Chapter 3

Topics in Set Theory

The language of set theory plays a fundamental role in much of modern mathematics. We will study the idea of relations between elements of two sets. In particular, the concept of a function from a set to another will enable us to define the cardinality of infinite sets. We then close with an introduction to group theory, which is the beginning of the modern study of abstract algebra.

3.1 Binary Relations

Definition. Let A and B be two sets. A *relation* R from A to B means a subset $R \subseteq A \times B$.

For example, the following are some, but not all, binary relations from the set $\{0, 1\}$ to the set $\{x, y, z\}$.

a) $\{(0, x), (1, y), (0, z)\}$
b) $\{(0, x), (0, z), (1, x), (1, z)\}$
c) $\{(1, x), (1, y), (1, z)\}$
d) $\{(0, x), (1, x), (0, y), (1, y), (0, z), (1, z)\}$

Test 3.1. How many different binary relations from $\{0, 1\}$ to $\{x, y, z\}$ can we have in all?

a) 8
b) 9
c) 32
d) 64

The adjective *binary* indicates that there are two sets involved. Since we are not interested in studying relations with more than two sets, from now on we agree that the term *relation* always refers to a binary relation.

Since relations are sets, with two relations R and S we are allowed to operate on them, e.g., using the operator union or intersection. We now introduce a new set operator which is customized to relations.

Definition. Suppose that $R \subseteq A \times B$ and $S \subseteq B \times C$ are two relations. Then $S \circ R$ is the relation from A to C given by

$$S \circ R = \{(a,c) \mid (a,b) \in R \wedge (b,c) \in S\}$$

The notation $S \circ R$ is read R *circle* S (yes, right to left!) and we refer to this set operation as the *composition* of R with S.

Example. Let $A = \{1,2,3,4\}$, $B = \{x,y,z\}$, and $C = \{4,5,9\}$. Consider two relations R and S given below, and find the elements of the relation $S \circ R \subseteq A \times C$.

$$R = \{(1,y),(1,z),(2,x),(2,y),(4,z)\} \subseteq A \times B$$
$$S = \{(x,4),(x,9),(y,5),(z,5),(z,9)\} \subseteq B \times C$$

Solution. The first element $(1,y) \in R$ *matches* with the element $(y,5) \in S$, resulting in the new element $(1,5) \in S \circ R$. Next, $(1,z) \in R$ and $(z,5) \in S$ yield the same $(1,5)$, whereas $(1,z)$ and $(z,9)$ give $(1,9)$. In all, seven elements are composed in this manner which make up the resulting set.

$$S \circ R = \{(1,5),(1,9),(2,4),(2,5),(2,9),(4,5),(4,9)\}$$

Definition. By the *inverse* of a relation $R \subseteq A \times B$, we mean the relation from B to A given by $R^{-1} = \{(b,a) \mid (a,b) \in R\}$.

For example, the inverse of $R = \{(1,0),(5,5),(9,-2)\} \subseteq \mathbb{N} \times \mathbb{Z}$ is the relation $R^{-1} = \{(0,1),(5,5),(-2,9)\} \subseteq \mathbb{Z} \times \mathbb{N}$.

Exercise* 3.2. Given two relations, $R \subseteq A \times B$ and $S \subseteq B \times C$, prove the set identity $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

3.1.1 Relations on a Set

For the time being, we shall focus only on relations $R \subseteq A \times B$ in the special case where $A = B$.

Definition. Let A be a given set. A relation R *on* A means a relation from A to itself, i.e., $R \subseteq A \times A$. In this case, we define $R^2 = R \circ R$, $R^3 = R \circ R^2$, and by induction, $R^n = R \circ R^{n-1}$ and $R^{-n} = (R^{-1})^n$ for all $n \in \mathbb{N}$.

Question. If $|A| = n$, how many relations on A are possible in all?

Exercise 3.3. Let $R = \{(1,3),(2,2),(2,4),(3,1),(4,3)\}$ be a relation on the set $A = \{1,2,3,4\}$. Find the elements of each relation given by the following compositions.
a) R^2
b) R^4
c) R^{-2}
d) $R \circ R^{-1}$

Question. Is it true that $R^4 = R^2 \circ R^2$?

Exercise* 3.4. Prove that $R^n \circ R^m = R^{m+n}$ for all $m, n \in \mathbb{N}$.

Definition. Given a set A, we define the *identity relation* on A to be the special relation $A^0 = \{(a,a) \mid a \in A\}$. Any relation R on A is then called

1) *reflexive* if $A^0 \subseteq R$.

2) *symmetric* if $R^{-1} = R$.

3) *anti-symmetric* if $R \cap R^{-1} \subseteq A^0$.

4) *transitive* if $R^2 \subseteq R$.

Question. What is the difference between A^0 and $A \times A$?

Exercise* 3.5. For any $R \subseteq A \times A$, show that $R \circ A^0 = R = A^0 \circ R$.

Example. Let $A = \{1,2,3,4\}$. For each relation $R \subseteq A \times A$ given below, determine whether R is reflexive, symmetric, anti-symmetric, or transitive.
a) $R = \{(1,1),(1,2),(2,1),(2,2),(2,4),(3,3),(4,2)\}$
b) $R = \{(1,1),(1,3),(2,2),(2,4),(3,1),(3,3),(4,2),(4,4)\}$
c) $R = \{(a,b) \in A \times A \mid a \leq b\}$
d) $R = \{(a,b) \in A \times A \mid a \bmod b = 1\}$

Solution. We note that $A^0 = \{(1,1),(2,2),(3,3),(4,4)\}$.

1) R is symmetric since $R^{-1} = R$ but not reflexive as $(4,4) \notin R$. Anti-symmetric is false, e.g., $(1,2) \in R \cap R^{-1}$. So is transitive false, because the composition of $(4,2)$ with $(2,4)$ yields $(4,4) \notin R$.

2) You can check that R is reflexive, symmetric, and transitive. Only anti-symmetric is false.

3) R is reflexive since $a \leq a$ for all $a \in A$. Now if $a \neq b$, either $a < b$ or $b < a$ but never both. It follows that R is anti-symmetric, but not symmetric. Lastly, R is transitive for if $a \leq b$ and $b \leq c$, then $a \leq c$.

4) $R = \{(1,2),(1,3),(1,4),(3,2),(4,3)\}$. This relation is anti-symmetric, but is neither symmetric nor reflexive. R is not transitive. (Why?)

Instead of using set notation, we may use the language of propositional logic to redefine the above definitions; we state the results as a theorem but leave the proof as a straightforward exercise.

Theorem 3.1. Let R be a relation on a set A. Then

1) R is reflexive if and only if $\forall a \in A : (a,a) \in R$.

2) R is symmetric if and only if $\forall a,b \in A : (a,b) \in R \rightarrow (b,a) \in R$.

3) R is anti-symmetric if and only if $(a,b) \in R \rightarrow (b,a) \notin R$ for all $a,b \in A$ with $a \neq b$.

4) R is transitive if and only if $(a,b) \in R \wedge (b,c) \in R \rightarrow (a,c) \in R$ for all $a,b,c \in A$.

Exercise 3.6. Determine whether each relation R on A is reflexive, symmetric, anti-symmetric, or transitive.

a) $A = \{2,4,6,8\}$ and $R = \{(a,b) \in A \times A \mid a+b > 4\}$
b) $A = \{2,4,6,8\}$ and $R = \{(a,b) \in A \times A \mid a \bmod b = 0\}$
c) $A = \{2,4,7,8,9\}$ and $R = \{(a,b) \in A \times A \mid a+b \text{ is even}\}$
d) $R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a < b\}$

Question. Is anti-symmetric the negation of symmetric?

Exercise* 3.7. Is it possible to have $R \subseteq A \times A$ which is both symmetric and anti-symmetric? Think of an example or explain why it is not possible.

Exercise 3.8. Let $A = \{1,2,3,4\}$. Give an example of a relation on A which satisfies the following properties.

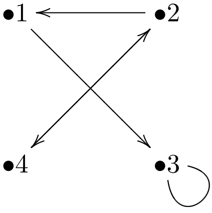
a) reflexive (T) symmetric (F) anti-symmetric (T) transitive (F)
b) reflexive (F) symmetric (F) anti-symmetric (F) transitive (F)
c) reflexive (F) symmetric (T) anti-symmetric (F) transitive (T)
d) reflexive (T) symmetric (T) anti-symmetric (F) transitive (T)

3.1.2 Digraphs and Zero-One Matrices

A relation R on A can be visually represented by a graph which is called the digraph of R, defined as follows.

Definition. Let R be a relation on a set A. The *digraph* of R is a picture in which the elements of A are drawn as dots (points) and each element $(a,b) \in R$ is represented by a line connecting them, with direction from a to b. We call the dots *vertices* (sometimes, *nodes*) and the lines *edges*. An edge $(a,a) \in R$ is also called a *loop*.

Example. Let $A = \{1, 2, 3, 4\}$ and $R = \{(1, 3), (2, 1), (2, 4), (3, 3), (4, 2)\}$. In drawing the digraph, we spread out the four vertices somewhat evenly, for the mere sake of better visibility. The five edges, one of which is a loop, are put in place accordingly, but note that the edges $(2, 4)$ and $(4, 2)$ are displayed as a single line with two directions.



(3.1)

Question. Looking at the digraph, how do we know if a relation is reflexive, symmetric, anti-symmetric, or transitive?

Exercise 3.9. Redo Exercise 3.8, presenting your solutions in digraphs.

Another way to represent a relation $R \subseteq A \times A$ is by use of a matrix. Recall that a matrix is a two-dimensional array of elements, whose entry in the ith row and jth column will be denoted by m_{ij}, or simply (i, j). For example, a matrix M with 3 rows and 4 columns, otherwise called a 3×4 matrix, can be represented as follows.

$$M = \begin{bmatrix} (1,1) & (1,2) & (1,3) & (1,4) \\ (2,1) & (2,2) & (2,3) & (2,4) \\ (3,1) & (3,2) & (3,3) & (3,4) \end{bmatrix}$$

Definition. Suppose that the elements of A have been enumerated so that we may write $A = \{a_1, a_2, a_3, \ldots, a_n\}$. A relation R on A can then be represented by the $n \times n$ *zero-one matrix* $[R]$ whose elements $(i, j) = 1$ if $(a_i, a_j) \in R$, and $(i, j) = 0$ otherwise.

Example. Let $R = \{(1, 1), (1, 3), (2, 1), (2, 3), (2, 4), (3, 3), (4, 2), (4, 3)\}$ be a relation on the set $A = \{1, 2, 3, 4\}$. These eight elements of R correspond to the 1's in the following 4×4 zero-one matrix—for instance, $(1, 3) \in R$ tells us that the first row, third column entry in $[R]$ is 1.

$$[R] = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

Exercise 3.10. Find $[R]$ for the relation R given by the digraph in (3.1).

Question. From the zero-one matrix, how do we know if a relation is reflexive, symmetric, anti-symmetric, or transitive?

Test 3.11. Which relation is anti-symmetric and transitive?

$$\text{a)} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \quad \text{b)} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad \text{c)} \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \quad \text{d)} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

Exercise* 3.12. Let $[R] = [(i,j)]$ denote the matrix of a relation R on a set $A = \{a_1, a_2, \ldots, a_n\}$. Find a formula to compute the entry $(i,j)_2$ belonging to $[R^2] = [(i,j)_2]$, the zero-one matrix of the relation R^2.

3.1.3 Transitive Closures

Elias wants to fly out of Amman to Santiago, Chile. He asks his travel agent to book him his airplane tickets. The first thing that the travel agent checks is whether there are direct flights. If there is none, perhaps Elias can make a transit somehere to connect with another flight. Sometimes two transits or more may be necessary for a traveler to reach his desired destination.

If A denotes the set of all airports in the world, the element $(a,b) \in R \subseteq A \times A$ tells us that there is a direct flight from a to b. Traveling from Amman to Santiago is at all possible, by direct flight or transits, if and only if the element (Amman, Santiago) belongs to the transitive closure of R, i.e.,

Definition. Let R be a relation on some set A. By the *transitive closure* of R we mean the relation on A given by

$$\overline{R} = R \cup R^2 \cup R^3 \cup \cdots \cup R^n$$

where $n = |A|$.

If, for instance, $(a,b) \in R^3$ then flying from a to b can be done with (at worse) three connecting flights, i.e., two transit times. Hence $(a,b) \in \overline{R}$ if and only if it is possible to connect from a to b, possibly by involving a number of transits.

Question. Why don't we need R^{n+1} in the definition of transitive closure?

Example. Let $A = \{1,2,3,4\}$ and $R = \{(1,3),(2,1),(2,4),(3,2),(4,4)\}$. Find the transitive closure of R.

Solution. We use the definition $R^n = R \circ R^{n-1}$ to find

$$\begin{aligned} R^2 &= \{(1,2),(2,3),(2,4),(3,1),(3,4),(4,4)\} \\ R^3 &= \{(1,1),(1,4),(2,2),(2,4),(3,3),(3,4),(4,4)\} \\ R^4 &= \{(1,3),(1,4),(2,1),(2,4),(3,2),(3,4),(4,4)\} \end{aligned}$$

Hence $\overline{R} = \{(1,1),(1,2),(1,3),(1,4),(2,1),(2,2),(2,3),(2,4),(3,1),(3,2),$ $(3,3),(3,4),(4,4)\} = A \times A - \{(4,1),(4,2),(4,3)\}$.

Exercise 3.13. Find the transitive closure of each relation given below, on the set $A = \{1,2,3,4\}$.

a) $R = \{(1,2),(2,1),(2,3),(3,4)\}$
b) $R = \{(1,1),(2,1),(2,4),(3,2),(4,3)\}$
c) $R = \{(1,1),(1,4),(2,1),(2,2),(3,3),(4,4)\}$
d) $R = \{(1,4),(2,1),(2,4),(3,2),(4,3)\}$

Test 3.14. The zero-one matrix of some relation R is provided below. Which matrix represents the transitive closure of R?

$$[R] = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$\text{a)} \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \quad \text{b)} \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \quad \text{c)} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \quad \text{d)} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Question. Given $[R]$, the zero-one matrix of some relation R, can you write a computer program which computes $[\overline{R}]$, the matrix of $\overline{R}$?

Theorem 3.2. Let R be a relation on A. The transitive closure of R is the smallest transitive relation on A which contains R as a subset.

Proof. We first show that $\overline{R}$ is transitive. Let (a,b) and (b,c) be two elements in $\overline{R}$. This means that $(a,b) \in R^i$ and $(b,c) \in R^j$ for some exponents $i, j \leq n$. It follows that $(a,c) \in R^{i+j}$, and hence $(a,c) \in R^k \subseteq \overline{R}$ for some $k \leq n$.

Now let S be another transitive relation on A such that $R \subseteq S$. To complete the proof, we will show that $\overline{R} \subseteq S$ by proving that $R^k \subseteq S$ for all $k \leq n$. By induction, suppose that we have established $R^k \subseteq S$. Then $R^{k+1} = R \circ R^k \subseteq S \circ S \subseteq S$ since S is transitive. $\bigtriangledown$

Exercise 3.15. Prove that $\overline{R} = R$ if and only if R is transitive.

Question. What can we say about $\overline{\overline{R}}$, i.e., the transitive closure of $\overline{R}$?

Exercise* 3.16. In a similar way, we may define the *reflexive closure* and *symmetric closure* of $R \subseteq A \times A$ to be the smallest reflexive, respectively symmetric, relation on A which contains R. Find a formula to find the reflexive closure of a given R, and similarly for symmetric closure.

3.1.4 Equivalence Relations

Definition. A relation R on a set A is an *equivalence relation* if R is reflexive, symmetric, and transitive. If R is an equivalence relation, for each $a \in A$ we define the *equivalence class* of a to be the set $[a] = \{x \in A \mid (a, x) \in R\}$.

Example. Let $A = \{1, 2, 3, 4, 5, 6\}$ and $R = \{(a, b) \in A \times A \mid a + b \text{ is even}\}$. Show that R is an equivalence relation and find all the equivalence classes of A under this relation.

Solution. We have $R = \{(1, 1), (1, 3), (1, 5), (2, 2), (2, 4), (2, 6), (3, 1), (3, 3), (3, 5), (4, 2), (4, 4), (4, 6), (5, 1), (5, 3), (5, 5), (6, 2), (6, 4), (6, 6)\}$ and note that R is reflexive, symmetric, and transitive. The equivalence classes are

$$\begin{array}{lll} [1] = \{1, 3, 5\} & [2] = \{2, 4, 6\} & [3] = \{1, 3, 5\} \\ [4] = \{2, 4, 6\} & [5] = \{1, 3, 5\} & [6] = \{2, 4, 6\} \end{array}$$

Hence there are only two distinct classes, i.e., $\{1, 3, 5\}$ and $\{2, 4, 6\}$.

Question. Is it always true that $a \in [a]$ for every equivalence class of $a \in A$?

Exercise 3.17. Prove that each R is an equivalence relation and find the equivalence classes.
a) $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a + b \text{ is even}\}$
b) $A = \{1, 2, 3, 4\}$ and $R = \{(a, b) \in A \times A \mid a = b\}$
c) $A = \{0, 5, 8, 9, 10, 11\}$ and $R = \{(a, b) \in A \times A \mid a \bmod 3 = b \bmod 3\}$
d) $A = \{1, 2, 3, 6, 7, 9, 11, 12\}$ and $R = \{(a, b) \in A \times A \mid a \equiv b \pmod 4\}$

Test 3.18. Which zero-one matrix represents an equivalence relation?

$$\text{a)} \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \quad \text{b)} \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \quad \text{c)} \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \quad \text{d)} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Theorem 3.3. Let R be an equivalence relation on a set A. For any $a, b \in A$, the following four propositions are equivalent one to another.

$$a \in [b] \quad \leftrightarrow \quad b \in [a] \quad \leftrightarrow \quad (a, b) \in R \quad \leftrightarrow \quad [a] = [b]$$

Moreover, if $(a, b) \notin R$ then $[a] \cap [b] = \emptyset$.

Proof. We have $(a, b) \in R$ if and only if $b \in [a]$. Since R is symmetric, $(a, b) \in R$ if and only if $(b, a) \in R$. This yields the equivalence among the first three. Moreover, since $a \in [a]$, then $[a] = [b]$ implies $a \in [b]$. Conversely, if $(a, b) \in R$ then $x \in [a]$ implies $(a, x) \in R$ and $(b, x) \in R$ by transitivity. Hence, $x \in [b]$ and $[a] \subseteq [b]$. By a symmetrical argument, then $[a] = [b]$.

To see the last claim, we show its contrapositive: let $x \in [a] \cap [b]$. Since $(a, x) \in R$ and $(b, x) \in R$, then $(a, b) \in R$, by symmetry and transitivity. $\bigtriangledown$

Theorem 3.3 says that the set A is *partitioned* into equivalence classes—the word partitioned means divided into disjoint subsets. The next theorem states that the congruence relation $a \equiv b \pmod{n}$ given in Section 1.2.1 is an equivalence relation on $\mathbb{Z}$—an important one, in fact.

Theorem 3.4. Let $n \geq 2$ be a fixed integer. The congruence relation $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \bmod n = b \bmod n\}$ is an equivalence relation on $\mathbb{Z}$ with exactly n *congruence classes* given by

$$[a]_n = \{kn + a \mid k \in \mathbb{Z}\}$$

for every integer a belonging in the interval $0 \leq a \leq n - 1$.

Proof. It is clear that R is reflexive, symmetric, and transitive. That there are n classes given by $[0], [1], \ldots, [n-1]$ is a consequence of Theorem 1.1 and Theorem 3.3. Moreover, $a \bmod n = b \bmod n$ if and only if n divides $a - b$, by Theorem 2.10, which holds exactly when $b = kn + a$ for any $k \in \mathbb{Z}$. $\bigtriangledown$

For example, with $n = 2$, there are two classes of integers, i.e., the set $[0]_2$ of even numbers and $[1]_2$ of odd numbers. Similarly for $n = 3$, the set $\mathbb{Z}$ is partitioned into three congruence classes:

$$\begin{aligned}
[0]_3 &= \{\ldots, -3, 0, 3, 6, 9, 12, 15, \ldots\} \\
[1]_3 &= \{\ldots, -2, 1, 4, 7, 10, 13, 16, \ldots\} \\
[2]_3 &= \{\ldots, -1, 2, 5, 8, 11, 14, 17, \ldots\}
\end{aligned}$$

Note that every integer belongs to exactly one class.

3.1.5 Partial Order Relations

Definition. A relation R on a set A is called a *partial order relation* when R is reflexive, anti-symmetric, and transitive.

Question. So what is the difference between an equivalence relation and a partial order relation?

Test 3.19. Which zero-one matrix represents a partial order relation?

$$\text{a)}\begin{bmatrix}1&1&0\\0&1&1\\0&0&1\end{bmatrix}\quad \text{b)}\begin{bmatrix}1&1&0\\0&1&1\\1&0&1\end{bmatrix}\quad \text{c)}\begin{bmatrix}1&1&1\\1&1&0\\1&0&1\end{bmatrix}\quad \text{d)}\begin{bmatrix}1&0&1\\0&1&1\\0&0&1\end{bmatrix}$$

A partial order relation R may be represented by its *Hasse diagram*, which can be obtained from the digraph of R in four simple steps:

1) Do not draw loops.

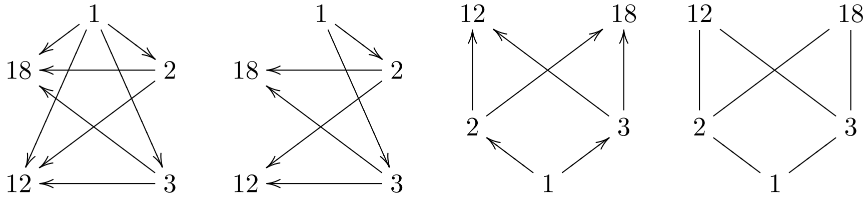
2) Whenever $(a,b) \in R$ and $(b,c) \in R$, do not draw (a,c).

3) Relocate the vertices of R such that each edge points upward.

4) Do not show the direction of each edge, i.e., remove the arrowheads.

Example. Let $A = \{1, 2, 3, 12, 18\}$ and $R = \{(a,b) \in A \times A \mid b \bmod a = 0\}$. Show that R is a partial order relation and draw its Hasse diagram.

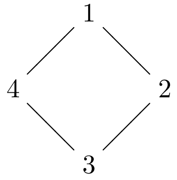
Solution. The fact that R is reflexive, anti-symmetric, and transitive can be easily seen from the digraph, and we show below how it appears following each of the four steps leading to the Hasse diagram of R.



Exercise 3.20. Prove that each relation given below is a partial order relation and then draw its Hasse diagram.
a) $R = \{(a,b) \in \mathbb{N} \times \mathbb{N} \mid a \leq b\}$
b) $A = \{2, 3, 12, 18, 36\}$ and $R = \{(a,b) \in A \times A \mid b \bmod a = 0\}$
c) $A = \{1, 2, 4, 8, 16\}$ and $R = \{(a,b) \in A \times A \mid b \bmod a = 0\}$
d) $A = \{1, 2, 3\}$ and $R = \{(X,Y) \in P(A) \times P(A) \mid X \subseteq Y\}$

Exercise* 3.21. Show that $R = \{(X,Y) \in P(A) \times P(A) \mid X \subseteq Y\}$ is a partial order relation on the power set of any set A.

Question. Suppose that the Hasse diagram has been found, as given below. How can we get back to the digraph or R?



(3.2)

Test 3.22. Which matrix corresponds to the Hasse diagram given in (3.2)?

$$\text{a)} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} \quad \text{b)} \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \quad \text{c)} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} \quad \text{d)} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

Theorem 3.5. The relation $R = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid b \bmod a = 0\}$ is a partial order relation on $\mathbb{N}$.

Proof. It is clear that $(a, a) \in R$ for every $a \in \mathbb{N}$ because $a \bmod a = 0$. Hence R is reflexive. If $a \bmod b = 0 = b \bmod a$, then both b/a and $a/b \in \mathbb{N}$. It follows that $b/a = 1 = a/b$ and $a = b$, so R is anti-symmetric. Finally to show transitive, if (a, b) and $(b, c) \in R$, then b/a and $c/b \in \mathbb{N}$. Hence $b/a \times c/b = c/a \in \mathbb{N}$, implying that $(a, c) \in R$. ▽

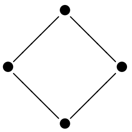
Question. Can you partially sketch the Hasse diagram for this partial order relation $b \bmod a = 0$ on $\mathbb{N}$?

Definition. A relation R on a set A is called a *total order* if R is a partial order such that for any two elements $a, b \in A$, either $(a, b) \in R$ or $(b, a) \in R$.

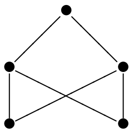
Exercise 3.23. Which ones of the partial order relations given in Exercise 3.20 are total order relations?

Test 3.24. Which Hasse diagram below represents a total order relation?

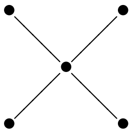
a)



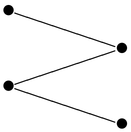
b)



c)



d)



Question. Can you see why the Hasse diagram of a total order relation can always be drawn as a straight line?

Theorem 3.6. The relation $R = \{(a, b) \in \mathbb{R} \times \mathbb{R} \mid a \leq b\}$ is a total order relation on $\mathbb{R}$.

Proof. Reflexive is clear. To see why R is transitive, note that $a \leq b$ and $b \leq c$ imply $a \leq c$. Finally, if $a \neq b$ we have either $a < b$ or $b < a$ but never both, hence R is anti-symmetric and a total order relation. ▽

Exercise* 3.25. Suppose that R is a total order relation on a set A. Prove that the symmetric closure of R is $A \times A$. See Exercise 3.16 for definition.

3.2 Functions

We consider again the concept of a relation from a set A to another, possibly different, set B. The familiar notion of a function which is normally taught in Calculus can now be presented as a binary relation.

Definition. Let A and B be two given sets. The relation $f \subseteq A \times B$ is a *function* from A to B if there is a unique element $(a, b) \in f$ for every $a \in A$. In such a case, we write $f : A \to B$. The element $b \in B$ for which $(a, b) \in f$ will be denoted by $b = f(a)$. Thus $f = \{(a, f(a)) \mid a \in A\}$.

Question. How do we define a function using the symbols $\exists$ and $\forall$?

For example, the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ refers to the relation $f = \{(x, x^2) \mid x \in \mathbb{R}\}$. The following are also some, but not all, possible functions from $\{1, 2, 3, 4\}$ to $\{a, b, c, d, e\}$.

a) $\{(1, a), (2, b), (3, c), (4, d)\}$
b) $\{(1, b), (2, c), (3, d), (4, e)\}$
c) $\{(1, b), (2, d), (3, b), (4, c)\}$
d) $\{(1, a), (2, a), (3, a), (4, a)\}$

Test 3.26. How many different functions from $\{1, 2, 3, 4\}$ to $\{a, b, c, d, e\}$ are possible?

a) 20
b) 120
c) 625
d) 1024

Question. By observing the zero-one matrix of a relation $R \subseteq A \times A$, how can we tell if R is a function?

Definition. The relation R on A given by $R = A^0$ defines a special function $\iota\delta_A : A \to A$ given by $\iota\delta_A(a) = a$ for every $a \in A$. Simply denoted by $\iota\delta$ if there is no ambiguity, this relation is called the *identity function* on A.

Definition. If $f : A \to B$ is a function, we call the set A the *domain* and B the *codomain* of f. Moreover, by the *range* of f we mean the subset of B given by $f(A) = \{f(a) \mid a \in A\}$.

For example, the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ has $\mathbb{R}$ for both its domain and codomain. The range of this f is the non-negative interval $[0, \infty) = \{x \in \mathbb{R} \mid x \geq 0\}$.

Exercise 3.27. Give the largest possible domain for each function below, and then find the range as well.

a) $f(x) = \lfloor x \rfloor$
b) $f(x) = \lceil x \rceil - \lfloor x \rfloor$
c) $f(x) = \dfrac{\log(1+x)}{\sqrt{x}}$
d) $f(m, n) = \gcd(m, n)$

Definition. A function $f : A \to B$ is *one-to-one* or *injective* if every $b \in B$ corresponds to at most one element $(a, b) \in f$. And f is *onto* or *surjective* when $f(A) = B$. If f is both injective and surjective, then we say that f is *bijective*. The noun *bijection* stands for a bijective function. Similarly, an *injection* (*surjection*) stands for an injective (surjective) function. The term *one-to-one correspondence* is a synonym for bijection.

Question. How do we define one-to-one using the symbols $\exists$ and $\forall$?

Note that a function $f : A \to B$ is injective if and only if the proposition $f(a) = f(a') \to a = a'$ holds for every two elements in A. For example, the function $f(x) = x^2$ is not one-to-one because, for instance, both $(2, 4) \in f$ and $(-2, 4) \in f$. The identity function $\iota\delta$, another example, is clearly a bijection on any domain A.

Exercise 3.28. Determine whether the function f is one-to-one or onto.

a) $f : \mathbb{R} \to \mathbb{R};\ f(x) = e^x$
b) $f : \mathbb{R} \to \mathbb{Z};\ f(x) = \lfloor x \rfloor$
c) $f : \mathbb{Z} \to \mathbb{Z};\ f(n) = n + 1$
d) $f : \mathbb{N} \times \mathbb{N} \to \mathbb{Z};\ f(m, n) = \gcd(m, n)$

Test 3.29. How many different one-to-one functions from $\{1, 2, 3, 4\}$ to $\{a, b, c, d, e, f\}$ are possible?

a) 24
b) 120
c) 360
d) 720

Test 3.30. How many different onto functions from $\{1, 2, 3, 4\}$ to $\{x, y, z\}$ are possible?

a) 6
b) 24
c) 33
d) 81

Question. If a function $f : A \to A$ is given by its zero-one matrix, how can we tell if it is one-to-one or onto?

Exercise* 3.31. Let $f : A \to B$ be a function. If $|A| = |B|$, and finite, prove that f is injective if and only if f is surjective.

Theorem 3.7. Consider two functions $f : A \to B$ and $g : B \to C$. The composition $g \circ f$ as a relation from A to C is again a function, i.e., the function $g \circ f : A \to C$ given by $g \circ f(a) = g(f(a))$ for every $a \in A$.

Proof. For every $a \in A$, there is a unique $(a, b) \in f$. With this $b \in B$, there is a unique $(b, c) \in g$. Hence every $a \in A$ corresponds to a unique $(a, c) \in g \circ f$, as desired. $\bigtriangledown$

Exercise 3.32. Find $g \circ f$ by describing $g(f(x))$, where $x \in \mathbb{R}$ and $n \in \mathbb{Z}$, assuming some suitable domain and range for each one.

a) $f(x) = 2x - 1$; $g(x) = x^2 + 1$
b) $f(x) = 6 - 2x$; $g(x) = 3 - x/2$
c) $f(n) = 1/n$; $g(x) = 1/x$
d) $f(n) = n/(n + 1)$; $g(x) = \lfloor x \rfloor$

Theorem 3.8. Let $f : A \to B$ and $g : B \to C$ be two functions. If both f and g are injective, or surjective, then $g \circ f$ is also injective, or surjective. Hence, if f and g are both bijective functions, so is $g \circ f$.

Proof. If f and g are onto, then $f(A) = B$ and $g(B) = C$. In that case, $g(f(A)) = C$ and $g \circ f : A \to C$ is onto. Suppose now $g(f(a)) = g(f(a'))$. If g is injective, then $f(a) = f(a')$. So if f is injective as well then $a = a'$, in which case $g \circ f$ is again an injection. $\bigtriangledown$

Definition. Let $f : A \to B$ be a function. By the *inverse* of f we mean the inverse of f as a relation, i.e., $f^{-1} = \{(f(a), a) \mid a \in A\} \subseteq B \times A$. Note that f^{-1} may or may not be a function. If $S \subseteq B$, we define the *inverse image* of S under the function f to be the subset of A given by $f^{-1}(S) = \{a \in A \mid f(a) \in S\}$.

Exercise 3.33. Which ones of the functions f given in Exercise 3.28 have an inverse f^{-1} which is again a function?

Exercise 3.34. Find $f^{-1}(S)$ using the functions f given in Exercise 3.28, where S is given below for each one, respectively.

a) $S = (0, 1]$
b) $S = \{0\}$
c) $S = [0]_2$
d) $S = \{0\}$

Test 3.35. Which one of the following statements is generally false?

a) $f(S \cup T) = f(S) \cup f(T)$
b) $f(S \cap T) = f(S) \cap f(T)$
c) $f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T)$

d) $f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$

Theorem 3.9. Let $f : A \to B$ be a function. Then f^{-1} is again a function if and only if f is bijective, in which case $f^{-1} : B \to A$ is also a bijection. Moreover, in such a case, we have $f^{-1} \circ f = \iota\delta_A$ and $f \circ f^{-1} = \iota\delta_B$.

Proof. Suppose that f is bijective. Since f is onto, for every $b \in B$ there is $(a, b) \in f$ and is unique since f is one-to-one. Hence, $f^{-1} : B \to A$ is a function. Conversely, suppose that f^{-1} is a function. Then every $b \in B$ corresponds to a unique $a \in A$ such that $f(a) = b$. This forces f to be both onto and one-to-one.

Since $(f^{-1})^{-1} = f$, we see that if f^{-1} is a function, then the argument above shows that f^{-1} is bijective. Moreover, if $f(a) = b$ then $f^{-1}(f(a)) = f^{-1}(b) = a$, showing that $f^{-1} \circ f = \iota\delta_A$. Similarly, $f \circ f^{-1} = \iota\delta_B$. $\bigtriangledown$

3.3 Cardinal Numbers

Recall that the term cardinality is so far defined for finite sets. We will now extend this concept to include infinite sets as well. Before that, however, we note the following properties about the cardinality of finite sets.

Theorem 3.10. Suppose that both A and B are finite sets. Then

1) $|A| \leq |B|$ if and only if there is an injection from A to B.

2) $|A| \geq |B|$ if and only if there is a surjection from A to B.

3) $|A| = |B|$ if and only if there is a bijection from A to B.

4) if $|A| = |B|$ then any function from A to B is injective if and only if surjective.

Proof. Assume that $|A| = m$, $|B| = n$. Moreover let $A = \{a_0, a_1, \ldots, a_{m-1}\}$ and $B = \{b_0, b_1, \ldots, b_{n-1}\}$. If $m \leq n$, define $f : A \to B$ by $f(a_k) = b_k$. Clearly then f is injective, and bijective if $m = n$. If $m \geq n$, we define $f : A \to B$ by $f(a_k) = b_{k \bmod n}$, which is a surjection.

Now suppose that $f : A \to B$ is any function. If f is surjective then $|f^{-1}(B)| \geq n$, and since $f^{-1}(B) \subseteq A$, then $m \geq n$. If f is injective then $|f(A)| = m$, and since $f(A) \subseteq B$, then $m \leq n$. If furthermore f is bijective, then $f(A) = B$ and $m = n$.

Lastly, let $m = n$. If f is one-to-one then $|f(A)| = |B|$, so $f(A) = B$ and f is onto. But if f is not one-to-one then $|f(A)| < |B|$, so f is not onto. $\bigtriangledown$

Based upon these observations, we redefine the term cardinality, now for arbitrary sets, as follows.

Definition. Every set S is associated with a *cardinal number,* which is called the *cardinality* of S and denoted by $|S|$, where we define the following relations involving two arbitrary sets A and B.

1) $|A| = |B|$ if there exists a bijection from A to B.

2) $|A| \preceq |B|$ if there exists an injection from A to B.

3) $|A| \prec |B|$ if $|A| \preceq |B|$ and $|A| \neq |B|$.

4) $|A| \succeq |B|$ if $|B| \preceq |A|$, and $|A| \succ |B|$ if $|B| \prec |A|$.

Intuitively the relation $|A| \preceq |B|$ says that B has "more" elements than A has, by means of one-to-one element matching. Since we are not actually counting the number of elements, this concept applies for infinite sets just as well as for finite sets.

While this definition of cardinality coincides with the old one for finite sets, justifying the use of the same name, the new notation $\preceq$ for "less than" is to keep us reminded that cardinal numbers are not assumed to obey the same law of ordering which applies to ordinary numbers.

Question. Why is it true that $|A| = |B|$ if and only if $|B| = |A|$?

Exercise 3.36. Prove that the relation $\preceq$ on cardinal numbers is reflexive, i.e., $|A| \preceq |A|$, and transitive, i.e., $|A| \preceq |B| \wedge |B| \preceq |C| \rightarrow |A| \preceq |C|$.

Definition. Denote the cardinality of $\mathbb{N}$ by $|\mathbb{N}| = \aleph_0$ (read *aleph naught*) and call a set A *countable* if $|A| \preceq \aleph_0$.

For example, the set $\mathbb{N}$ itself is countable, as is any subset $S \subseteq \mathbb{N}$ because the identity function $\iota\delta : S \rightarrow \mathbb{N}$ is certainly one-to-one. In fact, if $A \subseteq B$ then clearly $|A| \preceq |B|$.

Note that if $f : A \rightarrow \mathbb{N}$ is one-to-one, then the elements of $f(A)$ can be enumerated from least to greatest, $f(a_1) < f(a_2) < f(a_3) < \cdots$ Therefore, if A is countable, we may write $A = \{a_1, a_2, a_3, \ldots\}$ both for the finite as well as infinite cases.

Test 3.37. Which one of the following sets is countable?

a) $\{x \in \mathbb{Z} \mid -5 \leq x \leq 5\}$
b) $\{x \in \mathbb{Z} \mid x \leq 5\}$
c) $\mathbb{N} \cup \{0\}$
d) All of the above are countable sets.

Exercise 3.38. Prove that every subset of a countable set is countable.

Theorem 3.11. The set $\mathbb{Z}$ is countable. In particular, $|\mathbb{Z}| = \aleph_0$.

Proof. We show that the following function $f : \mathbb{Z} \to \mathbb{N}$ is a bijection.

$$f(n) = \begin{cases} 2n & \text{if } n > 0 \\ -2n+1 & \text{if } n \leq 0 \end{cases} \tag{3.3}$$

Suppose that $f(n) = f(m)$. Since $f(n)$ is even if $n > 0$ and odd if $n \leq 0$, then either both $n, m > 0$ or both $n, m \leq 0$. In the first case, $2n = 2m$ and $n = m$. Similarly in the second case, $-2n + 1 = -2m + 1$ and $n = m$. This shows that f is one-to-one. To show onto, let $z \in \mathbb{N}$. If z is even then $f(z/2) = z$. If z is odd, then $f(\frac{z-1}{-2}) = z$. This shows that $f(\mathbb{Z}) = \mathbb{N}$. $\triangledown$

Exercise 3.39. Prove that the union of two countable sets is countable.

Exercise* 3.40. Suppose that $A_1, A_2, A_3, \ldots$ are countable sets. Prove that $\bigcup_{n \geq 1} A_n$ is again countable.

We have seen that the relation $\preceq$ is reflexive and transitive. The next paramount theorem on cardinal numbers states that $\preceq$ is anti-symmetric too, hence a partial order relation.

Theorem 3.12 (Cantor-Schröeder-Bernstein)**.** For arbitrary sets A and B, if $|A| \preceq |B|$ and $|B| \preceq |A|$, then $|A| = |B|$.

Proof. Suppose that $f : A \to B$ and $g : B \to A$ are both injections. We shall construct a bijection in a rather sketchy manner as follows.

Let $A_1 = A$, $A_2 = g(B)$, and $A_n = g(f(A_{n-1}))$ for all $n \geq 3$. Observe, by induction, that $A_{n+1} \subseteq A_n$. Now let $S_n = A_n - A_{n+1}$ for $n \geq 1$, and let $S_{-1} = \bigcap_{n \geq 1} A_n$. It can be shown that A is partitioned into the subsets $S_{-1}, S_1, S_2, \ldots$, noting that S_n may actually be empty from some point on.

On the opposite side, let $B_0 = B$ and $B_n = f(A_n)$ for $n \geq 1$. Similarly, we have $B_{n+1} \subseteq B_n$, and let $T_n = B_n - B_{n+1}$ for $n \geq 0$. This time B is partitioned into $T_{-1}, T_0, T_1, \ldots$, where $T_{-1} = \bigcap_{n \geq 0} B_n$.

It is left as an exercise to show that $f(S_n) = T_n$ if n is odd, and $g(T_n) = S_{n+2}$ if n is even. The bijection we seek can now be constructed by putting together these "piecewise" bijections between the partitioning subsets. $\triangledown$

Theorem 3.13. The set $\mathbb{Q}$ is countable with $|\mathbb{Q}| = \aleph_0$.

Proof. We already have $|\mathbb{Q}| \succeq \aleph_0$. By Theorem 3.12, it suffices now to show $|\mathbb{Q}| \preceq \aleph_0$. Note that every rational number can be written m/n for some unique pair $(m, n) \in \mathbb{Z} \times \mathbb{N}$ with $\gcd(m, n) = 1$ (Exercise 2.59) if we agree to represent $0 = 0/1$. With the bijection f given in (3.3) earlier, the function $g(m/n) = (f(m), n)$ is clearly an injection $g : \mathbb{Q} \to \mathbb{N} \times \mathbb{N}$. In turn, the function $h(m, n) = 2^m \times 3^n$ is an injection $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, due to the uniqueness of prime factorization. The composition $h \circ g : \mathbb{Q} \to \mathbb{N}$ is then an injection which gives us $|\mathbb{Q}| \preceq |\mathbb{N}|$. $\triangledown$

Exercise 3.41. Prove that the cross product of two countable sets is again countable.

Our first example of a set that is not countable is the power set $P(\mathbb{N})$. By Theorem 3.12, it will suffice to show that $|P(\mathbb{N})| \succ \aleph_0$ for this claim. In fact, the cardinality of any set is always exceeded by that of its power set.

Theorem 3.14. For any set A, we have $|A| \prec |P(A)|$.

Proof. The function $f : A \to P(A)$ given by $f(a) = \{a\}$ is clearly an injection. To complete the proof, we show that if $g : A \to P(A)$ is any injection, then g is not onto. Simply let $S = \{a \in A \mid a \notin g(a)\} \in P(A)$. We claim that $g^{-1}(S) = \emptyset$, for if $g(a) = S$ for some $a \in A$, then $a \in S$ if and only if $a \notin g(a) = S$, a contradiction. Hence g cannot be onto. $\triangledown$

What is furthermore true is the fact that $\preceq$ is a total order relation on the set of cardinal numbers. We will not prove this claim, which depends on the so-called *well-ordering principle,* but we present a weaker version which suits our brief treatment on cardinal numbers.

Theorem 3.15. For any set A, exactly one of the relations $|A| \prec \aleph_0$ and $|A| = \aleph_0$ and $|A| \succ \aleph_0$ holds. In particular $|A| \prec \aleph_0$ if and only if A is finite.

Proof. Theorem 3.12 asserts that the three cases are mutually exclusive. It is obvious that there is an injection from any finite set A to $\mathbb{N}$, but never onto. Suppose now A is infinite; we will show that $|\mathbb{N}| \preceq |A|$. We claim that for every $n \in \mathbb{N}$, there is a subset $A_n \subseteq A$ with exactly n elements. Since $A \neq \emptyset$ this claim is true for $n = 1$. Using induction, we assume such A_n exists. Being infinite, $A \neq A_n$ so we can have $a \in A - A_n$. The subset $A_{n+1} = A_n \cup \{a\}$ completes the induction step.

Moreover, in the above construction we have $A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots \subseteq A$. Hence we have a subset $\{a_1, a_2, a_3, \ldots\} \subseteq A$ such that $a_k \in A_k$ and $a_k \neq a_j$ for all $j < k$. This gives the desired injection $f(n) = a_n$ from $\mathbb{N}$ to A. $\triangledown$

Definition. We call a set A *uncountable* if $|A| \succ \aleph_0$. Theorem 3.15 then asserts that being uncountable is indeed the negation of being countable. We also call A *countably infinite* when $|A| = \aleph_0$.

Hence, every set is either finite, countably infinite, or uncountable. In our definition, a countable set is either finite or countably infinite, but in other texts, the term countable is never used for finite sets.

For example, we have seen that both $\mathbb{Z}$ and $\mathbb{Q}$ are countably infinite sets, whereas $P(\mathbb{N})$ is uncountable. Another uncountable set is given by the real numbers.

Theorem 3.16. The set $\mathbb{R}$ is uncountable.

Proof. We will simply establish $|P(\mathbb{N})| \preceq |\mathbb{R}|$. Every $S \in P(\mathbb{N})$ corresponds to a unique infinite sequence $s_1, s_2, s_3, \ldots$, where $s_i = 1$ if $i \in S$ and $s_i = 0$ otherwise. (Recall the proof of Theorem 2.8.) Let $f : P(\mathbb{N}) \to \mathbb{R}$ be given by $f(s_1, s_2, s_3, \ldots) = \sum s_i \times 10^{-i}$, an infinite series convergent to a real number in the interval $[0, 1/9]$. For instance, $f(\emptyset) = 0$, $f(\mathbb{N}) = 0.\overline{1} = 1/9$, and $f(\{1, 4\}) = 0.1001$. We observe that f is one-to-one. $\bigtriangledown$

Definition. We define $|\mathbb{R}| = c$, and call this quantity the *cardinality of the continuum.*

Exercise 3.42. Prove that the set of real numbers in the interval $(0, \infty)$ has cardinality c.

It can be shown that $|P(\mathbb{N})| = c$. Cantor's *continuum hypothesis* claims that there is no cardinal number strictly between $\aleph_0$ and c. Nevertheless, there are cardinal numbers larger than c, e.g., $c \prec |P(\mathbb{R})| \prec |P(P(\mathbb{R}))| \prec \cdots$ In 1963 Paul Cohen proved that the continuum hypothesis is independent of the common axioms of set theory.

3.4 Introduction to Groups

Group theory is normally taught as a first course in abstract algebra. Without going into much depth, we shall introduce the study of groups as a natural extension of sets and relations. In particular, we will be content being able to prove Fermat's little theorem, a promise we made upon stating Theorem 1.12.

Definition. By a *binary operation* $\star$ on a set S, we simply mean a function $f : S \times S \to S$ which is expressed by writing $f(a, b) = a \star b$. We say that $\star$ is *commutative* when $a \star b = b \star a$ for all $(a, b) \in S \times S$.

In practical example, a binary operation on $S = \mathbb{R}$ can be the ordinary addition or multiplication, or something like $a \star b = a + b + ab$, as long as the given function has its codomain in S.

Definition. A *group* G is a set together with a binary operation $\star$ on G which satisfies the following three conditions.

1) The operation $\star$ is *associative,* i.e., $a \star (b \star c) = (a \star b) \star c$ for all elements $a, b, c \in G$.

2) There exists an *identity element* $e \in G$, which has the property that $a \star e = e \star a = a$ for every element $a \in G$.

3) With a fixed identity element $e \in G$, each element $a \in G$ has an *inverse* $b \in G$, i.e., one for which $a \star b = b \star a = e$.

Example. We give several examples of what a group might look like.

1) The set of integers $\mathbb{Z}$ together with ordinary addition, which we know associative, is a group. The number $e = 0$ is an identity element, and an inverse of $a \in \mathbb{Z}$ is $-a$, since $a + (-a) = 0$. In fact, $\mathbb{Q}$ and $\mathbb{R}$, under addition, are also groups. From now on, when we say *the* group $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$, it is understood that the operation involved is addition.

2) The set of non-zero rational numbers $\mathbb{Q}^*$ is a group under the usual multiplication. Here, an identity element is $e = 1$, and each $a/b \in \mathbb{Q}^*$ has an inverse b/a. Similarly, the set $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \neq 0\}$ is a group under multiplication. In the future, we refer to the groups $\mathbb{Q}^*$ and $\mathbb{R}^*$ without explicitly stating that they are under multiplication.

3) Note that $\mathbb{Z}^*$, the set of non-zero integers, is not a group under multiplication. If it were, the identity element would be $e = 1$. But then there will be no inverse for the element $2 \in \mathbb{Z}^*$.

4) The set $G = \{0\}$ under addition is a group, where 0 is the identity and only element in G. Essentially, this is the only kind of a group with one element, denoted by $\{e\}$, and it is called the *trivial group.*

5) The set $M(2, \mathbb{R})$ of 2×2 matrices with real entries is a group under matrix addition. Can you identify the identity element and inverses in this group? More generally, the set $M(n, S)$ of $n \times n$ matrices over S is a group under matrix addition, where S can be $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$.

6) The set $GL(2, \mathbb{R})$ of 2×2 matrices with non-zero determinants is also a group under matrix multiplication. We know from linear algebra that matrix multiplication is associative. The identity element here is $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, and recall that having a non-zero determinant is equivalent to being invertible.

Exercise 3.43. Let $G = \{x \in \mathbb{R} \mid x \neq -1\}$, and introduce the binary operation $a \star b = a + b + ab$ for all $a, b \in G$. Prove that G is a group.

Test 3.44. Which one of these four fails to be a group?

a) The set $\{3n \mid n \in \mathbb{Z}\}$ under addition.
b) The set $\{2^n \in \mathbb{Q} \mid n \in \mathbb{Z}\}$ under multiplication.
c) The set $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ under multiplication.
d) The set $\{A \in M(2, \mathbb{Z}) \mid \det A = \pm 1\}$ under matrix multiplication.

3.4.1 Some Basic Properties

Theorem 3.17. Every group has a unique identity element. Moreover, every element in a group has a unique inverse.

Proof. Let G be a group with two identity elements, e and f. Since e is identity, $e \star f = f$, and since f is identity, $e \star f = e$. Hence $e = f$. For the second claim, let $a \in G$ have two inverses b and c. Then $a \star b = a \star c = e$. Operate both sides by b from the left and then apply associativity to get

$$\begin{aligned} b \star (a \star b) &= b \star (a \star c) \\ (b \star a) \star b &= (b \star a) \star c \\ e \star b &= e \star c \\ b &= c \end{aligned}$$

This shows that a can have only one inverse. $\bigtriangledown$

Question. If $a \star b = a$ holds for two elements in a set S, can we conclude that S has an identity element, i.e., $e = b$?

From now on, we use the phrase *the* identity element, denoted by e, and *the* inverse of an element a, denoted by a^{-1}. Moreover, for convenience, we write ab instead of $a \star b$, unless sometimes when the operation is actually addition, then we write $a + b$ in order to avoid confusion. (Also, under addition, it is better to keep the notation for inverse as $-a$ instead of a^{-1}.) Due to associativity, we may then write the product abc without ambiguity, which generalizes to any finite number of elements, $a_1 a_2 a_3 \cdots a_n$, without the need of brackets.

Question. Is it true that $(a^{-1})^{-1} = a$ for any group element?

Exercise 3.45. Prove that $(ab)^{-1} = b^{-1}a^{-1}$ in any group.

Exercise* 3.46. If G and H are two groups, with their respective binary operations, prove that the direct product $G \times H = \{(g, h) \mid g \in G, h \in H\}$ is a group under the operation defined by $(g, h)(g', h') = (gg', hh')$.

Note that if a relation $ab = ac$ holds in a group, then $a^{-1}(ab) = a^{-1}(ac)$ and $b = c$ by associativity. This is a group property called the *cancellation law,* which may be applied left and right, as follows.

Theorem 3.18. Let G be a group and $a, b, c \in G$. If $ab = ac$ then $b = c$, and if $ba = ca$ then $b = c$.

Question. If $ab = a$ holds for two elements in a group G, can we conclude that the identity element of G is $e = b$?

As a precaution, we should not assume that cancellation laws always apply, unless we know that we are dealing with group elements. For example, we have $BA = CA$ with matrices

$$\begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} = \begin{bmatrix} 2 & 4 \\ 4 & 8 \end{bmatrix}$$

but $B \neq C$, seemingly contradicting the theorem.

Question. What is wrong with the above false counter-example?

Definition. We say that a group G is *abelian* when the binary operation $\star$ on G is commutative. Also, we say that the group G is *finite* or *infinite* referring to G as a set.

All the examples that we have seen so far are abelian groups, except $GL(2, \mathbb{R})$, since matrix multiplication is not commutative.

Exercise 3.47. Prove that a group G is abelian if and only if, for all the elements of G, any one of the following propositions holds.

a) $ab = ca \rightarrow b = c$
b) $axb = cxd \rightarrow ab = cd$
c) $(ab)^2 = a^2b^2$
d) $(ab)^{-1} = a^{-1}b^{-1}$

Exercise* 3.48. Prove that if $a^2 = e$ for every element a in a group G with identity e, then G is abelian.

3.4.2 The Groups $\mathbb{Z}_n$ and $\mathbb{U}_n$

Until now we have not encountered any finite groups—other than the trivial group, of course—but soon we will see two families of groups which have a finite number of elements.

For a fixed positive integer n, let us define the set

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

We have seen in Thereom 3.4 that the sets $[a]_n = \{a + nk \mid k \in \mathbb{Z}\}$, where $a \in \mathbb{Z}_n$, constitute the congruence (equivalence) classes under the relation $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \bmod n = b \bmod n\}$. Let us first claim some facts about these congruence classes.

Theorem 3.19. With $[a]_n = \{a + nk \mid k \in \mathbb{Z}\}$, suppose that $x \in [a]_n$ and $y \in [b]_n$. Then $x + y \in [a + b]_n$ and $xy \in [ab]_n$.

Question. How does this theorem compare with Theorem 1.11?

Proof. Let $x = a+nr$ and $y = b+ns$. Then $x+y = (a+b)+n(r+s) \in [a+b]_n$ and $xy = ab + n(as + br + nrs) \in [ab]_n$. ▽

Definition. On the set $\mathbb{Z}_n$, we define the binary operations *addition mod n* and *multiplication mod n* by, respectively,

$$a +_n b = (a + b) \bmod n$$
$$a \times_n b = ab \bmod n$$

It is clear that both operations are commutative. To illustrate, we describe in tabular form the addition and multiplication mod 4 on the set $\mathbb{Z}_4 = \{0, 1, 2, 3\}$.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Question. Can you see from the table why $\mathbb{Z}_4$ is *not* a group under $\times_4$?

Exercise 3.49. Construct the *multiplication* mod n table for $\mathbb{Z}_n$, for each $n = 5$, 6, 7, and 8. Ignoring the zero element, which tables suggest that we have a group?

We show now that $\mathbb{Z}_n$ is an abelian group under addition mod n.

1) By Theorem 3.19, $a +_n b \in [a + b]_n$. Hence, both $a +_n (b +_n c)$ and $(a +_n b) +_n c$ belong to $[a + b + c]_n$, and both lie in the range from 0 to $n - 1$. We conclude that, proving associativity,

$$a +_n (b +_n c) = (a +_n b) +_n c = (a + b + c) \bmod n$$

2) The identity element of $\mathbb{Z}_n$ is $e = 0$. This is obvious.

3) Every non-zero $a \in \mathbb{Z}_n$ has an inverse given by $-a = n - a$. This is true because $a +_n (n - a) = n \bmod n = 0$.

Exercise* 3.50. Show that $a \times_n (b +_n c) = (ab + ac) \bmod n$ for all elements $a, b, c \in \mathbb{Z}_n$.

We have hinted that in general $\mathbb{Z}_n$ is not a group under $\times_n$. Nevertheless, we will have a multiplicative group if we select only certain elements of $\mathbb{Z}_n$. More precisely, we consider the subset of $\mathbb{Z}_n$ defined by

$$\mathbb{U}_n = \{m \in \mathbb{Z}_n \mid \gcd(m, n) = 1\}$$

Take, for instance, $\mathbb{U}_{10} = \{1, 3, 7, 9\}$ with its multiplication table,

$\times_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Recall that $\gcd(m, n) = 1$ means that the two numbers have no common prime factor. Hence if $a, b \in \mathbb{U}_n$, then neither does ab have a common factor with n. In particular, we would have $1 = \gcd(ab, n) = \gcd(n, ab \bmod n)$ by Theorem 1.3. This shows that multiplication mod n is indeed a binary operation on $\mathbb{U}_n$.

Exercise 3.51. Construct the multiplication table for the set $\mathbb{U}_{12}$.

Question. If p is prime, what are the elements in $\mathbb{U}_p$?

To see why $\times_n$ is associative on $\mathbb{U}_n$, we similarly note that $a \times_n b \in [ab]_n$, so that we are able to conclude that

$$a \times_n (b \times_n c) = (a \times_n b) \times_n c = abc \bmod n$$

This time, the identity element of $\mathbb{U}_n$ is $e = 1$. Hence, for $\mathbb{U}_n$ to be a group, we are left to showing inverses. By Theorem 1.6, if $\gcd(m, n) = 1$ then we can find integers x and y such that $mx + ny = 1$. With these, $[mx]_n = [1]_n$ and so the inverse of m in $\mathbb{U}_n$ is given by $m^{-1} = x \bmod n$.

Exercise 3.52. Find the inverse of each element in the group $\mathbb{U}_{11}$.

We wrap up our introduction to these two finite groups by revealing their proper names.

Definition. Let $n \in \mathbb{N}$. The abelian group $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ under addition mod n is called the *group of integers mod n*. The elements $m \in \mathbb{Z}_n$ for which $\gcd(m, n) = 1$ are called *units*. And, the subset $\mathbb{U}_n = \{m \in \mathbb{Z}_n \mid \gcd(m, n) = 1\}$, which is an abelian group under multiplication mod n, is called the *group of units of $\mathbb{Z}_n$*.

3.4.3 Subgroups

Definition. A subset H of a group G is called a *subgroup* of G, in which case we write $H \subseteq G$, if H is itself a group under the same binary operation inherited from G.

Example. We illustrate the idea with several examples.

1) Since $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$ as sets, and all three are groups under addition, we may state that $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$, and that $\mathbb{Q}$ is a subgroup of $\mathbb{R}$.

2) The set $\mathbb{Q}^*$ under multiplication is a group and a subgroup of $\mathbb{R}^*$. The subset $\mathbb{Z}^*$ is not a subgroup of $\mathbb{Q}^*$, because $\mathbb{Z}^*$ is not a group under multiplication.

3) The subset $2\mathbb{Z}$ of even numbers is a subgroup of $\mathbb{Z}$ under addition. Note that the sum of two even numbers is again even, which says that addition is a binary operation on $2\mathbb{Z}$. That the three group axioms hold in $2\mathbb{Z}$ is easy to verify.

4) The set $S = \{1, -1\}$ forms a group under multiplication, so S is a subgroup of $\mathbb{Q}^*$. Although $\{1, -1\} \subseteq \mathbb{Z}^*$ as sets, we are not allowed to say that S is a subgroup of $\mathbb{Z}^*$, since the latter is not a group.

5) Every group is a subgroup of itself. Moreover, the trivial group $\{e\}$ can be viewed as a subgroup of every given group G.

6) The subset $\mathbb{U}_n$ is not a subgroup of $\mathbb{Z}_n$ even though both of them are groups, because they are defined with different binary operations.

7) The set $M(2, \mathbb{Z})$ is a subgroup of $M(2, \mathbb{R})$ under matrix addition.

Test 3.53. Which one of the following four sets is a subgroup of $\mathbb{Z}$?

a) $\{\pm 1\}$
b) $\{-1, 0, 1\}$
c) $\{6n \mid n \in \mathbb{Z}\}$
d) $\{2n + 1 \mid n \in \mathbb{Z}\}$

Exercise* 3.54. Prove that the group $GL(2, \mathbb{R})$ under matrix multiplication has a subgroup given by $SL(2, \mathbb{R})$, which consists of 2×2 matrices with determinant ± 1.

Observe that if $ab = a$ holds for two elements in a subgroup $H \subseteq G$, then by the cancellation law in G, we must have $b = e$. Similarly, if $ab = e$ then $b = a^{-1}$. We state these facts in the next theorem, followed by another theorem which serves as a subgroup test.

Theorem 3.20. If H is a subgroup of G, then the identity element of H is that of G. Moreover, for each $a \in H$, its inverse in H is the same $a^{-1} \in G$.

Exercise 3.55. If H and K are subgroups of G, prove that $H \cap K$ is also a subgroup of G. Conclude that the generalized intersection of any collection of subgroups is again a subgroup.

Exercise* 3.56. If H and K are subgroups of the same group G, is it true that $H \cup K$ is too a subgroup? Prove your claim or find a counter-example.

Theorem 3.21. A non-empty subset H of a group G is a subgroup if and only if $ab^{-1} \in H$ whenever $a, b \in H$.

Proof. Necessity is clear. Suppose the required condition is satisfied in H. Associativity in H is inherited from G. There is at least one element $a \in H$, hence $aa^{-1} = e \in H$. Also, for each $a \in H$ we have $ea^{-1} = a^{-1} \in H$. Last but not least, we have to verify that $a, b \in H$ implies $ab \in H$. This follows since $b \in H$ implies $b^{-1} \in H$, so $a, b \in H$ implies $a(b^{-1})^{-1} = ab \in H$. $\bigtriangledown$

Example. The set $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ under addition passes the subgroup test, since $nk + (-nj) = n(k - j) \in n\mathbb{Z}$. Thus $n\mathbb{Z} \subseteq \mathbb{Z}$. In particular, $2\mathbb{Z}$ is the subgroup of even numbers under addition.

Exercise* 3.57. Give a non-trivial example of a subgroup $H \subseteq \mathbb{Q}$ under addition, such that $\mathbb{Z} \subseteq H$.

It is not hard to see that Theorem 3.21 can also be presented as a two-step subgroup test: H is a subgroup if and only if (1) H is closed under multiplication, i.e., $a, b \in H \to ab \in H$ and (2) H is closed under inverse, i.e., $a \in H \to a^{-1} \in H$.

Exercise 3.58. Justify each subgroup relation $H \subseteq G$ claimed below.

a) $\{5n \mid n \in \mathbb{Z}\} \subseteq \mathbb{Z}$
b) $\{\pi^n \mid n \in \mathbb{Z}\} \subseteq \mathbb{R}^*$
c) $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z} \wedge a^2 - 2b^2 = 1\} \subseteq \mathbb{R}^*$
d) $\{A \in M(2, \mathbb{Z}) \mid \det A = \pm 1\} \subseteq GL(2, \mathbb{R})$

Exercise 3.59. Let H be a *finite* non-empty subset of a group G. Show that H is a subgroup of G, if $ab \in H$ whenever $a, b \in H$.

Exercise* 3.60. The *centralizer* of an element a in a group G is defined by $C(a) = \{x \in G \mid ax = xa\}$. Show that $C(a) \subseteq G$, and conclude that the *center* of a group, i.e., $Z(G) = \{x \in G \mid ax = xa \ \forall a \in G\}$ is also a subgroup of G, upon observing that $Z(G) = \bigcap_{a \in G} C(a)$.

3.4.4 Cyclic Groups

Definition. Suppose that G is a group and $a \in G$. For every $k \in \mathbb{N}$, we define a^k recursively by $a^1 = a$ and $a^k = a^{k-1}a$. In addition, let $a^0 = e$ and $a^{-k} = (a^{-1})^k$.

Theorem 3.22. Let G be a group, $a \in G$, and $j, k \in \mathbb{Z}$. Then,

1) $a^{-k} = (a^{-1})^k = (a^k)^{-1}$

2) $a^j a^k = a^{j+k} = a^k a^j$

3) $(a^j)^k = a^{jk} = (a^k)^j$

Proof. If $k \geq 0$, then $a^{-k}a^k = (a^{-1})^k a^k = e$ by associativity. This holds for $k \leq 0$ as well by symmetry, proving that $a^{-k} = (a^k)^{-1}$. Also, if $k \leq 0$, $(a^{-1})^k = ((a^{-1})^{-1})^{-k} = a^{-k}$, proving (1). The rest is an exercise. $\bigtriangledown$

Exercise 3.61. Complete the proof of Theorem 3.22.

Question. Is it true that $a^k b^k = (ab)^k$?

Consistent with our earlier agreement, when the group operation is addition, we have $a^k = a + a + \cdots + a$. In that case, we choose to write ka in place of a^k. This also agrees with the fact that $0a = 0$, the identity element of addition. Similarly, $-ka = k(-a)$.

Definition. Let G be a group and $a \in G$. Let us define the set

$$\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$$

and we will show that $\langle a \rangle$ is a subgroup of G, which we call the *cyclic subgroup of* G *generated by* a.

Theorem 3.23. For every $a \in G$, the set $\langle a \rangle$ is an abelian subgroup of G.

Proof. Commutativity is stated in Theorem 3.22, which also says that if $a^j, a^k \in \langle a \rangle$, then $a^j(a^k)^{-1} = a^j a^{-k} = a^{j-k} \in \langle a \rangle$. Hence, $\langle a \rangle$ passes the subgroup test of Theorem 3.21. $\bigtriangledown$

For example, the group $2\mathbb{Z}$ of even numbers is really the cyclic subgroup of $\mathbb{Z}$ generated by 2. And in general, we may write $n\mathbb{Z} = \langle n \rangle \subseteq \mathbb{Z}$.

Definition. Let G be a group and $a \in G$. If $\langle a \rangle = G$, then we call the group G *cyclic*. In such a case, then, G is generated by a, and so we call a a *generator* for the cyclic group G.

Question. Are all cyclic groups abelian? What about the converse?

Example. The group $\mathbb{Z}$ under addition is a cyclic group generated by 1. Similarly, $\mathbb{Z}_n = \langle 1 \rangle$ for all $n > 0$, under addition mod n. Another example is $\mathbb{U}_5 = \{1, 2, 3, 4\}$ under $\times_5$, where 2 and 3 are both generators.

Exercise 3.62. Find all the generators for the cyclic group $\mathbb{Z}_n$, for each $n = 8$, 9, 10, and 11.

Test 3.63. Which one of these four elements does *not* generate $\mathbb{Z}_{36}$?

a) 1
b) 15
c) 25
d) 35

Exercise 3.64. Find all the generators for the group $\mathbb{U}_n$, for each $n = 11$, 12, 13, and 14, if cyclic.

Unlike $\mathbb{Z}_n$, the group $\mathbb{U}_n$ is not always cyclic. In number theory, a generator for $\mathbb{U}_n$, if cyclic, is called a *primitive root* modulo n. It is known that primitive roots exist if and only if $n = 1, 2, 4, p^k$, or $2p^k$, for any prime $p > 2$ and $k \in \mathbb{N}$.

Exercise* 3.65. If a group has only three elements, prove that it must be cyclic.

Theorem 3.24. Any subgroup of a cyclic group is again cyclic.

Proof. Let $G = \langle a \rangle$ and $H \subseteq G$. If $H = \{e\}$ then $H = \langle e \rangle$, cyclic. Otherwise let $n \in \mathbb{N}$ be the least exponent for which $a^n \in H$. We claim that $H = \langle a^n \rangle$. Well, clearly $\langle a^n \rangle \subseteq H$. Now for each $a^m \in H$ we may write $m = qn + r$, with $q = \lfloor m/n \rfloor$ and $r = m \bmod n$. Then $a^r = a^m (a^{-n})^q \in H$. But since $0 \le r < n$, this would contradict the minimality of n, unless $r = 0$. Hence $a^m = (a^n)^q \in \langle a^n \rangle$, and it follows that $H \subseteq \langle a^n \rangle$. $\bigtriangledown$

Example. Since $\mathbb{Z}$ is cyclic, every subgroup $H \subseteq \mathbb{Z}$ is given by $H = \langle n \rangle = n\mathbb{Z}$, i.e., the set of multiples of some $n \in \mathbb{Z}$. Moreover, as shown in the proof, n is the least positive integer in H. In particular, knowing that the intersection of subgroups is again a subgroup, we have $m\mathbb{Z} \cap n\mathbb{Z} = c\mathbb{Z}$, where c is the least natural number which is a multiple of both m and n. This leads us to the next result.

Theorem 3.25. If $m, n \in \mathbb{N}$ then $m\mathbb{Z} \cap n\mathbb{Z} = \text{lcm}(m, n)\mathbb{Z}$. In particular, if $\gcd(m, n) = 1$, then $m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$.

Exercise* 3.66. Suppose that G and H are both cyclic groups. Give an example where $G \times H$ is cyclic, and another where $G \times H$ is not cyclic.

3.4.5 Cosets

Definition. Let H be a subgroup of a group G. For elements $a, b \in G$, we define the relation $a \sim b$ if and only if $ab^{-1} \in H$.

Your job is to prove that $a \sim b$ defines an equivalence relation on G. For example, if $G = \mathbb{Z}$, under addition, and $H = \langle n \rangle$, then $a \sim b$ if and only if $a - b \in \langle n \rangle$. But this is just the congruence relation $a \bmod n = b \bmod n$, which we proved in Theorem 3.4.

Exercise 3.67. Given $H \subseteq G$, verify that $R = \{(a, b) \mid a \sim b\}$ is indeed an equivalence relation on G, where $a \sim b$ if and only if $ab^{-1} \in H$.

Definition. We call the equivalence class of $a \in G$ under this relation the *coset* of a in G with respect to the subgroup H, given by

$$\begin{aligned} Ha &= \{b \in G \mid b \sim a\} \\ &= \{b \in G \mid ba^{-1} \in H\} \\ &= \{b \in G \mid ba^{-1} = h \wedge h \in H\} \\ &= \{b \in G \mid b = ha \wedge h \in H\} \\ &= \{ha \mid h \in H\} \end{aligned}$$

Hence, for example, with the relation $a \equiv b \pmod{n}$ on $\mathbb{Z}$, where $H = \langle n \rangle$, the cosets are the congruence classes $[a]_n$, in agreement with the fact that $Ha = \{h + a \mid h \in \langle n \rangle\} = \{nk + a \mid k \in \mathbb{Z}\} = [a]_n$.

Example. Consider $\mathbb{U}_7 = \{1, 2, 3, 4, 5, 6\}$ with its subgroup $\langle 2 \rangle = \{1, 2, 4\}$. For each element $a \in \mathbb{U}_7$, we compute the coset $\langle 2 \rangle a$:

$$\begin{array}{lll} \langle 2 \rangle 1 = \{1, 2, 4\} & \langle 2 \rangle 2 = \{2, 4, 1\} & \langle 2 \rangle 3 = \{3, 6, 5\} \\ \langle 2 \rangle 4 = \{4, 1, 2\} & \langle 2 \rangle 5 = \{5, 3, 6\} & \langle 2 \rangle 6 = \{6, 5, 3\} \end{array}$$

Note that in this example, only two of the cosets are distinct.

Exercise 3.68. Describe the cosets of each given group G, induced by the relation $a \sim b$, with respect to the subgroup $H \subseteq G$.

a) $\langle 18 \rangle \subseteq \mathbb{Z}_{24}$
b) $\langle 3 \rangle \subseteq \mathbb{U}_{13}$
c) $5\mathbb{Z} \subseteq \mathbb{Z}$
d) $\{\pm 1\} \subseteq \mathbb{Q}^*$

Definition. The number of distinct cosets, with respect to the subgroup $H \subseteq G$ and the relation $a \sim b$, is denoted by $[G{:}H]$. We call this quantity $[G{:}H]$ the *index* of H in G, which could happen to be infinite. Moreover, let us call $|G|$, i.e., the cardinality of the set G, the *order* of the group G.

From the properties of equivalence classes, we conclude that these cosets form a partition for the group G. From this fact, we now deduce a series of results leading to our goal of proving Fermat's little theorem.

Theorem 3.26. Let G be any group with a subgroup H. For each $a \in G$, we have $|Ha| = |H|$.

Proof. Every element in Ha is of the form ha for some $h \in H$. Moreover, $ha = h'a$ implies $h = h'$ by the cancellation law. This gives a one-to-one correspondence between Ha and H which proves the claim, regardless H is finite or infinite. $\bigtriangledown$

Theorem 3.27 (Lagrange's Theorem)**.** The order of any subgroup H divides the order of the group G, provided that G is finite. In such a case, $|G|/|H| = [G{:}H]$.

Proof. Let G be a finite group and $H \subseteq G$. There can be only finitely many cosets in G with respect to H, say $[G{:}H] = k$. Since G is partitioned into the k cosets, we have $k|H| = |G|$ by Theorem 3.26. $\bigtriangledown$

Exercise 3.69. Suppose that H and K are finite subgroups of G. If $\gcd(|H|, |K|) = 1$, show that $H \cap K$ is the trivial group.

Exercise* 3.70. Show that any group of prime order is cyclic and, in such a case, any non-identity element is a generator.

Definition. Let G be a group and $a \in G$. The *order* of a in G, denoted by $|a|$, is the smallest $n \in \mathbb{N}$ such that $a^n = e$. If there is no such number n, we let $|a| = |\langle a \rangle|$.

For example, in $\mathbb{U}_5$ we have $2^2 = 4$, $2^3 = 3$, and $2^4 = 1$; hence $|2| = 4$ in this group. Similarly, in $\mathbb{Z}_{12}$ we have $|2| = 6$. The next theorem explains why we choose the cardinal number $|a| = |\langle a \rangle|$ for an alternative.

Exercise 3.71. Suppose that $|a| = 12$ in the group G. Determine the order of $a^k \in G$, for each k in the range $1 \le k \le 12$.

Test 3.72. Given that $|a| = 24$ in G, what is the order of $a^{15} \in G$?
a) 8
b) 24
c) 72
d) 120

Theorem 3.28. Let a be an element of a group G. Then $|a| = |\langle a \rangle|$.

Proof. Let $|a| = n \in \mathbb{N}$ (else nothing to prove), and let $H = \{a, a^2, \ldots, a^n\}$. Note that $a^n = e$. First, we claim that $|H| = n$ by showing that the elements $a, a^2, \ldots, a^n$ are all distinct. To see why, suppose $a^j = a^k$ with $1 \le j < k \le n$. Then $a^{k-j} = e$ with $0 < k - j < n$, contradicting the minimality of n. Next, we would be done if $H = \langle a \rangle$. Clearly, $H \subseteq \langle a \rangle$. Now let $a^m \in \langle a \rangle$. We write $m = qn + r$, where $q = \lfloor m/n \rfloor$ and $r = m \bmod n$. Since $a^n = e$, then $a^m = (a^n)^q a^r = a^r \in H$ as $0 \le r < n$. Thus $\langle a \rangle \subseteq H$. $\bigtriangledown$

Theorem 3.29. The order of any element in a finite group divides the order of the group. As a consequence, for every $a \in G$, we have $a^{|G|} = e$.

Proof. For finite groups, $|a| = |\langle a \rangle| = n \in \mathbb{N}$, and by Lagrange's theorem, this quantity divides $|G|$. Hence, $a^{|G|} = (a^n)^{|G|/n} = e$. $\bigtriangledown$

And now, if p is a prime number, and if we let $a \in \mathbb{U}_p = \{1, 2, \ldots, p-1\}$ in Theorem 3.29, then $a^{p-1} \bmod p = 1$. With a touch from Theorem 3.19, or 1.11, Fermat's little theorem follows at last.

Theorem 3.30 (Fermat's Little Theorem)**.** Let $a \in \mathbb{Z}$ and p be a prime, not dividing a. Then $a^{p-1} \bmod p = 1$. More generally, if $\gcd(a, n) = 1$ then $a^{\phi(n)} \bmod n = 1$, where $\phi(n) = |\mathbb{U}_n|$.

Definition. The function $\phi(n) = |\mathbb{U}_n|$, with domain $\mathbb{N}$, is called the *Euler's phi function,* and the generalization of Fermat's little theorem for $\mathbb{U}_n$ is better known as Euler's theorem.

Exercise* 3.73. Evaluate $\phi(p^n)$, where p is a prime number and $n \geq 1$.

3.4.6 Finite Cyclic Groups

Given a cyclic group $G = \langle a \rangle$ of finite order n, we seek to identify the order of each element $a^k \in G$, where $1 \leq k \leq n$. Since every subgroup of G is generated by one element, as G itself is, such knowledge will lead to the classification of all the subgroups of G.

Theorem 3.31. Let $a \in G$, not assumed cyclic. Then $a^k = e$ if and only if $|a|$ divides k.

Proof. Let $|a| = n$ and write $k = qn + r$ with $0 \leq r < n$. We have $a^k = (a^n)^q a^r = a^r$. By the minimality of n, then $a^k = e$ if and only if $r = 0$. $\bigtriangledown$

Exercise 3.74. Let G and H be two finite cyclic groups. Show that $G \times H$ is again cyclic, if $\gcd(|G|, |H|) = 1$.

Exercise* 3.75. If $\gcd(m, n) > 1$, prove that $\mathbb{Z}_m \times \mathbb{Z}_n$ is *not* cyclic.

Theorem 3.32. Suppose $a \in G$, not assumed cyclic, such that $|a| = n$. Then $|a^m| = n/\gcd(m, n)$.

Proof. Assume first $\gcd(m, n) = 1$. Let $|a^m| = k$. Then $a^{mk} = e$ and n divides mk by Theorem 3.31. But n has no common factor with m, hence n must divide k. In particular, $k \geq n$. Since $(a^m)^n = (a^n)^m = e$, the minimality of k implies that $k = n$. Thus $|a^m| = n/\gcd(m, n)$.

Now suppose $\gcd(m,n) = d > 1$. Note that $s = n/d$ is the least natural number for which $(a^d)^s = e$. Thus $|a^d| = n/d$. Since $\gcd(m/d, n/d) = 1$, the same argument above gives $|a^m| = |(a^d)^{m/d}| = n/d = n/\gcd(m,n)$. $\bigtriangledown$

Test 3.76. Given that $|a| = 12$ in G, which one of the following four elements also has order 12?

a) a^{10}
b) a^{12}
c) a^{25}
d) a^{27}

Theorem 3.33. Let G be a cyclic group of order n, generated by a. Let $d \in \mathbb{N}$ be any divisor of n. Then,

1) $G = \langle a^m \rangle$ if and only if $\gcd(m,n) = 1$.

2) G has exactly $\phi(n)$ generators.

3) G has exactly $\phi(d)$ elements of order d.

4) G has a unique subgroup of order d.

Proof. We have $\langle a^m \rangle = \langle a \rangle$ if and only if $|a^m| = |a|$, i.e., if and only if $\gcd(m,n) = 1$, according to Theorem 3.32. Writing $G = \{e, a, a^2, \ldots, a^{n-1}\}$, we see that $G = \langle a^m \rangle$ if and only if $m \in \mathbb{U}_n$. Hence, G has $\phi(n)$ generators. This proves the first two claims.

Since $|a^{n/d}| = d$, we have a subgroup $\langle a^{n/d} \rangle$ of order d. To show uniqueness, suppose also $|\langle a^k \rangle| = d = n/\gcd(k,n)$. Then $\gcd(k,n) = n/d$. In particular, n/d divides k, and $a^k \in \langle a^{n/d} \rangle$. Hence $\langle a^k \rangle \subseteq \langle a^{n/d} \rangle$ and, being of the same size, we conclude that $\langle a^k \rangle = \langle a^{n/d} \rangle$, proving (4).

It also follows that every element b of order d will give us $\langle b \rangle = \langle a^{n/d} \rangle$. In particular, b generates the cyclic group of order d, and we have shown that there are $\phi(d)$ such generators. $\bigtriangledown$

Exercise 3.77. Let $m \in \mathbb{Z}_n$. Prove that $\mathbb{Z}_n = \langle m \rangle$ if and only if $m \in \mathbb{U}_n$.

Test 3.78. Given that $\mathbb{U}_{19}$ is cyclic, how many generators does it have?

a) 1
b) 6
c) 9
d) 18

Exercise* 3.79. Prove that $\mathbb{U}_n$ has exactly $\phi(\phi(n))$ generators, if cyclic.

Test 3.80. If G is cyclic and $|G| = 96$, how many elements have order 24?

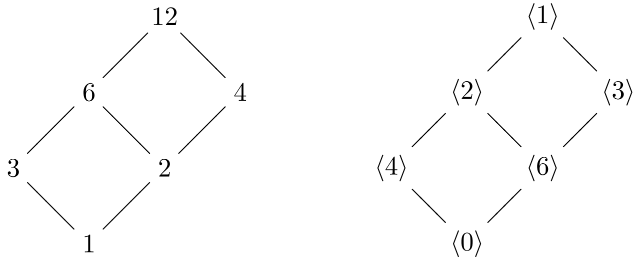
a) 0
b) 4
c) 8
d) 12

Exercise* 3.81. For every $n \in \mathbb{N}$, show that $\sum \phi(d) = n$, where d ranges over all the divisors of n.

Combined with Lagrange's theorem, Theorem 3.33 yields a one-to-one correspondence between subgroups of a cyclic group G and divisors of $|G|$. In fact, the subgroups are themselves cyclic, so for any two of them, the relation $H \subseteq K$ holds if and only if $|H|$ divides $|K|$.

And now, since *divisor-of* is a partial order relation on $|G|$, its Hasse diagram corresponds to that for the subgroups of G under the *subgroup-of* relation, which we call the *subgroup lattice* of the finite cyclic group G.

Example. To draw the subgroup lattice of $\mathbb{Z}_{12}$, we start with the set of positive divisors of 12, i.e., $A = \{1, 2, 3, 4, 6, 12\}$. For each $d \in A$, we identify the unique subgroup of order d—in this case $\langle 12/d \rangle$. Both Hasse diagrams, for $R = \{(a, b) \mid b \mod a = 0\}$ on A and for $S = \{(H, K) \mid H \subseteq K\}$ on the subgroups of G are compared side-by-side below.



Exercise 3.82. Draw the subgroup lattice for each of the cyclic groups $\mathbb{Z}_{30}$, $\mathbb{Z}_{36}$, and $\mathbb{U}_{17}$.

3.4.7 Permutation Groups

To conclude this section, we shall introduce an entirely different kind of groups, in the sense that they are not number sets. In fact, we will have a group of bijective functions on a finite set, otherwise known as permutations, and in particular, a family of permutation groups related to geometry.

Definition. By a *permutation* on a set A, we mean a function $f : A \to A$ which is one-to-one and onto. For $n \in \mathbb{N}$, we denote by S_n the set of all permutations on the set $\{1, 2, 3, \ldots, n\}$. It is not hard to see that $|S_n| = n!$ and that it is a group under function composition. We call S_n the *symmetric group* of degree n and call any subgroup of S_n a *permutation group.*

Exercise 3.83. Verify that S_n is a group of order $n!$ under composition.

Example. Consider S_6, the set of $6! = 720$ permutations on $\{1, 2, 3, 4, 5, 6\}$. An element $f \in S_6$ may be written in *cyclic notation*; e.g., $f = (1, 2, 5)(3, 6)$, which means that the function f is given by

$$\begin{array}{lll} f(1) = 2 & f(2) = 5 & f(3) = 6 \\ f(4) = 4 & f(5) = 1 & f(6) = 3 \end{array}$$

Note that 4 is missing in the notation; this is understood as $f(4) = 4$. In general, a number left unchanged by the permutation can be omitted from the cyclic notation, except when writing the identity permutation, i.e., $e = (1)$.

Definition. The term *cycle* refers to each bracketed part in the cyclic notation. It is intuitively clear that every permutation can be represented by *disjoint* cycles, i.e., where no two cycles contain a common term.

For example, the permutation $(1, 2, 5)(3, 6)$ is written in two disjoint cycles. Moreover, the terms in a cycle may be permuted in a circular manner, e.g., $(1, 2, 5) = (2, 5, 1) = (5, 1, 2)$.

Following convention, recall that composition is read from right to left, and it is generally non-commutative, e.g.,

$$(1, 2, 5)(3, 6) \circ (4, 6, 2, 1) = (1, 4, 3, 6, 5)$$
$$(4, 6, 2, 1) \circ (1, 2, 5)(3, 6) = (2, 5, 4, 6, 3)$$

But note that disjoint cycles commute: e.g., $(1, 2, 5) \circ (3, 6) = (1, 2, 5)(3, 6) = (3, 6) \circ (1, 2, 5)$.

Exercise 3.84. Show that S_n is non-abelian for all $n \geq 3$.

Exercise 3.85. Determine the order of each element of S_n given below.

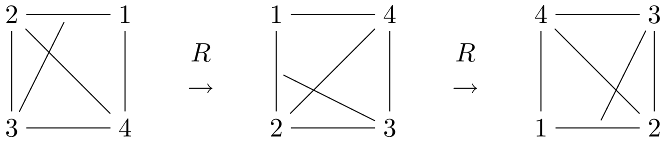
a) (2,1,5,6,4,3)
b) (2,1,5)(6,4,3)
c) (2,1,5)(6,4)
d) (2,1,5)(6,4)(3,9,7,8)

Exercise* 3.86. Draw the subgroup lattice for $\langle f \rangle$, a cyclic subgroup of S_5 generated by $f = (1, 2, 3)(4, 5)$.

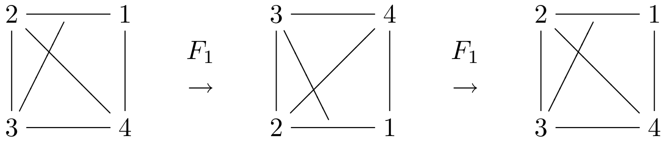
Consider a regular n-gon whose vertices are labeled 1 to n in a counterclockwise sequence. There are n symmetries which are obtained by rotations around the center. It is clear that these n rotations form a cyclic subgroup $\langle R\rangle$ of S_n, where $R = (1, 2, 3, \ldots, n)$, i.e., the $2\pi/n$ rotation.

Moreover, there are n symmetries which result from reflections across the n axes of symmetry. Note that $|F| = 2$ for each reflection $F \in S_n$. These $2n$ rotations and reflections form a permutation group, which is called the *dihedral group* of degree n, denoted by D_n.

Example. With $n = 4$, there are four rotations, $R = (1, 2, 3, 4), R^2, R^3$, and $R^4 = e$, which correspond to $\pi/2, \pi, 3\pi/2$, and 2π radians, respectively.



The four reflections can be represented by $F_1 = (1, 4)(2, 3)$, $F_2 = (2, 4)$, $F_3 = (1, 2)(3, 4)$, and $F_4 = (1, 3)$—symmetries with respect to the x-axis, the line $y = x$, the y-axis, and the line $y = -x$, respectively.



The claim that D_4 is a group is supported by its composition table below, keeping in mind that composition reads right to left.

Table 3.1: The composition table of the group D_4.

$\circ$	R	R^2	R^3	R^4	F_1	F_2	F_3	F_4
R	R^2	R^3	R^4	R	F_2	F_3	F_4	F_1
R^2	R^3	R^4	R	R^2	F_3	F_4	F_1	F_2
R^3	R^4	R	R^2	R^3	F_4	F_1	F_2	F_3
R^4	R	R^2	R^3	R^4	F_1	F_2	F_3	F_4
F_1	F_4	F_3	F_2	F_1	R^4	R^3	R^2	R
F_2	F_1	F_4	F_3	F_2	R	R^4	R^3	R^2
F_3	F_2	F_1	F_4	F_3	R^2	R	R^4	R^3
F_4	F_3	F_2	F_1	F_4	R^3	R^2	R	R^4

Exercise* 3.87. Describe the cosets of S_4 with respect to the subgroup D_4 and the relation $a \sim b$ as before.

Exercise 3.88. Construct the composition tables for D_3 and D_5, clearly distinguishing between the rotations and the reflections.

Being a finite subset of S_n, by Exercise 3.59, D_n is a subgroup if and only if it is closed under composition, meaning that $g \circ f \in D_n$ whenever $f, g \in D_n$. The key facts needed in the proof are summarized in the next two exercises.

Exercise 3.89. A rotation shifts the vertices of the n-gon but preserves their counter-clockwise circular ordering. A reflection, on the other hand, reverses the ordering in the clockwise direction. Prove these claims.

Exercise 3.90. In D_n, show that the composition of two rotations or two reflections is a rotation, whereas a mixed composition yields a reflection.

Exercise 3.91. Determine the order of each element in D_n.

Since $|D_n| = 2n$, in particular we have $D_3 = S_3$. Other than this exception, D_n is a proper subgroup of S_n and is non-abelian as S_n is.

Exercise 3.92. If $F \in D_n$ is a reflection, show that $F \circ R = R^{n-1} \circ F$, and conclude that D_n is non-abelian for all $n \geq 3$.

Exercise* 3.93. Prove that a subgroup of D_n is cyclic, if its order is odd.

Books to Read

1. E. D. Bolker, *Elementary Number Theory: An Algebraic Approach,* 1970, Dover Publications 2007.

2. P. J. Cohen, *Set Theory and the Continuum Hypothesis,* 1966, Dover Publications 2008.

3. J. F. Humphreys and M. Y. Prest, *Numbers, Groups and Codes,* Second Edition, Cambridge University Press 2004.

4. D. Joyner, *Adventures in Group Theory: Rubik's Cube, Merlin's Machine, and Other Mathematical Toys,* Second Edition, Johns Hopkins University Press 2008.