n - \{m\} \longrightarrow I_{n-1}, \qquad \phi(k) = \begin{cases} k, & k < m, \\ k-1, & k > m. \end{cases}$$

Define also

$$\phi^{-1} : I_{n-1} \longrightarrow I_n - \{m\}, \qquad \phi^{-1}(j) = \begin{cases} j, & j < m, \\ j+1, & j \geq m. \end{cases}$$

A direct check shows that ϕ and ϕ^{-1} are inverse bijections.

Now consider the composition

$$\psi = \phi \circ g \circ \phi^{-1} : I_{n-1} \to I_{n-1}.$$

The map ψ is injective, since it is a composition of injective maps. By the induction hypothesis, ψ is surjective, hence bijective. Since ϕ^{-1} is also bijective, the composition

$$\phi^{-1} \circ \psi = g \circ \phi^{-1}$$

is bijective. In particular, $g \circ \phi^{-1}$ is surjective onto $I_n - \{m\}$. This means that the restriction

$$g|_{I_n - \{m\}} : I_n - \{m\} \longrightarrow I_n - \{m\}$$

is surjective.

Now consider $g(m)$. Since $m \notin g(I_n)$ by assumption, we must have $g(m) \in I_n - \{m\}$. But because $g|_{I_n-\{m\}}$ is surjective, there exists some $j \in I_n - \{m\}$ with $g(j) = g(m)$, contradicting the injectivity of g. This contradiction shows that g must be surjective.

This completes the induction and the proof of the lemma.

(a) I_n is not equipollent to any of its proper subsets.

Assume, for a contradiction, that there exists a bijection $f : I_n \to S$ with $S \subsetneq I_n$. Let $i : S \hookrightarrow I_n$ denote the inclusion map. Then $i \circ f : I_n \to I_n$ is injective. By the Lemma, $i \circ f$ is surjective. But $(i \circ f)(I_n) = i(S) = S$, a proper subset of I_n, which is impossible. Hence I_n is not equipollent to any of its proper subsets.

(b) I_m and I_n are equipollent if and only if $m = n$.

If $m = n$, the identity map is a bijection. Conversely, suppose I_m and I_n are equipollent and assume $m \neq n$. Without loss of generality, let $m < n$. Then a bijection $I_m \to I_n$ would make I_n equipollent to a proper subset of itself, contradicting part (a). Thus $m = n$.

(c) I_m is equipollent to a subset of I_n but I_n is not equipollent to any subset of I_m if and only if $m < n$.

If $m < n$, the inclusion $I_m \hookrightarrow I_n$ is injective, so I_m is equipollent to the subset $I_m \subset I_n$. If I_n were equipollent to a subset of I_m, then I_n would be equipollent to a proper subset of itself, contradicting part (a). Hence the stated asymmetry holds when $m < n$.

Conversely, suppose the asymmetry in the statement holds. The existence of an injection $I_m \to I_n$ implies $m \leq n$. If $m = n$, then the two sets are equipollent, contradicting the assumption. Therefore $m < n$. This completes the proof.

Exercise 2. *(a) Every infinite set is equipollent to one of its proper subsets.*

(b) A set is finite if and only if it is not equipollent to one of its proper subsets [see Exercise 1].

Solution. (a) **Every infinite set is equipollent to one of its proper subsets (assuming the Axiom of Choice).**

Assume the Axiom of Choice in the form that every set admits a choice function. Let S be an infinite set. Using a choice function, we construct an infinite sequence of distinct elements of S.

Let $\mathcal{P}^*(S)$ denote the collection of all nonempty subsets of S, and let $c : \mathcal{P}^*(S) \to S$ be a choice function. Define inductively

$$S_1 = S, \qquad s_1 = c(S_1),$$

and, having chosen distinct elements $s_1, \dots, s_n$, set

$$S_{n+1} = S - \{s_1, \dots, s_n\}, \qquad s_{n+1} = c(S_{n+1}).$$

Since S is infinite, each S_{n+1} is nonempty, so the construction continues indefinitely. Thus we obtain an infinite sequence $(s_n)_{n\geq 1}$ of distinct elements of S.

Define a map $f : S \to S$ by

$$f(s_n) = s_{n+1} \quad (n \geq 1), \qquad f(x) = x \text{ for } x \notin \{s_n : n \geq 1\}.$$

Then f is injective: it is the identity off $\{s_n\}$, and on $\{s_n\}$ it is a shift. Moreover, f is not surjective, since s_1 is not in the image. Hence $f(S) \subsetneq S$, and since $f : S \to f(S)$ is a bijection, S is equipollent to a proper subset of itself.

Remark. The statement proved here is not provable in ZF alone. Without the Axiom of Choice, there may exist infinite sets that are not equipollent to any proper subset (so-called *Dedekind-finite* infinite sets). Thus part (a) genuinely requires some form of Choice.

(b) **A set is finite if and only if it is not equipollent to one of its proper subsets (assuming the Axiom of Choice).**

If S is finite, then S is equipollent to I_n for some n, and by Exercise 1(a) no finite set is equipollent to any proper subset of itself. Hence a finite set is not equipollent to a proper subset.

Conversely, suppose S is not finite, i.e. S is infinite. By part (a), assuming the Axiom of Choice, S is equipollent to a proper subset of itself. Therefore, a set is finite if and only if it is not equipollent to one of its proper subsets.

Exercise 3. *(a) $\mathbb{Z}$ is a denumerable set.*

(b) The set $\mathbb{Q}$ of rational numbers is denumerable. [Hint: show that $|\mathbb{Z}| \leq |\mathbb{Q}| \leq |\mathbb{Z}\times\mathbb{Z}| = |\mathbb{Z}|$.]

Solution. (a) **$\mathbb{Z}$ is denumerable.**

Define $f : \mathbb{N} \to \mathbb{Z}$ by

$$f(0) = 0, \qquad f(2n-1) = n, \qquad f(2n) = -n \quad (n \geq 1).$$

Then f is bijective: every integer occurs exactly once (positive integers at odd inputs, negative integers at even inputs, and 0 at 0). Hence $\mathbb{Z}$ is denumerable.

(b) $\mathbb{Q}$ **is denumerable.**

We show that $|\mathbb{Z}| \leq |\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}|$, and that $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{Z}|$.

First, $\mathbb{Z} \subset \mathbb{Q}$ via $n \mapsto n/1$, so the inclusion gives an injection $\mathbb{Z} \hookrightarrow \mathbb{Q}$; hence $|\mathbb{Z}| \leq |\mathbb{Q}|$.

Next define $g : \mathbb{Q} \to \mathbb{Z}\times\mathbb{Z}$ by sending each rational r to its reduced numerator–denominator pair: write $r = a/b$ with $a \in \mathbb{Z}$, $b \in \mathbb{Z} - \{0\}$, $\gcd(a, b) = 1$, and $b > 0$, and set $g(r) = (a, b)$. The representation a/b with these conditions is unique, so g is injective. Hence $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}|$.

Finally, $\mathbb{Z} \times \mathbb{Z}$ is denumerable. Since $\mathbb{Z}$ is denumerable by part (a), it suffices to exhibit a bijection $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and then transport it to $\mathbb{Z} \times \mathbb{Z}$ using a bijection $\mathbb{N} \to \mathbb{Z}$. For example, the Cantor pairing function

$$\pi(m, n) = \frac{(m + n)(m + n + 1)}{2} + n$$

is a bijection $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Therefore $\mathbb{Z} \times \mathbb{Z}$ is denumerable, i.e. $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{Z}|$.

Combining the inequalities,

$$|\mathbb{Z}| \leq |\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}| = |\mathbb{Z}|,$$

so $|\mathbb{Q}| = |\mathbb{Z}|$. Hence $\mathbb{Q}$ is denumerable.

Exercise 4. *If A, A', B, B' are sets such that $|A| = |A'|$ and $|B| = |B'|$, then $|A\times B| = |A'\times B'|$. If in addition $A \cap B = \varnothing = A' \cap B'$ then $|A \cup B| = |A' \cup B'|$. Therefore multiplication and addition of cardinals is well defined.*

Solution. Assume $|A| = |A'|$ and $|B| = |B'|$. Then there exist bijections $\alpha : A \to A'$ and $\beta : B \to B'$.

Products. Define

$$\Phi : A \times B \longrightarrow A' \times B', \qquad \Phi(a, b) = (\alpha(a), \beta(b)).$$

Then Φ is bijective. Indeed, its inverse is

$$\Psi : A' \times B' \longrightarrow A \times B, \qquad \Psi(a', b') = (\alpha^{-1}(a'), \beta^{-1}(b')).$$

Thus $|A \times B| = |A' \times B'|$.

Unions (disjoint case). Assume in addition that $A \cap B = \varnothing$ and $A' \cap B' = \varnothing$. Define $F : A \cup B \to A' \cup B'$ by

$$F(x) = \begin{cases} \alpha(x), & x \in A, \\ \beta(x), & x \in B. \end{cases}$$

This is well defined because $A \cap B = \varnothing$, so each $x \in A \cup B$ lies in exactly one of the two sets. Similarly, the map

$$G : A' \cup B' \to A \cup B, \qquad G(y) = \begin{cases} \alpha^{-1}(y), & y \in A', \\ \beta^{-1}(y), & y \in B', \end{cases}$$

is well defined because $A' \cap B' = \varnothing$. One checks immediately that $G \circ F = \mathrm{id}_{A \cup B}$ and $F \circ G = \mathrm{id}_{A' \cup B'}$, so F is a bijection. Hence $|A \cup B| = |A' \cup B'|$.

Therefore, if we define cardinal multiplication by $|A| \cdot |B| := |A \times B|$ and cardinal addition (for disjoint sets) by $|A| + |B| := |A \cup B|$, these operations depend only on the cardinalities of A and B, and not on the particular representatives chosen. In other words, addition and multiplication of cardinals are well defined.

Exercise 5. *For all cardinal numbers α, β, γ:*

(a) $\alpha + \beta = \beta + \alpha$ *and* $\alpha\beta = \beta\alpha$ *(commutative laws).*

(b) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ *and* $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ *(associative laws).*

(c) $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ *and* $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$ *(distributive laws).*

(d) $\alpha + 0 = \alpha$ *and* $\alpha 1 = \alpha$.

(e) If $\alpha \neq 0$, then there is no β such that $\alpha + \beta = 0$ and if $\alpha \neq 1$, then there is no β such that $\alpha\beta = 1$. Therefore subtraction and division of cardinal numbers cannot be defined.

Solution. Let α, β, γ be cardinals. Choose sets A, B, C such that $|A| = \alpha$, $|B| = \beta$, $|C| = \gamma$, and assume (replacing by equipollent copies if necessary) that A, B, C are pairwise disjoint. Recall that $\alpha + \beta := |A \cup B|$ (for disjoint representatives) and $\alpha\beta := |A \times B|$.

(a) **Commutativity.** Since $A \cup B = B \cup A$, we have $\alpha + \beta = |A \cup B| = |B \cup A| = \beta + \alpha$. Define $\tau : A \times B \to B \times A$ by $\tau(a, b) = (b, a)$. Then τ is a bijection, so $|A \times B| = |B \times A|$, i.e. $\alpha\beta = \beta\alpha$.

(b) **Associativity.** Because A, B, C are disjoint,

$$(\alpha + \beta) + \gamma = |(A \cup B) \cup C| = |A \cup (B \cup C)| = \alpha + (\beta + \gamma).$$

For products, define $\Phi : (A \times B) \times C \to A \times (B \times C)$ by $\Phi((a, b), c) = (a, (b, c))$. This is a bijection with inverse $(a, (b, c)) \mapsto ((a, b), c)$. Hence $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

(c) **Distributivity.** Since B and C are disjoint, so are $A \times B$ and $A \times C$ if we identify them as subsets of $A \times (B \cup C)$ via the inclusions $B \hookrightarrow B \cup C$ and $C \hookrightarrow B \cup C$. Define

$$\Phi : A \times (B \cup C) \longrightarrow (A \times B) \cup (A \times C)$$

by

$$\Phi(a, x) = \begin{cases} (a, x), & x \in B, \\ (a, x), & x \in C. \end{cases}$$

This is well defined (each $x \in B \cup C$ lies in exactly one of B, C) and is clearly bijective, with inverse given by the inclusion of the union into $A \times (B \cup C)$. Therefore

$$|A \times (B \cup C)| = |(A \times B) \cup (A \times C)|,$$

i.e. $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$. The identity $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$ follows similarly by swapping the roles of left and right factors.

(d) **Identities.** Let $0 = |\varnothing|$ and $1 = |\{*\}|$. If $A \cap \varnothing = \varnothing$, then $A \cup \varnothing = A$, so $\alpha + 0 = |A| = \alpha$. Also $A \times \{*\} \cong A$ via $a \mapsto (a, *)$, so $\alpha 1 = \alpha$.

(e) **No additive inverses and no multiplicative inverses in general.** If $\alpha \neq 0$, choose a nonempty set A with $|A| = \alpha$. For any set B disjoint from A, the union $A \cup B$ is nonempty, hence $|A \cup B| \neq 0$. Therefore there is no β such that $\alpha + \beta = 0$.

If $\alpha \neq 1$, then either $\alpha = 0$ or $\alpha \geq 2$. In either case, there is no β with $\alpha\beta = 1$. Indeed, if $\alpha = 0$ then $\alpha\beta = 0$ for all β. If $\alpha \geq 2$, let A be a set of cardinality α, so A has distinct elements $a_1 \neq a_2$. For any nonempty B, the two subsets $\{a_1\} \times B$ and $\{a_2\} \times B$ are disjoint and nonempty, so $A \times B$ has at least two elements and hence cannot have cardinality 1. If $B = \varnothing$, then $A \times B = \varnothing$ has cardinality 0. Thus $|A \times B| \neq 1$ for all B, i.e. there is no β with $\alpha\beta = 1$.

Therefore subtraction and division of cardinal numbers cannot be defined so as to make $(\text{Cardinals}, +, \cdot)$ into a ring or field in the usual way.

Exercise 6. *Let I_n be as in Exercise 1. If $A \sim I_m$ and $B \sim I_n$ and $A \cap B = \varnothing$, then $(A \cup B) \sim I_{m+n}$ and $A \times B \sim I_{mn}$. Thus if we identify $|A|$ with m and $|B|$ with n, then $|A| + |B| = m + n$ and $|A||B| = mn$.*

Solution. Let $A \sim I_m$ and $B \sim I_n$, and assume $A \cap B = \varnothing$. Choose bijections

$$f : A \longrightarrow I_m, \qquad g : B \longrightarrow I_n.$$

Unions. Define $h : A \cup B \to I_{m+n}$ by

$$h(x) = \begin{cases} f(x), & x \in A, \\ m + g(x), & x \in B. \end{cases}$$

This is well defined because $A \cap B = \varnothing$. It is injective: on A it agrees with the injection f; on B it agrees with the injection $x \mapsto m + g(x)$; and no value coming from A (which lies in $\{1, \ldots, m\}$) can equal a value coming from B (which lies in $\{m+1, \ldots, m+n\}$). It is surjective because every $t \in I_{m+n}$ satisfies either $1 \leq t \leq m$, in which case $t = f(a)$ for $a = f^{-1}(t) \in A$, or $m + 1 \leq t \leq m + n$, in which case $t = m + g(b)$ for $b = g^{-1}(t - m) \in B$. Hence h is a bijection and $(A \cup B) \sim I_{m+n}$.

Products. Define $\Phi : A \times B \to I_{mn}$ by

$$\Phi(a, b) = (f(a) - 1)\, n + g(b).$$

Since $1 \leq f(a) \leq m$ and $1 \leq g(b) \leq n$, we have $0 \leq (f(a) - 1)n \leq (m - 1)n$, so $\Phi(a, b) \in \{1, 2, \ldots, mn\} = I_{mn}$.

To see that Φ is injective, suppose $\Phi(a, b) = \Phi(a', b')$. Then

$$(f(a) - 1)n + g(b) = (f(a') - 1)n + g(b'),$$

so

$$(f(a) - f(a'))n = g(b') - g(b).$$

The right-hand side lies in $\{-(n-1), \dots, n-1\}$, while the left-hand side is a multiple of n. Hence both sides must be 0, so $f(a) = f(a')$ and $g(b) = g(b')$, and therefore $a = a'$ and $b = b'$.

For surjectivity, let $t \in I_{mn}$. By the division algorithm there exist unique integers q, r with

$$t - 1 = qn + r, \qquad 0 \le r \le n-1, \qquad 0 \le q \le m-1.$$

Set $i = q + 1 \in I_m$ and $j = r + 1 \in I_n$. Choose $a \in A$ with $f(a) = i$ and $b \in B$ with $g(b) = j$. Then

$$\Phi(a, b) = (i-1)n + j = qn + (r+1) = t.$$

Thus Φ is surjective, hence bijective, and $A \times B \sim I_{mn}$.

Therefore, identifying $|A|$ with m and $|B|$ with n, we obtain

$$|A| + |B| = m + n, \qquad |A|\,|B| = mn,$$

i.e. cardinal addition and multiplication agree with the usual addition and multiplication on finite cardinalities.

Exercise 7. *If $A \sim A'$, $B \sim B'$ and $f : A \to B$ is injective, then there is an injective map $A' \to B'$. Therefore the relation $\le$ on cardinal numbers is well defined.*

Solution. Assume $A \sim A'$ and $B \sim B'$, and let $f : A \to B$ be injective. Choose bijections $\alpha : A' \to A$ and $\beta : B \to B'$. Define

$$f' = \beta \circ f \circ \alpha \ : \ A' \longrightarrow B'.$$

Then f' is injective, since it is a composition of injective maps (α and β are bijections, hence injective, and f is injective). Thus there exists an injection $A' \to B'$, as required.

Consequently, if we define $|A| \le |B|$ to mean that there exists an injective map $A \to B$, then this relation depends only on the cardinalities of A and B, and not on the particular representatives chosen. Hence $\le$ on cardinal numbers is well defined.

Exercise 8. *An infinite subset of a denumerable set is denumerable.*

Solution. Let S be denumerable and let $T \subset S$ be an infinite subset. Choose a bijection $f : \mathbb{N} \to S$. Consider the set of indices

$$J = f^{-1}(T) = \{\, n \in \mathbb{N} : f(n) \in T \,\} \subset \mathbb{N}.$$

Since T is infinite and f is bijective, J is infinite.

We now enumerate J in increasing order. Define $j_0 = \min J$, and having defined $j_0 < \dots < j_k$, set

$$j_{k+1} = \min\bigl(J - \{j_0, \dots, j_k\}\bigr).$$

This is well defined because J is infinite, so after removing finitely many elements it is still nonempty, and $\mathbb{N}$ is well ordered.

Define $g : \mathbb{N} \to T$ by $g(k) = f(j_k)$. Then $g(k) \in T$ for all k, and g is injective since the j_k are distinct and f is injective. Moreover g is surjective onto T: if $t \in T$, then $t = f(n)$ for a unique $n \in \mathbb{N}$, and $n \in J$. Since (j_k) lists all elements of J, we have $n = j_k$ for some k, hence $t = f(n) = f(j_k) = g(k)$.

Thus g is a bijection $\mathbb{N} \to T$, so T is denumerable.

Exercise 9. *The infinite set of real numbers $\mathbb{R}$ is not denumerable (that is, $\aleph_0 < |\mathbb{R}|$). [Hint: it suffices to show that the open interval $(0,1)$ is not denumerable by Exercise 8. You may assume each real number can be written as an infinite decimal. If $(0,1)$ is denumerable there is a bijection $f : \mathbf{N}^* \to (0,1)$. Construct an infinite decimal (real number) $.a_1a_2\dots$ in $(0,1)$ such that a_n is not the nth digit in the decimal expansion of $f(n)$. This number cannot be in $\operatorname{Im} f$.]*

Solution. We prove that $(0,1)$ is not denumerable. Since $(0,1) \subset \mathbb{R}$, this implies $|\mathbb{R}| > \aleph_0$. (Equivalently, if $\mathbb{R}$ were denumerable then its infinite subset $(0,1)$ would be denumerable, contrary to what we prove below.)

Assume for contradiction that $(0,1)$ is denumerable. Then there exists a bijection $f : \mathbf{N}^* \to (0,1)$. For each $n \in \mathbf{N}^*$, write the decimal expansion of $f(n)$ as

$$f(n) = 0.d_{n1}d_{n2}d_{n3}\cdots,$$

where each $d_{nk} \in \{0,1,\dots,9\}$. We may (and do) choose the expansion so that it does *not* end in an infinite string of 9's; this makes the decimal representation unique.

Now define a new decimal

$$x = 0.a_1a_2a_3\cdots$$

by the rule

$$a_n = \begin{cases} 1, & d_{nn} \neq 1, \\ 2, & d_{nn} = 1. \end{cases}$$

Then each $a_n \in \{1,2\}$, so $x \in (0,1)$. Moreover, for every n we have $a_n \neq d_{nn}$ by construction. Hence $x \neq f(n)$ for every n, since x and $f(n)$ differ in the n-th decimal digit. Therefore $x \notin \operatorname{Im}(f)$, contradicting surjectivity of f.

Thus no bijection $\mathbf{N}^* \to (0,1)$ exists, so $(0,1)$ is not denumerable. Consequently $\mathbb{R}$ is not denumerable, i.e. $\aleph_0 < |\mathbb{R}|$.

Exercise 10. *If α,β are cardinals, define α^β to be the cardinal number of the set of all functions $B \to A$, where A, B are sets such that $|A| = \alpha$, $|B| = \beta$.*

(a) α^β is independent of the choice of A, B.

(b) $\alpha^{\beta+\gamma} = (\alpha^\beta)(\alpha^\gamma)$; $(\alpha\beta)^\gamma = (\alpha^\gamma)(\beta^\gamma)$; $\alpha^{\beta\gamma} = (\alpha^\beta)^\gamma$.

(c) If $\alpha \leq \beta$, then $\alpha^\gamma \leq \beta^\gamma$.

(d) If α, β are finite with $\alpha > 1$, $\beta > 1$ and γ is infinite, then $\alpha^\gamma = \beta^\gamma$.

(e) For every finite cardinal n, $\alpha^n = \alpha\alpha\cdots\alpha$ (n factors). Hence $\alpha^n = \alpha$ if α is infinite.

(f) If $P(A)$ is the power set of a set A, then $|P(A)| = 2^{|A|}$.

Solution. Let $|A| = \alpha$ and $|B| = \beta$. Write A^B for the set of all functions $B \to A$; by definition $\alpha^\beta = |A^B|$.

(a) α^β **is well defined.** Suppose A, A', B, B' satisfy $|A| = |A'| = \alpha$ and $|B| = |B'| = \beta$. Choose bijections $\varphi : A \to A'$ and $\psi : B' \to B$. Define

$$T : A^B \longrightarrow (A')^{B'}, \qquad T(f) = \varphi \circ f \circ \psi.$$

Then T is a bijection, with inverse $g \mapsto \varphi^{-1} \circ g \circ \psi^{-1}$. Hence $|A^B| = |(A')^{B'}|$, so α^β is independent of the choices of A, B.

(b) **Exponent laws.** Let $|A| = \alpha$, $|B| = \beta$, $|C| = \gamma$, and take $B \cap C = \varnothing$.

(i) $\alpha^{\beta+\gamma} = \alpha^\beta\,\alpha^\gamma$. A function $h : B \cup C \to A$ is uniquely determined by its restrictions $h|_B : B \to A$ and $h|_C : C \to A$. Conversely, any pair $(f, g) \in A^B \times A^C$ determines a unique $h \in A^{B\cup C}$ by $h|_B = f$, $h|_C = g$. Thus the map

$$A^{B\cup C} \longrightarrow A^B \times A^C, \qquad h \mapsto (h|_B, h|_C)$$

is a bijection, so $|A^{B\cup C}| = |A^B \times A^C|$, i.e. $\alpha^{\beta+\gamma} = (\alpha^\beta)(\alpha^\gamma)$.

(ii) $(\alpha\beta)^\gamma = (\alpha^\gamma)(\beta^\gamma)$. A function $u : C \to A \times B$ is equivalent to an ordered pair of functions (f, g) with $f : C \to A$ and $g : C \to B$, via $u(c) = (f(c), g(c))$. Hence

$$(A \times B)^C \sim A^C \times B^C,$$

so $|(A \times B)^C| = |A^C \times B^C|$, i.e. $(\alpha\beta)^\gamma = (\alpha^\gamma)(\beta^\gamma)$.

(iii) $\alpha^{\beta\gamma} = (\alpha^\beta)^\gamma$. Identify $B \times C$ as the domain. A function $F : B \times C \to A$ is equivalent to a function $\widetilde{F} : C \to A^B$ given by

$$\widetilde{F}(c)(b) = F(b, c).$$

This correspondence is bijective (currying/uncurrying), so

$$A^{B\times C} \sim (A^B)^C,$$

hence $\alpha^{\beta\gamma} = (\alpha^\beta)^\gamma$.

(c) **Monotonicity in the base.** Assume $\alpha \le \beta$. Choose sets A, B with $|A| = \alpha$, $|B| = \beta$, and an injection $i : A \hookrightarrow B$. For any set C with $|C| = \gamma$, define

$$I : A^C \longrightarrow B^C, \qquad I(f) = i \circ f.$$

If $I(f) = I(g)$, then $i \circ f = i \circ g$, and since i is injective we have $f = g$. Thus I is injective, so $|A^C| \le |B^C|$, i.e. $\alpha^\gamma \le \beta^\gamma$.

(d) **If α, β are finite > 1 and γ is infinite, then $\alpha^\gamma = \beta^\gamma$.**

Let $\gamma = |C|$ with C infinite. Since $\alpha > 1$, there exists an injection $\{0, 1\} \hookrightarrow A$, hence $2^\gamma \le \alpha^\gamma$ by (c). Also A is finite, so there is an injection $A \hookrightarrow \{0, 1\}^k$ for some $k \in \mathbb{N}$ (e.g. take k with $2^k \ge \alpha$). Then by (c)

$$\alpha^\gamma \le (2^k)^\gamma.$$

Using (b)(iii) and (b)(v) below, $(2^k)^\gamma = 2^{k\gamma}$. Since C is infinite and $k \ge 1$ is finite, $k\gamma = \gamma$ (there is a bijection $C \times I_k \cong C$), hence $(2^k)^\gamma = 2^\gamma$. Therefore $2^\gamma \le \alpha^\gamma \le 2^\gamma$, so $\alpha^\gamma = 2^\gamma$. The same argument gives $\beta^\gamma = 2^\gamma$, hence $\alpha^\gamma = \beta^\gamma$.

(e) **Finite exponents.** Let n be a finite cardinal and choose $I_n = \{1, \ldots, n\}$. A function $I_n \to A$ is the same as an n-tuple $(a_1, \ldots, a_n) \in A^n$. Thus

$$A^{I_n} \cong \underbrace{A \times \cdots \times A}_{n \text{ factors}},$$

so $\alpha^n = \alpha \cdot \alpha \cdots \alpha$ (n factors).

In particular, if α is infinite and $n \geq 1$ is finite, then $\alpha^n = \alpha$. (This uses the earlier result that $\alpha n = \alpha$ for infinite α and finite $n \geq 1$, proved by exhibiting a bijection $A \times I_n \sim A$ when A is infinite.)

(f) **Power sets.** Let $P(A)$ denote the power set of A. Identify a subset $S \subset A$ with its characteristic function $\chi_S : A \to \{0,1\}$, where $\chi_S(a) = 1$ if $a \in S$ and $\chi_S(a) = 0$ otherwise. The map
$$P(A) \longrightarrow \{0,1\}^A, \qquad S \mapsto \chi_S$$
is a bijection, with inverse $f \mapsto f^{-1}(\{1\})$. Hence $|P(A)| = |\{0,1\}^A| = 2^{|A|}$.

Exercise 11. *If I is an infinite set, and for each $i \in I$ A_i is a finite set, then $|\bigcup_{i\in I} A_i| \leq |I|$.*

Solution. Let I be infinite and suppose each A_i is finite. For each $i \in I$, choose a bijection $f_i : A_i \to I_{n_i}$ for some $n_i \in \mathbb{N}$. Since A_i is finite, there exists an injection $A_i \hookrightarrow \mathbb{N}$ (for instance, compose f_i with the inclusion $I_{n_i} \hookrightarrow \mathbb{N}$). Fix such an injection and denote it by $\phi_i : A_i \hookrightarrow \mathbb{N}$.

Define a map
$$F : \bigcup_{i\in I} A_i \longrightarrow I \times \mathbb{N}$$
by
$$F(x) = (i, \phi_i(x)) \quad \text{where } i \text{ is any index with } x \in A_i.$$
To make F well defined, replace $\bigcup_{i\in I} A_i$ by the disjoint union
$$\bigsqcup_{i\in I} A_i = \{(i,x) : i \in I,\ x \in A_i\},$$
which is equipollent to $\bigcup_{i\in I} A_i$ via $(i,x) \mapsto x$. On the disjoint union define
$$\widetilde{F} : \bigsqcup_{i\in I} A_i \longrightarrow I \times \mathbb{N}, \qquad \widetilde{F}(i,x) = (i, \phi_i(x)).$$
This map is injective: if $\widetilde{F}(i,x) = \widetilde{F}(j,y)$, then $(i, \phi_i(x)) = (j, \phi_j(y))$, hence $i = j$ and $\phi_i(x) = \phi_i(y)$. Since ϕ_i is injective, $x = y$. Thus $(i,x) = (j,y)$.

Therefore
$$\left| \bigsqcup_{i\in I} A_i \right| \leq |I \times \mathbb{N}|.$$
Because I is infinite, we have $|I \times \mathbb{N}| = |I|$ (since $|\mathbb{N}| = \aleph_0 \leq |I|$ and for infinite cardinals κ, $\kappa \cdot \aleph_0 = \kappa$). Hence
$$\left| \bigsqcup_{i\in I} A_i \right| \leq |I|.$$
Finally, the canonical surjection $\bigsqcup_{i\in I} A_i \to \bigcup_{i\in I} A_i$, $(i,x) \mapsto x$, shows $\left|\bigcup_{i\in I} A_i\right| \leq \left|\bigsqcup_{i\in I} A_i\right|$. Combining, we obtain
$$\left| \bigcup_{i\in I} A_i \right| \leq |I|.$$

Exercise 12. *Let α be a fixed cardinal number and suppose that for every $i \in I$, A_i is a set with $|A_i| = \alpha$. Then $|\bigcup_{i\in I} A_i| \le |I|\alpha$.*

Solution. Let I be an index set and suppose $|A_i| = \alpha$ for all $i \in I$. Choose a set A with $|A| = \alpha$. For each $i \in I$, choose a bijection $\varphi_i : A_i \to A$.

Consider the disjoint union

$$\bigsqcup_{i\in I} A_i = \{(i,x) : i \in I,\ x \in A_i\}.$$

Define

$$F : \bigsqcup_{i\in I} A_i \longrightarrow I \times A, \qquad F(i,x) = (i, \varphi_i(x)).$$

Then F is injective: if $F(i,x) = F(j,y)$, then $(i,\varphi_i(x)) = (j,\varphi_j(y))$, hence $i = j$ and $\varphi_i(x) = \varphi_i(y)$, and since φ_i is injective, $x = y$. Thus $(i,x) = (j,y)$.

Therefore

$$\left|\bigsqcup_{i\in I} A_i\right| \le |I \times A| = |I|\,|A| = |I|\,\alpha.$$

Finally, the canonical map $\bigsqcup_{i\in I} A_i \to \bigcup_{i\in I} A_i$, $(i,x) \mapsto x$, is surjective, so

$$\left|\bigcup_{i\in I} A_i\right| \le \left|\bigsqcup_{i\in I} A_i\right|.$$

Combining these inequalities gives

$$\left|\bigcup_{i\in I} A_i\right| \le |I|\,\alpha,$$

as required.

Chapter 1

Groups

1.1 Semigroups, Monoids, and Groups

Exercise 1. *Give examples other than those in the text of semigroups and monoids that are not groups.*

Solution. We give several standard examples, emphasizing which group axiom fails in each case.

Semigroups that are not monoids.

- *Positive integers under addition.* The set $\mathbf{N}^* = \{1, 2, 3, \dots\}$ with the operation $+$ is a semigroup: addition is associative. It is not a monoid, since there is no identity element in $\mathbf{N}^*$ for addition.

- *Nonempty strings under concatenation.* Let Σ be a nonempty alphabet and let Σ^+ be the set of all nonempty finite strings over Σ. Concatenation of strings is associative, so Σ^+ is a semigroup. It is not a monoid because the empty string (the identity for concatenation) is not included.

Monoids that are not groups.

- *Natural numbers under addition.* The set $\mathbb{N} = \{0, 1, 2, \dots\}$ with addition is a monoid: addition is associative and 0 is an identity. It is not a group because no element $n \geq 1$ has an additive inverse in $\mathbb{N}$.

- *Nonzero natural numbers under multiplication.* The set $\mathbf{N}^* = \{1, 2, 3, \dots\}$ with multiplication is a monoid, with identity 1. It is not a group because, for example, 2 has no multiplicative inverse in $\mathbf{N}^*$.

- *Endomorphisms of a set under composition.* Let X be a set with at least two elements, and let $\mathrm{End}(X)$ be the set of all functions $X \to X$. Under composition, this is a monoid: composition is associative and the identity map is the identity element. It is not a group, since non-bijective functions (for example, constant maps) have no inverse.

In each of these examples, the failure to be a group is due to the absence of inverses, even though associativity (and, for monoids, an identity element) is present.

Exercise 2. *Let G be a group (written additively), S a nonempty set, and $M(S, G)$ the set of all functions $f : S \to G$. Define addition in $M(S, G)$ as follows: $(f + g) : S \to G$ is given by $s \mapsto f(s) + g(s) \in G$. Prove that $M(S, G)$ is a group, which is abelian if G is.*

Solution. Let G be a group written additively and let $S \neq \varnothing$. Set $M(S, G) = \{f : S \to G\}$, and define addition pointwise by

$$(f + g)(s) = f(s) + g(s) \qquad (s \in S).$$

We verify the group axioms.

Closure. If $f, g \in M(S, G)$, then for each $s \in S$ the value $f(s) + g(s) \in G$, so $f + g : S \to G$ is a function into G. Hence $f + g \in M(S, G)$.

Associativity. For $f, g, h \in M(S, G)$ and $s \in S$,

$$\big((f+g)+h\big)(s) = (f+g)(s)+h(s) = (f(s)+g(s))+h(s) = f(s)+(g(s)+h(s)) = f(s)+(g+h)(s) = \big(f+(g+h)\big)(s),$$

using associativity in G. Since the two functions agree at every s, $(f + g) + h = f + (g + h)$.

Identity element. Let 0_G be the identity of G, and define $0 : S \to G$ by $0(s) = 0_G$ for all $s \in S$ (the zero function). Then for any $f \in M(S, G)$ and $s \in S$,

$$(f + 0)(s) = f(s) + 0_G = f(s), \qquad (0 + f)(s) = 0_G + f(s) = f(s).$$

Hence 0 is an identity element in $M(S, G)$.

Inverses. Given $f \in M(S, G)$, define $-f : S \to G$ by $(-f)(s) = -f(s)$, where $-f(s)$ denotes the inverse of $f(s)$ in G. Then for each $s \in S$,

$$(f + (-f))(s) = f(s) + (-f(s)) = 0_G,$$

so $f + (-f) = 0$. Similarly $(-f) + f = 0$. Thus every f has an inverse.

Therefore $M(S, G)$ is a group under pointwise addition.

Commutativity. If G is abelian, then for $f, g \in M(S, G)$ and all $s \in S$,

$$(f + g)(s) = f(s) + g(s) = g(s) + f(s) = (g + f)(s),$$

so $f + g = g + f$. Hence $M(S, G)$ is abelian whenever G is abelian.

Exercise 3. *Is it true that a semigroup which has a* left *identity element and in which every element has a* right *inverse (see Proposition 1.3) is a group?*

Solution. No. Let S be any set with at least two elements, and define a binary operation on S by

$$x * y = y \qquad (x, y \in S).$$

(This is the *right-zero semigroup*.)

Semigroup: The operation is associative, since

$$(x * y) * z = y * z = z = x * z = x * (y * z)$$

for all $x, y, z \in S$.

Left identity: Fix any element $e \in S$. Then for every $x \in S$,

$$e * x = x,$$

so e is a left identity.

Right inverses: For any $a \in S$, take $b = e$. Then

$$a * b = a * e = e,$$

so every element has a right inverse (with respect to the left identity e).

Not a group: e is not a two-sided identity unless S is a singleton. Indeed, for $x \neq e$,

$$x * e = e \neq x.$$

Hence S is not a monoid (with identity), and therefore cannot be a group.

Thus a semigroup can have a left identity and right inverses for all elements without being a group.

Exercise 4. *Write out a multiplication table for the group $D_4{}^*$.*

Solution.

$\cdot$	e	r	r^2	r^3	s	sr	sr^2	sr^3
e	e	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	e	sr^3	s	sr	sr^2
r^2	r^2	r^3	e	r	sr^2	sr^3	s	sr
r^3	r^3	e	r	r^2	sr	sr^2	sr^3	s
s	s	sr	sr^2	sr^3	e	r	r^2	r^3
sr	sr	sr^2	sr^3	s	r^3	e	r	r^2
sr^2	sr^2	sr^3	s	sr	r^2	r^3	e	r
sr^3	sr^3	s	sr	sr^2	r	r^2	r^3	e

Exercise 5. *Prove that the symmetric group on n letters, S_n, has order $n!$.*

Solution. Let S_n denote the symmetric group on n letters, i.e. the set of all bijections $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$. Thus $|S_n|$ is the number of permutations of an n-element set.

A permutation $\sigma \in S_n$ is determined by the ordered list $(\sigma(1), \sigma(2), \ldots, \sigma(n))$, where these values must be distinct and each lies in $\{1, \ldots, n\}$. We count the number of such lists.

There are n choices for $\sigma(1)$. After choosing $\sigma(1)$, there remain $n-1$ choices for $\sigma(2)$, since $\sigma(2) \neq \sigma(1)$. Continuing, after choosing $\sigma(1), \ldots, \sigma(k-1)$, there are $n-(k-1)$ choices for $\sigma(k)$. Therefore the total number of permutations is

$$n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 = n!.$$

Hence $|S_n| = n!$.

Exercise 6. *Write out an addition table for $Z_2 \oplus Z_2$. $Z_2 \oplus Z_2$ is called the* ***Klein four group****.*

Solution. Recall that $Z_2 = \{0, 1\}$ with addition mod 2. Thus

$$Z_2 \oplus Z_2 = \{(0,0), (1,0), (0,1), (1,1)\},$$

with addition defined componentwise modulo 2.

The addition table is:

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

From the table we see that:

- $(0,0)$ is the identity element.
- Every non-identity element has order 2.
- The operation is commutative.

Hence $Z_2 \oplus Z_2$, the Klein four group, is an abelian group in which every non-identity element is its own inverse.

Exercise 7. *If p is prime, then the nonzero elements of Z_p form a group of order $p-1$ under multiplication. [Hint: $\overline{a} \neq \overline{0} \implies (a,p) = 1$; use Introduction, Theorem 6.5.] Show that this statement is false if p is not prime.*

Solution. Let p be prime. Consider the set $Z_p^\times = Z_p - \{\overline{0}\}$ of nonzero residue classes modulo p, with multiplication modulo p.

Claim. If p is prime, then $Z_p^\times$ is a group under multiplication and $|Z_p^\times| = p - 1$.

Proof. Closure and associativity are inherited from integer multiplication modulo p, and the identity element is $\overline{1}$. It remains to show that every $\overline{a} \in Z_p^\times$ has a multiplicative inverse in $Z_p^\times$.

If $\overline{a} \neq \overline{0}$, then $p \nmid a$, hence $\gcd(a,p) = 1$ because p is prime. By Introduction, Theorem 6.5 (Bézout's identity), there exist integers x, y such that

$$ax + py = 1.$$

Reducing this congruence modulo p gives $ax \equiv 1 \pmod{p}$, hence $\overline{a}\,\overline{x} = \overline{1}$ in Z_p. Thus $\overline{x}$ is the inverse of $\overline{a}$, and $\overline{x} \neq \overline{0}$. Therefore.every element of $Z_p^\times$ has an inverse, so $Z_p^\times$ is a group.

Finally, Z_p has p elements, and removing $\overline{0}$ leaves $p-1$ elements, so $|Z_p^\times| = p - 1$.

The statement is false when p is not prime. Let $n \geq 2$ be composite. Then there exist integers a, b with $1 < a < n$, $1 < b < n$, and $n = ab$. In Z_n we have

$$\overline{a} \neq \overline{0}, \qquad \overline{b} \neq \overline{0}, \qquad \text{but} \qquad \overline{a}\,\overline{b} = \overline{ab} = \overline{n} = \overline{0}.$$

Thus $Z_n - \{\overline{0}\}$ contains nonzero elements whose product is $\overline{0}$. In particular, it is not closed under multiplication, so it cannot be a group.

For a concrete example, take $n = 4$: $\overline{2} \neq \overline{0}$ in Z_4, but $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$. Hence the nonzero elements of Z_4 do not form a group under multiplication.

Exercise 8. *(a) The relation given by $a \sim b \iff a - b \in \mathbb{Z}$ is a congruence relation on the additive group $\mathbb{Q}$ [see Theorem 1.5].*

(b) The set $\mathbb{Q}/\mathbb{Z}$ of equivalence classes is an infinite abelian group.

Solution. (a) $\sim$ **is a congruence relation on** $(\mathbb{Q}, +)$**.**

First note that $\sim$ is an equivalence relation:

- Reflexive: $a - a = 0 \in \mathbb{Z}$, so $a \sim a$.
- Symmetric: if $a \sim b$ then $a - b \in \mathbb{Z}$, hence $b - a = -(a-b) \in \mathbb{Z}$, so $b \sim a$.
- Transitive: if $a \sim b$ and $b \sim c$, then $a-b \in \mathbb{Z}$ and $b-c \in \mathbb{Z}$, so $(a-c) = (a-b)+(b-c) \in \mathbb{Z}$, hence $a \sim c$.

To check that it is a congruence relation (compatible with the group operation), let $a \sim b$ and $c \sim d$. Then $a - b \in \mathbb{Z}$ and $c - d \in \mathbb{Z}$, so

$$(a + c) - (b + d) = (a - b) + (c - d) \in \mathbb{Z},$$

which shows $a + c \sim b + d$. Thus $\sim$ is a congruence relation on the additive group $\mathbb{Q}$ (in the sense of Theorem 1.5).

(b) $\mathbb{Q}/\mathbb{Z}$ **is an infinite abelian group.**

Since $\sim$ is a congruence relation on the abelian group $(\mathbb{Q}, +)$, Theorem 1.5 implies that the set of equivalence classes $\mathbb{Q}/\mathbb{Z}$ becomes a group under

$$[a] + [b] = [a + b],$$

where $[a]$ denotes the $\sim$-equivalence class of a. This operation is well defined by part (a), the identity element is $[0]$, and the inverse of $[a]$ is $[-a]$. Moreover, because $\mathbb{Q}$ is abelian, $\mathbb{Q}/\mathbb{Z}$ is abelian.

It remains to show that $\mathbb{Q}/\mathbb{Z}$ is infinite. Consider the elements

$$\left[\frac{1}{n}\right] \in \mathbb{Q}/\mathbb{Z} \qquad (n \geq 2).$$

If $\left[\frac{1}{m}\right] = \left[\frac{1}{n}\right]$, then $\frac{1}{m} - \frac{1}{n} \in \mathbb{Z}$. But for $m, n \geq 2$ we have

$$-\frac{1}{2} < \frac{1}{m} - \frac{1}{n} < \frac{1}{2},$$

so the only integer it can equal is 0. Hence $\frac{1}{m} = \frac{1}{n}$, so $m = n$. Thus the elements $\left[\frac{1}{n}\right]$ are all distinct, giving infinitely many distinct elements of $\mathbb{Q}/\mathbb{Z}$.

Therefore $\mathbb{Q}/\mathbb{Z}$ is an infinite abelian group.

Exercise 9. *Let p be a fixed prime. Let R_p be the set of all those rational numbers whose denominator is relatively prime to p. Let R^p be the set of rationals whose denominator is a power of p ($p^i, i \geq 0$). Prove that both R_p and R^p are abelian groups under ordinary addition of rationals.*

Solution. Fix a prime p.

(1) The set R_p is an abelian group under addition.

By definition, R_p consists of those rationals $a/b \in \mathbb{Q}$ (in lowest terms, with $b > 0$) such that $\gcd(b, p) = 1$.

Closure. Let $\frac{a}{b}, \frac{c}{d} \in R_p$ with $\gcd(b, p) = \gcd(d, p) = 1$. Then

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Since $\gcd(b, p) = \gcd(d, p) = 1$, we also have $\gcd(bd, p) = 1$. When the fraction $\frac{ad+bc}{bd}$ is reduced to lowest terms, its denominator divides bd, hence is still relatively prime to p. Therefore $\frac{a}{b} + \frac{c}{d} \in R_p$.

Identity. $0 = \frac{0}{1} \in R_p$ because $\gcd(1, p) = 1$.

Inverses. If $\frac{a}{b} \in R_p$, then $-\frac{a}{b} \in R_p$ and $\frac{a}{b} + (-\frac{a}{b}) = 0$.

Associativity and commutativity. These are inherited from addition in $\mathbb{Q}$. Hence R_p is an abelian group under addition.

(2) The set R^p is an abelian group under addition.

By definition, R^p consists of rationals of the form $\frac{a}{p^i}$ with $a \in \mathbb{Z}$ and $i \geq 0$.

Closure. Let $\frac{a}{p^i}, \frac{c}{p^j} \in R^p$. Then

$$\frac{a}{p^i} + \frac{c}{p^j} = \frac{ap^j + cp^i}{p^{i+j}}.$$

This is again a rational whose denominator is a power of p, so it lies in R^p.

Identity. $0 = \frac{0}{p^0} \in R^p$.

Inverses. If $\frac{a}{p^i} \in R^p$, then $-\frac{a}{p^i} \in R^p$.

Associativity and commutativity. Again inherited from $\mathbb{Q}$. Therefore R^p is an abelian group under addition.

Exercise 10. *Let p be a prime and let $Z(p^\infty)$ be the following subset of the group $\mathbb{Q}/\mathbb{Z}$ (see Pg.27):*

$$Z(p^\infty) = \{\overline{a/b} \in \mathbb{Q}/\mathbb{Z} \mid a, b \in \mathbb{Z} \text{ and } b = p^i \text{ for some } i \geq 0\}.$$

Show that $Z(p^\infty)$ is an infinite group under the addition operation of $\mathbb{Q}/\mathbb{Z}$.

Solution. Fix a prime p. l Recall that $\mathbb{Q}/\mathbb{Z}$ is an abelian group under $\overline{x} + \overline{y} = \overline{x + y}$. We show that $Z(p^\infty)$ is an (infinite) subgroup.

Subgroup. Let $\overline{a/p^i}, \overline{c/p^j} \in Z(p^\infty)$ (where $i, j \geq 0$). Then in $\mathbb{Q}/\mathbb{Z}$,

$$\overline{\frac{a}{p^i}} + \overline{\frac{c}{p^j}} = \overline{\frac{a}{p^i} + \frac{c}{p^j}} = \overline{\frac{ap^j + cp^i}{p^{i+j}}}.$$

Since p^{i+j} is again a power of p, the sum lies in $Z(p^\infty)$. Also,

$$-\overline{\frac{a}{p^i}} = \overline{-\frac{a}{p^i}} = \overline{\frac{-a}{p^i}} \in Z(p^\infty),$$

and the identity element $\overline{0} = \overline{0/1}$ belongs to $Z(p^\infty)$ (take $i = 0$). Hence $Z(p^\infty)$ is a subgroup of $\mathbb{Q}/\mathbb{Z}$, and therefore a group (indeed abelian) under the induced operation.

Infinitude. Consider the elements $\overline{1/p^n} \in Z(p^\infty)$ for $n \geq 1$. We claim they are all distinct in $\mathbb{Q}/\mathbb{Z}$. If $\overline{1/p^m} = \overline{1/p^n}$, then

$$\frac{1}{p^m} - \frac{1}{p^n} \in \mathbb{Z}.$$

Assume $m < n$. Then

$$0 < \frac{1}{p^m} - \frac{1}{p^n} = \frac{p^{n-m}-1}{p^n} < \frac{p^{n-m}}{p^n} = \frac{1}{p^m} \leq 1,$$

so the difference is an integer strictly between 0 and 1, which is impossible. Thus $m = n$. Therefore the classes $\overline{1/p^n}$ are pairwise distinct, and $Z(p^\infty)$ is infinite.

Hence $Z(p^\infty)$ is an infinite group under addition in $\mathbb{Q}/\mathbb{Z}$.

Exercise 11. *The following conditions on a group G are equivalent: (i) G is abelian; (ii) $(ab)^2 = a^2b^2$ for all $a, b \in G$; (iii) $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$; (iv) $(ab)^n = a^nb^n$ for all $n \in \mathbb{Z}$ and all $a, b \in G$; (v) $(ab)^n = a^nb^n$ for three consecutive integers n and all $a, b \in G$. Show that (v) $\implies$ (i) is false if "three" is replaced by "two."*

Solution. We prove the implications

$$(i) \iff (ii) \iff (iii), \qquad (i) \implies (iv) \implies (v) \implies (i),$$

and then show that in (v) the phrase "three consecutive integers" cannot be weakened to "two consecutive integers."

$(i) \Rightarrow (ii)$. If G is abelian, then $ab = ba$, hence

$$(ab)^2 = abab = aabb = a^2b^2.$$

$(ii) \Rightarrow (i)$. Assume $(ab)^2 = a^2b^2$ for all $a, b \in G$. Then

$$abab = aabb.$$

Cancel a on the left to obtain $bab = abb$, and then cancel b on the right to obtain $ba = ab$. Thus G is abelian.

$(i) \Rightarrow (iii)$. If G is abelian, then $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$.

$(iii) \Rightarrow (i)$. Assume $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$. Taking inverses of both sides gives

$$ab = \left((ab)^{-1}\right)^{-1} = \left(a^{-1}b^{-1}\right)^{-1} = ba,$$

so G is abelian.

Thus $(i), (ii), (iii)$ are equivalent.

$(i) \Rightarrow (iv)$. Assume G is abelian. For $n \geq 0$,

$$(ab)^n = \underbrace{(ab)\cdots(ab)}_{n \text{ factors}} = \underbrace{a\cdots a}_{n \text{ factors}} \underbrace{b\cdots b}_{n \text{ factors}} = a^nb^n.$$

For $n < 0$, write $n = -m$ with $m > 0$. Then

$$(ab)^n = (ab)^{-m} = \left((ab)^{-1}\right)^m = (a^{-1}b^{-1})^m = a^{-m}b^{-m} = a^nb^n,$$

using commutativity. Hence (iv) holds.

$(iv) \Rightarrow (v)$. Immediate.

$(v) \Rightarrow (i)$. Assume that for some three consecutive integers $n = k, k+1, k+2$ we have

$$(ab)^n = a^n b^n \qquad \text{for all } a, b \in G.$$

We prove that G is abelian.

Step 1: From two consecutive exponents, get commutation with a power of b. Using the identities for k and $k+1$, we compute

$$(ab)^{k+1} = (ab)^k (ab) = a^k b^k ab,$$

and also

$$(ab)^{k+1} = a^{k+1} b^{k+1} = a^k a b^k b.$$

Equating these and cancelling a^k on the left gives

$$b^k ab = ab^k b.$$

Cancelling b on the right yields

$$b^k a = ab^k \qquad \text{for all } a, b \in G. \tag{1.1}$$

Applying the same argument to the consecutive pair $k+1, k+2$ gives

$$b^{k+1} a = ab^{k+1} \qquad \text{for all } a, b \in G. \tag{1.2}$$

Step 2: Consecutive powers force commutation with b. Since $\gcd(k, k+1) = 1$, there exist integers u, v such that

$$uk + v(k+1) = 1.$$

Hence, for every $b \in G$,

$$b = b^{uk+v(k+1)} = (b^k)^u \, (b^{k+1})^v.$$

By (1.1) and (1.2), every element $a \in G$ commutes with b^k and with b^{k+1}, hence also with all their integer powers and with their product. Therefore $ab = ba$ for all $a, b \in G$, so G is abelian.

Thus $(v) \Rightarrow (i)$.

Failure for "two consecutive integers". If in (v) we require the identity $(ab)^n = a^n b^n$ only for two consecutive integers, we may take $n = 0, 1$. But for every group and all a, b,

$$(ab)^0 = e = a^0 b^0, \qquad (ab)^1 = ab = a^1 b^1.$$

Thus the weakened condition holds in every group, including nonabelian groups (e.g. D_4), so it does not imply that G is abelian.

Exercise 12. *If G is a group, $a, b \in G$ and $bab^{-1} = a^r$ for some $r \in \mathbb{N}$, then $b^j ab^{-j} = a^{r^j}$ for all $j \in \mathbb{N}$.*

Solution. We prove the statement by induction on $j \in \mathbb{N}$.

Base case. For $j = 0$ we have $b^0 ab^{-0} = a$, and $a^{r^0} = a^1 = a$, so the formula holds. For $j = 1$ the formula is exactly the hypothesis $bab^{-1} = a^r$.

Inductive step. Assume for some $j \geq 0$ that

$$b^j ab^{-j} = a^{r^j}.$$

Conjugate both sides by b. Using bxb^{-1} as an automorphism of G, we obtain

$$b^{j+1}ab^{-(j+1)} = b\,(b^j ab^{-j})\,b^{-1} = b\,a^{r^j}\,b^{-1} = (bab^{-1})^{r^j}.$$

(The last equality uses the general fact that conjugation preserves powers: $bx^n b^{-1} = (bxb^{-1})^n$ for all $n \in \mathbb{N}$, proved by a short induction on n.)

Now apply the hypothesis $bab^{-1} = a^r$:

$$(bab^{-1})^{r^j} = (a^r)^{r^j} = a^{r \cdot r^j} = a^{r^{j+1}}.$$

Thus

$$b^{j+1}ab^{-(j+1)} = a^{r^{j+1}},$$

completing the induction.

Therefore $b^j ab^{-j} = a^{r^j}$ for all $j \in \mathbb{N}$.

Exercise 13. *If $a^2 = e$ for all elements a of a group G, then G is abelian.*

Solution. Assume that $a^2 = e$ for every $a \in G$. Then each element is its own inverse: indeed $a^2 = e$ implies $a^{-1} = a$.

Let $a, b \in G$. Consider $(ab)^2$. By the hypothesis, $(ab)^2 = e$, so

$$(ab)(ab) = e.$$

But $(ab)^{-1} = b^{-1}a^{-1} = ba$, since $a^{-1} = a$ and $b^{-1} = b$. Hence

$$e = (ab)(ab) \quad \Longrightarrow \quad (ab)^{-1} = ab.$$

Therefore $ab = ba$. Since a, b were arbitrary, G is abelian.

Exercise 14. *If G is a finite group of even order, then G contains an element $a \neq e$ such that $a^2 = e$.*

Solution. Let G be a finite group of even order. Consider the set

$$S = \{\, a \in G \mid a \neq e \,\}.$$

For each $a \in S$, either $a = a^{-1}$ or $a \neq a^{-1}$.

If $a \neq a^{-1}$, then the elements a and a^{-1} are distinct and can be paired together. Thus all elements of S that are *not* equal to their own inverse can be partitioned into disjoint pairs $\{a, a^{-1}\}$.

Since $|G|$ is even, $|S| = |G| - 1$ is odd. Removing an even number of elements (the paired elements) from the odd-sized set S leaves an odd number of elements. Hence there must exist at least one element $a \in S$ that is not paired with a distinct inverse, i.e. such that $a = a^{-1}$.

For this element $a \neq e$, we have $a = a^{-1}$, which implies

$$a^2 = e.$$

Thus G contains a non-identity element of order 2.

Exercise 15. *Let G be a nonempty finite set with an associative binary operation such that for all $a, b, c \in G$ $ab = ac \implies b = c$ and $ba = ca \implies b = c$. Then G is a group. Show that this conclusion may be false if G is infinite.*

Solution. **Finite case.** Assume G is a nonempty finite set with an associative binary operation, and that both left and right cancellation hold:

$$ab = ac \implies b = c, \qquad ba = ca \implies b = c.$$

Fix $a \in G$. Consider the left translation $L_a : G \to G$ given by $L_a(x) = ax$. Left cancellation says L_a is injective, hence (since G is finite) L_a is surjective. Hence for every $b \in G$ the equation

$$ax = b$$

has a solution $x \in G$.

Similarly, consider the right translation $R_a : G \to G$ given by $R_a(x) = xa$. Right cancellation implies R_a is injective, hence surjective. Hence for every $b \in G$ the equation

$$ya = b$$

has a solution $y \in G$.

Thus for all $a, b \in G$, both equations $ax = b$ and $ya = b$ are solvable in G. By Proposition 1.4, G is a group.

Infinite case (counterexample). Let $G = \mathbb{N} = \{0, 1, 2, \dots\}$ with the operation $+$. Addition is associative, and both cancellation laws hold:

$$a + b = a + c \implies b = c, \qquad b + a = c + a \implies b = c.$$

However $(\mathbb{N}, +)$ is not a group: although 0 is an identity, most elements have no additive inverses in $\mathbb{N}$ (for example, there is no $x \in \mathbb{N}$ with $1 + x = 0$). Hence the conclusion may fail when G is infinite.

Exercise 16. *Let $a_1, a_2, \dots$ be a sequence of elements in a semigroup G. Then there exists a unique function $\psi : \mathbf{N}^* \to G$ such that $\psi(1) = a_1$, $\psi(2) = a_1a_2$, $\psi(3) = (a_1a_2)a_3$ and for $n \geq 1$, $\psi(n+1) = (\psi(n))a_{n+1}$. Note that $\psi(n)$ is precisely the standard n product $\prod_{i=1}^{n} a_i$. [*Hint*: Applying the Recursion Theorem 6.2 of the Introduction with $a = a_1$, $S = G$ and $f_n : G \to G$ given by $x \mapsto xa_{n+2}$ yields a function $\varphi : \mathbb{N} \to G$. Let $\psi = \varphi\theta$, where $\theta : \mathbf{N}^* \to \mathbb{N}$ is given by $k \mapsto k - 1$.]*

Solution. Let G be a semigroup and let $a_1, a_2, \dots$ be a sequence in G. We apply the Recursion Theorem 6.2 from the Introduction in the form:

Given a set S, an element $a \in S$, and maps $f_n : S \to S$ $(n \in \mathbb{N})$, there exists a unique function $\varphi : \mathbb{N} \to S$ such that

$$\varphi(0) = a, \qquad \varphi(n+1) = f_n(\varphi(n)) \quad (n \in \mathbb{N}).$$

Take $S = G$ and $a = a_1$. For each $n \in \mathbb{N}$, define

$$f_n : G \to G, \qquad f_n(x) = x\, a_{n+2}.$$

Since G is a semigroup, the product $x\, a_{n+2}$ is defined for all $x \in G$, so each f_n is well defined. By the Recursion Theorem, there exists a unique $\varphi : \mathbb{N} \to G$ satisfying

$$\varphi(0) = a_1, \qquad \varphi(n+1) = \varphi(n)\, a_{n+2} \ \ (n \in \mathbb{N}).$$

Now define $\theta : \mathbf{N}^* \to \mathbb{N}$ by $\theta(k) = k - 1$, and set

$$\psi := \varphi \circ \theta : \mathbf{N}^* \to G.$$

Then

$$\psi(1) = \varphi(0) = a_1,$$
$$\psi(2) = \varphi(1) = \varphi(0)a_2 = a_1 a_2,$$

and in general for $n \geq 1$,

$$\psi(n+1) = \varphi(n) = \varphi(n-1)a_{n+1} = \psi(n)\, a_{n+1}.$$

Thus ψ satisfies exactly the required recursion, so it exists.

For uniqueness: if $\psi' : \mathbf{N}^* \to G$ is another function satisfying $\psi'(1) = a_1$ and $\psi'(n+1) = \psi'(n)a_{n+1}$, define $\varphi' : \mathbb{N} \to G$ by $\varphi'(n) = \psi'(n+1)$. Then

$$\varphi'(0) = \psi'(1) = a_1, \qquad \varphi'(n+1) = \psi'(n+2) = \psi'(n+1)a_{n+2} = \varphi'(n)a_{n+2} = f_n(\varphi'(n)).$$

Hence φ' satisfies the same recursion as φ, so by the Recursion Theorem $\varphi' = \varphi$, and therefore $\psi' = \varphi' \circ \theta = \varphi \circ \theta = \psi$. Thus ψ is unique.

Finally, by construction $\psi(n) = a_1 a_2 \cdots a_n$, i.e. the standard product $\prod_{i=1}^{n} a_i$.