Solutions to *Algebra* by Thomas W. Hungerford

Steven Sabean

January 11, 2026

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 $s_1, \ldots, s_n$, set

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

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 $j_0 < \cdots < j_k$, 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) $.a_1a_2\ldots$ 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 $d_{nk} \in \{0,1,\ldots,9\}$. 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) $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$ and all $a, b \in G$; (v) $(ab)^n = a^n b^n$ 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 $n \geq 0$,

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

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

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

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 $b^0 a b^{-0} = a$, 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

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

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

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

(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

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

completing the induction.

Therefore $b^j a b^{-j} = a^{r^j}$ 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 $\psi(1) = a_1$, $\psi(2) = a_1 a_2$, $\psi(3) = (a_1 a_2) a_3$ 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 $x \mapsto x a_{n+2}$ 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

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

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 $\prod_{i=1}^{n} a_i$.

1.2 Homomorphisms and Subgroups

Exercise 1. *If $f : G \to H$ is a homomorphism of groups, then $f(e_G) = e_H$ and $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$. Show by example that the first conclusion may be false if G, H are monoids that are not groups.*

Solution. Let $f : G \to H$ be a group homomorphism.

(1) $f(e_G) = e_H$**.** Since $e_G e_G = e_G$, applying f and using the homomorphism property gives

$$f(e_G) = f(e_G e_G) = f(e_G)f(e_G).$$

Multiply on the left by $f(e_G)^{-1}$ (which exists because H is a group) to obtain $e_H = f(e_G)$. Hence $f(e_G) = e_H$.

(2) $f(a^{-1}) = f(a)^{-1}$ **for all** $a \in G$**.** We have $aa^{-1} = e_G$. Applying f gives

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(e_G) = e_H.$$

Thus $f(a^{-1})$ is an inverse of $f(a)$, so $f(a^{-1}) = f(a)^{-1}$.

Monoid counterexample. The conclusion $f(e_G) = e_H$ can fail for homomorphisms of monoids that are not groups, because cancellation/inverses need not exist in the codomain.

Let $G = (\mathbb{N}, \cdot)$ with identity 1, and let $H = (\mathbb{N}, \cdot)$ with identity 1. Define $f(n) = 0$ for all n. Then $f(mn) = 0 = 0 \cdot 0 = f(m)f(n)$, so f is a monoid homomorphism, but

$$f(e_G) = f(1) = 0 \neq 1 = e_H.$$

Thus $f(e_G) = e_H$ may fail for monoids that are not groups.

Exercise 2. *A group G is abelian if and only if the map $G \to G$ given by $x \mapsto x^{-1}$ is an automorphism.*

Solution. Define $\iota : G \to G$ by $\iota(x) = x^{-1}$.

(⇒) If G is abelian, then for all $x, y \in G$,

$$\iota(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \iota(x)\iota(y),$$

so ι is a homomorphism. Since $\iota \circ \iota = \mathrm{id}_G$, it is bijective. Hence ι is an automorphism.

(⇐) If ι is an automorphism, then it is a homomorphism, so

$$(xy)^{-1} = \iota(xy) = \iota(x)\iota(y) = x^{-1}y^{-1} \qquad (\forall x, y \in G).$$

By Exercise 11 of §1.1 (equivalent conditions for a group to be abelian), the identity $(xy)^{-1} = x^{-1}y^{-1}$ for all x, y implies that G is abelian.

Therefore G is abelian if and only if $x \mapsto x^{-1}$ is an automorphism.

Exercise 3. *Let Q_8 be the group (under ordinary matrix multiplication) generated by the complex matrices $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, where $i^2 = -1$. Show that Q_8 is a nonabelian group of order* 8. *Q_8 is called the **quaternion group**. [*Hint*: Observe that $BA = A^3B$, whence every element of Q_8 is of the form A^iB^j Note also that $A^4 = B^4 = I$, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element of Q_8.]*

Solution. Let

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \qquad (i^2 = -1),$$

and let $Q_8 = \langle A, B \rangle \leq GL_2(\mathbb{C})$.

Step 1: Use Theorem 2.8 to describe elements of $\langle A, B \rangle$. By Theorem 2.8, the subgroup $\langle A, B \rangle$ consists of all finite products in which the factors are powers of A and B, i.e. every element of Q_8 can be written as a word of the form

$$A^{m_1}B^{n_1}A^{m_2}B^{n_2} \cdots A^{m_t}B^{n_t}, \qquad (m_k, n_k \in \mathbb{Z}).$$

Step 2: Basic relations. Direct computation gives

$$A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I \quad \Rightarrow \quad A^4 = I,$$

$$B^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I \quad \Rightarrow \quad B^4 = I.$$

Also

$$AB = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad BA = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = -AB.$$

Since $A^3 = -A$, we have $A^3B = -(AB) = BA$; hence

$$BA = A^3B. \tag{1.3}$$

Step 3: Normal form A^iB^j with $0 \le i \le 3$, $j \in \{0,1\}$. Using (1.3), we can move any B past any A to the right at the cost of replacing A by $A^3 = A^{-1}$. Repeating this process, any word

$$A^{m_1}B^{n_1} \cdots A^{m_t}B^{n_t}$$

can be rewritten as A^iB^j for some integers i, j. Reducing exponents modulo 4 using $A^4 = B^4 = I$, we may assume $0 \le i \le 3$ and $0 \le j \le 3$. But since $B^2 = -I = A^2$, we have

$$A^iB^j = \begin{cases} A^i, & j \equiv 0 \pmod 2, \\ A^iB, & j \equiv 1 \pmod 2, \end{cases}$$

so in fact every element is of the form A^iB^j with $0 \le i \le 3$ and $j \in \{0,1\}$. Hence $|Q_8| \le 8$.

Step 4: There are at least eight distinct elements. The eight matrices

$$I,\ A,\ A^2 = -I,\ A^3 = -A,\ B,\ AB,\ A^2B = -B,\ A^3B = -AB$$

are all distinct. Indeed, the first four have only real entries, whereas $B, AB, -B, -AB$ have nonreal entries, so no A^i can equal any A^kB. Also $B \ne -B$, $AB \ne -AB$, and $B \ne \pm AB$ since B is off-diagonal while AB is diagonal. Thus $|Q_8| \ge 8$.

Combining with $|Q_8| \le 8$, we conclude $|Q_8| = 8$, and

$$Q_8 = \{\pm I,\ \pm A,\ \pm B,\ \pm AB\}.$$

Step 5: Nonabelian. Since $BA = -AB$ and $AB \ne BA$, the group Q_8 is not abelian.

Therefore Q_8 is a nonabelian group of order 8.

Exercise 4. *Let H be the group (under matrix multiplication) of real matrices generated by $C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Show that $H$is a nonabelian group of order 8 which is not isomorphic to the quaternion group of Exercise 3, but is isomorphic to the group ${D_4}^*$.*

Solution. Let

$$C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

and let $H = \langle C, D \rangle \le GL_2(\mathbb{R})$.

Step 1: Relations and a normal form. A direct computation gives

$$C^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I \quad \Rightarrow \quad C^4 = I, \qquad D^2 = I.$$

Also

$$DC = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad CD = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

so $DC = -CD$. Since $C^3 = -C$, we have

$$C^{-1} = C^3 = -C,$$

and hence

$$DCD = -C = C^{-1}.$$

Equivalently,

$$DC = C^{-1}D. \tag{1.4}$$

Using (1.4), any word in C and D can be rewritten by moving each D to the right at the cost of inverting a power of C. By Theorem 2.8, every element of H is a finite product of powers of C and D, hence every element can be written in the form C^iD^j with $i \in \mathbb{Z}$, $j \in \{0, 1\}$. Using $C^4 = I$, we may assume $0 \le i \le 3$. Therefore

$$H \subset \{\, C^iD^j : 0 \le i \le 3,\ j \in \{0, 1\} \,\},$$

so $|H| \le 8$.

Step 2: There are eight distinct elements and H is nonabelian. The matrices

$$I,\ C,\ C^2 = -I,\ C^3 = -C,\ D,\ CD,\ C^2D = -D,\ C^3D = -CD$$

are all distinct (for instance, D is symmetric while CD is diagonal). Hence $|H| \ge 8$, so $|H| = 8$. Moreover $CD \ne DC$ (indeed $DC = -CD$), so H is nonabelian.

Step 3: H is not isomorphic to Q_8. In H, the element $D \ne I$ satisfies $D^2 = I$, so H has an element of order 2. In the quaternion group $Q_8 = \{\pm I, \pm A, \pm B, \pm AB\}$, the only element of order 2 is $-I$; all other nonidentity elements have order 4. Therefore $H \nsim Q_8$, since an isomorphism preserves element orders.

Step 4: $H \sim {D_4}^*$. Let ${D_4}^* = \langle r, s \mid r^4 = e,\ s^2 = e,\ srs = r^{-1} \rangle$ be the dihedral group of order 8. Define a map $\varphi : {D_4}^* \to H$ on generators by

$$\varphi(r) = C, \qquad \varphi(s) = D.$$

The defining relations are satisfied in H:

$$\varphi(r)^4 = C^4 = I, \qquad \varphi(s)^2 = D^2 = I, \qquad \varphi(s)\varphi(r)\varphi(s) = DCD = C^{-1} = \varphi(r)^{-1}.$$

Hence φ extends to a well-defined homomorphism ${D_4}^* \to H$. Its image contains C and D, so it contains $\langle C, D \rangle = H$; thus φ is surjective. Since $|{D_4}^*| = 8 = |H|$, a surjective homomorphism between finite groups of the same order is injective. Therefore φ is an isomorphism, and $H \sim {D_4}^*$.

Thus H is a nonabelian group of order 8, not isomorphic to Q_8, but isomorphic to ${D_4}^*$.

Exercise 5. *Let S be a nonempty subset of a group G and define a relation on G by $a \sim b$ if and only if $ab^{-1} \in S$. Show that $\sim$ is an equivalence relation if and only if S is a subgroup of G.*

Solution. Let S be a nonempty subset of a group G, and define a relation on G by

$$a \sim b \iff ab^{-1} \in S.$$

(⇒) Assume $\sim$ is an equivalence relation. We show that S is a subgroup of G.

Since $\sim$ is reflexive, for every $a \in G$ we have $a \sim a$, hence $aa^{-1} = e \in S$. In particular, S is nonempty and contains the identity.

Let $x, y \in S$. Because $x \in S$, we have $x \sim e$; because $y \in S$, we have $y \sim e$. Since $\sim$ is symmetric, $e \sim y$, and since it is transitive,

$$x \sim e \text{ and } e \sim y \implies x \sim y.$$

Thus $xy^{-1} \in S$.

Therefore S is nonempty and satisfies $xy^{-1} \in S$ for all $x, y \in S$. By Theorem 2.5, S is a subgroup of G.

(⇐) Conversely, assume S is a subgroup of G. We verify that $\sim$ is an equivalence relation.

- *Reflexive:* For any $a \in G$, $aa^{-1} = e \in S$, so $a \sim a$.
- *Symmetric:* If $a \sim b$, then $ab^{-1} \in S$. Since S is a subgroup, $(ab^{-1})^{-1} = ba^{-1} \in S$, so $b \sim a$.
- *Transitive:* If $a \sim b$ and $b \sim c$, then $ab^{-1} \in S$ and $bc^{-1} \in S$. Since S is a subgroup,

  $$(ab^{-1})(bc^{-1}) = ac^{-1} \in S,$$

  so $a \sim c$.

Thus $\sim$ is an equivalence relation.

Hence $\sim$ is an equivalence relation on G if and only if S is a subgroup of G.

Exercise 6. *A nonempty finite subset of a group is a subgroup if and only if it is closed under the product in G.*

Solution. Let H be a nonempty finite subset of a group G.

(⇒) If H is a subgroup of G, then it is closed under the product in G by definition.

(⇐) Conversely, assume H is closed under the product in G. We show that H is a subgroup.

Fix $a \in H$. Consider the map $L_a : H \to H$ given by $L_a(x) = ax$. Closure under products implies L_a is well defined. Moreover, L_a is injective: if $ax = ay$, then by left cancellation in G we have $x = y$. Since H is finite, L_a is surjective. Therefore there exists $e \in H$ such that $L_a(e) = ae = a$. Cancelling a on the left gives $e = e_G$, so $e_G \in H$.

Next, since L_a is surjective and $e_G \in H$, there exists $b \in H$ such that $ab = e_G$. Then $b = a^{-1}$. Hence $a^{-1} \in H$ for every $a \in H$.

Now H is nonempty, closed under products, contains e_G, and contains inverses; therefore H is a subgroup of G.

(Equivalently, one may apply Theorem 2.5: since $a^{-1} \in H$, we have $ab^{-1} \in H$ for all $a, b \in H$, so $H \leq G$.)

Exercise 7. *If n is a fixed integer, then $\{kn \mid k \in \mathbb{Z}\} \subset \mathbb{Z}$ is an additive subgroup of $\mathbb{Z}$, which is isomorphic to $\mathbb{Z}$.*

Solution. Fix an integer n and let

$$n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\} \subset \mathbb{Z}.$$

Subgroup. The set $n\mathbb{Z}$ is nonempty since $0 = 0 \cdot n \in n\mathbb{Z}$. If $kn, \ell n \in n\mathbb{Z}$, then

$$kn + \ell n = (k + \ell)n \in n\mathbb{Z}.$$

Also $-(kn) = (-k)n \in n\mathbb{Z}$. Hence $n\mathbb{Z}$ is a subgroup of the additive group $(\mathbb{Z}, +)$.

Isomorphism with $\mathbb{Z}$ (for $n \neq 0$). Assume $n \neq 0$. Define $\varphi : \mathbb{Z} \to n\mathbb{Z}$ by

$$\varphi(k) = kn.$$

Then φ is a homomorphism:

$$\varphi(k + \ell) = (k + \ell)n = kn + \ell n = \varphi(k) + \varphi(\ell).$$

It is surjective by definition of $n\mathbb{Z}$. If $\varphi(k) = \varphi(\ell)$, then $kn = \ell n$, so $(k - \ell)n = 0$. Since $n \neq 0$, it follows that $k - \ell = 0$, hence $k = \ell$. Thus φ is injective. Therefore φ is an isomorphism, and $n\mathbb{Z} \cong \mathbb{Z}$.

Remark (the case $n = 0$). If $n = 0$, then $n\mathbb{Z} = \{0\}$, the trivial subgroup, which is not isomorphic to $\mathbb{Z}$.

Exercise 8. *The set $\{\sigma \in S_n \mid \sigma(n) = n\}$ is a subgroup of S_n which is isomorphic to S_{n-1}.*

Solution. Let

$$H = \{\sigma \in S_n \mid \sigma(n) = n\}.$$

H is a subgroup of S_n.

The identity permutation satisfies $e(n) = n$, so $e \in H$, hence $H \neq \varnothing$. If $\sigma, \tau \in H$, then

$$(\sigma\tau)(n) = \sigma(\tau(n)) = \sigma(n) = n,$$

so $\sigma\tau \in H$. If $\sigma \in H$, then $\sigma(n) = n$ implies $\sigma^{-1}(n) = n$ (apply σ^{-1} to both sides), so $\sigma^{-1} \in H$. Thus $H < S_n$.

$H \sim S_{n-1}$.

Define a map

$$\varphi : H \to S_{n-1}$$

by restriction: for $\sigma \in H$, let $\varphi(\sigma)$ be the permutation of $\{1, 2, \ldots, n-1\}$ given by $\varphi(\sigma)(k) = \sigma(k)$. This is well defined: since $\sigma(n) = n$, the set $\{1, \ldots, n-1\}$ is σ-invariant, so $\sigma(k) \in \{1, \ldots, n-1\}$ whenever $k \leq n - 1$.

Moreover φ is a homomorphism because restriction commutes with composition:

$$\varphi(\sigma\tau)(k) = (\sigma\tau)(k) = \sigma(\tau(k)) = \varphi(\sigma)(\varphi(\tau)(k)) = (\varphi(\sigma)\varphi(\tau))(k).$$

It is injective: if $\varphi(\sigma) = \varphi(\tau)$, then $\sigma(k) = \tau(k)$ for all $k \le n-1$, and also $\sigma(n) = n = \tau(n)$, hence $\sigma = \tau$.

It is surjective: given any $\pi \in S_{n-1}$, define $\widetilde{\pi} \in S_n$ by

$$\widetilde{\pi}(k) = \pi(k) \ (1 \le k \le n-1), \qquad \widetilde{\pi}(n) = n.$$

Then $\widetilde{\pi} \in H$ and $\varphi(\widetilde{\pi}) = \pi$.

Thus φ is a bijective homomorphism, so $H \sim S_{n-1}$.

Exercise 9. *Let $f : G \to H$ be a homomorphism of groups, A a subgroup of G, and B a subgroup of H.*

(a) Ker f *and $f^{-1}(B)$ are subgroups of G.*

(b) $f(A)$ is a subgroup of H.

Solution. Let $f : G \to H$ be a group homomorphism, $A < G$, and $B < H$.

(a) **Ker f and $f^{-1}(B)$ are subgroups of G.**

Recall $\operatorname{Ker} f = \{g \in G : f(g) = e_H\}$. It is nonempty since $f(e_G) = e_H$, so $e_G \in \operatorname{Ker} f$. If $x, y \in \operatorname{Ker} f$, then

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)\, f(y)^{-1} = e_H e_H^{-1} = e_H,$$

so $xy^{-1} \in \operatorname{Ker} f$. By Theorem 2.5, $\operatorname{Ker} f < G$.

Next, $f^{-1}(B) = \{g \in G : f(g) \in B\}$ is nonempty since $e_H \in B$ and $e_G \in f^{-1}(B)$. If $x, y \in f^{-1}(B)$, then $f(x), f(y) \in B$, and since $B \le H$,

$$f(xy^{-1}) = f(x)f(y)^{-1} \in B.$$

Hence $xy^{-1} \in f^{-1}(B)$. By Theorem 2.5, $f^{-1}(B) < G$.

(b) **$f(A)$ is a subgroup of H.**

First, $f(A) \neq \varnothing$ since $e_G \in A$ implies $e_H = f(e_G) \in f(A)$. Let $u, v \in f(A)$. Then $u = f(a)$ and $v = f(b)$ for some $a, b \in A$. Since $A \le G$, we have $ab^{-1} \in A$. Therefore

$$uv^{-1} = f(a)\, f(b)^{-1} = f(a)\, f(b^{-1}) = f(ab^{-1}) \in f(A).$$

By Theorem 2.5 (applied in H), it follows that $f(A) < H$.

Exercise 10. *List all subgroups of $Z_2 \oplus Z_2$. Is $Z_2 \oplus Z_2$ isomorphic to Z_4?*

Solution. Write $V = Z_2 \oplus Z_2 = \{(0,0), (1,0), (0,1), (1,1)\}$ under componentwise addition mod 2.

Subgroups. Every subgroup of V must contain $(0,0)$. Also, since every nonidentity element has order 2, any subgroup generated by a nonzero element has exactly two elements.

Thus the subgroups are:

$$\{(0,0)\},$$

$$\langle(1,0)\rangle = \{(0,0),(1,0)\}, \qquad \langle(0,1)\rangle = \{(0,0),(0,1)\}, \qquad \langle(1,1)\rangle = \{(0,0),(1,1)\},$$

and the whole group

$$V = \{(0,0),(1,0),(0,1),(1,1)\}.$$

There are no other subgroups: any subgroup containing two distinct nonzero elements contains their sum as well, hence all three nonzero elements, and so it must be all of V.

Is $Z_2 \oplus Z_2 \sim Z_4$? No. In $Z_2 \oplus Z_2$, every nonidentity element has order 2. But Z_4 has an element of order 4 (namely $\bar{1}$). Since an isomorphism preserves element orders, $Z_2 \oplus Z_2$ cannot be isomorphic to Z_4.

Exercise 11. *If G is a group, then $C = \{a \in G \mid ax = xa \text{ for all } x \in G\}$ is an abelian subgroup of G. C is called the* ***center*** *of G.*

Solution. Let

$$C = \{a \in G \mid ax = xa \text{ for all } x \in G\}.$$

C is a subgroup of G. First, $e \in C$ since $ex = xe = x$ for all $x \in G$; hence $C \neq \varnothing$. Let $a, b \in C$. For any $x \in G$,

$$(ab^{-1})x = a(b^{-1}x) = a(xb^{-1}) = (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1}),$$

using that a and b commute with every element of G. Thus $ab^{-1} \in C$. By Theorem 2.5, $C < G$.

C is abelian. If $a, b \in C$, then a commutes with every element of G, in particular with b; hence $ab = ba$. Therefore C is abelian.

Thus C is an abelian subgroup of G, called the *center* of G.

Exercise 12. *The group D_4^* is not cyclic, but can be generated by two elements. The same is true of S_n (nontrivial). What is the minimal number of generators of the additive group $\mathbb{Z} \oplus \mathbb{Z}$?*

Solution. We claim that the additive group $\mathbb{Z} \oplus \mathbb{Z}$ has minimal number of generators equal to 2.

(1) Two generators suffice. Let $e_1 = (1,0)$ and $e_2 = (0,1)$. Then every $(m,n) \in \mathbb{Z} \oplus \mathbb{Z}$ can be written as

$$(m,n) = m(1,0) + n(0,1) = me_1 + ne_2,$$

so $\mathbb{Z} \oplus \mathbb{Z} = \langle e_1, e_2 \rangle$.

(2) One generator does not suffice. If $\mathbb{Z} \oplus \mathbb{Z}$ were generated by a single element v, then it would be cyclic, i.e. $\mathbb{Z} \oplus \mathbb{Z} = \langle v \rangle$. But any cyclic subgroup generated by $v = (a,b)$ is

$$\langle(a,b)\rangle = \{k(a,b) : k \in \mathbb{Z}\},$$

which lies on the line through the origin of slope b/a (or the y-axis if $a = 0$). In particular, it cannot contain both $(1,0)$ and $(0,1)$. Hence $\mathbb{Z} \oplus \mathbb{Z}$ is not cyclic.

Therefore at least two generators are necessary.

Combining (1) and (2), the minimal number of generators of $\mathbb{Z} \oplus \mathbb{Z}$ is 2.

Exercise 13. *If $G = \langle a \rangle$ is a cyclic group and H is any group, then every homomorphism $f : G \to H$ is completely determined by the element $f(a) \in H$.*

Solution. Let $G = \langle a \rangle$ be cyclic and let $f : G \to H$ be a homomorphism.

Every element of G has the form a^n for some $n \in \mathbb{Z}$. Using the homomorphism property and induction on $n \geq 0$, we have

$$f(a^n) = f(a)^n \qquad (n \geq 0).$$

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

$$f(a^n) = f(a^{-m}) = f(a^{-1})^m = f(a)^{-m} = f(a)^n,$$

using $f(a^{-1}) = f(a)^{-1}$. Hence

$$f(a^n) = f(a)^n \qquad \text{for all } n \in \mathbb{Z}.$$

Therefore, for any $g \in G$ with $g = a^n$,

$$f(g) = f(a^n) = f(a)^n,$$

so the value of f on all of G is determined uniquely by the single element $f(a) \in H$.

Exercise 14. *The following cyclic subgroups are all isomorphic: the multiplicative group $\langle i \rangle$ in $\mathbb{C}$, the additive group Z_4 and the subgroup $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \right\rangle$ of S_4.*

Solution. Each of the three groups listed is cyclic of order 4, hence all three are isomorphic to Z_4. We verify this explicitly.

(1) $\langle i \rangle < \mathbb{C}^\times$.

Since $i^4 = 1$ and the powers are

$$i^0 = 1, \quad i^1 = i, \quad i^2 = -1, \quad i^3 = -i, \quad i^4 = 1,$$

the subgroup $\langle i \rangle = \{1, i, -1, -i\}$ has 4 elements, so $|\langle i \rangle| = 4$. Thus $\langle i \rangle \sim Z_4$ via

$$\phi : Z_4 \to \langle i \rangle, \qquad \phi(\overline{k}) = i^k,$$

which is a well-defined isomorphism (additive in Z_4, multiplicative in $\langle i \rangle$).

(2) The subgroup generated by a 4-cycle in S_4.

Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1\,2\,3\,4).$$

Then

$$\sigma^2 = (1\,3)(2\,4), \qquad \sigma^3 = (1\,4\,3\,2), \qquad \sigma^4 = e,$$

and $\sigma^k \neq e$ for $1 \leq k \leq 3$. Hence $|\langle \sigma \rangle| = 4$, so $\langle \sigma \rangle \sim Z_4$ via

$$\psi : Z_4 \to \langle \sigma \rangle, \qquad \psi(\overline{k}) = \sigma^k,$$

which is a well-defined isomorphism.

Conclusion.

Since $\langle i \rangle \sim Z_4$ and $\langle \sigma \rangle \sim Z_4$, it follows that all three cyclic groups are isomorphic.

Exercise 15. *Let G be a group and* $\operatorname{Aut} G$ *the set of all automorphisms of* G*.*

(a) $\operatorname{Aut} G$ *is a group with composition of functions as binary operation. [*Hint*: $1_G \in \operatorname{Aut} G$ is an identity; inverses exist by Theorem 2.3.]*

(b) $\operatorname{Aut} \mathbb{Z} \sim Z_2$ *and* $\operatorname{Aut} Z_6 \sim Z_2$*;* $\operatorname{Aut} Z_8 \sim Z_2 \oplus Z_2$*;* $\operatorname{Aut} Z_p \sim Z_{p-1}$ *(p prime).*

(c) *What is* $\operatorname{Aut} Z_n$ *for arbitrary* $n \in \mathbb{N}^*$*?*

Solution. Let G be a group and $\operatorname{Aut}(G)$ the set of all automorphisms of G.

(a) $\operatorname{Aut}(G)$ **is a group under composition.**

Composition of functions is associative. The identity map $1_G : G \to G$ is an automorphism and serves as the identity element. If $\varphi \in \operatorname{Aut}(G)$, then φ is bijective, so it has an inverse function φ^{-1}; by Theorem 2.3 (inverse of an isomorphism is an isomorphism), φ^{-1} is also an automorphism. Hence every element has an inverse in $\operatorname{Aut}(G)$, so $\operatorname{Aut}(G)$ is a group.

(b) **Examples.**

General fact for cyclic groups. Let $C = \langle a \rangle$ be cyclic of order n. Any homomorphism $f : C \to C$ is determined by $f(a) = a^k$. Moreover, f is an automorphism iff $f(a)$ is a generator of C, i.e. iff $\gcd(k, n) = 1$. Thus

$$\operatorname{Aut}(C) \ \sim\ (\mathbb{Z}/n\mathbb{Z})^\times,$$

via $k \mapsto (a \mapsto a^k)$.

Applying this:

- $\operatorname{Aut}(\mathbb{Z}) \sim \{\pm 1\} \sim Z_2$, since an automorphism is determined by $f(1) \in \mathbb{Z}$, and surjectivity forces $f(1) = \pm 1$.
- $\operatorname{Aut}(Z_6) \sim (\mathbb{Z}/6\mathbb{Z})^\times = \{\overline{1}, \overline{5}\} \sim Z_2$.
- $\operatorname{Aut}(Z_8) \sim (\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\} \sim Z_2 \oplus Z_2$, since each nontrivial element has order 2 (e.g. $\overline{3}^2 = \overline{1}$, $\overline{5}^2 = \overline{1}$, $\overline{7}^2 = \overline{1}$).
- If p is prime, then $\operatorname{Aut}(Z_p) \sim (\mathbb{Z}/p\mathbb{Z})^\times$, which is cyclic of order $p-1$. Hence $\operatorname{Aut}(Z_p) \sim Z_{p-1}$.

(c) $\operatorname{Aut}(Z_n)$ **for arbitrary** $n \in \mathbf{N}^*$**.**

Let $Z_n = \langle \overline{1} \rangle$. Any homomorphism $f : Z_n \to Z_n$ is determined by $f(\overline{1}) = \overline{k}$, and then $f(\overline{m}) = \overline{km}$. Such an f is an automorphism iff $\overline{k}$ is a generator of the additive cyclic group Z_n, i.e. iff $\gcd(k, n) = 1$. Therefore

$$\operatorname{Aut}(Z_n) \ \sim\ (\mathbb{Z}/n\mathbb{Z})^\times,$$

the multiplicative group of units modulo n.

In particular,

$$|\operatorname{Aut}(Z_n)| = \varphi(n),$$

Euler's totient function.

(*Optional structure remark.* Using the Chinese remainder theorem and the decomposition $n = \prod p_i^{e_i}$, one gets $(\mathbb{Z}/n\mathbb{Z})^\times \sim \prod (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$, so $\operatorname{Aut}(Z_n)$ reduces to understanding prime powers.)

Exercise 16. *For each prime p the additive subgroup $Z(p^\infty)$ of $\mathbb{Q}/\mathbb{Z}$ (Exercise 1.10) is generated by the set $\{\overline{1/p^n} \mid n \in \mathbb{N}^*\}$.*

Solution. Fix a prime p. Recall

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

Let

$$S = \left\{\overline{1/p^n} \;\middle|\; n \in \mathbb{N}^*\right\} \subset Z(p^\infty).$$

We show that $\langle S \rangle = Z(p^\infty)$.

($\subset$). Since $S \subset Z(p^\infty)$ and $Z(p^\infty)$ is a subgroup of $\mathbb{Q}/\mathbb{Z}$, it follows that $\langle S \rangle \subset Z(p^\infty)$.

($\supset$). Let $\overline{a/p^i} \in Z(p^\infty)$ be arbitrary. If $a \geq 0$, then in the additive group $\mathbb{Q}/\mathbb{Z}$,

$$\overline{\frac{a}{p^i}} = \underbrace{\overline{\frac{1}{p^i}} + \cdots + \overline{\frac{1}{p^i}}}_{a \text{ times}} = a\,\overline{\frac{1}{p^i}} \in \langle S \rangle.$$

If $a < 0$, write $a = -m$ with $m > 0$. Then

$$\overline{\frac{a}{p^i}} = -\,\overline{\frac{m}{p^i}}$$

and $\overline{m/p^i} \in \langle S \rangle$ by the previous case, hence $\overline{a/p^i} \in \langle S \rangle$ as well (subgroups are closed under additive inverses).

Thus every element of $Z(p^\infty)$ lies in $\langle S \rangle$, so $Z(p^\infty) \subset \langle S \rangle$.

Therefore $\langle \overline{1/p^n} \mid n \in \mathbb{N}^* \rangle = Z(p^\infty)$.

Exercise 17. *Let G be an abelian group and let H, K be subgroups of G. Show that the join $H \vee K$ is the set $\{ab \mid a \in H, b \in K\}$. Extend this result to any finite number of subgroups of G.*

Solution. Let G be an abelian group and let $H, K < G$. Recall that the join $H \vee K$ is the subgroup of G generated by $H \cup K$, i.e. $H \vee K = \langle H \cup K \rangle$.

Set

$$S = \{ab \mid a \in H,\ b \in K\}.$$

We show $H \vee K = S$.

Step 1: S is a subgroup of G. Clearly $e = e \cdot e \in S$, so $S \neq \varnothing$. If $a_1b_1, a_2b_2 \in S$ with $a_i \in H$, $b_i \in K$, then (using that G is abelian)

$$(a_1b_1)(a_2b_2)^{-1} = (a_1b_1)(b_2^{-1}a_2^{-1}) = a_1a_2^{-1}\,b_1b_2^{-1} \in HK,$$

since $a_1a_2^{-1} \in H$ and $b_1b_2^{-1} \in K$. Hence S is closed under xy^{-1}, so by Theorem 2.5 it is a subgroup of G.

Step 2: $H \vee K \subset S$. Since $H \subset S$ (take $b = e$) and $K \subset S$ (take $a = e$), we have $H \cup K \subset S$. Because S is a subgroup, it contains the subgroup generated by $H \cup K$, i.e. $H \vee K = \langle H \cup K \rangle \subset S$.

Step 3: $S \subset H \vee K$**.** If $a \in H$ and $b \in K$, then $a \in H \vee K$ and $b \in H \vee K$, hence $ab \in H \vee K$. Therefore $S \subset H \vee K$.

Combining Steps 2 and 3 gives $H \vee K = S = \{ab \mid a \in H,\ b \in K\}$.

Finite extension. Let $H_1, \ldots, H_m < G$. Define

$$S_m = \{a_1 a_2 \cdots a_m \mid a_i \in H_i\}.$$

By the same argument (or by induction using the two-subgroup case), S_m is a subgroup of G containing each H_i, hence it contains the join $\bigvee_{i=1}^m H_i$. Conversely, every element of S_m is a product of elements from the H_i, so it lies in the subgroup generated by $\bigcup_i H_i$, i.e. in $\bigvee_i H_i$. Thus

$$\bigvee_{i=1}^{m} H_i \;=\; \{a_1 a_2 \cdots a_m \mid a_i \in H_i\}.$$

Exercise 18. *(a) Let G be a group and $\{H_i \mid i \in I\}$ a family of subgroups. State and prove a condition that will imply that $\bigcup_{i \in I} H_i$ is a subgroup, that is, that $\bigcup_{i\in I} H_i = \langle \bigcup_{i \in I} H_i \rangle$.*

(b) Give an example of a group G and a family of subgroups $\{H_i \mid i \in I\}$ such that $\bigcup_{i\in I} H_i \neq \langle \bigcup_{i\in I} H_i \rangle$.

Solution. (a) A sufficient (and standard) condition is that the family $\{H_i \mid i \in I\}$ be *linearly ordered by inclusion*: for all $i, j \in I$, either $H_i \subset H_j$ or $H_j \subset H_i$. (That is, the family forms an ascending chain.)

Assume this condition. Let

$$H = \bigcup_{i \in I} H_i.$$

We show that $H < G$. Clearly $H \neq \varnothing$ since each H_i is nonempty. Let $a, b \in H$. Then $a \in H_i$ and $b \in H_j$ for some $i, j \in I$. By the chain condition, we may assume $H_i \subset H_j$ (after possibly interchanging i and j). Then $a, b \in H_j$, so

$$ab^{-1} \in H_j \subset H.$$

Hence H is closed under ab^{-1}. By Theorem 2.5, H is a subgroup of G. In particular, $H = \langle H \rangle = \langle \bigcup_{i\in I} H_i \rangle$.

(b) Example where the union is not a subgroup: take $G = \mathbb{Z}$ (additively), $H_1 = 2\mathbb{Z}$, $H_2 = 3\mathbb{Z}$. Then

$$H_1 \cup H_2 = 2\mathbb{Z} \cup 3\mathbb{Z}$$

is not a subgroup, since $2 \in H_1$ and $3 \in H_2$, but $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$. On the other hand, $\langle 2\mathbb{Z} \cup 3\mathbb{Z} \rangle = \mathbb{Z}$, because $1 = 3 - 2$ lies in the subgroup generated by 2 and 3. Thus

$$\bigcup_{i \in \{1,2\}} H_i \neq \left\langle \bigcup_{i \in \{1,2\}} H_i \right\rangle.$$

Exercise 19. *(a) The set of all subgroups of a group G, partially ordered by set theoretic inclusion, forms a complete lattice (Introduction, Exercises 7.1 and 7.2) in which the g.l.b. of $\{H_i \mid i \in I\}$ is $\bigcap_{i\in I} H_i$ and the l.u.b. is $\langle \bigcup_{i\in I} H_i \rangle$.*

(b) Exhibit the lattice of subgroups of the groups S_3, $D_4{}^*$, Z_6, Z_{27}, and Z_{36}.

Solution. (a) Let $\mathrm{Sub}(G)$ be the set of all subgroups of G, ordered by inclusion.

Greatest lower bounds. If $\{H_i \mid i \in I\} \subset \mathrm{Sub}(G)$, then $\bigcap_{i\in I} H_i$ is a subgroup (nonempty since it contains e, and closed under ab^{-1} because each H_i is). It is a lower bound, and if K is any subgroup with $K \subset H_i$ for all i, then $K \subset \bigcap_i H_i$. Hence

$$\mathrm{g.\,l.\,b.}\{H_i\} = \bigcap_{i\in I} H_i.$$

Least upper bounds. Let $U = \bigcup_{i\in I} H_i$. Any upper bound K of the family satisfies $H_i \subset K$ for all i, hence $U \subset K$. Since K is a subgroup containing U, it contains the subgroup generated by U, i.e. $\langle U \rangle \subset K$. Thus $\langle U \rangle$ is the least upper bound:

$$\mathrm{l.\,u.\,b.}\{H_i\} = \left\langle \bigcup_{i\in I} H_i \right\rangle.$$

Therefore $\mathrm{Sub}(G)$ is a complete lattice with meet $\wedge = \cap$ and join $\vee = \langle \cup \rangle$.

(b) Below are the subgroup lattices (given as Hasse-diagram descriptions). Vertices are subgroups; an edge indicates *covering* (no subgroup strictly in between).

(1) S_3. Subgroups:

$$\{e\}, \quad \langle(12)\rangle,\ \langle(13)\rangle,\ \langle(23)\rangle \text{ (order 2)}, \quad A_3 = \langle(123)\rangle \text{ (order 3)}, \quad S_3.$$

Inclusions (covers):

$$\{e\} \lessdot \langle(12)\rangle,\ \langle(13)\rangle,\ \langle(23)\rangle,\ A_3, \qquad \langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle,\ A_3 \lessdot S_3.$$

(2) $D_4{}^*$ (order 8). Use the standard presentation $D_4{}^* = \langle r, s \mid r^4 = e,\ s^2 = e,\ srs = r^{-1}\rangle$. Subgroups (10 total):

$$\{e\},\ \langle r^2 \rangle;$$

four reflection subgroups of order 2:

$$\langle s \rangle,\ \langle sr \rangle,\ \langle sr^2 \rangle,\ \langle sr^3 \rangle;$$

one cyclic subgroup of order 4:

$$\langle r \rangle = \{e, r, r^2, r^3\};$$

two Klein-four subgroups:

$$V_1 = \langle r^2, s \rangle = \{e, r^2, s, sr^2\}, \qquad V_2 = \langle r^2, sr \rangle = \{e, r^2, sr, sr^3\};$$

and $D_4{}^*$ itself.

Cover relations:

$$\{e\} \lessdot \langle r^2\rangle,\ \langle s\rangle,\ \langle sr\rangle,\ \langle sr^2\rangle,\ \langle sr^3\rangle;$$

$$\langle r^2\rangle \lessdot \langle r\rangle,\ V_1,\ V_2;$$

$$\langle s\rangle, \langle sr^2\rangle \lessdot V_1, \qquad \langle sr\rangle, \langle sr^3\rangle \lessdot V_2;$$

$$\langle r\rangle,\ V_1,\ V_2 \lessdot {D_4}^*.$$

(3) Z_6 **(additive).** Since Z_6 is cyclic, there is exactly one subgroup for each divisor of 6: orders $1, 2, 3, 6$. Concretely:

$$\{0\}, \quad \langle 3\rangle \text{ (order 2)}, \quad \langle 2\rangle \text{ (order 3)}, \quad Z_6.$$

This lattice has the two chains:

$$\{0\} \lessdot \langle 3\rangle \lessdot Z_6 \quad \text{and} \quad \{0\} \lessdot \langle 2\rangle \lessdot Z_6,$$

with $\langle 2\rangle$ and $\langle 3\rangle$ incomparable.

(4) Z_{27}**.** Divisors are $1, 3, 9, 27$, hence unique subgroups of these orders:

$$\{0\} \lessdot \langle 9\rangle \lessdot \langle 3\rangle \lessdot Z_{27}.$$

(Here $\langle 3\rangle$ has order 9, $\langle 9\rangle$ has order 3.)

(5) Z_{36}**.** Divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$, hence one subgroup of each order. A convenient label is H_d for the unique subgroup of order d. The cover relations (Hasse edges) correspond to *maximal* proper inclusions, i.e. $H_{d_1} \lessdot H_{d_2}$ when $d_1 \mid d_2$ and there is no divisor strictly between them.

Covers are:

$$H_1 \lessdot H_2,\ H_3;$$

$$H_2 \lessdot H_4,\ H_6; \qquad H_3 \lessdot H_6,\ H_9;$$

$$H_4 \lessdot H_{12}; \qquad H_6 \lessdot H_{12},\ H_{18}; \qquad H_9 \lessdot H_{18};$$

$$H_{12} \lessdot H_{36}; \qquad H_{18} \lessdot H_{36}.$$

(Equivalently, you can picture this as the divisor lattice of 36, turned upside down.)

1.3 Cyclic Groups

Exercise 1. *Let a, b be elements of group G. Show that $|a| = |a^{-1}|$; $|ab| = |ba|$, and $|a| = |cac^{-1}|$ for all $c \in G$.*

Solution. Let G be a group.

(1) $|a| = |a^{-1}|$**.** If $|a| = n < \infty$, then $a^n = e$, hence $(a^{-1})^n = (a^n)^{-1} = e$, so $|a^{-1}| \mid n$. Conversely, if $(a^{-1})^m = e$, then taking inverses gives $a^m = e$, so $|a| \mid m$. Thus $|a| = |a^{-1}|$. If $|a| = \infty$ and $(a^{-1})^n = e$ for some $n \geq 1$, then taking inverses gives $a^n = e$, a contradiction. Hence $|a^{-1}| = \infty$ as well.

(2) $|ab| = |ba|$**.** Note that

$$ba = a^{-1}(ab)a.$$

Thus ba is conjugate to ab. By part (3) below (applied with $c = a^{-1}$), conjugate elements have the same order, so $|ba| = |ab|$.

(3) $|a| = |cac^{-1}|$ **for all** $c \in G$**.** If $|a| = n < \infty$, then

$$(cac^{-1})^n = ca^n c^{-1} = cec^{-1} = e,$$

so $|cac^{-1}| \mid n$. Conversely, if $(cac^{-1})^m = e$, then

$$e = (cac^{-1})^m = ca^m c^{-1},$$

so $a^m = e$, hence $|a| \mid m$. Therefore $|cac^{-1}| = |a|$. If $|a| = \infty$, the same argument shows cac^{-1} cannot have finite order, so $|cac^{-1}| = \infty$.

Thus $|a| = |a^{-1}|$, $|ab| = |ba|$, and $|a| = |cac^{-1}|$ for all $c \in G$.

Exercise 2. *Let G be an abelian group containing elements a and b of orders m and n respectively. Show that G contains an element whose order is the least common multiple of m and n. [*Hint*: first try the case when $(m, n) = 1$.]*

Solution. Let G be abelian, and let $|a| = m$, $|b| = n$. Put

$$\ell = \operatorname{lcm}(m, n).$$

We will construct an element of order ℓ.

Lemma. If $x, y \in G$ commute and $|x| = r$, $|y| = s$ with $(r, s) = 1$, then $|xy| = rs$.

Proof. Since $xy = yx$, we have $(xy)^{rs} = x^{rs}y^{rs} = e$, so $|xy| \mid rs$. If $(xy)^k = e$, then $x^k = y^{-k}$, so $x^k \in \langle x \rangle \cap \langle y \rangle$. Any element of $\langle x \rangle \cap \langle y \rangle$ has order dividing both r and s, hence (since $(r, s) = 1$) must be e. Thus $x^k = e = y^k$, so $r \mid k$ and $s \mid k$, hence $rs \mid k$. Therefore $|xy| = rs$.

Now write the prime-power factorization

$$\ell = \prod_p p^{\gamma_p}, \qquad \gamma_p = \max\{v_p(m), v_p(n)\},$$

where the product is over the finitely many primes dividing ℓ.

For each such prime p, define an element $x_p \in G$ of order p^{γ_p} as follows. If $\gamma_p = v_p(m)$ (so $p^{\gamma_p} \mid m$), set

$$x_p = a^{m/p^{\gamma_p}}.$$

Then (in the cyclic subgroup $\langle a \rangle$) we have

$$|x_p| = \frac{m}{\gcd(m,\ m/p^{\gamma_p})} = \frac{m}{m/p^{\gamma_p}} = p^{\gamma_p}.$$

If instead $\gamma_p = v_p(n)$, set
$$x_p = b^{n/p^{\gamma_p}},$$
and the same computation gives $|x_p| = p^{\gamma_p}$.

Now define
$$x = \prod_{p|\ell} x_p.$$
Since G is abelian, all the x_p commute. Moreover, the orders $|x_p| = p^{\gamma_p}$ are pairwise relatively prime for distinct primes p. Applying the lemma repeatedly, we obtain
$$|x| = \prod_{p|\ell} |x_p| = \prod_{p|\ell} p^{\gamma_p} = \ell = \operatorname{lcm}(m,n).$$
Thus G contains an element of order $\operatorname{lcm}(m,n)$.

Exercise 3. *Let G be an abelian group of order pq, with $(p,q)=1$. Assume there exist $a,b \in G$ such that $|a| = p$, $|b| = q$ and show that G is cyclic.*

Solution. Let G be abelian with $|G| = pq$, where $(p,q)=1$, and suppose there exist elements $a,b \in G$ with $|a| = p$ and $|b| = q$.

Since G is abelian, a and b commute. By the coprime-order lemma (from the previous exercise), the element
$$x = ab$$
has order
$$|x| = |a||b| = pq.$$
Hence $\langle x\rangle$ is a cyclic subgroup of G of order pq. But $|\langle x\rangle| = |G|$, so $\langle x\rangle = G$.

Therefore G is cyclic.

Exercise 4. *If $f : G \to H$ is a homomorphism, $a \in G$, and $f(a)$ has finite order in H, then $|a|$ is infinite or $|f(a)|$ divides $|a|$.*

Solution. Let $f : G \to H$ be a homomorphism and let $a \in G$. Suppose $f(a)$ has finite order $|f(a)| = n$.

Then $(f(a))^n = e_H$, so
$$e_H = (f(a))^n = f(a^n).$$
Hence $a^n \in \operatorname{Ker} f$.

If $|a| = \infty$, we are done.

Otherwise $|a| = m < \infty$. Then $a^m = e_G$, and since $f(a^n) = e_H$, we have $f(a)^n = e_H$. By definition of order, n is the least positive integer with this property. But $f(a)^m = f(a^m) = e_H$ as well, so $n \mid m$. Therefore $|f(a)|$ divides $|a|$.

Thus $|a| = \infty$ or $|f(a)| \mid |a|$.

Exercise 5. *Let G be the multiplicative group of all nonsingular 2×2 matrices with rational entries. Show that $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ has order 4 and $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ has order 3, but ab has infinite order. Conversely, show that the additive group $Z_2 \oplus \mathbb{Z}$ contains nonzero elements a, b of infinite order such that $a+b$ has finite order.*

Solution. Let $G = GL_2(\mathbb{Q})$.

(1) The elements a and b. Let

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

Compute

$$a^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I, \qquad \text{so} \qquad a^4 = (a^2)^2 = (-I)^2 = I.$$

Since $a \neq I$ and $a^2 = -I \neq I$, it follows that $|a| = 4$.

Next let

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

A direct multiplication gives

$$b^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \qquad b^3 = b^2 b = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$$

Since $b \neq I$, we conclude $|b| = 3$.

(2) The element ab has infinite order. Compute

$$ab = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = u.$$

We claim $u^n \neq I$ for all $n \geq 1$. In fact one checks by induction that

$$u^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \qquad (n \in \mathbb{N}^*).$$

Indeed, for $n = 1$ this is u. If $u^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, then

$$u^{n+1} = u^n u = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}.$$

Since $n \neq 0$ for $n \geq 1$, we have $u^n \neq I$. Thus $|ab| = \infty$.

(3) In $Z_2 \oplus \mathbb{Z}$ we can have $|a| = |b| = \infty$ but $|a+b| < \infty$. Work in the additive group $Z_2 \oplus \mathbb{Z}$. Let

$$a = (\overline{1}, 1), \qquad b = (\overline{1}, -1).$$

Then for $k \in \mathbb{Z}$,

$$ka = (k\overline{1}, k) = (\overline{k}, k),$$

which equals $(\overline{0}, 0)$ only when $k = 0$. Hence $|a| = \infty$. Similarly $|b| = \infty$.

But

$$a + b = (\overline{1} + \overline{1},\, 1 + (-1)) = (\overline{0}, 0),$$

so $a + b$ has order 1 (finite).

Thus $GL_2(\mathbb{Q})$ contains torsion elements whose product has infinite order, while $Z_2 \oplus \mathbb{Z}$ contains infinite-order elements whose sum has finite order.

Exercise 6. *If G is a cyclic group of order n and $k|n$, then G has exactly one subgroup of order k.*

Solution. Let $G = \langle a \rangle$ be a cyclic group of order n, and let $k \mid n$.

Existence. Define
$$H = \langle a^{n/k} \rangle.$$
Since
$$|a^{n/k}| = \frac{n}{\gcd(n, n/k)} = \frac{n}{n/k} = k,$$
the subgroup H has order k.

Uniqueness. Let $K < G$ be any subgroup of order k. Since G is cyclic, every subgroup of G is cyclic, so $K = \langle a^m \rangle$ for some integer m. The order of a^m is
$$|a^m| = \frac{n}{\gcd(n, m)}.$$
Since $|K| = k$, we must have
$$\frac{n}{\gcd(n,m)} = k \quad \Longrightarrow \quad \gcd(n,m) = \frac{n}{k}.$$
This implies that m is a multiple of n/k, so
$$\langle a^m \rangle = \langle a^{n/k} \rangle.$$
Hence $K = H$.

Therefore G has exactly one subgroup of order k.

Exercise 7. *Let p be prime and H a subgroup of $Z(p^\infty)$ (Exercise 1.10).*

(a) *Every element of $Z(p^\infty)$ has finite order p^n for some $n \geq 0$.*

(b) *If at least one element of H has order p^k and no element of H has order greater than p^k, then H is the cyclic subgroup generated by $\overline{1/p^k}$, whence $H \cong Z_{p^k}$.*

(c) *If there is no upper bound on the orders of elements of H, then $H = Z(p^\infty)$; [see Exercise 2.16].*

(d) *The only proper subgroups of $Z(p^\infty)$ are the finite cyclic groups $C_n = \langle \overline{1/p^n} \rangle$ $(n = 1, 2, \ldots)$. Furthermore, $\langle 0 \rangle = C_0 < C_1 < C_2 < C_3 < \ldots$.*

(e) *Let $x_1, x_2, \ldots$ be elements of an abelian group G such that $|x_1| = p, px_2 = x_1, px_3 = x_2, \ldots, px_{n+1} = x_n, \ldots$. The subgroup generated by the x_i $(i \geq 1)$ is isomorphic to $Z(p^\infty)$. [Hint: Verify that the map induced by $x_i \mapsto \overline{1/p^i}$ is a well-defined isomorphism.]*

Solution. Fix a prime p. Recall
$$Z(p^\infty) = \left\{ \overline{a/p^i} \in \mathbb{Q}/\mathbb{Z} \mid a \in \mathbb{Z},\ i \geq 0 \right\},$$
and from Exercise 2.16 it is generated by $\{\overline{1/p^n} \mid n \geq 1\}$.

(a) Let $x = \overline{a/p^i} \in Z(p^\infty)$. Then
$$p^i x = \overline{a} = \overline{0},$$
so x has finite order dividing p^i. Hence $|x| = p^n$ for some $0 \le n \le i$. (In particular, $|\overline{0}| = p^0 = 1$.)

(b) Assume $H < \mathbb{Z}(p^\infty)$ contains an element of order p^k and no element of H has order $> p^k$. Let $x \in H$ have order p^k. In the cyclic group $\langle x \rangle$ there is a unique subgroup of order p^j for each $0 \le j \le k$, and in particular $\langle x \rangle$ contains an element of order p^j for each $j \le k$.

We claim $H = \langle x \rangle$. Suppose $y \in H$. Then $|y| = p^t$ for some $t \le k$ by (a). Consider the subgroup $\langle x \rangle$ of order p^k. Since $Z(p^\infty)$ has exactly one subgroup of order p^t, namely $\langle \overline{1/p^t} \rangle$ (by the cyclic-group result applied to $\langle \overline{1/p^k} \rangle \cong Z_{p^k}$), both $\langle y \rangle$ and the unique subgroup of $\langle x \rangle$ of order p^t must coincide. Hence $y \in \langle x \rangle$. Therefore $H \subseteq \langle x \rangle$, and since $x \in H$, equality holds: $H = \langle x \rangle$.

Finally, any element of order p^k generates the unique subgroup of order p^k, which is $\langle \overline{1/p^k} \rangle$. Hence
$$H = \left\langle \overline{1/p^k} \right\rangle \cong Z_{p^k}.$$

(c) Assume there is no upper bound on the orders of elements of H. Then for each $n \ge 1$ there exists $x_n \in H$ with $|x_n| \ge p^n$. By (a), $|x_n|$ is a power of p, so in particular H contains an element of order exactly p^n: if $|x_n| = p^t$ with $t \ge n$, then $p^{t-n} x_n$ has order p^n.

Thus H contains an element of order p^n for every $n \ge 1$, hence it contains the unique subgroup of order p^n, namely $\langle \overline{1/p^n} \rangle$. Therefore
$$\left\langle \overline{1/p^n} \right\rangle \subset H \quad \text{for all } n \ge 1.$$

But $Z(p^\infty)$ is generated by $\{\overline{1/p^n} \mid n \ge 1\}$ (Exercise 2.16), so H contains all generators of $Z(p^\infty)$, hence $H = Z(p^\infty)$.

(d) Let $H \le Z(p^\infty)$ be a proper subgroup. By (c), the orders of elements of H are bounded, so by (b) we have
$$H = \left\langle \overline{1/p^k} \right\rangle =: C_k$$
for some $k \ge 0$ (with $C_0 = \langle 0 \rangle$). Hence the only proper subgroups are the finite cyclic groups C_n $(n \ge 0)$.

Moreover, since $\overline{1/p^n}$ has order p^n, we have strict inclusions
$$C_0 < C_1 < C_2 < \cdots,$$
and indeed $C_n \subset C_{n+1}$ because
$$\overline{\frac{1}{p^n}} = p \cdot \overline{\frac{1}{p^{n+1}}} \in C_{n+1}.$$

(e) Let G be abelian and suppose elements $x_1, x_2, \dots \in G$ satisfy
$$|x_1| = p, \qquad px_2 = x_1, \qquad px_3 = x_2, \ \dots, \ px_{n+1} = x_n, \ \dots$$

Let $K = \langle x_i \mid i \geq 1 \rangle \leq G$. Define a map on generators by

$$\phi(x_i) = \overline{1/p^i} \in Z(p^\infty).$$

Since $Z(p^\infty)$ is abelian and $\phi(px_{i+1}) = p\,\phi(x_{i+1})$, we have

$$\phi(px_{i+1}) = p \cdot \overline{1/p^{i+1}} = \overline{1/p^i} = \phi(x_i),$$

so ϕ respects the defining relations $px_{i+1} = x_i$. Also $|x_1| = p$ matches $|\overline{1/p}| = p$, so no further relation is forced at level x_1. Hence ϕ extends to a well-defined homomorphism $\Phi : K \to Z(p^\infty)$.

The map Φ is surjective because the elements $\overline{1/p^i}$ generate $Z(p^\infty)$ (Exercise 2.16), and each $\overline{1/p^i}$ lies in the image.

To see injectivity, suppose $\Phi\big(\sum_{i=1}^N c_i x_i\big) = 0$ for some integers c_i. Choose N large enough so all terms occur. Then

$$0 = \sum_{i=1}^{N} c_i\, \overline{1/p^i} \in \mathbb{Q}/\mathbb{Z}.$$

Multiplying by p^N gives

$$0 = \sum_{i=1}^{N} c_i\, p^{N-i}\, \overline{1} \;=\; \overline{\sum_{i=1}^{N} c_i p^{N-i}},$$

so $\sum_{i=1}^N c_i p^{N-i} \in \mathbb{Z}$. But this holds automatically; what we really get is that $\sum_{i=1}^N c_i/p^i \in \mathbb{Z}$, hence $\sum_{i=1}^N c_i/p^i = 0$ in $Z(p^\infty)$. Using the relations $x_i = p^{N-i}x_N$, we have in K:

$$\sum_{i=1}^{N} c_i x_i = \left(\sum_{i=1}^{N} c_i p^{N-i}\right) x_N.$$

The coefficient is divisible by p^N exactly when $\sum c_i/p^i \in \mathbb{Z}$, so the above element is 0 in K because $p^N x_N = x_0 := 0$. Therefore $\ker \Phi = 0$, and Φ is injective.

Hence Φ is an isomorphism $K \cong Z(p^\infty)$.

Exercise 8. *A group that has only a finite number of subgroups must be finite.*

Solution. Assume G is a group with only finitely many subgroups. We prove G is finite by contrapositive.

Suppose G is infinite. Choose an element $a \in G$ with $a \neq e$. If a has infinite order, then G contains the infinite cyclic subgroup $\langle a \rangle \cong \mathbb{Z}$. But $\mathbb{Z}$ has infinitely many distinct subgroups $n\mathbb{Z}$ ($n \in \mathbb{N}^*$), hence $\langle a \rangle$ has infinitely many subgroups, and therefore G has infinitely many subgroups.

If instead every nonidentity element of G has finite order, then G is an infinite torsion group. Pick an infinite sequence of distinct elements $a_1, a_2, \ldots$ in G. The cyclic subgroups $\langle a_i \rangle$ are finite. If only finitely many distinct cyclic subgroups occurred among them, then their union would be a finite union of finite sets, hence finite, contradicting that $\{a_i\}$ is infinite. Therefore the subgroups $\langle a_i \rangle$ yield infinitely many distinct subgroups of G.

In either case, an infinite group has infinitely many subgroups. Hence, if G has only finitely many subgroups, G must be finite.

Exercise 9. *If G is an abelian group, then the set T of all elements of G with finite order is a subgroup of G. [Compare Exercise 5.]*

Solution. Let G be an abelian group and let

$$T = \{x \in G \mid |x| < \infty\}.$$

We show $T < G$ using Theorem 2.5.

First, $e \in T$, since $|e| = 1$, so $T \neq \varnothing$. Let $a, b \in T$. Then $|a| = m$ and $|b| = n$ for some positive integers m, n. Because G is abelian, $ab^{-1} = ab^{-1} = a(b^{-1})$ and a commutes with b^{-1}. Also $|b^{-1}| = |b| = n$. Hence

$$(ab^{-1})^{mn} = a^{mn}(b^{-1})^{mn} = (a^m)^n\big((b^{-1})^n\big)^m = e,$$

so ab^{-1} has finite order, i.e. $ab^{-1} \in T$.

Therefore T is nonempty and closed under ab^{-1}; by Theorem 2.5, T is a subgroup of G.

Exercise 10. *An infinite group is cyclic if and only if it is isomorphic to each of its proper subgroups.*

Solution. **($\Rightarrow$)** Suppose G is infinite cyclic. Then $G \cong \mathbb{Z}$. Every proper subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some integer $n \geq 2$, and the map

$$\mathbb{Z} \to n\mathbb{Z}, \qquad k \mapsto nk$$

is an isomorphism (additively). Hence every proper subgroup of G is isomorphic to G.

($\Leftarrow$) Conversely, suppose G is an infinite group that is isomorphic to each of its proper subgroups.

First, G must contain an element of infinite order. Indeed, if every element of G had finite order, then every cyclic subgroup $\langle x \rangle$ would be finite. Choose any $x \neq e$; then $\langle x \rangle$ is a proper finite subgroup, so $G \cong \langle x \rangle$ would force G to be finite, a contradiction. Thus there exists $a \in G$ with $|a| = \infty$.

Now consider the cyclic subgroup $\langle a \rangle$. It is infinite, hence $\langle a \rangle \cong \mathbb{Z}$. If $\langle a \rangle = G$, then G is cyclic and we are done. If $\langle a \rangle \neq G$, then $\langle a \rangle$ is a proper subgroup, so by hypothesis $G \cong \langle a \rangle$. Therefore $G \cong \mathbb{Z}$, and in particular G is cyclic.

Hence an infinite group is cyclic if and only if it is isomorphic to each of its proper subgroups.

1.4 Cosets and Counting

Exercise 1. *Let G be a group and $\{H_i \mid i \in\}$ a family of subgroups. Then for any $a \in G$, $(\bigcup_i H_i)a = \bigcup_i H_i a$.*

Solution. Let G be a group, $\{H_i \mid i \in I\}$ a family of subgroups, and $a \in G$. We prove the set equality

$$\left(\bigcap_{i\in I} H_i\right) a \;=\; \bigcap_{i\in I}(H_i a).$$

($\subseteq$). Let $x \in (\bigcap_i H_i)\, a$. Then $x = ha$ for some $h \in \bigcap_i H_i$. Thus $h \in H_i$ for every i, so $x = ha \in H_i a$ for every i. Hence $x \in \bigcap_i (H_i a)$.

($\supseteq$). Let $x \in \bigcap_i (H_i a)$. Then for each i there exists $h_i \in H_i$ such that $x = h_i a$. Multiplying on the right by a^{-1} gives
$$xa^{-1} = h_i \in H_i \quad \text{for all } i,$$
so $xa^{-1} \in \bigcap_i H_i$. Therefore $x = (xa^{-1})a \in (\bigcap_i H_i)a$.

Thus $(\bigcap_i H_i)a = \bigcap_i (H_i a)$.

Exercise 2. *(a) Let H be the cyclic subgroup (of order 2) of S_3 generated by $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Then no left coset of H (except H itself) is also a right coset. There exists $a \in S_3$ such that $aH \cap Ha = \{a\}$.*

(b) If K is the cyclic subgroup (of order 3) of S_3 generated by $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, then every left coset of K is also a right coset of K.

Solution. Work in S_3. Let
$$h = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12), \qquad H = \langle h \rangle = \{e, (12)\}.$$

(a) **No left coset of H other than H is a right coset.** The left cosets of H are H, $(13)H$, and $(23)H$. Compute:
$$(13)H = \{(13), (13)(12)\} = \{(13), (123)\},$$
since $(13)(12) = (123)$, and
$$(23)H = \{(23), (23)(12)\} = \{(23), (132)\},$$
since $(23)(12) = (132)$.

The right cosets are H, $H(13)$, and $H(23)$. Compute:
$$H(13) = \{(13), (12)(13)\} = \{(13), (132)\},$$
since $(12)(13) = (132)$, and
$$H(23) = \{(23), (12)(23)\} = \{(23), (123)\},$$
since $(12)(23) = (123)$.

Thus
$$(13)H = \{(13), (123)\} \neq \{(13), (132)\} = H(13),$$
and similarly
$$(23)H = \{(23), (132)\} \neq \{(23), (123)\} = H(23).$$
The remaining left coset is H itself, which equals the right coset H. Hence no left coset of H (except H) is also a right coset.

There exists $a \in S_3$ with $aH \cap Ha = \{a\}$. Take $a = (13)$. Then
$$aH = (13)H = \{(13), (123)\}, \qquad Ha = H(13) = \{(13), (132)\}.$$
Therefore
$$aH \cap Ha = \{(13)\} = \{a\}.$$

(b) Let

$$k = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123), \qquad K = \langle k \rangle = \{e, (123), (132)\}.$$

This subgroup has index 2 in S_3. Hence there are exactly two left cosets: K and gK for any $g \notin K$; likewise there are exactly two right cosets: K and Kg.

Take $g = (12) \notin K$. Then

$$gK = \{(12), (12)(123), (12)(132)\} = \{(12), (23), (13)\},$$

and

$$Kg = \{(12), (123)(12), (132)(12)\} = \{(12), (13), (23)\}.$$

Thus $gK = Kg$. Since any left coset other than K must equal gK, and any right coset other than K must equal Kg, it follows that every left coset of K is also a right coset of K.

Exercise 3. *The following conditions on a finite group G are equivalent.*

(i) G is prime.

(ii) $G \neq \langle e \rangle$ and G has no proper subgroups,

(iii) $G \cong Z_p$ for some prime p.

Solution. Let G be a finite group. We prove $(i) \Leftrightarrow (ii) \Leftrightarrow (iii)$.

(i)⇒(ii). If G is prime, then $|G| = p$ for some prime p, so $G \neq \langle e \rangle$. If $H \leq G$ is a subgroup, then $|H|$ divides $|G| = p$ (Lagrange's Theorem), hence $|H| = 1$ or $|H| = p$. Therefore $H = \langle e \rangle$ or $H = G$, so G has no proper subgroups.

(ii)⇒(iii). Assume $G \neq \langle e \rangle$ and G has no proper subgroups. Pick $a \in G$ with $a \neq e$. Then $\langle a \rangle$ is a nontrivial subgroup of G, hence must be all of G. Thus G is cyclic: $G = \langle a \rangle$. If $|G| = n$ were composite, say $n = rs$ with $1 < r < n$, then by the cyclic-group subgroup theorem, G would have a (unique) subgroup of order r, which would be proper—contradiction. Hence $|G| = p$ is prime, and $G \cong Z_p$.

(iii)⇒(i). If $G \cong Z_p$ for a prime p, then $|G| = p$, so G is prime.

Therefore (i), (ii), and (iii) are equivalent.

Exercise 4. *(Euler-Fermat) Let a be an integer and p a prime such that $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$. [*Hint*: Consider $\overline{a} \in Z_p$ and the multiplicative group of nonzero elements of Z_p; see Exercise 1.7.] It follows that $a^p \equiv a \pmod{p}$ for any integer a.*

Solution. Let p be prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Then $\overline{a} \neq \overline{0}$ in Z_p, so $\overline{a}$ lies in the multiplicative group

$$Z_p^{\times} = Z_p \setminus \{\overline{0}\},$$

which has order $|Z_p^{\times}| = p - 1$ (Exercise 1.7).

By Lagrange's Theorem, the order of $\overline{a}$ divides $|Z_p^\times| = p-1$, hence

$$\overline{a}^{p-1} = \overline{1}.$$

Translating back to congruences, this says

$$a^{p-1} \equiv 1 \pmod{p}.$$

Multiplying both sides by a gives $a^p \equiv a \pmod{p}$ when $p \nmid a$. If $p \mid a$, then $a \equiv 0 \pmod{p}$, so $a^p \equiv 0 \equiv a \pmod{p}$. Thus $a^p \equiv a \pmod{p}$ for every integer a.

Exercise 5. *Prove that there are only two distinct groups of order* 4 *(up to isomorphism), namely Z_4 and $Z_2 \oplus Z_2$. [*Hint*: By Lagrange's Theorem 4.6 a group of order* 4 *that is not cyclic must consist of an identity and three elements of order* 2*.]*

Solution. Let G be a group with $|G| = 4$.

Case 1: G has an element of order 4. Then G is cyclic, hence $G \cong Z_4$.

Case 2: G has no element of order 4. Then G is not cyclic. By Lagrange's Theorem, the order of any element of G divides 4, so every nonidentity element has order 2. Thus G consists of e and three elements a, b, c with

$$a^2 = b^2 = c^2 = e.$$

We first show G is abelian. For any $x, y \in G$, we have

$$(xy)^{-1} = y^{-1}x^{-1}.$$

But every element is its own inverse, so $x^{-1} = x$ and $y^{-1} = y$, and also $(xy)^{-1} = xy$. Hence

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx,$$

so G is abelian.

Now choose two distinct nonidentity elements, say $a \neq b$. Then $ab \neq e$ (otherwise $a = b^{-1} = b$). Also $ab \neq a$ and $ab \neq b$ (by cancellation). Hence ab is the third nonidentity element. Therefore

$$G = \{e, a, b, ab\}.$$

Define $\varphi : Z_2 \oplus Z_2 \to G$ by

$$\varphi(\overline{0}, \overline{0}) = e, \quad \varphi(\overline{1}, \overline{0}) = a, \quad \varphi(\overline{0}, \overline{1}) = b, \quad \varphi(\overline{1}, \overline{1}) = ab.$$

Since $a^2 = b^2 = e$ and $ab = ba$, one checks that φ is a homomorphism: it respects addition mod 2 in each coordinate (e.g. $a \cdot a = e$, $b \cdot b = e$, and $a \cdot b = ab$). It is clearly bijective, hence an isomorphism. Thus $G \cong Z_2 \oplus Z_2$.

Therefore, up to isomorphism, the only groups of order 4 are Z_4 and $Z_2 \oplus Z_2$.

Exercise 6. *Let H, K be subgroups of a group G. Then HK is a subgroup of G if and only if $HK = KH$,* *Solution.* Let $H, K < G$.

(⇒) Assume HK is a subgroup of G. Then HK is closed under inverses, so

$$(HK)^{-1} = HK.$$

But

$$(HK)^{-1} = \{(hk)^{-1} \mid h \in H,\ k \in K\} = \{k^{-1}h^{-1} \mid h \in H,\ k \in K\} = KH,$$

since H and K are subgroups. Hence $HK = KH$.

(⇐) Conversely, assume $HK = KH$. We show that HK is a subgroup of G.

First, $e = ee \in HK$, so $HK \neq \varnothing$. Let $x, y \in HK$. Then $x = h_1k_1$ and $y = h_2k_2$ for some $h_1, h_2 \in H$, $k_1, k_2 \in K$. Then

$$xy^{-1} = h_1k_1(k_2^{-1}h_2^{-1}) = h_1(k_1k_2^{-1})h_2^{-1}.$$

Since $k_1k_2^{-1} \in K$ and $HK = KH$, there exist $h_3 \in H$ and $k_3 \in K$ such that

$$k_1k_2^{-1}h_2^{-1} = h_3k_3.$$

Thus

$$xy^{-1} = h_1h_3k_3 \in HK,$$

because $h_1h_3 \in H$ and $k_3 \in K$. Hence HK is closed under xy^{-1}.

By Theorem 2.5, HK is a subgroup of G.

Therefore HK is a subgroup of G if and only if $HK = KH$.

Exercise 7. *Let G be a group of order $p^k m$, with p prime and $(p, m) = 1$. Let H be a subgroup of order p^k and K a subgroup of order p^d, with $0 < d \leq k$ and $K \not\subset H$. Show that HK is not a subgroup of G.*

Solution. Assume for contradiction that HK is a subgroup of G.

Since $|H| = p^k$ and $|K| = p^d$, we have $|H \cap K| = p^r$ for some $0 \leq r \leq d$. Because $K \not\subset H$, we have $H \cap K \neq K$, hence $r < d$.

Now, since HK is a subgroup, we have $HK = KH$ (Exercise 4.6), and thus Theorem 4.7 applies:

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{p^k \cdot p^d}{p^r} = p^{k+d-r}.$$

Since $r < d$, we have $k + d - r > k$, so $|HK|$ is a power of p strictly larger than p^k.

But $HK < G$, so by Lagrange's Theorem $|HK|$ divides $|G| = p^k m$. The only powers of p dividing $p^k m$ are at most p^k (because $(p, m) = 1$). Thus no subgroup of G can have order $p^{k+d-r} > p^k$, a contradiction.

Therefore HK is not a subgroup of G.

Exercise 8. *If H and K are subgroups of finite index of a group G such that $[G : H]$ and $[G : K]$ are relatively prime, then $G = HK$.*

Solution. Let $H, K < G$ with $[G : H] = m$, $[G : K] = n$, and $(m, n) = 1$. Consider $H \cap K$.

Since $H \cap K < H$, we may count cosets inside H:

$$[G : H \cap K] = [G : H]\,[H : H \cap K] = m\,[H : H \cap K].$$

Similarly,

$$[G : H \cap K] = [G : K]\,[K : H \cap K] = n\,[K : H \cap K].$$

Hence $m \mid [G : H \cap K]$ and $n \mid [G : H \cap K]$. Because $(m, n) = 1$, it follows that

$$mn \mid [G : H \cap K].$$

On the other hand, the natural map

$$G/(H \cap K) \;\longrightarrow\; G/H \times G/K, \qquad g(H \cap K) \mapsto (gH, gK)$$

is injective, so

$$[G : H \cap K] \le [G : H]\,[G : K] = mn.$$

Therefore $[G : H \cap K] = mn$.

Now apply Theorem 4.7 (the product formula) to H and K:

$$|HK : H| = [K : H \cap K] \quad \text{equivalently} \quad [HK : H] = [K : H \cap K].$$

Translating to indices in G,

$$[G : HK] = \frac{[G : H]}{[HK : H]} = \frac{m}{[K : H \cap K]}.$$

But

$$[K : H \cap K] = \frac{[G : H \cap K]}{[G : K]} = \frac{mn}{n} = m,$$

so $[K : H \cap K] = m$, and hence

$$[G : HK] = \frac{m}{m} = 1.$$

Thus $HK = G$.

Exercise 9. *If H, K and N are subgroups of a group G such that $H < N$, then $HK \cap N = H(K \cap N)$.*

Solution. Assume $H, N, K < G$ and $H \subset N$. We prove

$$HK \cap N \;=\; H(K \cap N).$$

($\subset$). Let $x \in HK \cap N$. Then $x \in HK$, so $x = hk$ for some $h \in H$, $k \in K$. Also $x \in N$. Since $h \in H \subset N$, we have $h^{-1} \in N$, and therefore

$$k = h^{-1}x \in N.$$

Thus $k \in K \cap N$, and so $x = hk \in H(K \cap N)$.

($\supset$). Let $x \in H(K \cap N)$. Then $x = hk$ with $h \in H$ and $k \in K \cap N$. Clearly $x \in HK$. Also $h \in H \subset N$ and $k \in N$, so $hk \in N$. Hence $x \in HK \cap N$.

Therefore $HK \cap N = H(K \cap N)$.

Exercise 10. *Let H, K, N be subgroups of a group G such that $H < K$, $H \cap N = K \cap N$, and $HN = KN$. Show that $H = K$.*

Solution. Assume $H, K, N < G$ with $H \subset K$, $H \cap N = K \cap N$, and $HN = KN$. We prove $H = K$.

Since $H \subset K$, it suffices to show $K \subset H$. Let $k \in K$. Because $KN = HN$, we have $k \in KN = HN$, so there exist $h \in H$ and $n \in N$ such that

$$k = hn.$$

Then

$$n = h^{-1}k \in K$$

because $h^{-1} \in H \subset K$ and $k \in K$. Hence $n \in K \cap N$. By the hypothesis $K \cap N = H \cap N$, it follows that $n \in H \cap N \subset H$.

Therefore $k = hn \in H$, since $h \in H$ and $n \in H$. Thus $K \subset H$, and hence $H = K$.

Exercise 11. *Let G be a group of order $2n$; then G contains an element of order 2. If n is odd and G abelian, there is only one element of order 2.*

Solution. Let $|G| = 2n$.

Existence of an element of order 2. Consider the set $G - \{e\}$. If $a \in G - \{e\}$ and $a \neq a^{-1}$, then the elements a and a^{-1} form a 2-element pair. Thus $G - \{e\}$ is partitioned into disjoint pairs $\{a, a^{-1}\}$, together with the elements satisfying $a = a^{-1}$, i.e. $a^2 = e$. If there were no element $a \neq e$ with $a^2 = e$, then every element of $G - \{e\}$ would lie in a 2-element pair, so $|G - \{e\}|$ would be even. But

$$|G - \{e\}| = 2n - 1$$

is odd, a contradiction. Hence there exists $a \neq e$ with $a^2 = e$, i.e. an element of order 2.

Uniqueness when n is odd and G is abelian. Assume now that n is odd and G is abelian. Let

$$T = \{x \in G \mid x^2 = e\}.$$

Then T is a subgroup of G: it is nonempty, and if $x^2 = e$ and $y^2 = e$, then (using commutativity)

$$(xy)^2 = x^2y^2 = e, \qquad (x^{-1})^2 = (x^2)^{-1} = e,$$

so $xy \in T$ and $x^{-1} \in T$. Thus $T < G$.

Every element of T has order 1 or 2, so T is an elementary abelian 2-group; in particular $|T| = 2^r$ for some $r \geq 0$. By Lagrange's Theorem, $|T|$ divides $|G| = 2n$. Since n is odd, the largest power of 2 dividing $2n$ is 2. Hence $|T|$ must be 1 or 2. But we already proved there exists an element of order 2, so $|T| = 2$.

Therefore $T = \{e, t\}$ for a unique element $t \neq e$ with $t^2 = e$, i.e. G has exactly one element of order 2.

Exercise 12. *If H and K are subgroups of a group G, then $[H \vee K : H] \geq [K : H \cap K]$.*

Solution. Let $H, K < G$, and set $L = H \vee K = \langle H \cup K \rangle$. Consider the map

$$\phi : K/(H \cap K) \longrightarrow L/H, \qquad \phi\big(k(H \cap K)\big) = kH.$$

We first check that ϕ is well defined. If $k(H \cap K) = k'(H \cap K)$, then $k^{-1}k' \in H \cap K \subset H$, so $k'H = kH$. Hence ϕ is well defined.

Next we show that ϕ is injective. Suppose $\phi(k(H \cap K)) = \phi(k'(H \cap K))$. Then $kH = k'H$, so $k^{-1}k' \in H$. Since also $k^{-1}k' \in K$, we have $k^{-1}k' \in H \cap K$, hence $k(H \cap K) = k'(H \cap K)$.

Thus ϕ is an injection, so

$$\left|K/(H \cap K)\right| \;\le\; \left|L/H\right|.$$

Equivalently,

$$[K : H \cap K] \;\le\; [L : H] = [H \vee K : H].$$

This is the desired inequality.

Exercise 13. *If $p > q$ are primes, a group of order pq has at most one subgroup of order p. [*Hint*: Suppose H, K are distinct subgroups of order p. Show $H \cap K = \langle e \rangle$; use Exercise 12 to get a contradiction.]*

Solution. Let $|G| = pq$ with primes $p > q$. Suppose, for contradiction, that G has two distinct subgroups H and K of order p.

Since $|H| = |K| = p$ is prime and $H \neq K$, we must have

$$H \cap K \neq H \quad \text{and} \quad H \cap K \neq K.$$

By Lagrange's Theorem, $|H \cap K|$ divides $|H| = p$, hence $|H \cap K| = 1$ or p. The second possibility would force $H \cap K = H$, i.e. $H \subset K$, hence $H = K$, contrary to assumption. Therefore

$$H \cap K = \langle e \rangle.$$

Now apply Exercise 12 with these H and K:

$$[H \vee K : H] \;\ge\; [K : H \cap K] = [K : \langle e \rangle] = |K| = p.$$

Hence

$$|H \vee K| = [H \vee K : H] \cdot |H| \;\ge\; p \cdot p = p^2.$$

But $H \vee K < G$, so $|H \vee K| \le |G| = pq$. Thus $p^2 \le pq$, which implies $p \le q$, contradicting $p > q$.

Therefore G has at most one subgroup of order p.

Exercise 14. *Let G be a group and $a, b \in G$ such that (i) $|a| = 4 = |b|$; (ii) $a^2 = b^2$. (iii) $ba = a^3b = a^{-1}b$; (iv) $a \neq b$; (v) $G = \langle a, b \rangle$. Show that $|G| = 8$ and $G \cong Q_8$ (See Exercise 2.3; observe that the generators A, B of Q_8 also satisfy (i)-(v).)*

Solution. Let G be a group with elements $a, b \in G$ satisfying (i)–(v).

Step 1: $a^2 = b^2$ is central and has order 2. Set $z = a^2 = b^2$. Since $|a| = 4$, we have $z \neq e$ and $z^2 = a^4 = e$, so $|z| = 2$. Also,

$$az = a(a^2) = a^3 = (a^2)a = za,$$

so z commutes with a. And

$$bz = b(b^2) = b^3 = (b^2)b = zb,$$

so z commutes with b. Since $G = \langle a, b \rangle$, it follows that $z \in Z(G)$.

Step 2: Every element of G can be written as a^ib^j with $0 \le i \le 3$, $0 \le j \le 1$. From (iii) we have $ba = a^{-1}b$. Multiplying on the right by b^{-1} gives

$$bab^{-1} = a^{-1}.$$

Equivalently,

$$ba^i = a^{-i}b \qquad \text{for all } i \in \mathbb{Z},$$

which follows by induction on i (and also holds for negative i by inverses). Thus any word in $a^{\pm 1}$ and $b^{\pm 1}$ can be rearranged by moving all b's to the right at the cost of inverting powers of a, yielding a product a^ib^j.

Moreover, since $b^2 = z = a^2$, we can reduce any power b^j to $j \in \{0,1\}$ at the cost of multiplying by a power of a^2, which is already a power of a. And since $a^4 = e$, we can reduce i modulo 4. Hence every element of G is of the form a^ib^j with $0 \le i \le 3$, $j \in \{0,1\}$. Therefore $|G| \le 8$.

Step 3: These eight elements are distinct, so $|G| = 8$. Consider the set

$$S = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

First, e, a, a^2, a^3 are distinct because $|a| = 4$. Next, $b \notin \langle a \rangle$: if $b = a^i$, then $b^2 = a^{2i}$ would be e when i is even or a^2 when i is odd; but $b \ne a$ by (iv), and if $b = a^3$ then $ba = a^3a = a^4 = e$, contradicting (iii). Thus $b \notin \langle a \rangle$.

Now suppose $a^ib = a^jb$. Right-multiplying by b^{-1} gives $a^i = a^j$, so $i \equiv j \pmod 4$. Hence b, ab, a^2b, a^3b are distinct. Also none of a^ib lies in $\langle a \rangle$: if $a^ib = a^j$, then $b = a^{j-i} \in \langle a \rangle$, contradiction. Therefore the four elements b, ab, a^2b, a^3b are distinct from e, a, a^2, a^3.

Thus $|S| = 8$. Since $G = \langle a, b \rangle$ and every element of G is of the form a^ib^j, we have $G = S$. Hence $|G| = 8$.

Step 4: $G \cong Q_8$. Let $Q_8 = \langle A, B \rangle$ be the quaternion group, where A, B satisfy the same relations:

$$|A| = |B| = 4, \quad A^2 = B^2, \quad BAB^{-1} = A^{-1}.$$

Define $\varphi : G \to Q_8$ by $\varphi(a) = A$, $\varphi(b) = B$. By Step 2, every element of G has a representative a^ib^j with $0 \le i \le 3$, $j \in \{0,1\}$. Using the relations $a^4 = e$, $b^2 = a^2$, and $bab^{-1} = a^{-1}$ (and the corresponding relations for A, B), any two representations of the same element of G are connected by applications of these relations, so φ is well defined and is a homomorphism.

Moreover, φ is surjective since $Q_8 = \langle A, B \rangle$. Finally, $|G| = |Q_8| = 8$, so a surjective homomorphism $G \to Q_8$ must be injective as well. Therefore φ is an isomorphism, and $G \cong Q_8$.