MA291: Introduction to Higher Mathematics

Dylan C. Beck

Acknowledgements

Primarily, the contents of this document were created in the Fall 2022 and Spring 2023 semesters at Baker University. I am grateful to the students in MA291 (Introduction to Higher Mathematics) — especially those who assisted in the enhancement of these notes with comments and suggestions.

Contents

Chapter 1

Sets, Relations, and Functions

Contemporary mathematics is communicated rigorously using sets, symbols, functions, relations, certain computational tools, and proofs; thus, it is imperative for us to develop the necessary diction, grammar, and syntax in order for us to effectively communicate. We accomplish this formally via the tools of set theory and the calculus of logic. Even now, these branches of mathematics enjoy an ongoing ubiquity and significance that makes them an active area of research, but we will not trouble ourselves with these subtle complexities. (Explicitly, if it matters to the reader, we will adopt the standard axioms of the Zermelo-Fraenkel set theory with the Axiom of Choice.)

1.1 Describing a Set

We define a **set** X as a collection of like objects, e.g., the names of the 2021-2022 Golden State Warriors, the groceries on this week's shopping list, or any collection of real numbers. We refer to an arbitrary object x of X as an **element** (or **member**) of X. If x is an element of X, then we write $x \in X$ to denote that "x is an element (or member) of the set X." We may also say in this case that x "belongs to" or "lies in" X, or we may wish to emphasize that X "contains" x. Conversely, if y does not lie in X, then we write $y \notin X$ to signify this fact symbolically.

Order and repetition are irrelevant notions when considering the elements of a set. Explicitly, the set W consisting only of the real numbers 1 and -1 can be realized as $W = \{-1, 1\}$ or $W = \{1, -1\}$ or $W = \{-1, 1, -1, 1\}$. Out of desire for simplicity, we will list only the distinct elements of a set. If there are "few enough" distinct elements of a set X, then we can explicitly write down X using curly braces. Observe that $X = \{1, 2, 3, 4, 5, 6\}$ is the unique set consisting of the first six positive integers. Unfortunately, as the number of members of X increases, such an explicit expression of X becomes cumbersome to write down; instead, we may use **set-builder notation** to express a set whose members possess a closed-form. Explicitly, set-builder notation exhibits an arbitrary element x of the attendant set X followed by a bar $\mid$ and a list of qualitative information about x, e.g.,

$$X = \{1, 2, 3, 4, 5, 6\} = \{x \mid x \text{ is an integer and } 1 \leq x \leq 6\}.$$

Even more, set-builder notation can be used to write down infinite sets. We will henceforth fix the following notation for the natural numbers $\mathbb{Z}_{\geq 0} = \{n \mid n \text{ is a non-negative integer}\}$, the integers $\mathbb{Z} = \{n \mid n \text{ is an integer}\}$, and the rational numbers $\mathbb{Q} = \left\{\frac{a}{b} \mid a \text{ and } b \text{ are integers such that } b \neq 0\right\}$. Using the rational numbers, one can construct the real numbers $\mathbb{R} = \{x \mid x \text{ is a real number}\}$.

Example 1.1.1. Crucially, we must be able to transition between set-builder notation and curly brace notation. Given the set $S = \{n \mid n \text{ is an integer such that } |n| \leq 3\}$, we find that $-3 \leq n \leq 3$, hence there are $3 - (-3) + 1 = 7$ elements of S. We have that $S = \{-3, -2, -1, 0, 1, 2, 3\}$.

Example 1.1.2. Consider the finite set $T = \{-7, -5, -3, \dots, 11, 13\}$. We have used an ellipsis here to signify that the pattern repeats up to the integer 11. Each of the integers -7, -5, -3, 11, and 13 are odd integers, hence the set T consists of all odd integers t such that $-7 \leq t \leq 13$. Put another way, we may use set-builder notation to express that $T = \{t \mid t \text{ is an odd integer and } -7 \leq t \leq 13\}$. We could have perhaps more easily described this set as $T = \{t \in \mathbb{Z} \mid t \text{ is odd and } -7 \leq t \leq 13\}$.

Example 1.1.3. Consider the infinite set $U = \{x^2 \mid x \in \mathbb{Z}_{\geq 0}\}$. Every element of U is the square of some non-negative integers, hence we have that $U = \{0, 1, 4, 9, \dots\}$. Once again, we use an ellipsis to signify to the reader that the pattern continues; however, in this case, it does so indefinitely.

One important consideration in the arithmetic of sets is the number of elements that belong to the set. For instance, it is clear that the set $X = \{1, 2, 3, 4, 5, 6\}$ consists of six elements, but the set $Y = \{1, 2, 3, 4, 5\}$ possesses five elements. Observe that this immediately distinguishes the sets X and Y. We refer to the number of elements in a finite set X as the **cardinality** of X, denoted by $\#X$ or $|X|$. Like we previously mentioned, we have that $|X| = 6$ and $|Y| = 5$. Cardinality can be defined even for infinite sets, but additional care must be taken in this case, so we will not bother.

Example 1.1.4. Consider the following four sets written in set-builder notation.

$$A = \{n \in \mathbb{Z}_{\geq 0} \mid n \leq 9\} \qquad C = \{x \in \mathbb{R} \mid x^2 - 2 = 0\}$$
$$B = \{q \in \mathbb{Q}_{\geq 0} \mid q \leq 9\} \qquad D = \{q \in \mathbb{Q} \mid q^2 - 2 = 0\}$$

(a.) List all of the elements of A.

(b.) List at least three elements of B that do not lie in A. Can we find more than three elements of B that do not lie in A? Exactly how many elements of B do not lie in A?

(c.) List all of the elements of C.

(d.) Explain how many elements lie in D.

(e.) Compute the cardinality of A, C, and D.

1.2 Subsets

Like with the arithmetic of real numbers, there are mathematical operations on sets that allow us, e.g., to compare them; take their differences; and combine them. Every element of $Y = \{1, 2, 3, 4, 5\}$ is also an element of $X = \{1, 2, 3, 4, 5, 6\}$, for instance, but the element $6 \in X$ is not contained in Y. We express this by saying that Y is a **proper subset** of X: the additional modifier "proper" is used to indicate that X and Y are not the same set (because they do not have the same members). Put into symbols, we write that $Y \subsetneq X$ whenever it is true that (i.) every element of Y is also an element of X and (ii.) there exists an element of X that is not contained in Y; this can be read as "Y is contained in X, but Y does not equal X." We may also say that Y is "included in" X or that Y "lies in" X. One other way to indicate that Y is a (proper) subset of X is by saying that X is a (proper) **superset** of Y, in which case we write that $X \supseteq Y$ (or $X \supsetneq Y$ if the containment is proper). Observe that if we could step through the paper and look at the superset containment $X \supseteq Y$ from the other side, we would see nothing more than $Y \subseteq X$; however, it is sometimes preferable to use this notation to emphasize that X is the object of our concern rather than Y.

Containment of subsets is **transitive** in the sense that if $X \subseteq Y$ and $Y \subseteq Z$, then $X \subseteq Z$: indeed, every element $x \in X$ is an element of Y so that $x \in Y$; moreover, every element of Y is an element of Z so that $x \in Z$ ultimately holds. Compare this with inequalities of real numbers.

Example 1.2.1. Consider the sets $A = \{-1, 1\}$, $B = \{-1, 0, 1\}$, and $C = \{-2, -1, 1, 2\}$. Observe that the strict inclusions $A \subsetneq B$ and $A \subsetneq C$ hold, but neither $B \subseteq C$ or $C \subseteq B$ holds.

Example 1.2.2. Every non-negative integer is an integer; every integer is a rational number; and every rational number is a real number. Consequently, we have that $\mathbb{Z}_{\geq 0} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$. Each of these containments is strict because -1 is an integer that is not non-negative; $\frac{1}{2}$ is a rational number that is not an integer; and $\sqrt{2}$ is a real number that is not a rational number. We will refer to the collection of real numbers that are not rational as **irrational numbers**.

Example 1.2.3. Consider the set $U = \{1, 2, 3, 4, 5\}$ with subsets A and B such that

(i.) $|A| = |B| = 3$;

(ii.) 1 lies in A but does not lie in B;

(iii.) 2 lies in B but does not lie in A;

(iv.) 3 lies in either A or B but not both;

(v.) 4 lies in either A or B but not both; and

(vi.) 5 lies in either A or B but not both.

List all possibilities for A in curly brace notation; then, determine the corresponding sets B.

Equality of sets is determined by simultaneous subset and superset containments. Explicitly, a pair of sets X and Y are equal if and only if it holds that $X \subseteq Y$ and $X \supseteq X$. Put another way, the sets X and Y are equal if and only if X and Y possess exactly the same elements: indeed, for any element $x \in X$, we have that $x \in Y$ because $X \subseteq Y$, and for any element $y \in Y$, we have that $y \in X$ because $X \supseteq Y$. Crucially, one can demonstrate that two finite sets are equal if and only if they have the same cardinality and one of the sets is a subset of the other.

Often, we will view a set X as a subset of a specified **universal set** (or **ambient set**) U. Explicitly, in each of the examples from the previous two sections, we typically dealt with integers, hence we could have taken the ambient set as $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$. Context will usually make this clear.

1.3 Set Operations

Consider the sets $X = \{1, 2, 3, 4, 5, 6\}$ and $Y = \{1, 2, 3, 4, 5\}$ of the previous section. We introduce the **relative complement** of Y with respect to X to formalize our previous observation that 6 belongs to X but does not belong to Y. By definition, the relative complement of Y with respect to X is the set consisting of the elements of X that are not elements of Y. We use the symbolic notation $X \setminus Y = \{w \in X \mid w \notin Y\}$ to denote the relative complement of Y with respect to X, e.g., we have that $X \setminus Y = \{6\}$ in our running example. We may view the relative complement of Y with respect to X as the "set difference" of X and Y. Conversely, the two sets X and Y "overlap" in $\{1, 2, 3, 4, 5\}$ because they both contain the elements 1, 2, 3, 4, and 5. We define the **intersection** $X \cap Y = \{w \mid w \in X \text{ and } w \in Y\}$ of the sets X and Y as the set consisting of those elements that belong to both X and Y; in this case, we have that $X \cap Y = \{1, 2, 3, 4, 5\}$.

Order does not matter with respect to the intersection of two sets. Explicitly, for any sets X and Y, we have that $X \cap Y = Y \cap X$ because every element that lies in both X and Y lies in both Y and X. Consequently, set intersection is a **commutative** (or **order-invariant**) operation.

Example 1.3.1. Draw a **Venn diagram** to visually represent the sets X, Y, $X \setminus Y$, and $X \cap Y$.

Example 1.3.2. Consider the sets $A = \{1, 2, 3, \dots, 10\}$, $B = \{1, 4, 9\}$, and $C = \{1, 3, 5, 7, 9\}$. We have that $A \setminus B = \{2, 3, 5, 6, 7, 8, 10\}$, $A \setminus C = \{2, 4, 6, 8, 10\}$, $B \setminus C = \{4\}$, and $C \setminus B = \{3, 4, 7\}$. Each of the sets A and B is a proper subset of A, and we have that $A \cap B = B$ and $A \cap C = C$.

Crucially, if $B \subseteq A$, then $A \cap B = B$: indeed, every element of B is an element of A, hence we have that $A \cap B \supseteq B$. Conversely, every element of $A \cap B$ is an element of B so that $A \cap B \subseteq B$.

Example 1.3.3. Consider the sets $D = \{1, 3, 5, 7\}$, $E = \{1, 4, 7, 10\}$, and $F = \{2, 5, 8, 11\}$. We have that $D \setminus E = \{3, 5\}$, $D \setminus F = \{1, 3, 7\}$, $E \setminus D = \{4, 10\}$, and $F \setminus D = \{2, 8, 11\}$. Even more, we have that $D \cap E = \{1, 7\}$, $D \cap F = \{5\}$, and E and F have no elements in common.

Consider the finite sets $V = \{1, 2, 3\}$ and $W = \{4, 5, 6\}$. Because none of the elements of V belongs to W and none of the elements of W belongs to V, the intersection of V and W does not possess any elements; it is empty! Conventionally, this is called the **empty set**; it is denoted by $\emptyset$. Put another way, our observations thus far in this paragraph can be stated as $V \cap W = \emptyset$. We will soon see that the empty set is a proper subset of every nonempty set. Going back to our discussion of V and W, we remark that the keen reader might have noticed that $W = X \setminus V$ and $V = X \setminus W$, i.e., every element of X lies in either V or W but not both (because there are no elements that lie in both V and W). We say in this case that the set X is the **union** of the two sets V and W, and we write $X = V \cup W$. Generally, the union of two sets X and Y is the set consisting of all objects that are either an element of X or an element of Y — that is, $X \cup Y = \{w \mid w \in X \text{ or } w \in Y\}$. Like the set intersection, set union is also a commutative (or order-invariant) operation.

Example 1.3.4. Consider the sets A, B, and C of Example 1.3.2. Each of the elements of B and C are elements of A, hence we have that $A \cup B = A$, $A \cup C = A$, and $B \cup C = \{1, 3, 4, 5, 7, 9\}$.

Crucially, if $B \subseteq A$, then $A \cup B = A$: indeed, every element of A is an element of $A \cup B$, hence we have that $A \cup B \supseteq A$. Conversely, every element of $A \cup B$ is an element of A and $A \cup B \subseteq A$.

Example 1.3.5. Consider the sets D, E, and F of Example 1.3.3. Excluding any overlap, we have that $D \cup E = \{1, 3, 4, 5, 7, 10\}$, $D \cup F = \{1, 2, 3, 5, 7, 8, 11\}$, and $E \cup F = \{1, 2, 4, 5, 7, 8, 10, 11\}$.

Every set X gives rise to a unique set consisting of all possible subsets of X. Explicitly, for any set X, the **power set** $P(X)$ is the set of all subsets of X — including the empty set.

Example 1.3.6. Consider the set $U = \{-1, 0, 1\}$. Counting the empty set, there are eight subsets of U. Each subset is composed by either including or excluding a given element of U. Label the elements of U in order; then, construct an ordered triple consisting of check marks ✓ and crosses $\times$ corresponding respectively to whether an element of U is included or excluded.

$$\begin{array}{ll} \times\times\times\colon \emptyset & \checkmark\checkmark\times\colon \{-1,0\} \\ \checkmark\times\times\colon \{-1\} & \checkmark\times\checkmark\colon \{-1,1\} \\ \times\checkmark\times\colon \{0\} & \times\checkmark\checkmark\colon \{0,1\} \\ \times\times\checkmark\colon \{1\} & \checkmark\checkmark\checkmark\colon \{-1,0,1\} \end{array}$$

Consequently, we have that $P(U) = \{\emptyset, \{-1\}, \{0\}, \{1\}, \{-1, 0\}, \{-1, 1\}, \{0, 1\}, \{-1, 0, 1\}\}$.

Crucially, if U is a finite set, then $|P(U)| = 2^{|U|}$: indeed, every subset of U is uniquely determined by its elements, and each element of U can either be included or excluded from a given subset.

1.4 Indexed Collections of Sets

Often, we wish to consider data coming from more than simply two sets. We achieve this by first creating an **index set** I that contains all of the labels for the sets in question. Explicitly, if we are dealing with three distinct sets X_1, X_2, and X_3, then our index set can be taken as $I = \{1, 2, 3\}$ to indicate the first, second, and third set. Order of set intersections and set unions does not matter, so if our intention is to work with these objects, then we need not worry about the order of the labels of our sets; otherwise, we can label our sets in an order-appropriate manner. We have that

$$X_1 \cap X_2 \cap X_3 = \{x \mid x \in X_1 \text{ and } x \in X_2 \text{ and } x \in X_3\} \text{ and}$$
$$X_1 \cup X_2 \cup X_3 = \{x \mid x \in X_1 \text{ or } x \in X_2 \text{ or } x \in X_3\}.$$

Consequently, in order for an element to lie in the intersection $X_1 \cap X_2 \cap X_3$ of three sets, it must lie in each of the three sets; on the other hand, an element belongs to the union $X_1 \cup X_2 \cup X_3$ if and only if it belongs to at least one of the three sets. Generally, if we wish to consider a finite number $n \geq 2$ of sets $X_1, X_2, \dots, X_n$, then we may consider the index set $I = \{1, 2, \dots, n\} = [n]$. We introduce the following notation to represent the set intersection and set union of n sets.

$$\bigcap_{i \in [n]} X_i = \bigcap_{i=1}^{n} X_i = X_1 \cap X_2 \cap \cdots \cap X_n = \{x \mid x \in X_i \text{ for each integer } 1 \leq i \leq n\} \text{ and}$$
$$\bigcup_{i \in [n]} X_i = \bigcup_{i=1}^{n} X_i = X_1 \cup X_2 \cup \cdots \cup X_n = \{x \mid x \in X_i \text{ for some integer } 1 \leq i \leq n\}.$$

Crucially, observe the language with respect to intersection ("for each") and union ("for some").

Example 1.4.1. Consider the sets $A_1 = \{1, 2\}, A_2 = \{2, 3\}, \dots, A_{10} = \{10, 11\}$. Consequently, our index set is $I = \{1, 2, \dots, 10\} = [10]$ and $A_i = \{i, i+1\}$ for each integer $1 \leq i \leq 10$. We have that

$$\bigcap_{i=1}^{10} A_i = \{a \mid a \in A_i \text{ for each integer } 1 \leq i \leq 10\} = \emptyset,$$

$$\bigcap_{i=j}^{j+1} A_i = \{a \mid a \in A_j \text{ and } a \in A_{j+1}\} = \{j+1\}, \text{ and}$$

$$\bigcap_{i=j}^{k} A_i = \{a \mid a \in A_i \text{ for each integer } 1 \leq j \leq k \leq 10\} = \begin{cases} \{j, j+1\} & \text{if } k = j, \\ \{j+1\} & \text{if } k = j+1, \text{ and} \\ \emptyset & \text{if } k \geq j+2. \end{cases}$$

Consequently, the intersection of these sets is typically empty; however, the union satisfies that

$$\bigcup_{i=1}^{10} A_i = \{a \mid a \in A_i \text{ for some integer } 1 \leq i \leq 10\} = \{1, 2, \dots, 11\},$$

$$\bigcup_{i=3}^{7} A_i = \{a \mid a \in A_i \text{ for some integer } 3 \leq i \leq 7\} = \{3, 4, \dots, 8\}, \text{ and}$$

$$\bigcup_{i=j}^{k} A_i = \{a \mid a \in A_i \text{ for some integer } 1 \leq j \leq k \leq 10\} = \{j, j+1, \dots, k+1\}.$$

Example 1.4.2. Consider the index set $L = \{a, b, c, \dots, z\}$ consisting of all 26 letters of the English alphabet. We may define for each letter $\ell \in L$ the set W_ℓ consisting of all English words that contain the letter ℓ; this induces an indexed collection of sets $\{W_\ell\}_{\ell \in L}$. Certainly, we have that

$$\bigcap_{\ell \in L} W_\ell = \emptyset \text{ and } \bigcup_{\ell \in L} W_\ell = \{\text{words in the English language}\}$$

because there is no word in the English language that consists of all letters of the alphabet. Even more, consider the set $V = \{a, e, i, o, u\}$ of all vowels in the English language. We note that $\cap_{\ell \in V} W_\ell$ consists of many words, including satisfying words like "facetious" and "sequoia." Conversely, the word "why" does not belong to $\cup_{\ell \in V} W_\ell$ because it does not contain any of the letters a, e, i, o, or u.

We need not confine ourselves to the case that our index set is finite. Explicitly, we may consider any collection of sets $\{X_i\}_{i \in I}$ indexed by any nonempty (possibly infinite) set I. We have that

$$\bigcap_{i \in I} X_i = \{x \mid x \in X_i \text{ for each element } i \in I\} \text{ and}$$

$$\bigcup_{i \in I} X_i = \{x \mid x \in X_i \text{ for some element } i \in I\}.$$

We may also refer to the elements $i \in I$ as **indices**; the set $\{X_i\}_{i \in I}$ is an indexed collection of sets.

Example 1.4.3. Consider the infinite index set $I = \mathbb{Z}_{\geq 0}$ consisting of all non-negative integers. We may construct an indexed collection of sets $\{X_i\}_{i \in I}$ by declaring that $X_i = \{i, i+1\}$ for each element $i \in I$. Conventionally, the intersection and union over this infinite index set are written as

$$\bigcap_{i \in I} X_i = \bigcap_{i=0}^{\infty} X_i \text{ and } \bigcup_{i \in I} X_i = \bigcup_{i=0}^{\infty} X_i.$$

Computing the former gives the empty set, but the latter yields the index set $I = \mathbb{Z}_{\geq 0}$.

Example 1.4.4. Consider the infinite index set $\mathbb{Z}_{\geq 1}$ consisting of all positive integers. Each positive integer n gives rise to a closed interval of real numbers

$$C_n = \left[-\frac{1}{n}, \frac{1}{n}\right] = \left\{x \in \mathbb{R} : -\frac{1}{n} \leq x \leq \frac{1}{n}\right\}.$$

Each of these intervals is **nested** within the preceding interval: explicitly, for each integer $n \geq 1$, we have that $C_n \supseteq C_{n+1}$ because for any real number $x \in C_{n+1}$, we have that $x \in C_n$ because

$$-\frac{1}{n} < -\frac{1}{n+1} \leq x \leq \frac{1}{n+1} < \frac{1}{n}.$$

Consequently, it follows that $C_1 \supseteq C_2 \supseteq \cdots$ so that the indexed collection of sets $\{C_n\}_{n=1}^\infty$ forms a **descending chain** of sets. Generally, it is true for descending chains of subsets that the union of all sets in the chain is the largest set in the chain. Put another way, we have that $\cup_{n=1}^\infty C_n = C_1$. On the other hand, the only real number x satisfying that $|x| \leq -\frac{1}{n}$ for all integers $n \geq 1$ is $x = 0$: indeed, if $|x| > 0$, then we can find an integer $n \geq 1$ sufficiently large such that $|x| > -\frac{1}{n}$. We conclude therefore that $\cap_{n=1}^\infty C_n = \{x \in \mathbb{R} : -\frac{1}{n} \leq x \leq \frac{1}{n} \text{ for each integer } n \geq 1\} = \{0\}$.

1.5 Partitions of Sets

We say that two sets X_i and X_j are **disjoint** if $X_i \cap X_j = \emptyset$. Even more, if the indexed collection of sets $\{X_i\}_{i \in I}$ satisfy the condition that X_i and X_j are disjoint for every pair of distinct indices $i, j \in I$, then we say that the set $\{X_i\}_{i \in I}$ is **pairwise disjoint** (or **mutually exclusive**). Often, we will abuse terminology by saying that the sets X_i are pairwise disjoint for each element $i \in I$.

Example 1.5.1. Consider the sets $A = \{1, 4, 7\}$, $B = \{2, 5, 8\}$, and $C = \{3, 6, 9\}$. One can readily verify that $A \cap B = A \cap C = B \cap C = \emptyset$, hence the set $\{A, B, C\}$ is pairwise disjoint.

Example 1.5.2. Consider the sets $D = \{1, 3, 5, 7\}$, $E = \{2, 4, 6, 8\}$, and $F = \{3, 5, 7, 9\}$. We have that $D \cap E = E \cap F = \emptyset$ but $D \cap F = \{3, 5, 7\}$, hence $\{D, E, F\}$ is not pairwise disjoint.

Observe that if $X_i = \emptyset$ for any element $i \in I$, then $X_i \cap X_j = \emptyset$ for all elements $j \in I$ because X_i is empty, hence any indexed collection of sets $\{X_i\}_{i \in I}$ containing the empty set is pairwise disjoint. Consequently, we may restrict our attention to collections of nonempty pairwise disjoint sets. We say that an indexed collection of sets $\mathcal{P} = \{X_i \mid i \in I\}$ form a **partition** of a set X if and only if

(i.) X_i is nonempty for each element $i \in I$;

(ii.) $X = \cup_{i \in I} X_i$; and

(iii.) the sets X_i are pairwise disjoint, i.e., $X_i \cap X_j = \emptyset$ for every pair of distinct indices $i, j \in I$.

We note that every set X admits a partition $\mathcal{X} = \{\{x\} \mid x \in X\}$ indexed by the **singleton** sets $\{x\}$ for each element $x \in X$; however, many of the sets we will consider throughout this course admit more interesting partitions. Explicitly, every integer is either even or odd but not both; the quality of being odd or even is called the **parity** of an integer. Consequently, the integers $\mathbb{Z}$ can be partitioned via $\mathcal{P} = \{\mathbb{E}, \mathbb{O}\}$ such that $\mathbb{E} = \{n \mid n \text{ is an even integer}\}$ and $\mathbb{O} = \{n \mid n \text{ is an odd integer}\}$.

Example 1.5.3. Consider the pairwise disjoint nonempty sets $A = \{1, 4, 7\}$, $B = \{2, 5, 8\}$, and $C = \{3, 6, 9\}$ of Example 1.5.1. Considering that $A \cup B \cup C = \{1, 2, \dots, 9\}$, it follows that the set $\mathcal{P} = \{A, B, C\}$ constitutes a partition of the finite set $[9] = \{1, 2, \dots, 9\}$.

Conversely, even though the nonempty sets $D = \{1, 3, 5, 7\}$, $E = \{2, 4, 6, 8\}$, and $F = \{3, 5, 7, 9\}$ of Example 1.5.2 satisfy $[9] = D \cup E \cup F$, they are not pairwise disjoint and do not partition $[9]$.

Example 1.5.4. Consider the set of integers $\mathbb{Z}$. We have already seen that it is possible to partition $\mathbb{Z}$ into two sets (namely, every integer is either even or odd but not both); we will demonstrate that it is possible to partition $\mathbb{Z}$ into three sets. Given any integer n, divide n by 3; the remainder of this division is unique and must be 0, 1, or 2. Consequently, every integer n can be written as $n = 3q + i$ for some unique integers q and $0 \leq i \leq 2$. Consequently, we have that $\mathbb{Z} = R_0 \cup R_1 \cup R_2$ is a partition of the integers with $R_i = \{3q + i \mid q \in \mathbb{Z}\}$ for each integer $0 \leq i \leq 2$.

Example 1.5.5. Every nonzero rational number can be written uniquely as a **reduced fraction** $\frac{p}{q}$ for some nonzero integers p and q that have no common divisors other than 1. Consider the indexed collection of sets $\{D_q\}_{q=1}^{\infty}$ of nonzero reduced fractions with denominator q, i.e.,

$$D_q = \left\{ \frac{p}{q} : p \in \mathbb{Z} \setminus \{0\} \text{ and } p \text{ and } q \text{ have no common divisors other than } 1 \right\}.$$

Explicitly, we have that

$$D_1 = \{\dots, -2, -1, 1, 2, \dots\},\ D_2 = \left\{\dots, -\frac{3}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{3}{2}, \dots\right\}, \text{ and } D_3 = \left\{\dots, -\frac{2}{3}, -\frac{1}{3}, \frac{1}{3}, \frac{2}{3}, \dots\right\}.$$

Later in the semester, we will prove that D_b and D_q are disjoint for any pair of distinct positive integers b and q. Considering that every nonzero rational number can be written as a reduced fraction, it follows that the collection of nonzero rational numbers is partitioned by $\{D_q\}_{q=1}^{\infty}$.

1.6 Cartesian Products of Sets

Given any sets X and Y, for any elements $x_1, x_2 \in X$, the **ordered pair** (x_1, x_2) is an ordered list of the elements x_1 and x_2 that specifies that x_1 comes first and x_2 comes second. We refer in this case to x_1 as the first **coordinate** of (x_1, x_2) and x_2 is the second coordinate of (x_1, x_2). Crucially, the ordered pairs (x_1, x_2) and (x_2, x_1) are equal if and only if $x_1 = x_2$. Given any other element $x_3 \in X$, the ordered pairs (x_1, x_2) and (x_2, x_3) are equal if and only if $x_1 = x_2$ and $x_2 = x_3$. We are familiar already with ordered pairs of real numbers: indeed, the concept arises naturally in our high school mathematics courses from intermediate algebra to calculus. Consider the collection $X \times Y$ of all ordered pairs (x, y) of elements $x \in X$ and $y \in Y$. We refer to the set $X \times Y$ as the **Cartesian product** of X and Y. Put into symbols, the Cartesian product of the sets X and Y is the set

$$X \times Y = \{(x, y) \mid x \in X \text{ and } y \in Y\}.$$

Example 1.6.1. Consider the sets $X = \{-1, 1\}$ and $Y = \{1, 2, 3\}$. We have that

$$X \times Y = \{(-1, 1), (-1, 2), (-1, 3), (1, 1), (1, 2), (1, 3)\} \text{ and}$$
$$Y \times X = \{(1, -1), (1, 1), (2, -1), (2, 1), (3, -1), (3, 1)\}.$$

Consequently, the Cartesian product of sets is in general not commutative. Explicitly, the above sets $X \times Y$ and $Y \times X$ are not equal because $(-1, 1) \in X \times Y$ and $(-1, 1) \notin Y \times X$.

We may also consider the Cartesian product of a set with itself. We have that

$$X \times X = \{(-1,-1), (-1,1), (1,-1), (1,1)\} \text{ and}$$
$$Y \times Y = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3)\}.$$

Example 1.6.2. Observe that the Cartesian product $\mathbb{Z} \times \mathbb{Z} = \{(a, b) \mid a \text{ and } b \text{ are integers}\}$ is the collection of all integer points in the **Cartesian plane** $\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x \text{ and } y \text{ are real numbers}\}$.

Example 1.6.3. Given any real function $f : \mathbb{R} \to \mathbb{R}$, the **graph** of the function f consists of all ordered pairs $(x, f(x))$ such that x is in the **domain** of f. Explicitly, if we assume that D_f is the domain of f and R_f is the **range** of f, then the graph of f is given by the Cartesian product

$$G_f = D_f \times R_f = \{(x, f(x)) \mid x \in D_f \text{ and } f(x) \in R_f\}.$$

Concretely, if $f(x) = 2x + 3$, then it follows that $G_f = \{(x, 2x + 3) \mid x \in \mathbb{R}\}$.

If X and Y are finite sets with cardinalities $|X|$ and $|Y|$, then the Cartesian product $X \times Y$ has cardinality $|X| \cdot |Y|$ because an element of $X \times Y$ is uniquely determined by the ordered pair (x, y). Consequently, we have that $\emptyset \times Y = X \times \emptyset = \emptyset$ for any sets X and Y.

1.7 Relations

Given any sets X and Y, a **relation from** X to Y is any subset R of the Cartesian product $X \times Y$. Explicitly, a relation R from X to Y consists of ordered pairs whose first component lies in X and whose second component lies in Y. We will say that some element $x \in X$ is **related to** an element $y \in Y$ by R (or that x and y are related by R) if it holds that $(x, y) \in R$, and we will write $x \mathrel{R} y$ in this case; otherwise, if $(x, y) \notin R$, then x is not related to y by R, and we write $x \not\mathrel{R} y$.

Example 1.7.1. Consider the sets $X = \{-1, 1\}$ and $Y = \{1, 2, 3\}$ of Example 1.6.1. We may define the relation $R = \{(1, 1), (1, 2), (1, 3)\}$ from X to Y. Under this relation, it holds that $1 \mathrel{R} 1$, $1 \mathrel{R} 2$, and $1 \mathrel{R} 3$ so that 1 is related to each of the elements of Y. Conversely, we have that $-1 \not\mathrel{R} 1$, $-1 \not\mathrel{R} 2$, and $-1 \not\mathrel{R} 3$ so that -1 is not related to any of the elements of Y.

Every relation R from a set X to a set Y induces two important sets: namely, the collection

$$\operatorname{dom}(R) = \{x \in X \mid (x, y) \in R \text{ for some element } y \in Y\}$$

consists of all elements in X are related to some element of Y by R; it is the **domain** of the relation R from X to Y. Likewise, the **range** of the relation R from X to Y is given by

$$\operatorname{range}(R) = \{y \in Y \mid (x, y) \in R \text{ for some element } x \in X\}$$

and consists of all elements of Y that are related to some element of X by R. Crucially, we note that the domain of a relation R from X to Y only concerns the first coordinate of an element of R, and the range of R only takes into account the second coordinate of an element of R.

Example 1.7.2. Consider the relation $R = \{(1,1),(1,2),(1,3)\}$ from $X = \{-1,1\}$ to $Y = \{1,2,3\}$ of Example 1.7.1. We have that $\operatorname{dom}(R) = \{1\}$ and $\operatorname{range}(R) = \{1,2,3\} = Y$.

Given any relation R from a set X to a set Y, we may define the **inverse relation**

$$R^{-1} = \{(y,x) \mid (x,y) \in R\}.$$

Crucially, if R is a relation from X to Y, then R^{-1} is a relation from Y to X, i.e., $R^{-1} \subseteq Y \times X$.

Example 1.7.3. Consider the relation $R = \{(1,1),(1,2),(1,3)\}$ from $\{-1,1\}$ to $\{1,2,3\}$ of Example 1.7.1. We have that $R^{-1} = \{(1,1),(2,1),(3,1)\}$, $\operatorname{dom}(R^{-1}) = \{1,2,3\}$, and $\operatorname{range}(R^{-1}) = \{1\}$.

We refer to a subset R of the Cartesian product $X \times X$ as a **relation on** X. Every set X admits a relation Δ_X called the **diagonal** of X that consists precisely of the elements of $X \times X$ of the form (x,x). Put another way, the diagonal of X is the relation $\Delta_X = \{(x,x) \mid x \in X\}$. Observe that if X is a finite set with cardinality $|X|$, then the cardinality of $X \times X$ is $|X|^2$, hence there are a total of $2^{|X|^2}$ possible relations on a set X because there are as many subsets of $X \times X$.

Example 1.7.4. Consider the set $X = \{-1,1\}$. We may define relations

$$\begin{aligned}
\Delta_X &= \{(-1,-1),(1,1)\} \text{ with } \operatorname{dom}(\Delta_X) = \{-1,1\} = \operatorname{range}(\Delta_X), \\
R_1 &= \{(-1,1),(1,-1)\} \text{ with } \operatorname{dom}(R_1) = \{-1,1\} = \operatorname{range}(R_1), \text{ and} \\
R_2 &= \{(-1,-1),(-1,1)\} \text{ with } \operatorname{dom}(R_2) = \{-1\} \text{ and } \operatorname{range}(R_2) = \{-1,1\}.
\end{aligned}$$

Observe that $\Delta_X^{-1} = \Delta_X$ and $R_1^{-1} = R_1$ but $R_2^{-1} = \{(-1,-1,),(1,-1)\}$ (R_2 is not its own inverse).

1.8 Properties of Relations

We will continue to assume that X is an arbitrary set. Recall that a relation on X is by definition a subset R of the Cartesian product $X \times X$. We say that R is **reflexive** if and only if $(x,x) \in R$ for all elements $x \in X$ if and only if R contains the diagonal Δ_X of X (i.e., $R \supseteq \Delta_X$). Even more, if it holds that $(y,x) \in R$ whenever $(x,y) \in R$, then R is **symmetric**. Last, if $(x,y) \in R$ and $(y,z) \in R$ together imply that $(x,z) \in R$, then we refer to the relation R as **transitive**.

Example 1.8.1. Consider the following relations on the set $X = \{x,y,z\}$.

$$\begin{aligned}
R_1 &= \{(x,y),(y,z)\} \\
R_2 &= \{(x,x),(x,y),(y,y),(y,z),(z,z)\} \\
R_3 &= \{(x,y),(y,x)\} \\
R_4 &= \{(x,y),(y,z),(x,z)\} \\
R_5 &= \{(x,x),(x,y),(y,x),(y,y),(y,z),(z,y),(z,z)\} \\
R_6 &= \{(x,x),(x,y),(x,z),(y,y),(y,z),(z,z)\} \\
R_7 &= \{(x,x),(x,y),(y,x)\} \\
R_8 &= \{(x,x),(x,y),(x,z),(y,x),(y,y),(y,z),(z,x),(z,y),(z,z)\}
\end{aligned}$$

Observe that R_1 is not reflexive because (x,x) does not lie in R_1; it is not symmetric because (x,y) lies in R_1 but (y,x) does not lie in R_1; and it is not transitive because (x,y) and (y,z) both lie in

R_1 but (x, z) does not lie in R_1. We note that R_2 is reflexive, but it is not symmetric because it contains (x, y) but not (y, x), and it is not transitive because it contains (x, y) and (y, z) but not (x, z). Continuing along these same lines, the reader can deduce the following table.

	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8
reflexive		✓			✓	✓		✓
symmetric			✓		✓		✓	✓
transitive				✓		✓	✓	✓

Example 1.8.2. Consider the relation R defined on the set of integers $\mathbb{Z}$ such that $x \mathrel{R} y$ if and only if $x \leq y$. Certainly, every integer is equal to itself, hence we have that $x \leq x$ for all integers x so that R is reflexive; however, it is not symmetric because $0 < 1$ so that $0 \mathrel{R} 1$ but $1 \not\mathrel{R} 0$. Last, R is transitive because if $x \mathrel{R} y$ and $y \mathrel{R} z$, then $x \leq y \leq z$ so that $x \leq z$ and $x \mathrel{R} z$. Later, we will return to this relation to discuss the property that if $x \mathrel{R} y$ and $y \mathrel{R} x$, then $x = y$.

Example 1.8.3. Consider the relation R' defined on the set of integers $\mathbb{Z}$ such that $x \mathrel{R'} y$ if and only if $x \neq y$. Contrary to Example 1.8.2, this relation is symmetric but neither reflexive nor transitive. Explicitly, we have that $0 = 0$ so that $0 \not\mathrel{R'} 0$ and R' is not reflexive. Likewise, we have that $0 \neq 1$ and $1 \neq 0$ so that $0 \mathrel{R'} 1$ and $1 \mathrel{R'} 0$ but $0 \not\mathrel{R'} 0$, hence R' is not transitive.

Example 1.8.4. Consider the relation D defined on the set of real numbers $\mathbb{R}$ such that $x \mathrel{D} y$ if and only if $|x - y| \leq 1$. One can readily verify that D is reflexive and symmetric: indeed, we have that $|x - x| = 0$ so that $x \mathrel{D} x$ and $|y - x| = |x - y|$ so that $y \mathrel{D} x$ if and only if $x \mathrel{D} y$; however, $0 \mathrel{D} 1$ and $1 \mathrel{D} 2$ do not together imply that $0 \mathrel{D} 2$ because $|2 - 0| > 1$, so D is not transitive.

1.9 Equivalence Relations

Relations that are reflexive, symmetric, and transitive are distinguished as **equivalence relations**.

Example 1.9.1. Consider any set X. We may define a relation R on X by declaring that $x \mathrel{R} y$ if and only if $x = y$. Equality is reflexive because $x = x$ holds for all elements $x \in X$; it is symmetric because $x = y$ implies that $y = x$ for any elements $x, y \in X$; and it is transitive because if $x = y$ and $y = z$, then $x = y = z$ implies that $x = z$ for all elements $x, y, z \in X$. Consequently, equality is an equivalence relation. We will return to this example in various contexts throughout the course. We can synthesize the content of this example as the following important proposition.

Proposition 1.9.2. *Given any set X, the diagonal $\Delta_X = \{(x, x) \mid x \in X\}$ of X is an equivalence relation on X. Explicitly, every set admits at least one equivalence relation on itself.*

Proof. Observe that as a relation on X, the diagonal of X captures equality of the elements of X: if $(x, y) \in \Delta_X$, then we must have that $x = y$, and if $x = y$, then $(x, y) \in \Delta_X$. Put another way, the relation Δ_X can be identified with the equality equivalence relation of Example 1.9.1. □

Example 1.9.3. Consider the collection $\mathcal{C}^1(\mathbb{R})$ of functions $f : \mathbb{R} \to \mathbb{R}$ whose first derivatives $f'(x)$ are continuous for all real numbers x. Let R denote the relation on $\mathcal{C}^1(\mathbb{R})$ defined by $(f, g) \in R$ if and only if $f'(x) = g'(x)$ for all real numbers x. Because R is defined by equality and equality is reflexive, symmetric, and transitive, it follows that R is an equivalence relation on $\mathcal{C}^1(\mathbb{R})$.

Example 1.9.4. Consider the relation R defined the set of integers $\mathbb{Z}$ such that $x \, R \, y$ if and only if $y - x$ is even (i.e., divisible by 2). Considering that $x - x = 0$ is an even integer, it follows that R is reflexive. Even more, if $y - x$ is even, then $x - y = -(y - x)$ is even, hence $y \, R \, x$ holds for all pairs of integers x and y such that $x \, R \, y$. Last, if $y - x$ and $z - y$ are both even integers, then $z - x = (z - y) + (y - x)$ is even (because each term is divisible by 2). Consequently, the relations $x \, R \, y$ and $y \, R \, z$ together yield that $x \, R \, z$. We conclude that R is an equivalence relation on $\mathbb{Z}$.

Example 1.9.5. Often, it is useful to determine if a relation is an equivalence relation by examining its elements explicitly. Consider the following relation defined on the set $[5] = \{1, 2, 3, 4, 5\}$.

$$R = \{(1,1), (1,3), (1,5), (2,2), (2,4), (3,1), (3,3), (3,5), (4,2), (4,4), (5,1), (5,3), (5,5)\}$$

Considering that R contains the diagonal of $[5]$, it follows that R is reflexive. Put another way, we have that $(x, x) \in R$ for all elements $x \in [5]$. Even more, for each element $(x, y) \in R$, we have that $(y, x) \in R$ so that R is symmetric. Last, one can readily verify that if (x, y) and (y, z) both lie in R, then (x, z) lies in R, hence R is transitive. We conclude that R is an equivalence relation on $[5]$.

Let E denote an equivalence relation on an arbitrary set X. Often, it is convenient to adopt the notation that $x \, E \, y$ if and only if $(x, y) \in E$, in which case we may also say that x and y are **equivalent modulo** E. (We note that this convention is due to Carl Friedrich Gauss; it can be understood as asserting that x and y are "the same except for differences accounted for by E.") We define the **equivalence class** $[x]$ of an element $x \in X$ modulo E as the collection of elements $y \in X$ that are equivalent to x modulo E, i.e., $[x] = \{y \in X \mid y \, E \, x\} = \{y \in X \mid (y, x) \in E\}$.

Example 1.9.6. Every element of a set X lies in its own equivalence class modulo the equivalence relation $\Delta_X = \{(x, x) \mid x \in X\}$ because the only elements of Δ_X are the ordered pairs (x, x). Consequently, the equivalence class of any element $x \in X$ is the singleton $[x] = \{x\}$.

Example 1.9.7. Consider the equivalence relation R defined on the set $\mathcal{C}^1(\mathbb{R})$ of Example 1.9.3. By the Mean Value Theorem, if $f'(x) = g'(x)$ for all real numbers x, then there exists a real number C such that $g(x) = f(x) + C$. Conversely, if $g(x) = f(x) + C$ for some real number C, then $f'(x) = g'(x)$. We conclude that the equivalence classes of $\mathcal{C}^1(\mathbb{R})$ modulo R are given precisely by the sets $[f] = \{g \in \mathcal{C}^1(\mathbb{R}) \mid (g, f) \in R\} = \{g \in \mathcal{C}^1(\mathbb{R}) \mid g(x) = f(x) + C \text{ for some real number } C\}$.

Example 1.9.8. Consider the equivalence relation R of Example 1.9.4. By definition, if x is an even integer, then $x - 0$ is an even integer, hence $(x, 0)$ lies in R. Conversely, if $(x, 0)$ lies in R, then $x = x - 0$ is an even integer. We conclude that $[0] = \{x \in R \mid (x, 0) \in R\} = \{x \in R \mid x \text{ is even}\}$. On the other hand, if x is an odd integer, then $x - 1$ is an even integer, hence $(x, 1)$ lies in R. Even more, if $(x, 1)$ lies in R, then $y = x - 1$ is an even integer so that $x = y + 1$ is an odd integer. Considering this as a statement of equivalence modulo R, we have that $[1] = \{x \in R \mid (x, 1) \in R\} = \{x \in R \mid x \text{ is odd}\}$. Every integer is either even or odd, hence these are the only equivalence classes of $\mathbb{Z}$ modulo R.

Example 1.9.9. Consider the equivalence relation R of Example 1.9.5. Each of the integers 1, 3, and 5 are equivalent modulo R because $(1, 3)$ and $(3, 5)$ lie in the equivalence relation R. On the other hand, the integers 2 and 4 are equivalent modulo R because $(2, 4)$ lies in R; thus, there are two distinct equivalence classes modulo R — namely, $[1] = \{1, 3, 5\} = [3] = [5]$ and $[2] = \{2, 4\} = [4]$.

1.10 Properties of Equivalence Classes

Our next propositions illustrate that a pair of equivalence classes of X modulo E are either equal or disjoint; as a corollary, we obtain a relationship between equivalence relations and partitions.

Proposition 1.10.1. *Consider any equivalence relation E an an arbitrary set X. Given any elements $x, y \in X$, we have that $[x] = [y]$ if and only if (x, y) lies in E.*

Proof. We will assume first that $[x] = [y]$. Consequently, for any element $z \in X$ such that $z \in [x]$, we have that $(z, x) \in E$. By assumption, if $z \in [x]$ holds, then $z \in [y]$ holds so that $(z, y) \in E$. By the symmetry of the equivalence relation E, we have that $(x, z) \in E$; then, the transitivity of the equivalence relation E yields that $(x, y) \in E$ because both (x, z) and (z, y) lie in E.

Conversely, we will assume that $(x, y) \in E$. We must demonstrate that $[x] \subseteq [y]$ and $[y] \subseteq [x]$. Given any element $z \in [x]$, we have that $(z, x) \in E$. By assumption that $(x, y) \in E$, the transitivity of E yields that $(z, y) \in E$ so that $z \in [y]$. Likewise, for any element $w \in [y]$, we have that $(w, y) \in E$. By the symmetry of the equivalence relation E, we have that $(y, x) \in E$ by assumption that $(x, y) \in E$, hence the transitivity of E yields that $(w, x) \in E$ so that $w \in [x]$. □

Proposition 1.10.2. *Every pair of equivalence classes of a set X modulo an equivalence relation E are either equal or disjoint. Explicitly, for any elements $x, y \in E$, either $[x] = [y]$ or $[x] \cap [y] = \emptyset$.*

Proof. Consider any pair $[x]$ and $[y]$ of equivalence classes of X modulo the equivalence relation E. We have nothing to prove if $[x]$ and $[y]$ are disjoint, so if they are not disjoint, then it suffices to show that $[x] = [y]$. Consequently, we may assume that there exists an element $w \in [x] \cap [y]$. Crucially, by definition of the equivalence classes of X modulo E, we have that $(w, x) \in E$ and $(w, y) \in E$. By assumption that E is an equivalence relation, it follows that $(x, w) \in E$ by symmetry, hence the transitivity of E together with the inclusions $(x, w), (w, y) \in E$ yield that $(x, y) \in E$. By Proposition 1.10.1, we conclude that $[x] = [y]$, and the claim of the proposition is established. □

Corollary 1.10.3. *Let X be an arbitrary set. Every equivalence relation on X induces a partition of X. Conversely, every partition of X induces an equivalence relation on X.*

Proof. By Proposition 1.10.2, if E is an equivalence relation on X, then the collection $\mathcal{P}$ of distinct equivalence classes of X modulo E is pairwise disjoint. Even more, every equivalence class of X modulo E is nonempty because E is reflexive. Last, every element $x \in X$ belongs to some equivalence class of X modulo E — namely $[x]$ — hence it follows that $X = \cup_{S \in \mathcal{P}} X_S$.

Conversely, suppose that $\mathcal{P} = \{X_i \mid i \in I\}$ is a partition of X indexed by some set I. Consider the relation $E_\mathcal{P} = \{(x, y) \mid x, y \in X_i \text{ for some index } i \in I\} \subseteq X \times X$. By definition of a partition, every element $x \in X$ lies in X_i for some index $i \in I$, hence $(x, x) \in E_\mathcal{P}$ for every element $x \in X$, i.e., $E_\mathcal{P}$ is reflexive. By definition of $E_\mathcal{P}$, if $(x, y) \in E_\mathcal{P}$, then $(y, x) \in E_\mathcal{P}$, hence $E_\mathcal{P}$ is symmetric. Last, if $(x, y), (y, z) \in E_\mathcal{P}$, then $x, y \in X_i$ and $y, z \in X_j$ for some indices $i, j \in I$. By definition of a partition, we have that $X_i \cap X_j = \emptyset$ if and only if i and j are distinct, hence we must have that $i = j$ by assumption that $y \in X_i \cap X_j$. We conclude that $(x, z) \in X_i$ so that $(x, z) \in E_\mathcal{P}$, i.e., $E_\mathcal{P}$ is transitive. Ultimately, this shows that the set $E_\mathcal{P}$ is an equivalence relation on X. □

Example 1.10.4. Consider the equivalence relation R of Example 1.9.5. By Corollary 1.10.3, the collection of distinct equivalence classes of [5] modulo R provide a partition of [5]. By Example

1.9.9, the distinct equivalence classes of $[5]$ modulo R are $[1] = \{1, 3, 5\}$ and $[2] = \{2, 4\}$, hence the underlying partition of $[5]$ induced by the equivalence relation R is $\mathcal{P} = \{[1], [2]\} = \{\{1, 3, 5\}, \{2, 4\}\}$.

Example 1.10.5. Consider the following partition $\mathcal{P} = \{R_0, R_1, R_2, R_3\}$ of the set of integers $\mathbb{Z}$.

$$R_0 = \{\dots, -8, -4, 0, 4, \dots\} \qquad R_2 = \{\dots, -6, -2, 2, 6, \dots\}$$
$$R_1 = \{\dots, -7, -3, 1, 5, \dots\} \qquad R_3 = \{\dots, -5, -1, 3, 7, \dots\}$$

By Corollary 1.10.3, the distinct sets in the partition $\mathcal{P}$ constitute the distinct equivalence classes of an equivalence relation $E_{\mathcal{P}}$ of $\mathbb{Z}$. Explicitly, we have that $(x, y) \in E_{\mathcal{P}}$ if and only if $x, y \in R_i$ for some integer $1 \leq i \leq 4$. Consequently, the distinct equivalence classes of $\mathbb{Z}$ modulo the equivalence relation $E_{\mathcal{P}}$ are R_0, R_1, R_2, and R_3. Observe that $(0, 4) \in E_{\mathcal{P}}$ holds because $0, 4 \in R_0$ and $(1, 5) \in E_{\mathcal{P}}$ holds because $1, 5 \in R_1$, but neither $(0, 2)$ nor $(1, 3)$ lie in $E_{\mathcal{P}}$. By Proposition 1.10.1, a pair of equivalence classes are distinct if and only if their **representatives** are related, hence the distinct equivalence classes of $\mathbb{Z}$ modulo $E_{\mathcal{P}}$ are $[0]$, $[1]$, $[2]$, and $[3]$ or similarly $[4]$, $[5]$, $[6]$, and $[7]$ and so on.

1.11 Partial Orders

We say that a relation R on an arbitrary set X is **antisymmetric** if for every pair of elements $x, y \in X$, the inclusions $(x, y) \in R$ and $(y, x) \in R$ together imply that $x = y$. Equivalence relations are reflexive, symmetric, and transitive relations on a set; however, if we replace the requirement of the symmetry condition with the property of antisymmetry, then we obtain a **partial order** on the set. Explicitly, a partial order P on X is a subset $P \subseteq X \times X$ that is reflexive, antisymmetric, and transitive. Every set admits at least one partial order. Once again, it is simply the diagonal.

Proposition 1.11.1. *If X is any set, the diagonal Δ_X of X is a partial order on X.*

Like with equivalence relations, there are interesting examples of partial orders.

Example 1.11.2. Observe that the real numbers $\mathbb{R}$ are partially ordered via the usual less-than-or-equal-to $\leq$. Put another way, the relation $P = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$ is a partial order on $\mathbb{R}$. Explicitly, we have that $x = x$ so that $x \leq x$ and $(x, x) \in P$ for all real numbers x. Likewise, if we have that $(x, y), (y, x) \in P$, then $x \leq y$ and $y \leq x$ together imply that $x = y$. Last, if we assume that $(x, y), (y, z) \in P$, then $x \leq y$ and $y \leq z$ together imply that $x \leq z$ so that $(x, z) \in P$.

Example 1.11.3. Divisibility constitutes a partial order on the non-negative integers $\mathbb{Z}_{\geq 0}$. Explicitly, consider the relation $D = \{(a, b) \mid a \text{ divides } b\} \subseteq \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$. Observe that a divides a, hence D is reflexive. Even more, if a divides b and b divides a, then there exist integers m and n such that $b = am$ and $a = bn$; together, these identities yield that $a = bn = amn$. Certainly, if $a = 0$, then $b = 0$, hence we may assume that a is nonzero. Cancelling a factor of a from both sides gives that $mn = 1$, which in turn implies that $m = n = 1$ because a and b are non-negative. Ultimately, this proves that $a = b$, hence D is antisymmetric. Last, if a divides b and b divides c, then a divides c: indeed, we have that $b = am$ and $c = bn$ together yield that $c = bn = (am)n = a(mn)$.

Every set admits a partial order, hence every set is a **partially ordered set**; however, there can be many ways to view a set as a partially ordered set. We say that a pair of elements p and q of a partial order P on a set X are **comparable** if it holds that either $(p, q) \in P$ or

$(q, p) \in P$; otherwise, the elements p and q are said to be **incomparable**. Every pair of distinct prime numbers are incomparable with respect to the partial order of divisibility on the non-negative integers. Conversely, if every pair of elements $p, q \in P$ are comparable, then P is a **total order** on X. Observe that if $Y \subseteq X$, then we may define a partial order $P|_Y = \{(y_1, y_2) \in Y \times Y \mid (y_1, y_2) \in P\}$ on Y by viewing the elements of Y as elements of X. If $P|_Y$ is a total order on $Y \subseteq X$, then we say that Y is a **chain** (with respect to P) in X. We say that an element $x_0 \in X$ is an **upper bound** of Y (with respect to P) if it holds that $(y, x_0) \in P$ for every element $y \in Y$. We will also say that an element $x_0 \in X$ is **maximal** (with respect to P) if it does not hold that $(x_0, x) \in P$ for any element $x \in X \setminus \{x_0\}$. Our next theorem combines these ingredients to comprise one of the most ubiquitous results in mathematics (and especially in the ideal theory of commutative algebra).

Theorem 1.11.4 (Zorn's Lemma)**.** *Let X be an arbitrary set. Let P be a partial order on X. If every chain Y in X has an upper bound in Y, then Y admits a maximal element $y_0 \in Y$.*

1.12 Congruence Modulo n

We say that a nonzero integer a **divides** an integer b if there exists an integer c such that $b = ac$. We will write $a \mid b$ in this case, and we will often say that b is **divisible by** a. Given any nonzero integer n, we say that a pair of integers a and b are **congruent modulo** n if it holds that n divides $b - a$. Conventionally, if a and b are congruent modulo n, we write $b \equiv a \pmod{n}$.

Example 1.12.1. We have that $7 \equiv 3 \pmod{4}$ because $7 - 3 = 4$ is divisible by 4.

Example 1.12.2. We have that $5 \equiv 21 \pmod{4}$ because $5 - 21 = -16 = 4(-4)$ is divisible by 4.

Example 1.12.3. We have that $11 \not\equiv 8 \pmod{4}$ because $11 - 8 = 3$ is not divisible by 4.

Proposition 1.12.4. *Consider any nonzero integer n and any integers a, b, and c.*

(1.) *We have that $a \equiv 0 \pmod{n}$ if and only if n divides a.*

(2.) *We have that $b \equiv a \pmod{n}$ if and only if $b - a \equiv 0 \pmod{n}$.*

(3.) *We have that $a \equiv a \pmod{n}$ for any integer a.*

(4.) *We have that $b \equiv a \pmod{n}$ if and only if $a \equiv b \pmod{n}$.*

(5.) *If $b \equiv a \pmod{n}$ and $c \equiv b \pmod{n}$, then $c \equiv a \pmod{n}$.*

(6.) *We have that $b \equiv a \pmod{n}$ if and only if $-b \equiv -a \pmod{n}$.*

(7.) *We have that $b \equiv a \pmod{n}$ if and only if $b + c \equiv a + c \pmod{n}$.*

(8.) *If $b \equiv a \pmod{n}$, then $cb \equiv ca \pmod{n}$.*

(9.) *If $b \equiv a \pmod{n}$, then $b^k \equiv a^k \pmod{n}$ for any integer $k \geq 0$.*

Proof. (1.) We have that $a \equiv 0 \pmod{n}$ if and only if n divides $a - 0$ if and only if n divides a.

(2.) By definition and the first property of congruence modulo n, we have that $b \equiv a \pmod{n}$ if and only if n divides $b - a$ if and only if $b - a \equiv 0 \pmod{n}$.

(3.) Considering that $a - a = 0 = n \cdot 0$, it follows that n divides $a - a$ so that $a \equiv a \pmod{n}$.

(4.) We have that $b \equiv a \pmod{n}$ if and only if n divides $b - a$ if and only if n divides $-(a - b)$ if and only if n divides $a - b$ if and only if $a \equiv b \pmod{n}$.

(5.) Given that $b \equiv a \pmod{n}$ and $c \equiv b \pmod{n}$, by definition, there exist integers k and ℓ such that $b - a = nk$ and $c - b = n\ell$. Observe that $c - a = (c - b) + (b - a) = nk + n\ell = n(k + \ell)$, hence n divides $c - a$ so that $c \equiv a \pmod{n}$ by definition of congruence modulo n.

(6.) We have that $b \equiv a \pmod{n}$ if and only if n divides $b - a$ if and only if $b - a = nk$ for some integer k if and only if $-b + a = (-b) - (-a) = n(-k)$ for some integer k if and only if n divides $-b - (-a)$ if and only if $-b \equiv -a \pmod{n}$ by definition of congruence modulo n.

(7.) By definition of congruence modulo n, we have that $b \equiv a \pmod{n}$ if and only if n divides $b - a$ if and only if n divides $(b + c) - (a + c)$ if and only if $b + c \equiv a + c \pmod{n}$.

(8.) By definition of congruence modulo n, if $b \equiv a \pmod{n}$, then n divides $b - a$ so that n divides $c(b - a)$. Considering that $c(b - a) = cb - ca$, it follows that $cb \equiv ca \pmod{n}$.

(9.) By the eight property of congruence modulo n, we have that $b^2 = b \cdot b \equiv b \cdot a \pmod{n}$ and $a^2 = a \cdot a \equiv a \cdot b \pmod{n}$. Considering that $b \cdot a = a \cdot b$, the fifth property of congruence modulo n yields that $b^2 = b \cdot b \equiv b \cdot a = a \cdot b \equiv a \cdot a = a^2 \pmod{n}$. By the same rationale, we have that $b^3 = b \cdot b^2 \equiv b \cdot a^2 = a \cdot a^2 = a^3 \pmod{n}$. Continuing in this manner, the desired result follows. □

Given any nonzero integer n, consider the relation R defined on the set of integers $\mathbb{Z}$ such that $a \, R \, b$ if and only if $b \equiv a \pmod{n}$. We refer to R as **congruence modulo** n. By the third, fourth, and fifth properties of Proposition 1.12.4, congruence modulo n is an equivalence relation on $\mathbb{Z}$.

Proposition 1.12.5. *Congruence modulo any nonzero integer n is an equivalence relation on $\mathbb{Z}$.*

Consider the equivalence class $[a]$ of any integer a modulo the equivalence relation of congruence modulo n. Conventionally, we refer to $[a]$ as the class of a **modulo** n. By definition, we have that

$$[a] = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\} = \{b \in \mathbb{Z} \mid b - a = nq \text{ for some integer } q\} = \{nq + a \mid q \in \mathbb{Z}\}.$$

Consequently, the equivalence class of a modulo n consists of sums of integer multiples of n and a.

Example 1.12.6. Congruence modulo 2 is an equivalence relation on $\mathbb{Z}$ with equivalence classes

$$[0] = \{2q + 0 \mid q \in \mathbb{Z}\} = \{\dots, -4, -2, 0, 2, 4, \dots\} \text{ and}$$
$$[1] = \{2q + 1 \mid q \in \mathbb{Z}\} = \{\dots, -3, -1, 1, 3, 5, \dots\}.$$

By Proposition 1.10.2, these are all of the distinct equivalence classes of $\mathbb{Z}$ modulo 2.

Example 1.12.7. Congruence modulo 3 is an equivalence relation on $\mathbb{Z}$ with equivalence classes

$$[0] = \{3q + 0 \mid q \in \mathbb{Z}\} = \{\dots, -6, -3, 0, 3, 6, \dots\},$$
$$[1] = \{3q + 1 \mid q \in \mathbb{Z}\} = \{\dots, -5, -2, 1, 4, 7, \dots\}, \text{ and}$$
$$[2] = \{3q + 2 \mid q \in \mathbb{Z}\} = \{\dots, -4, -1, 2, 5, 8, \dots\}.$$

By Proposition 1.10.2, these are all of the distinct equivalence classes of $\mathbb{Z}$ modulo 3.

Proposition 1.12.8. *Given any nonzero integer n, the distinct equivalence classes of $\mathbb{Z}$ modulo n are $[i] = \{nq + i \mid q \in \mathbb{Z}\}$ for each integer $0 \leq i \leq n-1$. Particularly, there are exactly n of them.*

Congruence modulo a nonzero integer gives rise to other interesting equivalence relations.

Example 1.12.9. Consider the relation R on the set of integers $\mathbb{Z}$ defined by $a \, R \, b$ if and only if $5b \equiv 2a \pmod 3$. We claim that R is an equivalence relation.

1.) We demonstrate first that $a \, R \, a$. By definition, we must prove that $5a \equiv 2a \pmod 3$. But this is true because $5a - 2a = 3a$ is divisible by 3 for all integers a.

2.) We establish next that if $a \, R \, b$, then $b \, R \, a$. By definition, if $a \, R \, b$, then $5b \equiv 2a \pmod 3$ so that $5b - 2a = 3k$ for some integer k. Consequently, we have that $2a - 5b = 3(-k)$. By adding $3a$ and $3b$ to both sides of this equation, we obtain $5a - 2b = 3(-k) + 3a + 3b = 3(-k + a + b)$. We conclude that $5a - 2b$ is divisible by 3 so that $5a \equiv 2b \pmod 3$ and $b \, R \, a$.

3.) Last, if $a \, R \, b$ and $b \, R \, c$, then $5b \equiv 2a \pmod 3$ and $5c \equiv 2b \pmod 3$. By definition, there exist integers k and ℓ such that $5b - 2a = 3k$ and $5c - 2b = 3\ell$. By taking their sum, we find that
$$5c - 3b - 2a = (5c - 2b) + (5b - 2a) = 3\ell + 3k = 3(\ell + k)$$
so that $5c - 2a = 3(\ell + k + b)$; therefore, 3 divides $5c - 2a$ so that $5c \equiv 2a \pmod 3$ and $a \, R \, c$.

By definition, the equivalence class of a modulo R is given by
$$[a] = \{b \in \mathbb{Z} \mid a \, R \, b\} = \{b \in \mathbb{Z} \mid 5b \equiv 2a \pmod 3\} = \{b \in \mathbb{Z} \mid 5b - 2a = 3k \text{ for some integer } k\}.$$
Consequently, the class of a modulo R is $[a] = \{b \in \mathbb{Z} \mid 5b = 3k + 2a \text{ for some integer } k\}$. Checking some small values of b yields that $[0] = \{\dots, -6, -3, 0, 3, 6, \dots\}$. Likewise, by definition and a brute-force check, we have that $[1] = \{b \in \mathbb{Z} \mid 5b = 3k + 2 \text{ for some integer } k\} = \{\dots, -5, -2, 1, 4, 7, \dots\}$ and $[2] = \{b \in \mathbb{Z} \mid 5b = 3k+4 \text{ for some integer } k\} = \{\dots, -4, -1, 2, 5, 8, \dots\}$. Every integer belongs to one of these three distinct equivalence classes modulo R, hence this is an exhaustive list.

1.13 The Definition of a Function

Consider any sets X and Y. We have seen previously that a relation from X to Y is any subset of the Cartesian product $X \times Y$. We say that a relation f from X to Y is a **function** if and only if every element of X is the first component of one and only one ordered pair in f. Explicitly, a function $f : X \to Y$ is merely an assignment of each element $x \in X$ to a unique (but not necessarily distinct) element $f(x) \in Y$ called the **image** of x under f. We refer to the set X as the **domain** of $f : X \to Y$; the **codomain** of f is Y; and the **range** of f is the set $\operatorname{range}(f) = \{f(x) \mid x \in X\}$ of second coordinates of elements in f. Out of desire for notational convenience, we may sometimes omit the letter $f : X \to Y$ when defining a function and simply use an arrow $X \to Y$ to indicate the sets involved and an arrow $x \mapsto y$ to declare the image $y \in Y$ of the element $x \in X$.

Example 1.13.1. Consider the relation $f = \{(-1, 1), (1, -1)\}$ defined on $X = \{-1, 1\}$. Each of the elements of X is the first component of one and only one ordered pair in f, hence $f : X \to X$ is a function; its domain and range are both X. Conventionally, we might recognize this function as $f(x) = -x$ because it has the effect of swapping the signs of each element $x \in X$.

Example 1.13.2. Consider the relation $g = \{(x, x-1) \mid x \in \mathbb{R}\}$ defined on the set of real numbers $\mathbb{R}$. Every real number is the first component of one and only one ordered pair in g, hence $g : \mathbb{R} \to \mathbb{R}$ is a function; its domain and range are both $\mathbb{R}$. Conventionally, we might recognize this function as $g(x) = x - 1$ because the ordered pairs $(x, y) \in g$ satisfy that $y = x - 1$ for each real number x.

Example 1.13.3. Often in calculus, a function is defined simply by declaring a rule, e.g., $h(x) = x^2$. Conventionally, the domain of such a function is assumed to be the **natural domain**, i.e., the largest subset of the real numbers for which $h(x)$ can be defined. Considering that the square of any real number is itself a real number, it follows that the domain of $h(x)$ is all real numbers; the range of $h(x)$ is the collection of all non-negative real numbers because if $x \in \mathbb{R}$, then $x^2 \geq 0$.

But strictly speaking, a function intimately depends on its domain and its codomain. We will soon see that the functions $h : \mathbb{R} \to \mathbb{R}_{\geq 0}$ defined by $h(x) = x^2$ and $k : \mathbb{R}_{\geq 0} \to \mathbb{R}$ defined by $k(x) = x^2$ are quite different from one another — even though the underlying rule of both functions is the same. Even more, both of these functions are different from $\ell : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ defined by $\ell(x) = x^2$.

Example 1.13.4. Consider the equivalence relation R defined on the set $[5] = \{1, 2, 3, 4, 5\}$ as in Example 1.8.4. Because the ordered pairs $(1, 1)$ and $(1, 3)$ lie in R, it follows that R is not a function. Generally, an equivalence relation R will never be a function because if (x, y) and (y, x) both lie in R, then by definition, we must have that $(x, x) \in R$ so that R is not a function.

Every set X possesses an **identity function** $\mathrm{id}_X : X \to X$ defined by $\mathrm{id}_X(x) = x$. If X is a subset of Y, then the **inclusion** $X \subseteq Y$ can be viewed as the function $X \to Y$ that sends $x \mapsto x$, where the symbol x appearing to the left of the arrow $\mapsto$ is viewed as an element of X, and the symbol x appearing to the right of the arrow $\mapsto$ is viewed as an element of Y; in the usual notation, the inclusion may be thought of as the function $i : X \to Y$ defined by $i(x) = x$. Even more, every set X induces a function $\delta_X : X \to X \times X$ that is called the **diagonal function** (of X) and defined by $\delta_X(x) = (x, x)$. Later in the course, we will prove that the diagonal Δ_X of X is exactly the image of the diagonal function δ_X of X, hence there should be no confusion in terminologies.

Even if we have never thought of it as such, algebraic operations such as addition, subtraction, multiplication, and division can be viewed as functions. Explicitly, addition of real numbers is the function $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defined by $(x, y) \mapsto x + y$. Crucially, the sum of two real numbers is a real number, hence this function is **well-defined**, i.e., the image of every element lies in the codomain of the function. Generally, if X is any set, the function $* : X \times X \to X$ that sends $(x, y) \mapsto x * y$ is a **binary operation** if and only if $x * y$ is an element of X for every pair of elements $x, y \in X$. Like we mentioned, addition and multiplication are binary operations on the real numbers $\mathbb{R}$.

Consider any pair of functions $f : X \to Y$ and $g : X \to Y$. Given any element $x \in X$, there exist unique elements $f(x), g(x) \in Y$ such that $(x, f(x)) \in f$ and $(x, g(x)) \in g$. Consequently, if f and g are equal as sets so that $f = g$, then $(x, f(x))$ lies in g; the uniqueness of $g(x)$ yields in turn that $f(x) = g(x)$. Conversely, if $f(x) = g(x)$ for every element $x \in X$, then we have that

$$f = \{(x, f(x)) \mid x \in X\} = \{(x, g(x)) \mid x \in X\} = g$$

so that f and g are equal as sets. We have proved the following important fact about functions.

Proposition 1.13.5. *Given any sets X and Y, a pair of functions $f : X \to Y$ and $g : X \to Y$ are equal as sets if and only if $f(x) = g(x)$ for all elements $x \in X$.*

Each time we define a function $f : X \to Y$, for every subset $V \subseteq X$, we implicitly distinguish the collection of elements $y \in Y$ such that $y = f(v)$ for some element $v \in V$; this is denoted by

$$f(V) = \{f(v) \mid v \in V\}$$

and called the **image** of V (in Y) under f. Conversely, if $W \subseteq Y$, then the collection of elements $x \in X$ such that $f(x) \in W$ is the **inverse image** of W (in X) under f. Explicitly, we have that

$$f^{-1}(W) = \{x \in X \mid f(x) \in W\}.$$

Example 1.13.6. Consider the function $f = \{(u, 1), (v, 2), (w, 3), (x, 3), (y, 2), (z, 1)\}$ from the set $X = \{u, v, w, x, y, z\}$ to $Y = [6] = \{1, 2, 3, 4, 5, 6\}$. We have that $\operatorname{range}(f) = \{1, 2, 3\}$, but it holds that $\operatorname{range}(f) = f(\{u, v, w\}) = f(\{u, x, y\}) = f(\{x, y, z\})$ to name a few. Even more, we have that

$$f^{-1}(\{2, 3\}) = \{v, w, x, y\} \text{ and } f^{-1}(\{4, 5, 6\}) = \emptyset$$

because the elements $4, 5, 6 \in Y$ do not belong to the second component of any ordered pair in f.

Example 1.13.7. Consider the function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^2$. Observe that for any real number x such that $-1 \leq x \leq 1$, we have that $0 \leq x^2 \leq 1$, hence it follows that $g([-1, 1]) = [0, 1]$. On the other hand, $-3 < x \leq 2$, then $0 \leq x^2 < 9$ implies that $g((-3, 2]) = [0, 9)$.

Even if the sets X and Y are finite with small cardinalities $|X|$ and $|Y|$, the number of functions $f : X \to Y$ grows astonishingly quickly. Explicitly, a function $f : X \to Y$ is uniquely determined by choosing for each element $x \in X$ one and only one element $y \in Y$ such that $f(x) = y$. Consequently, for each element $x \in X$, there are $|Y|$ possible choices for $f(x)$. By denoting the set of functions $f : X \to Y$ as $Y^X = \{f \subseteq X \times Y \mid f : X \to Y \text{ is a function}\}$, we have that $|Y^X| = |Y|^{|X|}$.

Example 1.13.8. Consider the sets $X = \{u, v, w, x, y, z\}$ and $Y = [6] = \{1, 2, 3, 4, 5, 6\}$ of Example 1.13.6. We have that $|X| = 6 = |Y|$, hence there are $|Y|^{|X|} = 6^6$ possible functions $f : X \to Y$.

1.14 One-to-One and Onto Functions

We introduce two indispensable properties of a function $f : X \to Y$ from a set X to a set Y. We say that f is **one-to-one** (or **injective**) if every pair of distinct elements $x_1, x_2 \in X$ induce distinct elements $f(x_1), f(x_2) \in Y$. Equivalently, we say that f is one-to-one if every equality $f(x_1) = f(x_2)$ of elements of Y yields the corresponding equality $x_1 = x_2$ of elements of X.

Example 1.14.1. Consider the function $f = \{(-1, 1), (1, -1)\}$ from the set $X = \{-1, 1\}$ to itself. Each of the elements $x \in X$ corresponds to a distinct element $f(x) \in X$, hence f is one-to-one.

Example 1.14.2. Consider the real function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 3x + 4$. Observe that if $f(x_1) = f(x_2)$, then $3x_1 + 4 = 3x_2 + 4$ so that $3x_1 = 3x_2$ and $x_1 = x_2$; thus, f is one-to-one.

Example 1.14.3. Consider the real function $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ defined by $f(x) = x^2$. Observe that if $f(x_1) = f(x_2)$, then $x_1^2 = x_2^2$. By taking the square root of both sides and using the fact that the domain of f consists of non-negative real numbers, it follows that $x_1 = x_2$ so that f is one-to-one.

Example 1.14.4. Consider the function $f = \{(u, 1), (v, 2), (w, 3), (x, 3), (y, 2), (z, 1)\}$ from the set $X = \{u, v, w, x, y, z\}$ to $Y = [6] = \{1, 2, 3, 4, 5, 6\}$. Considering that $f(u) = 1 = f(z)$ but $u \neq z$, it follows that f is not one-to-one; the same holds for $f(v) = 2 = f(y)$ and $f(w) = 3 = f(x)$.

Example 1.14.5. Consider the real function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^2$. Considering that $g(-1) = 1 = g(1)$ but $-1 \neq 1$, it follows that g is not one-to-one. Compare with Example 1.14.3.

Example 1.14.6. We say that a real function f is **increasing** if $x_1 < x_2$ implies that $f(x_1) < f(x_2)$ for all real numbers x_1 and x_2 in the domain of f. If f is differentiable on an open interval (a, b) (i.e., $f'(x)$ exists for all real numbers $a < x < b$), then by the Mean Value Theorem, we have that f is increasing on (a, b) if and only if $f'(x) > 0$ for all real numbers $a < x < b$. Explicitly, if f is increasing on (a, b), then for any real numbers $a < x_1 < x_2 < b$, we have that $f(x_2) - f(x_1) > 0$. By the Mean Value Theorem, there exists a real number $x_1 < c < x_2$ such that

$$f'(c) = \frac{f(x_2) - f(x_1)}{x_2 - x_1} > 0.$$

Conversely, if $f'(x) > 0$ for all real numbers $a < x < b$, then for any real numbers $a < x_1 < x_2 < b$, the Mean Value Theorem guarantees the existence of a real number $x_1 < c < x_2$ such that

$$f(x_2) - f(x_1) = f'(c)(x_2 - x_1) > 0.$$

Consequently, any function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^{2n+1}$ for some integer $n \geq 0$ is increasing on any open interval not containing 0 because $f'(x) = (2n + 1)x^{2n} > 0$ on any such interval.

Even more, we say that $f : X \to Y$ is **onto** (or **surjective**) if for every element $y \in Y$, there exists an element $x \in X$ such that $y = f(x)$. One way to think about the surjective property is that every element of the codomain Y is "mapped onto" or "covered" by an element of X. Even more simply, a function $f : X \to Y$ is surjective if and only if $Y = \operatorname{range}(f) = \{f(x) \mid x \in X\}$.

Example 1.14.7. Consider the function $f = \{(-1, 1), (1, -1)\}$ from the set $X = \{-1, 1\}$ to itself. Each of the elements $y \in X$ can be written as $y = f(x)$ for some element $x \in X$, hence f is onto.

Example 1.14.8. Consider the real function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 3x + 4$. We claim that f is onto. By definition, for any real number y, we must furnish a real number x such that $y = f(x) = 3x + 4$. But if $y = 3x + 4$, then $3x = y - 4$ so that $x = \frac{1}{3}(y - 4)$. Computing $f(x)$ yields

$$f(x) = 3x + 4 = 3 \cdot \frac{1}{3}(y - 4) + 4 = (y - 4) + 4 = y$$

because $x = \frac{1}{3}(y - 4)$ by construction, as desired. Consequently, it follows that f is onto.

Example 1.14.9. Consider the real function $f : \mathbb{R} \to \mathbb{R}_{\geq 0}$ defined by $f(x) = x^2$. Given any real number $y \geq 0$, we claim that there exists a real number x such that $y = x^2$. By taking $x = \sqrt{y}$ (this is well-defined because $y \geq 0$), it follows that $f(x) = x^2 = (\sqrt{y})^2 = y$ so that f is onto.

Example 1.14.10. Consider the function $f = \{(u, 1), (v, 2), (w, 3), (x, 3), (y, 2), (z, 1)\}$ from the set $X = \{u, v, w, x, y, z\}$ to $Y = [6] = \{1, 2, 3, 4, 5, 6\}$. Considering that 4, 5, and 6 are not the image of any element of X under f, it follows that f is not onto.

Example 1.14.11. Consider the sets $X = \{a, b, c\}$ and $Y = \{0, 1, 2, 3\}$. We cannot possibly find a function $f : X \to Y$ that is onto because the cardinality of X is strictly smaller than the cardinality of Y; therefore, it is impossible to assign to each element $y \in Y$ a unique element $x \in X$.

1.15 Bijective Functions

We say that a function $f : X \to Y$ is **bijective** if f is both injective and surjective. We may think of a bijection $f : X \to Y$ simply as a relabelling of the elements of Y using the names of elements of X; in this way, two sets X and Y are "essentially the same" if there exists a bijection $f : X \to Y$. Often, this property of a bijective function is emphasized in the literature by using the terminology of "one-to-one correspondence" between X and Y in place of "bijection" from X to Y.

Proposition 1.15.1. *Consider any pair of arbitrary finite sets X and Y.*

(a.) *If there exists an injective function $f : X \to Y$, then $|X| \leq |Y|$.*

(b.) *If $|X| \leq |Y|$, then there exists an injective function $f : X \to Y$.*

(c.) *If there exists a surjective function $f : X \to Y$, then $|X| \geq |Y|$.*

(d.) *If $|X| \geq |Y|$, then there exists a surjective function $f : X \to Y$.*

(e.) *If there exists a bijective function $f : X \to Y$, then $|X| = |Y|$.*

(f.) *If $|X| = |Y|$, then there exists a bijective function $f : X \to Y$.*

(g.) *If $|X| = |Y|$, then a function $f : X \to Y$ is injective if and only if it is surjective.*

Proof. We will assume throughout the proof that $|X| = m$ and $|Y| = n$ are non-negative integers. Certainly, if either m or n is zero, then the empty function satisfies the desired properties. Consequently, we may assume that neither m nor n is zero. We will assume for notational convenience that $X = \{x_1, x_2, \ldots, x_m\}$ and $Y = \{y_1, y_2, \ldots, y_n\}$. We turn our attention to each claim in turn.

(a.) We will assume that there exists an injective function $f : X \to Y$. Consequently, every element $y \in Y$ corresponds to at most one element $x \in X$ via $y = f(x)$. Considering that every element $x \in X$ corresponds to a unique element $f(x) \in Y$, we conclude that $|X| \leq |Y|$.

(b.) Observe that if $m \leq n$, then we may define an injective function $f : X \to Y$ by declaring that $f(x_i) = y_i$ for each integer $1 \leq i \leq m$. Explicitly, f is a function because every element $x_i \in X$ corresponds to exactly one element $y_i = f(x_i) \in Y$. Even more, f is injective since for each element $y_i \in Y$, there is at most one element $x_i \in X$ such that $y_i = f(x_i)$ by assumption that $n \geq m$.

(c.) We will assume that there exists a surjective function $f : X \to Y$. Consequently, for every element $y \in Y$, there exists an element $x \in X$ such that $y = f(x)$. Considering that every element $x \in X$ corresponds to a unique element $f(x) \in Y$, we conclude that $|X| \geq |Y|$.

(d.) Conversely, if $m \geq n$, then we may define a surjective function $f : X \to Y$ by declaring that $f(x_i) = y_i$ for each integer $1 \leq i \leq m$. We have already seen in the previous paragraph that such a relation is a function; however, by assumption that $m \geq n$, it follows that f is surjective because for every element $y_i \in Y$, there exists an element $x_i \in X$ such that $y_i = f(x_i)$.

(e.) Combined, parts (a.) and (c.) imply that $|X| \leq |Y|$ and $|X| \geq |Y|$ so that $|X| = |Y|$.

(f.) Combined, parts (b.) and (d.) yield a bijective function $f : X \to Y$ defined by $f(x_i) = y_i$.

(g.) Last, we will assume that $m = n$. Consider any function $f : X \to Y$. Observe that if f is injective, then every element of X maps to a distinct element of Y under f, hence range(f) is a subset of Y of the same cardinality as Y. We conclude that range$(f) = Y$ so that f is surjective.

Conversely, if f is surjective, then for every element $y \in Y$, there exists an element $x \in X$ such that $y = f(x)$. By assumption that $m = n$, the element $x \in X$ such that $y = f(x)$ is uniquely determined by y, hence the image of $x \in X$ under f is unique so that f is injective. □

Caution: if X and Y are infinite sets, then there need not exist a bijective function $f : X \to Y$. Explicitly, there is no bijection $f : \mathbb{Q} \to \mathbb{R}$ between the rational numbers and the real numbers.

Caution: if X and Y are infinite sets, then a function $f : X \to Y$ can be injective without being surjective (and vice-versa). Explicitly, the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = 2x$ is injective but not surjective, and the function $g : \mathbb{Q} \to \mathbb{Z}$ defined by $g(p/q) = p$ is surjective but not injective.

By Proposition 1.15.1, a pair of nonempty sets admit a bijection if and only if they have the same number of elements (or cardinality). Given any nonempty set X of cardinality n, the collection of bijective functions $f : X \to X$ is an extremely important object in commutative algebra and combinatorics called the **symmetric group on the finite set** X and denoted by $\mathfrak{S}_X$.

Proposition 1.15.2. *Given any nonempty sets X and Y with $|X| = |Y| = n$, there are $n! = n(n-1)(n-2)\cdots 2\cdot 1$ distinct bijective functions $f : X \to Y$. Consequently, we have that $|\mathfrak{S}_X| = |X| = n!$.*

Proof. Every bijective function $f : X \to Y$ is uniquely determined by the images of the elements of X under f. Consequently, if we assume that $X = \{x_1, x_2, \dots, x_n\}$, then there are n distinct choices for the value of $f(x_1)$; then, there are $n-1$ distinct choices for $f(x_2)$ other than $f(x_1)$; likewise, there are $n-2$ distinct choices for $f(x_3)$ other than $f(x_1)$ and $f(x_2)$. Continuing in this manner, there are $n-i+1$ choices for $f(x_i)$ for each integer $1 \leq i \leq n$, hence there are $n!$ bijective functions between X and Y: indeed, there are a total of $n! = n(n-1)(n-2)\cdots 2\cdot 1$ possibilities. □

Example 1.15.3. Observe that the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = -x$ is bijective. Explicitly, if $f(x) = f(y)$, then $-x = -y$ yields that $x = y$ so that f is one-to-one. Likewise, every integer n is the image of $-n$ under f because $n = -(-n) = f(-n)$, hence f is onto.

Example 1.15.4. Consider the function $f : \mathbb{R} \setminus \{3\} \to \mathbb{R} \setminus \{1\}$ defined by

$$f(x) = \frac{x-2}{x-3}.$$

Cross-multiplying denominators, we note that $f(x) = f(y)$ if and only if $(x-2)(y-3) = (x-3)(y-2)$ if and only if $xy - 3x - 2y + 6 = xy - 2x - 3y + 6$ if and only if $x = y$, hence f is one-to-one. Conversely, we will prove that f is onto. Behind the scenes, we solve the following equation for x.

$$y = \frac{x-2}{x-3}$$

Observe that this holds if and only if $(x-3)y = x-2$ if and only if $xy - 3y = x - 2$ if and only if $xy - x = 3y - 2$ if and only if $x(y-1) = 3y - 2$ if and only if

$$x = \frac{3y-2}{y-1}.$$

Consequently, for every real number $y \in \mathbb{R} \setminus \{1\}$, we have that $y = f(x)$ so that f is onto.

1.16 Composition of Functions

Given any pair of functions $f : X \to Y$ and $g : Y \to Z$ between any sets X, Y, and Z, we may construct a function $g \circ f : X \to Z$ called the **composite function** defined by $(g \circ f)(x) = g(f(x))$. We may also refer to the function $g \circ f$ as g **composed with** f or the **composition** of f under g.

Example 1.16.1. Consider the sets $X = \{-1, 1\}$, $Y = \{x, y, z\}$, and $Z = \{1, 2, 3\}$. We may define some functions $f : X \to Y$ and $g : Y \to Z$ by $f = \{(-1, x), (1, z)\}$ and $g = \{(x, 2), (y, 3), (z, 1)\}$. Observe that the composite function $g \circ f : X \to Z$ satisfies $(g \circ f)(-1) = g(f(-1)) = g(x) = 2$ and $(g \circ f)(1) = g(f(1)) = g(z) = 1$. Consequently, we find that $g \circ f = \{(-1, 2), (1, 1)\}$.

Example 1.16.2. Consider the sets $A = \{a, b, c, d\}$, $B = \{b, c, d, e\}$, and $C = \{c, d, e, f\}$. We may define a pair of functions $f : A \to B$ and $g : B \to C$ such that $f = \{(a, b), (b, c), (c, d), (d, e)\}$ and $g = \{(b, c), (c, d), (d, e), (e, f)\}$. Observe that the composite function $g \circ f : A \to C$ satisfies that

$$\begin{aligned} (g \circ f)(a) &= g(f(a)) = g(b) = c, & (g \circ f)(c) &= g(f(c)) = g(d) = e, \text{ and} \\ (g \circ f)(b) &= g(f(b)) = g(c) = d, & (g \circ f)(d) &= g(f(d)) = g(e) = f. \end{aligned}$$

Consequently, we find that $g \circ f : A \to C$ satisfies that $g \circ f = \{(a, c), (b, d), (c, e), (d, f)\}$.

Example 1.16.3. Composition of functions is a common technique in calculus. (Recall that the Chain Rule for Derivatives gives a formula for the derivative of a composite function.) Consider the functions $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = e^x$ and $g(x) = |x|$. We have that

$$\begin{aligned} &f \circ g : \mathbb{R} \to \mathbb{R} \text{ is defined by } (f \circ g)(x) = f(g(x)) = e^{g(x)} = e^{|x|} \text{ and} \\ &g \circ f : \mathbb{R} \to \mathbb{R} \text{ is defined by } (g \circ f)(x) = g(f(x)) = |f(x)| = |e^x| = e^x. \end{aligned}$$

Crucially, the latter holds because $e^x > 0$ for all real numbers x, hence it follows that $g \circ f = f$.

Proposition 1.16.4. *Consider any pair of functions $f : X \to Y$ and $g : Y \to Z$.*

(a.) *If f and g are injective, then $g \circ f$ is injective.*

(b.) *If f and g are surjective, then $g \circ f$ is surjective.*

Put another way, composition of functions preserves injectivity and surjectivity.

Proof. (a.) We must prove that if $(g \circ f)(x_1) = (g \circ f)(x_2)$, then $x_1 = x_2$. By assumption that g is injective, if $g(f(x_1)) = (g \circ f)(x_1) = (g \circ f)(x_2) = g(f(x_2))$, then $f(x_1) = f(x_2)$. But by the same rationale applied to the injective function f, we conclude that $x_1 = x_2$, as desired.

(b.) We must prove that for every element $z \in Z$, there exists an element $x \in X$ such that $z = (g \circ f)(x)$. By assumption that g is surjective, for every element $z \in Z$, there exists an element $y \in Y$ such that $z = g(y)$. Even more, by hypothesis that f is surjective, there exists an element $x \in X$ such that $y = f(x)$. Combined, these observations yield that $z = g(y) = g(f(x)) = (g \circ f)(x)$. □

Corollary 1.16.5. *Consider any pair of functions $f : X \to Y$ and $g : Y \to Z$. If f and g are bijective, then $g \circ f$ is bijective. Put another way, the composition of bijective functions is bijective.*

Proposition 1.16.6. *Consider any functions $f : W \to X$, $g : X \to Y$, and $h : Y \to Z$. We have that $h \circ (g \circ f) = (h \circ g) \circ f$. Put another way, composition of functions is associative.*

Proof. We must prove that $[h \circ (g \circ f)](w) = [(h \circ g) \circ f](w)$ for all elements $w \in W$ by Proposition 1.13.5. We will assume that $f(w) = x$, $g(x) = y$, and $h(y) = z$. By definition of the composite function, we have that $(g \circ f)(w) = g(f(w)) = g(x) = y$ and $(h \circ g)(x) = h(g(x)) = h(y) = z$ so that $[h \circ (g \circ f)](w) = h((g \circ f)(w)) = h(y) = z$ and $[(h \circ g) \circ f](w) = (h \circ g)(f(w)) = (h \circ g)(x) = z$. □

Remark 1.16.7. We note that in order to define the composition $g \circ f$ of any function $f : X \to Y$ under any other function $g : Y \to Z$, it is sufficient but not strictly necessary to assume that the domain of g is the codomain of f. Generally, the composite function $g \circ f$ is well-defined for any function $g : Y' \to Z$ so long as $Y' \supseteq \operatorname{range}(f)$. For instance, for the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$, we have that $\operatorname{range}(f) = \{f(x) \mid x \in \mathbb{R}\} = \{x^2 \mid x \in \mathbb{R}\} = \mathbb{R}_{\geq 0}$, hence for any function $g : \mathbb{R}_{\geq 0} \to \mathbb{R}$, the composition $g \circ f$ of f under g is well-defined. Explicitly, if we assume that $g(x) = \sqrt{x}$, then $(g \circ f)(x) = g(f(x)) = g(x^2) = \sqrt{x^2} = |x|$; however, if $g(x) = \ln(x)$ on its natural domain, then the composite function $g \circ f$ is not well-defined because $\ln(0)$ is not well-defined.

1.17 Inverse Functions

Considering that any function $f : X \to Y$ between two sets X and Y is by definition a relation, there exists an inverse relation f^{-1} from Y to X defined by $f^{-1} = \{(y, x) \mid (x, y) \in f\}$. One natural curiosity regarding the nature of the inverse relation f^{-1} of a function f is to ask whether the inverse relation f^{-1} of a function f must be a function. Certainly, the answer is no. One can readily verify that the relation $f = \{(-1, 1), (1, 1)\}$ on the set $X = \{-1, 1\}$ is a function, but its inverse relation $f^{-1} = \{(1, -1), (1, 1)\}$ is not a function because $f^{-1}(1)$ is not well-defined since $(1, -1)$ and $(1, 1)$ both lie in f^{-1}. Consequently, it seems that in order for the inverse relation f^{-1} of a function $f : X \to Y$ to be a function, we require that every element $f(x) \in \operatorname{range}(f)$ corresponds uniquely to an element $x \in X$. Put another way, we must have that f is injective. Conversely, by definition, if $f^{-1} : Y \to X$ is a function, then for every element $y \in Y$, we require that $f^{-1}(x)$ is an element of X. Explicitly, we require that for every element $y \in Y$, there exists an element $x \in X$ such that $y = f(x)$. Put another way, we must have that f is surjective. We are lead to the following.

Proposition 1.17.1. *Given any function $f : X \to Y$, the inverse relation f^{-1} is a function if and only if f is bijective. Even more, f^{-1} is bijective if and only if f is bijective.*

Proof. Observe that if f is bijective, then for every element $y \in Y$, there exists a unique element $x \in X$ such that $y = f(x)$. We may therefore define a relation f^{-1} from Y to X by declaring that $y \, f^{-1} \, x$ if and only if $x \, f \, y$, i.e., $y = f(x)$. Observe that f^{-1} is a function because for every element $y \in Y$, there exists one and only one element $x \in X$ such that $y = f(x)$ because f is bijective.

Conversely, suppose that $f^{-1} = \{(y, x) \mid (x, y) \in f\}$ is a function $f^{-1} : Y \to X$. By definition of a function, for every element $y \in Y$, there exists an element $x \in X$ such that $(y, x) \in f^{-1}$. But this implies that for every element $y \in Y$, there exists an element $x \in X$ such that $(x, y) \in f$ or $y = f(x)$, hence f is surjective. Even more, for every element $y \in Y$, the element $x \in X$ such that $y = f(x)$ is uniquely determined so that if $(y, x_1), (y, x_2) \in f^{-1}$, then $x_1 = x_2$. By definition of the inverse relation, we find that if $f(x_1) = f(x_2)$, then $x_1 = x_2$, hence f is injective, as desired.

Last, we will prove that $(f^{-1})^{-1} = f$, hence f^{-1} is bijective if and only if f is bijective (because its inverse relation is a function). By definition, we have that $(f^{-1})^{-1} = \{(x, y) \mid (y, x) \in f^{-1}\}$. Observe that if $(x, y) \in (f^{-1})^{-1}$, then $(y, x) \in f^{-1}$ yields that $(x, y) \in f$ and $(f^{-1})^{-1} \subseteq f$. Conversely, for any element $(x, y) \in f$, we have that $(y, x) \in f^{-1}$ so that $(x, y) \in (f^{-1})^{-1}$ and $(f^{-1})^{-1} \supseteq f$. □

Once we have identified that a function $f : X \to Y$ admits an inverse function $f^{-1} : Y \to X$, we seek an explicit definition of that inverse function. We achieve this via the following proposition.

Proposition 1.17.2. *Given any bijective function $f : X \to Y$, the inverse function $f^{-1} : Y \to X$ satisfies that $f^{-1} \circ f = \mathrm{id}_X$ and $f \circ f^{-1} = \mathrm{id}_Y$. Conversely, if $g : Y \to X$ is any function such that $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$, then $g = f^{-1}$. Put another way, the inverse function $f^{-1} : Y \to X$ of any bijection $f : X \to Y$ is the unique function $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$.*

Proof. Consider any bijection $f : X \to Y$. By Proposition 1.17.1, the inverse relation $f^{-1} : Y \to X$ is a function. By definition of the inverse relation, we have that $f^{-1}(f(x)) = x = \mathrm{id}_X(x)$ for every element $x \in X$ so that $f^{-1} \circ f = \mathrm{id}_X$. Likewise, suppose that $f^{-1}(y) = x$. Considering that $f = (f^{-1})^{-1}$, it follows that $f(f^{-1}(y)) = y = \mathrm{id}_Y(y)$ for every element $y \in Y$ so that $f \circ f^{-1} = \mathrm{id}_Y$.

We will assume next that $g : Y \to X$ is any function such that $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$. Observe that $g = g \circ \mathrm{id}_Y = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1} = \mathrm{id}_X \circ f^{-1} = f^{-1}$ by Proposition 1.16.6. □

Example 1.17.3. We proved in Example 1.15.3 that the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = -x$ is bijective; its inverse function $f^{-1} : \mathbb{Z} \to \mathbb{Z}$ is defined by $f^{-1}(x) = -x$.

Example 1.17.4. We proved in Example 1.15.4 that the function $f : \mathbb{R} \setminus \{3\} \to \mathbb{R} \setminus \{1\}$ defined by

$$f(x) = \frac{x-2}{x-3}$$

is bijective. Observe that its inverse function is $f^{-1} : \mathbb{R} \setminus \{1\} \to \mathbb{R} \setminus \{3\}$ defined by

$$f^{-1}(x) = \frac{3x-2}{x-1}.$$

Remark 1.17.5. Generally, Proposition 1.17.2 provides an algorithm for determining the inverse function $f^{-1} : Y \to X$ of any function $f : X \to Y$ that can be defined by an explicit rule $y = f(x)$. Explicitly, we may solve the equation $y = f(x)$ in terms of x to find that $x = f^{-1}(y)$.

Example 1.17.6. Consider the function $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq} 0$ defined by $f(x) = x^2$. Observe that if $f(x_1) = f(x_2)$, then $x_1^2 = x_1^2$ yields that $(x_1 - x_2)(x_1 + x_2) = x_1^2 - x_2^2 = 0$. By the **Zero-Product Property** for real numbers, we conclude that either $x_1 - x_2 = 0$ or $x_1 + x_2 = 0$. Considering that $x_1, x_2 \geq 0$, the identity $x_1 + x_2 = 0$ holds if and only if $x_1 = x_2 = 0$; otherwise, we must have that $x_1 - x_2 = 0$ so that $x_1 = x_2$ and f is injective. Even more, for any real number $y \geq 0$, the real number $\sqrt{y}$ is well-defined and satisfies that $y = (\sqrt{y})^2 = f(\sqrt{y})$, hence f is onto; this can also be achieved by noticing that $y = f(x) = x^2$ if and only if $x = \sqrt{y}$. Consequently, we find that f is a bijective function with inverse $f^{-1} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ defined by $f^{-1}(x) = \sqrt{x}$.

Currently, our strategy for computing the inverse function of a bijective function is somewhat backwards: in order to determine that the inverse relation of a function is a function, we must prove that the function is bijective. But this requires us to establish that the function is onto, and this necessitates the computation of the inverse function. We make the process more efficient as follows.

Proposition 1.17.7. *Consider any function $f : X \to Y$. If there exists a function $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$, then f and g are bijective functions satisfying that $g = f^{-1}$.*

Proof. We will prove that f is bijective. By Propositions 1.17.1 and 1.17.2, the result will follow. Consider any elements $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$. By hypothesis, we have that

$$x_1 = \mathrm{id}_X(x_1) = (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = \mathrm{id}_X(x_2) = x_2.$$

We conclude that f is injective. Conversely, for every element $y \in Y$, we have that

$$y = \mathrm{id}_Y(y) = (f \circ g)(y) = f(g(y)).$$

Considering that $g(y) = x$ is an element of X, we conclude that $y = f(x)$ so that f is onto. $\square$

Example 1.17.8. Consider the function $f : \mathbb{R} \to \mathbb{R}_{>0}$ defined by $f(x) = e^x$. By elementary calculus, we have that $f'(x) = e^x > 0$ for all real numbers x, hence $f(x)$ is one-to-one by Example 1.14.6. We know that the function $g : \mathbb{R}_{>0} \to \mathbb{R}$ defined by $g(x) = \ln(x)$ satisfies that

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) = \ln(e^x) = x \text{ for all real numbers } x \text{ and} \\ (f \circ g)(x) &= f(g(x)) = e^{\ln(x)} = x \text{ for all real numbers } x > 0, \end{aligned}$$

hence we conclude by Proposition 1.17.7 that f is bijective with inverse function $g = f^{-1}$.

Example 1.17.9. Consider the rational function $f : \mathbb{R} \setminus \{2\} \to \mathbb{R} \setminus \{1\}$ defined by

$$f(x) = \frac{2x+3}{2x-4}.$$

By the Quotient Rule, the derivative of $f(x)$ is the function $f' : \mathbb{R} \setminus 2 \to \mathbb{R} \setminus \{1\}$ defined by

$$f'(x) = \frac{2(2x-4) - 2(2x+3)}{(2x-4)^2} = -\frac{14}{(2x-4)^2}.$$

Considering that $(2x-4)^2 > 0$ for all real numbers $x \neq 2$, it follows that $f'(x) < 0$ for all real numbers $x \neq 2$ so that f is **decreasing**. By Example 1.14.6, it follows that f is one-to-one. (One can also use algebraic manipulation as in Example 1.15.4 to verify this.) We will next solve the equation $y = f(x)$ to find a function $x = f^{-1}(y)$, and we will verify that f^{-1} is the inverse of f.

$$y = f(x) = \frac{2x+3}{2x-4}$$

$$y(2x-4) = 2x+3$$

$$2xy - 4y = 2x+3$$

$$2xy - 2x = 4y+3$$

$$x(2y-2) = 4y+3$$

$$x = \frac{4y+3}{2y-2} = f^{-1}(y)$$

Consider the function $f^{-1} : \mathbb{R} \setminus \{1\} \to \mathbb{R} \setminus \{2\}$ defined by

$$f^{-1}(x) = \frac{4x+3}{2x-2}.$$

We will verify that $(f^{-1} \circ f)(x) = x$ for all real numbers $x \neq 2$ and $(f \circ f^{-1})(x) = x$ for all real numbers $x \neq 1$. By Proposition 1.17.7, we will conclude that f^{-1} is the inverse of f.

$$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = \frac{4f(x)+3}{2f(x)-2} = \frac{4 \cdot \frac{2x+3}{2x-4} + 3}{2 \cdot \frac{2x+3}{2x-4} - 2} = \frac{4(2x+3)+3(2x-4)}{2(2x+3)-2(2x-4)} = \frac{14x}{14} = x$$

$$(f \circ f^{-1})(x) = f(f^{-1}(x)) = \frac{2f^{-1}(x)+3}{2f^{-1}(x)-4} = \frac{2 \cdot \frac{4x+3}{2x-2} + 3}{2 \cdot \frac{4x+3}{2x-2} - 4} = \frac{2(4x+3)+3(2x-2)}{2(4x+3)-4(2x-2)} = \frac{14x}{14} = x$$

1.18 Chapter 1 Overview

A **set** X is a collection of distinct objects called **elements** (or **members**) of X that (typically) possess common properties. Elements of X are written as the lowercase x. If X possesses only finitely many elements $x_1, x_2, \dots, x_n$, then we may describe the set using the **explicit notation** $X = \{x_1, x_2, \dots, x_n\}$. Often, it is most convenient to express a set X using **set-builder notation** $X = \{x \mid P(x)\}$ for some property $P(x)$ common to all elements $x \in X$. We assume the existence of a set $\emptyset$ that does not possess any elements; it is the **empty set**. Every collection of sets comes equipped with certain operations that allow us to combine, compare, and take differences of sets.

- The **union** of the sets X and Y is the set $X \cup Y = \{w \mid w \in X \text{ or } w \in Y\}$.
- The **intersection** of the sets X and Y is the set $X \cap Y = \{w \mid w \in X \text{ and } w \in Y\}$.
- The **relative complement** of X with respect to Y is the set $Y \setminus X = \{w \in Y \mid w \notin X\}$.

We say that Y is a **subset** of X if every element of Y is an element of X, in which case we write $Y \subseteq X$; if Y is a subset of X and there exists an element of X that is not an element of Y, then Y is a **proper subset** of X, in which case we write $Y \subsetneq X$. Observe that Y is a (proper) subset of X if and only if $X \cap Y = Y$ (and $X \cup Y = X$). If $Y \subseteq X$ and $X \subseteq Y$, then $X = Y$; otherwise, the sets X and Y are distinct. One other way to distinguish a (finite) set X is by the number of elements X possesses, called the **cardinality** of X and denoted by $|X|$ or $\#X$ if the bars are ambiguous.

Conveniently, we may with large collections of sets by considering another set I as an **index set**; then, we denote by $\{X_i \mid i \in I\}$ the family of sets **indexed** by I. If each set X_i is a subset of some set U, we refer to U as our **universal set**. By definition, the union of the sets X_i is the set

$$\bigcup_{i \in I} X_i = \{u \mid u \in X_i \text{ for some element } i \in I\}$$

so that membership of an element $u \in U$ in this arbitrary union is characterized by $u \in \cup_{i \in I} X_i$ if and only if $u \in X_i$ for some index $i \in I$. Likewise, the arbitrary intersection of these sets is

$$\bigcap_{i \in I} X_i = \{u \mid u \in X_i \text{ for all elements } i \in I\}$$

with membership of an element $u \in U$ in the intersection characterized by $u \in \cap_{i \in I} X_i$ if and only if $u \in X_i$ for all indices $i \in I$. We say that two sets X_i and X_j are **disjoint** if $X_i \cap X_j = \emptyset$; if $X_i \cap X_j = \emptyset$ for all distinct indices $i, j \in I$, then the sets in $\{X_i \mid i \in I\}$ are **pairwise disjoint** or **mutually exclusive**. We say that $\mathcal{P} = \{X_i \mid i \in I\}$ forms a **partition** of the set U if and only if

(i.) X_i is nonempty for each index $i \in I$;

(ii.) $U = \cup_{i \in I} X_i$; and

(iii.) the sets X_i are pairwise disjoint (i.e., $X_i \cap X_j = \emptyset$ for every pair of distinct indices $i, j \in I$).

We define the **Cartesian product** of two sets X and Y to be the set consisting of all ordered pairs (x, y) such that $x \in X$ and $y \in Y$, i.e., $X \times Y = \{(x, y) \mid x \in X \text{ and } y \in Y\}$. Cardinality of finite sets X and Y is multiplicative in the sense that $|X \times Y| = |X| \cdot |Y|$. We refer to any subset R of the Cartesian product $X \times Y$ as a **relation** from the set X to the set Y. We say that an element $x \in X$ is **related to** an element $y \in Y$ under R if $(x, y) \in R$, and we write that $x \, R \, y$ in this case. Every relation $R \subseteq X \times Y$ induces a relation $R^{-1} \subseteq Y \times X$ called the **inverse relation** defined by

$$R^{-1} = \{(y, x) \mid (x, y) \in R\}.$$

If X is an arbitrary set, then a relation on X is a subset R of the Cartesian product $X \times X$. Every set X admits a relation called the **diagonal** (of X) and defined by $\Delta_X = \{(x, x) \mid x \in X\}$. We say that a relation R on X is **reflexive** if and only if $(x, x) \in R$ for all elements $x \in X$; **symmetric** if and only if $(x, y) \in R$ implies that $(y, x) \in R$; **antisymmetric** if and only if $(x, y) \in R$ and $(y, x) \in R$ implies that $x = y$; and **transitive** if and only if $(x, y) \in R$ and $(y, z) \in R$ together imply that $(x, z) \in R$. **Equivalence relations** are precisely the reflexive, symmetric, and transitive relations; **partial orders** are precisely the reflexive, antisymmetric, and transitive relations. Every equivalence relation E on X induces a partition of E via the **equivalence classes** of elements of X. Explicitly, we say that two elements $x, y \in X$ are **equivalent modulo** E if and only if $(x, y) \in E$, in which case we write that $x \; E \; y$; the equivalence class of an element $x_0 \in X$ is the collection of elements $x \in X$ that are equivalent to x_0 modulo E, i.e., the equivalence class of x_0 is $[x_0] = \{x \in X \mid x \; E \; x_0\} = \{x \in X \mid (x, x_0) \in E\}$. Every element of X belongs to one and only one equivalence class of X modulo E, hence X is partitioned by the collection of distinct equivalence classes modulo E (cf. Proposition 1.10.2 and Corollary 1.10.3). Every set admits a partial order, hence every set is a **partially ordered set**; however, there can be many ways to view a set as a partially ordered set because there can be many different partial orders on a set. If P is a partial order on a set X, then we say that a pair of elements $p, q \in P$ are **comparable** if either $(p, q) \in P$ or $(q, p) \in P$; otherwise, we say that p and q are **incomparable**. We say that a partial order P on X is a **total order** on X if every pair of elements $p, q \in P$ are comparable. Every partial order P of X induces a partial order on the subsets $Y \subset X$ via $P|_Y = \{(y_1, y_2) \in Y \times Y \mid (y_1, y_2) \in P\}$; if $P|_Y$ is a total order on $Y \subseteq X$, then we say that Y is a **chain** (with respect to P) in X. We say that an element $x_0 \in X$ is an **upper bound** on Y (with respect to P) if $(y, x) \in P$ for every element $y \in Y$. We will also say that an element $x_0 \in X$ is **maximal** (with respect to P) if it does not hold that $(x_0, x) \in P$ for any element $x \in X \setminus \{x_0\}$. Zorn's Lemma asserts that if P is a partial order on an arbitrary set X such that every chain Y in X has an upper bound in Y, then Y admits a maximal element $y_0 \in Y$ (with respect to P). We will make use of this throughout the course.

We define a **function** $f : X \to Y$ with **domain** X and **codomain** Y by declaring for each element $x \in X$ a unique (but not necessarily distinct) element $f(x) \in Y$. Every function $f : X \to Y$ induces a subset $f(V) = \{f(v) \mid v \in V\}$ of Y for every subset $V \subseteq X$ called the **image** of V (in Y) under f. Given any subset $W \subseteq Y$, we may also consider the **inverse image** of W (in X) with respect to f, i.e., $f^{-1}(W) = \{x \in X \mid f(x) \in W\}$. We say that $f : X \to Y$ is **injective** if it holds that $f(x_1) = f(x_2)$ implies that $x_1 = x_2$ for any pair of elements $x_1, x_2 \in X$. On the other hand, if for every element $y \in Y$, there exists an element $x \in X$ such that $y = f(x)$, then $f : X \to Y$ is **surjective**. If a function $f : X \to Y$ is both injective and surjective, then it is **bijective**.

Given any functions $f : X \to Y$ and $g : Y \to Z$, we may define a function $g \circ f : X \to Z$ called the **composite function** of f under g by declaring that $(g \circ f)(x) = g(f(x))$ for every element $x \in X$; the process of creating a composition function as **function composition**. Composition of functions is **associative**, i.e., $h \circ (g \circ f) = (h \circ g) \circ f$ whenever all composite functions are **well-defined**. Composition of functions preserves the property that two functions are injective or surjective. Every function $f : X \to Y$ is a relation from X to Y, hence there exists an inverse relation f^{-1} from Y to X; this inverse relation f^{-1} is a function if and only if f is bijective. Crucially, the **inverse function** $f^{-1} : Y \to X$ of a bijective function $f : X \to Y$ is the unique function satisfying that $f^{-1} \circ f = \mathrm{id}_X$ and $f \circ f^{-1} = \mathrm{id}_Y$ for the **identity function** $\mathrm{id}_X : X \to X$ defined by $\mathrm{id}_X(x) = x$.

Quite generally, if $f : X \to Y$ is an injective function, then the function $F : X \to \mathrm{range}(f)$ defined by $F(x) = f(x)$ is bijective. Consequently, there exists a function $F^{-1} : \mathrm{range}(f) \to X$ defined by $F^{-1}(y) = x$ for every element $y = f(x)$. Computing the inverse function F^{-1} corresponding to the induced function F amounts to solving the equation $y = F(x)$ in terms of x; the solution has the form $F^{-1}(y) = x$, and it is precisely this function F^{-1} that is the desired inverse function of F.

1.19 Chapter 1 Exercises

Exercise 1.19.1. Express each of the following sets in set-builder notation.

(a.) $S = \{1, 4, 7, 10\}$

(b.) $T = \{-5, -4, -3, 3, 4, 5\}$

(c.) $U = \{-19, -18, \dots, -4, 4, 5, \dots, 19\}$

(d.) $V = \{2, 3, 5, 7, 11, 13, 17, 19, \dots\}$

(e.) $W = \{\dots, -3, -1, 1, 3, \dots\}$

(f.) $X = \left\{1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \dots\right\}$

(g.) $Y = \left\{\frac{1}{9}, -\frac{1}{3}, 1, -3, 9, \dots\right\}$

(h.) $Z = \{\dots, -2\pi, -\pi, 0, \pi, 2\pi, \dots\}$

Exercise 1.19.2. Express each of the following sets in explicit notation.

(a.) $S = \left\{s \in \mathbb{R} \mid s^2 + \frac{4}{3}s + \frac{1}{3} = 0\right\}$

(b.) $T = \{t \in \mathbb{R} \mid \tan(t) = 0\}$

(c.) $U = \left\{u \in \mathbb{R} : \frac{d}{du}\sqrt{u^2 + 1} = 0\right\}$

(d.) $V = \{v \in \mathbb{N} \mid v^2 + 1 = 26\}$

(e.) $W = \{w \in \mathbb{Z} : w \text{ is odd and } |w| < 10\}$

(f.) $X = \{x \in \mathbb{R} \mid x^3 - 6x^2 + 11x - 6 = 0\}$

(g.) $Y = \{y \in \mathbb{R} \mid y^4 + 3 = 0\}$

(h.) $Z = \left\{z \in \mathbb{R} : \lim_{x \to z} \dfrac{x^2}{x^4 - 2x^2 + 1} = \infty\right\}$

Exercise 1.19.3. Consider the following sets.

- $W = \{1, 2, 3, \dots, 10\}$
- $X = \{1, 3, 5, 7, 9\}$
- $Y = \{2, 4, 6, 8, 10\}$
- $\mathbb{E} = \{n \mid n \text{ is an even integer}\}$
- $\mathbb{O} = \{n \mid n \text{ is an odd integer}\}$
- $\mathbb{Z} = \{n \mid n \text{ is an integer}\}$

Use the set operations $\subseteq$, $\cup$, $\cap$, and $\setminus$ to describe as many relations among these sets as possible.

Exercise 1.19.4. Let $W, X, Y, \mathbb{E}, \mathbb{O}$, and $\mathbb{Z}$ be the sets defined in Exercise 1.19.3.

(a.) Compute the number of elements of $X \times Y$.

(b.) List at least three distinct elements of $\mathbb{O} \times \mathbb{E}$.

(c.) List all elements of the diagonal Δ_X of X.

(d.) Every odd integer can be written as $2k + 1$ for some integer k, and every even integer can be written as 2ℓ for some integer ℓ. Express the sets $\mathbb{O}$ and $\mathbb{E}$ in set-builder notation accordingly.

(e.) Convince yourself that $\mathbb{O}$ and $\mathbb{E}$ have "essentially the same" number of elements; then, find a function $f : \mathbb{O} \to \mathbb{E}$ such that f is injective and f is surjective. Observe that this gives a rigorous justification of the fact that $\mathbb{O}$ and $\mathbb{E}$ have "essentially the same" number of elements.

(f.) Convince yourself that $\mathbb{O}$ and $\mathbb{Z}$ have "essentially the same" number of elements; then, find a function $f : \mathbb{O} \to \mathbb{Z}$ such that f is injective and f is surjective. Conclude from this exercise and the previous one that there are "as many" odd (or even) integers as there are integers.

Exercise 1.19.5. Let $\mathbb{Z}$ denote the set of integers.

(a.) Provide a partition of $\mathbb{Z}$ into three sets.

(**Hint:** What are the possible remainders of an integer modulo 3?)

(b.) Provide a partition of $\mathbb{Z}$ into four sets.

(c.) Provide a partition of $\mathbb{Z}$ into n sets for any positive integer n.

Exercise 1.19.6. Consider the set W consisting of all words in the English language.

(a.) Prove that $R = \{(v, w) \in W \times W \mid v \text{ and } w \text{ begin with the same letter}\}$ is an equivalence relation on W; then, determine the number of distinct equivalence classes of W modulo R.

(b.) Prove that $R = \{(v, w) \in W \times W \mid v \text{ and } w \text{ have the same number of letters}\}$ is an equivalence relation on W; then, describe the equivalence class of the word "awesome."

Exercise 1.19.7. Let $\mathbb{Z}$ be the set of integers. Prove that $(a, b)\ R\ (c, d)$ if and only if $ad = bc$ on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ is an equivalence relation. Describe the collection of distinct equivalence classes.

(**Hint:** For the second part of the problem, try replacing the notation (a, b) with a/b, instead.)

Exercise 1.19.8. Let X be an arbitrary set. Consider the collection $S = \{Y \mid Y \subseteq X\}$. Prove that the inclusion $\subseteq$ defines a partial order P on S such that $(Y_1, Y_2) \in P$ if and only if $Y_1 \subseteq Y_2$; then, either prove that P is a total order on S, or provide a counterexample to show that it is not.

Exercise 1.19.9. List the maximal elements of the subset $S = \{0, 1, 2, 3, 4, 5, 6, 7\}$ of the set $\mathbb{Z}_{\geq 0}$ of non-negative integers with respect to the partial order D of divisibility.

(**Hint:** List as many pairs of comparable elements of S as necessary to compute the chains in S with three or four elements; then, use this information deduce the maximal elements of S.)

Exercise 1.19.10. Complete the following using modular arithmetic.

(a.) If $a \equiv 1 \pmod 6$, find the least positive x for which $5a + 4 \equiv x \pmod 6$.

(b.) If $a \equiv 4 \pmod 7$ and $b \equiv 5 \pmod 7$, find the least positive x for which $6a - 3b \equiv x \pmod 7$.

(c.) (Modular Exponentiation) Use the fact that $2^{2023} \equiv 8 \pmod{10}$ to find $2022^{2023} \pmod{10}$.

Exercise 1.19.11. Consider any nonzero integer n and any integers a and b. If $ab \equiv 0 \pmod n$, then must it be true that $a \equiv 0 \pmod n$ or $b \equiv 0 \pmod n$? Explain.

Exercise 1.19.12. Let p be any prime number. Prove that if a and b are any integers such that $ab \equiv 0 \pmod p$, then either $a \equiv 0 \pmod p$ or $b \equiv 0 \pmod p$.

Exercise 1.19.13. Let X and Y be arbitrary sets.

(a.) Prove that if there exists a function $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$, then f is injective.

(b.) Prove that if there exists a function $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$, then f is surjective.

Chapter 2

Logic and Basic Proof Techniques

2.1 Statements

We have thus far garnered a working knowledge of set theory — including the theory of relations and functions — and we have seen some mathematical proofs. We turn our attention next to fleshing out some details regarding the calculus of logic that will soon assist us with proof writing. We will assume throughout this section that P and Q are **statements**, i.e., P and Q are complete sentences that assert some property or quality that can be unambiguously measured as true (T) or false (F).

Example 2.1.1. "Every positive whole number is an integer" is an example of a true statement.

Example 2.1.2. "The integer 10 is divisible by 3" is an example of a false statement.

Example 2.1.3. "The weather in Kansas City is lovely this time of year" is not a statement because some individuals might think so while others might not: its truth value is ambiguous.

Example 2.1.4. Generally, any sentence that is declarative (e.g., any command), interrogative (e.g., any question), or exclamatory (e.g., any observation) is not a statement because these sentences have no truth values. Examples of each of the aforementioned types of sentence are provided below.

Declarative:	"Don't forget to mow the lawn, son."
Interrogative:	"How about those Chiefs?"
Exclamatory:	"What a story, Mark!"

We will refer to the verity of a statement as its **truth value**. We need not be able to readily determine the truth value of a sentence in order for it to be a valid statement; indeed, there are many unsolved statements throughout mathematics. Generally, a statement whose truth value is undetermined is called a **conjecture**. Other common examples of statements in mathematics whose verity is undetermined are those that involve a potentially unknown or variable quantity x. We have encountered statements of these kinds throughout many of our mathematics courses.

Example 2.1.5. "The real number x is irrational" is an example of a valid statement; it is neither true nor false, but rather, its truth value depends explicitly on the value of the real number x.

Conventionally, any declarative statement of the form $P(x)$ for some variable quantity x is called an **open sentence**; the set of possible values that x can assume is called the **domain** of x; and the truth value of $P(x)$ depends explicitly upon the determination of the variable x.

Example 2.1.6. Observe that the statement $P(x)$ that "the real number x is irrational" is an open sentence; the domain of x is the set of real numbers; and $P(x)$ is true if and only if $x \in \mathbb{R} \setminus \mathbb{Q}$.

We will typically represent an open sentence in the variable x by $P(x)$, and we will separate $P(x)$ from the open sentence it represents with a colon, as the following example illustrates.

Example 2.1.7. Consider the open sentence $P(x) : x^2 - 1 = 0$. Observe that $P(x)$ is a true statement if and only if $x = \pm 1$, hence the natural domain for the statement $P(x)$ is the integers.

Example 2.1.8. Consider the open sentence $P(x) : x^2 + 1 = 0$. Observe that $P(x)$ is a true statement if and only if $x = \pm\sqrt{-1}$, hence $P(x)$ is false if the domain of x is any subset of $\mathbb{R}$.

We note that it is possible to define an open sentence for any (finite) number of variables.

Example 2.1.9. Consider the open sentence $P(x, y) : x^2 + y^2 \geq 0$. Considering that $x^2 + y^2 \geq 0$ for any pair of real numbers x and y, it follows that $P(x, y)$ is a true statement if the domain of x and y is any subset of $\mathbb{R}$; however, if the domains of x and y are both $\mathbb{C}$, then $P(2i, i)$ is false.

Example 2.1.10. Consider the open sentence $P(x, y) : x + y$ is a positive prime number; assume that the domain of x is $X = \{1, 2, 3, 4\}$ and the domain of y is $Y = \{-1, -2, -3, -4\}$. Observe that $P(x, y)$ is true if and only if $(x, y) \in \{(3, -1), (4, -1), (4, -2)\}$; otherwise, $P(x, y)$ is false.

Conventionally, if we are dealing with finitely many statements $P_1, P_2, \dots, P_n$ simultaneously, then it is convenient to collect the truth values of these statements in a **truth table**. Each column of a truth table contains one statement and all of its possible truth values relative to the other statements; the first row of a truth table contains the variables that represent the statements; and the subsequent rows of the truth table contain the possible truth values of each statement relative to the other. Considering that any statement attains one and only truth value, a truth table for the n statements $P_1, P_2, \dots, P_n$ will possess n columns and $2^n + 1$ rows as follows.

P
T
F

P	Q
T	T
T	F
F	T
F	F

P	Q	R
T	T	T
T	T	F
T	F	T
T	F	F
F	T	T
F	T	F
F	F	T
F	F	F

Table 2.1: the truth tables for one, two, and three statements

2.2 Conjunction, Disjunction, and Negation

We examine next the myriad ways to construct new statements from any number of given statements. We concern ourselves first with a statement P. We refer to the statement "not P" (or more precisely "it is not the case that P") as the **negation** of P; symbolically, the negation of any statement P is denoted by $\neg P$. Often, it is possible to represent the negation $\neg P$ of a statement P in a less clunky way than simply by "it is not the case that P," as the following examples illustrate.

Example 2.2.1. Consider the statement $P :$ The integer 2 is even. Observe that the negation $\neg P$ is the statement $\neg P :$ It is not the case that the integer 2 is even. Considering that any integer must be either even or odd, we can rephrase the negation as $\neg P :$ The integer 2 is odd. Observe that P is a true statement while its negation $\neg P$ is a false statement.

Example 2.2.2. Consider the statement $P :$ The integer 111 is prime. Observe that the negation $\neg P$ is the statement $\neg P :$ It is not the case that the integer 111 is prime. Even less clunky is the representation of $\neg P$ as $\neg P :$ The integer 111 is not prime. Better yet, we can say that $\neg P :$ The integer 111 is composite. Observe that in this case, P is false while $\neg P$ is the true statement.

Ultimately, it ought to be clear to the reader that the statements P and $\neg P$ have opposite truth values: if P is true, then $\neg P$ must be false; however, if P is false, then $\neg P$ must be true.

P	$\neg P$
T	F
F	T

Table 2.2: the truth table for the negation $\neg P$

Even more, we will soon see for any statement P, it is the case that either P is true or $\neg P$ is true. Before we arrive at this conclusion, we must discuss other ways to create new statements from a pair of statements P and Q. One way to do so is by considering the case that either the statement P is true or the statement Q is true. Put into symbols, the **disjunction** $P \vee Q$ is the statement "either it is the case that P or it is the case that Q" for which the upside-down wedge $\vee$ denotes the connective "or." Compare the similarities between the disjunction $\vee$ and the set union $\cup$.

Example 2.2.3. Consider the following pair of statements.

$$P : \text{ Topeka is the capital of Kansas.}$$
$$Q : \text{ The real number } \sqrt{2} \text{ is a root of } x^2 - 2.$$

We may construct the disjunction $P \vee Q$ by placing the connective "or" between the statements.

$$P \vee Q : \text{ Either Topeka is the capital of Kansas or the real number } \sqrt{2} \text{ is a root } x^2 - 2.$$

Both of the statements P and Q are in fact true, hence the disjunction $P \vee Q$ is true.

Example 2.2.4. Consider the following pair of statements.

$$P : \text{ Kansas City is the capital of Missouri.}$$
$$Q : \text{ The real number } \pi \text{ is transcendental.}$$

We may construct the disjunction $P \vee Q$ by placing the connective "or" between the statements.

$$P \vee Q : \text{ Either Kansas City is the capital of Missouri or the real number } \pi \text{ is transcendental.}$$

Even though the statement P is false (the capital of Missouri is Jefferson City), the disjunction $P \vee Q$ is true because π is a transcendental number (this fact is non-trivial, but it is well-known).

Example 2.2.5. Consider the following pair of statements.

$$P: \text{ The square root of } -1 \text{ is a real number}$$
$$Q: \text{ The integer 11 is composite.}$$

We may construct the disjunction $P \vee Q$ by placing the connective "or" between the statements.

$$P \vee Q: \text{ Either the square root of } -1 \text{ is a real number or the integer 11 is composite.}$$

Both of these statements are false: $\sqrt{-1}$ is a non-real complex number, and 11 is prime. Consequently, the disjunction $P \vee Q$ is a false statement because neither P nor Q is a true statement.

Crucially, if either of the statements P or Q is true, then the disjunction $P \vee Q$ must also be true; however, if neither of the statements P or Q is true, then $P \vee Q$ must be false.

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Table 2.3: the truth table for the disjunction $P \vee Q$

We may also think about when both of the statements P and Q are true simultaneously. Put another way, we may consider the statement "it is the case that both P and Q," called the **conjunction** $P \wedge Q$. Compare the similarities between the conjunction $\wedge$ and the set intersection $\cap$.

Example 2.2.6. Consider the following pair of statements.

$$P: \text{ Bogotá is the capital of Colombia.}$$
$$Q: \text{ The real number 1 is less than the real number } \sqrt{2}.$$

We may construct the conjunction $P \wedge Q$ by placing the connective "and" between the statements.

$$P \wedge Q: \text{Bogotá is the capital of Colombia, and the real number 1 is less than the real number } \sqrt{2}.$$

Both of the statements P and Q are in fact true, hence the disjunction $P \wedge Q$ is true.

Example 2.2.7. Consider the following pair of statements.

$$P: \text{ Leticia is the capital of Colombia.}$$
$$Q: \text{ The identity function on a set } X \text{ is injective.}$$

We may construct the conjunction $P \wedge Q$ by placing the connective "and" between the statements.

$$P \wedge Q: \text{ Leticia is the capital of Colombia, and the identity function on a set } X \text{ is injective.}$$

Because the statement P is false (the capital of Colombia is Bogotá), the conjunction $P \wedge Q$ is false. Explicitly, it is not the case that both P and Q are true, so $P \wedge Q$ is false.

Example 2.2.8. Consider the following pair of statements.

$$P: \text{ We have that } \cos(k\pi) = 0 \text{ for all integers } k.$$
$$Q: \text{ The integer 8 is a perfect square.}$$

We may construct the conjunction $P \wedge Q$ by placing the connective "and" between the statements.

$$P \vee Q: \text{ We have that } \cos(k\pi) = 0 \text{ for all integers } k, \text{ and integer 8 is a perfect square.}$$

Both of these statements are false: indeed, $\cos(k\pi) = (-1)^k$ for all integers k, and $\sqrt{8} = 2\sqrt{2}$ is not an integer. Consequently, the conjunction $P \wedge Q$ is false because neither P nor Q is true.

We note that the conjunction $P \wedge Q$ of statements P and Q is true if and only if both P and Q are true. Consequently, if either of the statements P or Q is false, then $P \wedge Q$ is false. Be careful not to confuse the upside-down wedge $\vee$ (meaning "or") with the right-side up $\wedge$ (meaning "and").

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Table 2.4: the truth table for conjunction $P \wedge Q$

We are now in a position to state and prove two fundamental principles in the calculus of logic.

Theorem 2.2.9 (Law of the Excluded Middle)**.** *If P is any statement, then $P \vee \neg P$ is true.*

Proof. Given any statement P, consider the disjunction $P \vee \neg P$. Observe that if P is true, then $P \vee \neg P$ is true. Conversely, if P is false, then $\neg P$ is true, hence $P \vee \neg P$ is true. □

P	$\neg P$	$P \vee \neg P$
T	F	T
F	T	T

Table 2.5: the Law of the Excluded Middle

Theorem 2.2.10 (Law of Non-Contradiction)**.** *If P is any statement, then $P \wedge \neg P$ is false.*

Proof. Given any statement P, consider the conjunction $P \vee \neg P$. Observe that if P is true, then $\neg P$ is false, hence $P \wedge \neg P$ is false. Conversely, if P is false, then $P \wedge \neg P$ is false. □

P	$\neg P$	$P \wedge \neg P$
T	F	F
F	T	F

Table 2.6: the Law of Non-Contradiction

2.3 Conditional and Biconditional Statements

We will be interested primarily in statements of the form $P \implies Q$ in which the two-tailed arrow $\implies$ reads "implies." Under this convention, the entire statement $P \implies Q$ can be read either as "P implies Q" or "If P, then Q." Unsurprisingly, a statement of this form is called a **conditional statement** or an **implication**. We refer to the statement P in this construction as the **antecedent**; the statement Q is called the **consequent**. Observe that the statement $P \implies Q$ is false if and only if Q is false while P is true; otherwise, the conditional statement $P \implies Q$ is true.

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

Table 2.7: the truth table for the implication $P \implies Q$

Example 2.3.1. Consider the following pairs of statements.

P : Madrid is the capital of Spain.
Q : The integer 3 is odd.

We may construct the implication $P \implies Q$ as follows.

$P \implies Q$: If Madrid is the capital of Spain, then the integer 3 is odd.

Considering that both P and Q are true statements, it follows that $P \implies Q$ is true.

Example 2.3.2. Consider the following pairs of statements.

P : The integer 3 divides the integer 243.
Q : The integer 3 is even.

We may construct the implication $P \implies Q$ as follows.

$P \implies Q$: If the integer 3 divides the integer 243, then the integer 3 is even.

Observe that $243 = 81 \cdot 3$, hence 3 divides 243; however, we know well that 3 is not an even integer. Consequently, the conditional statement $P \implies Q$ is false: indeed, we are lying here.

On the other hand, if P is false, then according to Table 2.7, the implication $P \implies Q$ is true regardless of the truth value of Q; in this case, the conditional statement $P \implies Q$ is called a **vacuous truth**, or equivalently, we say that $P \implies Q$ is **vacuously** true. Essentially, the idea is that the antecedent P cannot be satisfied because it is false, so the implication must be true.

Example 2.3.3. Consider the following pairs of statements.

P : The integer 17 is greater than the integer 38.
Q : Dr. Beck is a multi-instrumentalist.

We may construct the implication $P \implies Q$ as follows.

$P \implies Q:$ If the integer 17 is greater than the integer 38, then Dr. Beck is a multi-instrumentalist.

Considering that the antecedent P is false (its negation $\neg P : 17 < 38$ is in fact the true statement), it follows that the conditional statement $P \implies Q$ is vacuously true.

One way to justify this result (as promised by Table 2.7) is that no lies were told: Dr. Beck is a multi-instrumentalist, so there was no harm in (falsely) assuming that 17 is greater than 38.

Example 2.3.4. Consider the following pairs of statements.

$P:$ The integer 17 is greater than the integer 38.

$Q:$ Dr. Beck is a multi-millionaire.

We may construct the implication $P \implies Q$ as follows.

$P \implies Q:$ If the integer 17 is greater than the integer 38, then Dr. Beck is a multi-millionaire.

Considering that the antecedent P is false (its negation $\neg P : 17 < 38$ is in fact the true statement), it follows that the conditional statement $P \implies Q$ is vacuously true. (Unfortunately, for Dr. Beck, this makes no difference for his situation: the integer 17 is less than the integer 38.)

One way to verify this result is that no lies were told: Dr. Beck is in fact not a multi-millionaire, but on the other hand, there was nothing guaranteed unless 17 were greater than 38.

We will typically say that "P implies Q" or "Q if P" if the conditional statement $P \implies Q$ is true. Conventionally, if P implies Q, then we say that P is **sufficient** for Q. One can rephrase this by saying that P is sufficient for Q when it is true that Q is true if P is given. Crucially as Table 2.7 illustrates, the statement P may be either true or false; it does not matter. Equivalently, we may say that "P only if Q" if the conditional statement $P \implies Q$ is true. We declare in this case that Q is **necessary** for P. In summary, each of the following statements is equivalent.

- $P \implies Q$
- If P, then Q.
- Q if P.
- P only if Q.
- P is sufficient for Q.
- Q is necessary for P.

By Example 2.3.3, if P is sufficient for Q, then it might not be true that P is necessary for Q; however, if P is both necessary and sufficient for Q, then both of the conditional statements $P \implies Q$ and $Q \implies P$ are true. We say in this case that P is true if and only if Q is true, and we represent this relationship symbolically by $P \iff Q$. We may occasionally use express that the statements P and Q are **(materially) equivalent** if P is true if and only if Q is true.. Put another way, the material equivalence $P \iff Q$ is simply the conjunction $(P \implies Q) \wedge (Q \implies P)$.

References

[CPZ18] G. Chartrand, A.D. Polimeni, and P. Zhang. *Mathematical Proofs: a Transition to Advanced Mathematics*. 4th ed. Pearson Education, Inc., 2018.

[DW00] J.P. D'Angelo and D.B. West. *Mathematical Thinking: Problem Solving and Proofs*. Upper Saddle River, NJ: Prentice-Hall, 2000.