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 $|$ 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 $T = \{-7, -5, -3, \ldots, 11, 13\}$. 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 $U = \{0, 1, 4, 9, \ldots\}$. 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 $A = \{1, 2, 3, \ldots, 10\}$, $B = \{1, 4, 9\}$, 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.

$\times\times\times$: $\emptyset$ ✓✓$\times$: $\{-1, 0\}$
✓$\times\times$: $\{-1\}$ ✓$\times$✓: $\{-1, 1\}$
$\times$✓$\times$: $\{0\}$ $\times$✓✓: $\{0, 1\}$
$\times\times$✓: $\{1\}$ ✓✓✓: $\{-1, 0, 1\}$

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 $X_1, X_2, \ldots, X_n$, then we may consider the index set $I = \{1, 2, \ldots, n\} = [n]$. 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 $A_1 = \{1, 2\}, A_2 = \{2, 3\}, \ldots, A_{10} = \{10, 11\}$. Consequently, our

index set is $I = \{1, 2, \ldots, 10\} = [10]$ 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

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

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

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

Example 1.4.2. Consider the index set $L = \{a, b, c, \ldots, z\}$ 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 $A \cup B \cup C = \{1, 2, \ldots, 9\}$, it follows that the set $\mathcal{P} = \{A, B, C\}$ constitutes a partition of the finite set $[9] = \{1, 2, \ldots, 9\}$.

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

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

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 $x \; R \; y$ in this case; otherwise, if $(x, y) \notin R$, then x is not related to y by R, and we write $x \not R \; y$.

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 $1 \; R \; 1$, $1 \; R \; 2$, and $1 \; R \; 3$ so that 1 is related to each of the elements of Y. Conversely, we have that $-1 \not R \; 1$, $-1 \not R \; 2$, and $-1 \not R \; 3$ 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

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

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

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

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 $\text{dom}(R) = \{1\}$ and $\text{range}(R) = \{1,2,3\} = Y$.

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 $R^{-1} = \{(1,1),(2,1),(3,1)\}$, $\text{dom}(R^{-1}) = \{1,2,3\}$, and $\text{range}(R^{-1}) = \{1\}$.

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

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

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 $x \; R \; y$ 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 $0 \; R \; 1$ but $1 \not R \; 0$. Last, R is transitive because if $x \; R \; y$ and $y \; R \; z$, then $x \leq y \leq z$ so that $x \leq z$ and $x \; R \; z$. Later, we will return to this relation to discuss the property that if $x \; R \; y$ and $y \; R \; x$, then $x = y$.

Example 1.8.3. Consider the relation R' defined on the set of integers $\mathbb{Z}$ such that $x \; R' \; y$ 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 $0 \not R' \; 0$ and R' is not reflexive. Likewise, we have that $0 \neq 1$ and $1 \neq 0$ so that $0 \; R' \; 1$ and $1 \; R' \; 0$ but $0 \not R' \; 0$, hence R' is not transitive.

Example 1.8.4. Consider the relation D defined on the set of real numbers $\mathbb{R}$ such that $x \; D \; y$ 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 $x \; D \; x$ and $|y - x| = |x - y|$ so that $y \; D \; x$ if and only if $x \; D \; y$; however, $0 \; D \; 1$ and $1 \; D \; 2$ do not together imply that $0 \; D \; 2$ 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 $x \; R \; y$ 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

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

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

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

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 $[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$. Likewise, by definition and a brute-force check, we have that $[1] = \{b \in \mathbb{Z} \mid 5b = 3k + 2 \text{ for some integer } k\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$ and $[2] = \{b \in \mathbb{Z} \mid 5b = 3k+4 \text{ for some integer } k\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$. 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 $\text{range}(f) = \{f(x) \mid x \in X\}$ 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 range$(f) = \{1, 2, 3\}$, but it holds that 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 $Y = \text{range}(f) = \{f(x) \mid x \in X\}$.

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 $X = \{x_1, x_2, \ldots, x_n\}$, 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

$$(g \circ f)(a) = g(f(a)) = g(b) = c, \qquad (g \circ f)(c) = g(f(c)) = g(d) = e, \text{ and}$$
$$(g \circ f)(b) = g(f(b)) = g(c) = d, \qquad (g \circ f)(d) = g(f(d)) = g(e) = f.$$

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

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

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 $Y' \supseteq \text{range}(f)$. For instance, for the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$, we have that $\text{range}(f) = \{f(x) \mid x \in \mathbb{R}\} = \{x^2 \mid x \in \mathbb{R}\} = \mathbb{R}_{\geq 0}$, 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 $f(x) \in \text{range}(f)$ 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. □

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

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

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 $x_1, x_2, \ldots, x_n$, then we may describe the set using the **explicit notation** $X = \{x_1, x_2, \ldots, x_n\}$. 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.) $U = \{-19, -18, \ldots, -4, 4, 5, \ldots, 19\}$

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

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

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

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

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

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

Exercise 1.19.3. Consider the following sets.

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

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, but 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 $P_1, P_2, \ldots, P_n$ 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 $P_1, P_2, \ldots, P_n$ 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, but 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, but $\neg P$ 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 : Topeka is the capital of Kansas.

Q : The real number $\sqrt{2}$ is a root of $x^2 - 2$.

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

$P \vee Q$: Either Topeka is the capital of Kansas or the real number $\sqrt{2}$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 : Kansas City is the capital of Missouri.

Q : The real number π is transcendental.

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

$P \vee Q$: Either Kansas City is the capital of Missouri or the real number π 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 : The square root of -1 is a real number

Q : The integer 11 is composite.

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

$P \vee Q$: Either the square root of -1 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 : Bogotá is the capital of Colombia.

Q : 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.

$P \wedge Q$: 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 : Leticia is the capital of Colombia.

Q : The identity function on a set X is injective.

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

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

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

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 and 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.

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

We will fix our attention throughout the rest of the course primarily on conditional statements in which P and Q are open sentences. Consider the following examples along these lines.

Example 2.3.5. Consider the following pairs of statements about a positive integer n.

$P(n)$: The integer $n^4 + 1$ is prime.

$Q(n)$: The integer $n^2 + 1$ is prime.

By plugging in different values of the integer $n \geq 1$, we obtain explicit statements $P(n)$ and $Q(n)$.

$P(1)$: The integer 2 is prime.

$P(2)$: The integer 17 is prime.

$P(3)$: The integer 82 is prime.

$P(4)$: The integer 257 is prime.

$P(5)$: The integer 626 is prime.

$Q(1)$: The integer 2 is prime.

$Q(2)$: The integer 5 is prime.

$Q(3)$: The integer 10 is prime.

$Q(4)$: The integer 17 is prime.

$Q(5)$: The integer 26 is prime.

Consider the conditional statement $P(n) \implies Q(n)$ defined as follows.

$$P(n) \implies Q(n): \text{ If the integer } n^4+1 \text{ is prime, then the integer } n^2+1 \text{ is prime.}$$

By Table 2.7, we know that $P(n) \implies Q(n)$ is false if and only if $P(n)$ is true and $Q(n)$ is false. Consequently, the statement $P(n) \implies Q(n)$ is true for all integers $1 \leq n \leq 5$. Quite astonishingly, this statement is in fact true for all integers $1 \leq n \leq 27$; however, we have that $28^4+1 = 614657$ is prime and $28^2+1 = 785$ is not prime, hence the statement $P(28) \implies Q(28)$ is false.

Example 2.3.6. Consider the following pairs of statements about an integer $n \geq 2$.

$$P(n): \text{ The integer } n^2+1 \text{ is prime.}$$
$$Q(n): \text{ The integer } n^4-1 \text{ is prime.}$$

By definition, the conditional statement $P(n) \implies Q(n)$ is given as follows.

$$P(n) \implies Q(n): \text{ If the integer } n^2+1 \text{ is prime, then the integer } n^4-1 \text{ is prime.}$$

By Table 2.7, we know that $P(n) \implies Q(n)$ is false if and only if $P(n)$ is true and $Q(n)$ is false. Considering that $n^4-1 = (n^2-1)(n^2+1)$ is divisible by n^2+1 for all integers n, it follows that n^4-1 is composite for all integers n, hence the open sentence $Q(n)$ is false for every integer n. We conclude that the conditional statement $P(n) \implies Q(n)$ is false for all integers $n \geq 2$.

Example 2.3.7. Consider the following pairs of statements about a pair of real numbers x and y.

$$P(x,y): \text{ We have that } x+y=1.$$
$$Q(x,y): \text{ We have that } x^2+y^2=1.$$

By definition, the conditional statement $P(x,y) \implies Q(x,y)$ is given as follows.

$$P(x,y) \implies Q(x,y): \text{ If } x+y=1, \text{ then } x^2+y^2=1.$$

By Table 2.7, we know that $P(x,y) \implies Q(x,y)$ is false if and only if $P(x,y)$ is true and $Q(x,y)$ is false. Observe that if $x+y=1$, then $y=1-x$ so that $y^2 = x^2-2x+1$. Consequently, it follows that $x^2+y^2 = 2x^2-2x+1$; thus, the open sentence $Q(x,y)$ is true if and only if $2x^2-2x+1=1$ if and only if $2x^2-2x=0$ if and only if $2x(x-1)=0$ if and only if $x=0$ or $x=1$. We conclude that the statement $P(x,y) \implies Q(x,y)$ is true if and only if $x=0$ and $y=1$ or $x=1$ and $y=0$.

Given any pair of statements P and Q, the conditional statement $Q \implies P$ formed by swapping the antecedent and the consequent is called the **converse** of the conditional statement $P \implies Q$. Like the implication $P \implies Q$, its converse $Q \implies P$ can be understood in different ways.

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

Example 2.3.8. Consider the following pairs of statements.

$$P: \text{ The integer 17 is greater than the integer 38.}$$
$$Q: \text{ Dr. Beck is a multi-instrumentalist.}$$

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

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

Unlike the implication $P \implies Q$ (which is vacuously true), the converse $Q \implies P$ is false: Dr. Beck is a multi-instrumentalist, but the integer 17 is not greater than the integer 38.

Example 2.3.9. 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 converse $Q \implies P$ of the implication $P \implies Q$ as follows.

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

Considering that the antecedent Q is false, the conditional statement $Q \implies P$ is vacuously true. One way to verify this result is that no lies were told: Dr. Beck is not a multi-millionaire.

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

Table 2.8: the truth table for the converse $Q \implies P$ of the implication $P \implies Q$

By Examples 2.3.3 and 2.3.8, even if P is sufficient for Q, it is not necessarily 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 will typically say 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 $(P \implies Q) \wedge (Q \implies P)$. Each of the following statements concerning the biconditional statement $P \iff Q$ is equivalent.

- $P \iff Q$
- P if and only if Q.
- P is (materially) equivalent to Q.
- P is necessary and sufficient for Q.

P	Q	$P \implies Q$	$Q \implies P$	$(P \implies Q) \wedge (Q \implies P)$	$P \iff Q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

Table 2.9: the truth table for the biconditional $P \iff Q$

Put another way, we have that $P \iff Q$ is true if and only if P and Q have the same truth value.

Example 2.3.10. Consider the following statements.

$$\begin{aligned} P:&\ \text{The integer 3 divides the integer 243.}\\ Q:&\ \text{The integer 3 is even.}\\ R:&\ \text{The integer 17 is greater than the integer 38.}\\ S:&\ \text{The integer 2027 is prime.} \end{aligned}$$

Considering that P and S are true statements, but Q and R are false statements, it follows that $P \iff S$ and $Q \iff R$ are both true statements and $P \iff Q$, $P \iff R$, $Q \iff S$, and $R \iff S$ are all false statements. Examples of these statements in words are provided below.

$$\begin{aligned} P \iff Q:&\ \text{The integer 3 divides the integer 243 if and only if 3 is even.}\\ P \iff S:&\ \text{The integer 3 divides the integer 243 if and only if the integer 2027 is prime.}\\ Q \iff R:&\ \text{The integer 3 is even if and only if the integer 17 is greater than the integer 38.} \end{aligned}$$

Example 2.3.11. Consider the following statements about an integer n.

$$\begin{aligned} P(n):&\ \text{The integer } n \text{ is even.}\\ Q(n):&\ \text{The integer } n^2 \text{ is even.} \end{aligned}$$

We construct the biconditional statement $P(n) \iff Q(n)$ as follows.

$$P(n) \iff Q(n):\ \text{The integer } n \text{ is even if and only if the integer } n^2 \text{ is even.}$$

By definition, an integer n is even if and only if $n = 2k$ for some integer k. Consequently, if n is even, then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$ is even. Conversely, if n^2 is even, then there exists an integer k such that $n^2 = 2k$. Considering that 2 is prime, we must have that 2 divides n, hence n is even. We conclude therefore that the statement $P(n) \iff Q(n)$ is true for all integers n.

Example 2.3.12. Consider the following statements about an integer n.

$$\begin{aligned} P(n):&\ \text{The integer } n \text{ is odd.}\\ Q(n):&\ \text{The integer } n^2 \text{ is odd.} \end{aligned}$$

We construct the biconditional statement $P(n) \iff Q(n)$ as follows.

$P(n) \iff Q(n)$: In order for the integer n to be odd, it is necessary and sufficient that n^2 is odd.

Example 2.3.13. Consider the following pairs of statements about a pair of real numbers x and y.

$$\begin{aligned} P(x,y):&\ \text{We have that } x^2 + y^2 = 1.\\ Q(x,y):&\ \text{We have that } (x,y) \in \mathbb{R}^2 \text{ lies on a circle of radius 1 centered at } (0,0). \end{aligned}$$

By definition, the statements $P(x,y) \implies Q(x,y)$ and $Q(x,y) \implies P(x,y)$ are as follows.

$P(x,y) \implies Q(x,y)$: If $x^2 + y^2 = 1$, then $(x,y) \in \mathbb{R}^2$ lies on a circle of radius 1 centered at $(0,0)$.
$Q(x,y) \implies P(x,y)$: If $(x,y) \in \mathbb{R}^2$ lies on a circle of radius 1 centered at $(0,0)$, then $x^2 + y^2 = 1$.

Recall that the equation of a circle of radius r centered at (h, k) is given by

$$(x-h)^2 + (y-k)^2 = r^2.$$

Consequently, the conditional statement $Q(x,y) \implies P(x,y)$ is true by definition. Conversely, if $x^2+y^2=1$, then $(x-0)^2+(y-0)^2 = 1^2$ implies that the point $(x,y) \in \mathbb{R}^2$ lies on a circle of radius 1 centered at $(0,0)$. Put another way, we have that $P(x,y) \implies Q(x,y)$ is true. Ultimately, these observations together yield that the biconditional statement $P(x,y) \iff Q(x,y)$ is true.

2.4 Tautologies and Contradictions

2.5 Tautologies and Contradictions

By the Law of the Excluded Middle, the statement $P \vee \neg P$ ("P or not P") is always true; it is a **tautology**. Generally, a tautology is any statement that is true for all possible truth inputs.

Example 2.5.1. Given any statements P and Q, the statement $(\neg Q) \vee (P \implies Q)$ is a tautology. We can convince ourselves of this by realizing that $P \implies Q$ is true if either P is false or P and Q are both true. Consequently, the statement $(\neg Q) \vee (P \implies Q)$ is true in the case that P is false or P and Q are both true. But if Q is false, then $\neg Q$ is true, hence $(\neg Q) \vee (P \implies Q)$ is true. Let us construct a truth table to verify this. We will see that all values of $(\neg Q) \vee (P \implies Q)$ are T.

P	Q	$\neg Q$	$P \implies Q$	$(\neg Q) \vee (P \implies Q)$
T	T	F	T	T
T	F	T	F	T
F	T	F	T	T
F	F	T	T	T

Table 2.10: the truth table for $(\neg Q) \vee (P \implies Q)$

Example 2.5.2. Given any statements P and Q, the statement $[(P \vee Q) \wedge (\neg Q)] \implies P$ is a tautology: indeed, it suffices to check that all of its values in the following truth table are T.

P	Q	$\neg Q$	$P \vee Q$	$(P \vee Q) \wedge (\neg Q)]$	$[(P \vee Q) \wedge (\neg Q)] \implies P$
T	T	F	T	F	T
T	F	T	T	T	T
F	T	F	T	F	T
F	F	T	F	F	T

Table 2.11: the truth table for $[(P \vee Q) \wedge (\neg Q)] \implies P$

Bearing this in mind, when Beyoncé says, "I break the internet: top two, and I ain't number two" on the track "Top Off" by DJ Khaled, it means that she is number one.

By the Law of Non-Contradiction, the statement $P \wedge \neg P$ ("P and not P") is always false; it is a **contradiction** because it is a statement that is false for all possible truth inputs.

Example 2.5.3. Given any statements P and Q, the statement $P \wedge [P \implies (Q \wedge \neg Q)]$ is a contradiction. We can verify this by convincing ourselves (by the Law of Non-Contradiction) that $Q \wedge \neg Q$ is false; therefore, the conditional statement $P \implies (Q \wedge \neg Q)$ is false so long as P is true. On the other hand, $P \implies (Q \wedge \neg Q)$ is true so long if P is false. Combined, these two observations yield that P and $P \implies (Q \wedge \neg Q)$ take opposite truth values, so their conjunction is false.

P	Q	$\neg Q$	$Q \wedge \neg Q$	$P \implies (Q \wedge \neg Q)$	$P \wedge [P \implies (Q \wedge \neg Q)]$
T	T	F	F	F	F
T	F	T	F	F	F
F	T	F	F	T	F
F	F	T	F	T	F

Table 2.12: the truth table for $P \wedge [P \implies (Q \wedge \neg Q)]$

Example 2.5.4. Given any statements P and Q, the statement $P \wedge [P \implies (Q \wedge \neg Q)]$ is a contradiction. We can verify this by convincing ourselves (by the Law of Non-Contradiction) that $Q \wedge \neg Q$ is false; therefore, the conditional statement $P \implies (Q \wedge \neg Q)$ is false so long as P is true. On the other hand, $P \implies (Q \wedge \neg Q)$ is true so long if P is false. Combined, these two observations yield that P and $P \implies (Q \wedge \neg Q)$ take opposite truth values, so their conjunction is false.

P	Q	$\neg P$	$P \wedge Q$	$Q \implies \neg P$	$(P \wedge Q) \wedge (Q \implies \neg P)$
T	T	F	T	F	F
T	F	F	F	T	F
F	T	T	F	T	F
F	F	T	F	T	F

Table 2.13: the truth table for $(P \wedge Q) \wedge (Q \implies \neg P)$

2.6 Logical Equivalence

Given any statements P and Q, recall from Table 2.7 that the conditional statement $P \implies Q$ is vacuously true if P is false; therefore, in order to determine the truth value of $P \implies Q$, it suffices to consider the case that P is true. Unfortunately, in some situations, it is difficult to establish the verity of Q even if P is known to be true. Under these circumstances, it is not possible to determine if the statement $P \implies Q$ is true or false because this depends entirely on whether Q is true or false; however, it is possible in some cases to extract a statement $S(P, Q)$ depending on P and Q that is **logically equivalent** to the implication $P \implies Q$. We say that two statements S_1 and S_2 are logically equivalent if and only if their values in a truth table are equal; if this is the case, then we write $S_1 \equiv S_2$ to assert symbolically that S_1 and S_2 are logically equivalent. Consequently, if we could demonstrate that the statement $S(P, Q)$ were true, then $P \implies Q$ must be true, as well.

We concern ourselves primarily with the interplay between the conjunction, disjunction, implication, and negation. We seek to establish several statements that are logically equivalent to the conditional statement $P \implies Q$. By the previous paragraph, if the statement P is false, then the

implication $P \implies Q$ is vacuously true. Even more, if the statement Q is true, then the implication $P \implies Q$ must be true regardless of the truth value of P. Consequently, it seems that the statements $P \implies Q$ and $\neg P \vee Q$ are logically equivalent, as the following truth table illustrates.

P	Q	$\neg P$	$P \implies Q$	$\neg P \vee Q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Table 2.14: the truth table for the implication $P \implies Q$ and the disjunction $\neg P \vee Q$

Proposition 2.6.1. *Given any statements P and Q, we have that $(P \implies Q) \equiv (\neg P \vee Q)$.*

Consider the statement $\neg Q \implies \neg P$ called the **contrapositive** of the implication $P \implies Q$. Observe that if Q is true, then $\neg Q$ is false, hence the statement $\neg Q \implies \neg P$ is vacuously true. Likewise, if Q is true, then the statement $P \implies Q$ is true regardless of the verity of P. Conversely, if Q is false, then $\neg Q$ is true, hence $\neg Q \implies \neg P$ is true if and only if $\neg P$ is true if and only if P is false. Consequently, we are lead to the following truth table and the subsequent proposition.

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

Table 2.15: the truth table for the contrapositive $\neg Q \implies \neg P$ of the implication $P \implies Q$

Proposition 2.6.2. *Given any statements P and Q, we have that $(P \implies Q) \equiv (\neg Q \implies \neg P)$.*

Example 2.6.3. Consider the following statements.

P : Bob earns an A on his final exam in MA291.

Q : Bob earns an A as his final grade in MA291.

Let us assume that if Bob earns an A on his final exam in MA291, then Bob earns an A as his final grade in MA291. Consider the following statements regarding Bob's grade in MA291.

R : Either Bob does not earn an A on his final exam or Bob earns an A as his final grade.

S : If Bob does not earn an A as his final grade, then Bob did not earn an A on his final exam.

Observe that the statement R is true: indeed, if Bob does not earn an A on his final exam in MA291, then there is no promise as to what his final grade in MA291 will be, so no lies have been told regardless of the outcome. On the other hand, if Bob earns an A as his final grade, then it does not matter what he earned on his final exam because he will surely be happy with his grade. Likewise, the statement S is true: indeed, if Bob does not earn an A as his final grade in MA291, then he must not have earned an A on his final exam because that would have guaranteed him an A in the course. We have corroborated the logical equivalence of the statements $P \implies Q$, $\neg P \vee Q$, and $\neg Q \implies \neg P$ for the statements at hand, as guaranteed by Propositions 2.6.1 and 2.6.2.

Example 2.6.4. Consider the following statements.

P : It is overcast in Kansas City.

Q : Bob brings an umbrella to work.

Let us assume that if it is overcast in Kansas City, then Bob brings an umbrella to work. Observe that if Bob does not bring an umbrella to work, then it must not be overcast in Kansas City; otherwise, if it were overcast in Kansas City, then Bob would have brought an umbrella to work. Even more, we know that either it is sunny in Kansas City or Bob brings an umbrella to work: indeed, if Bob does not bring an umbrella to work, then it must be sunny in Kansas City. Each of these observations bears out the logical equivalence of $P \implies Q$, $\neg Q \implies \neg P$, and $\neg P \vee Q$.

Often, it is useful to determine when the conditional statement $P \implies Q$ is false (i.e., P does not provide sufficient information from which to deduce Q). By Table 2.7, we have that $P \implies Q$ is false if and only if P is true and Q is false if and only if $P \wedge \neg Q$ is true, hence the statements $\neg(P \implies Q)$ and $P \wedge \neg Q$ are logically equivalent, as the following truth table illustrates.

P	Q	$\neg Q$	$P \implies Q$	$\neg(P \implies Q)$	$P \wedge \neg Q$
T	T	F	T	F	F
T	F	T	F	T	T
F	T	F	T	F	F
F	F	T	T	F	F

Table 2.16: the truth table for the negated implication $\neg(P \implies Q)$ and the disjunction $P \wedge \neg Q$

Proposition 2.6.5. *Given any statements P and Q, we have that $\neg(P \implies Q) \equiv (P \wedge \neg Q)$.*

Example 2.6.6. Consider the following statements.

P : Bob earns an A on his final exam in MA291.

Q : Bob earns an A as his final grade in MA291.

Observe that if Bob earns an A on his final exam in MA291 but Bob does not earn an A as his final grade in MA291, then it is a lie to say that if Bob earns an A on his final exam in MA291, then Bob earns an A as his final grade in MA291; this illustrates the result of Proposition 2.6.5.

By Table 2.3, if $P \vee Q$ is false, then neither P nor Q is true. Likewise, by Table 2.4, if $P \wedge Q$ is false, then either P is false or Q is false. Combined, these observations form **De Morgan's Laws**.

P	Q	$\neg P$	$\neg Q$	$P \vee Q$	$\neg(P \vee Q)$	$\neg P \wedge \neg Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P \vee \neg Q$
T	T	F	F	T	F	F	T	F	F
T	F	F	T	T	F	F	F	T	T
F	T	T	F	T	F	F	F	T	T
F	F	T	T	F	T	T	F	T	T

Table 2.17: the truth table for $\neg(P \vee Q)$ and $\neg(P \wedge Q)$

Theorem 2.6.7 (De Morgan's Laws)**.** *Let P and Q be any statements.*

(a.) *We have that $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$, i.e., $\neg(P \vee Q)$ is logically equivalent to $\neg P \wedge \neg Q$.*

(b.) *We have that $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$, i.e., $\neg(P \wedge Q)$ is logically equivalent to $\neg P \vee \neg Q$.*

Example 2.6.8. Consider the following statements.

$$P: \text{ It is overcast in Kansas City.}$$
$$Q: \text{ Bob brings an umbrella to work.}$$

Observe that if it is not the case that either it is overcast in Kansas City or Bob brings an umbrella to work, then it must be the case that neither it is overcast in Kansas City nor Bob brings an umbrella to work. Likewise, if it is not the case that it is overcast in Kansas City and Bob brings an umbrella to work, then it must be the case that either it is not overcast in Kansas City or Bob does not bring an umbrella to work. We have thus verified De Morgan's Laws for the given statements.

2.7 Quantified Statements

Often, we seek to determine the verity of an open sentence for all possible values in its domain. Explicitly, if $P(x)$ is any open sentence that depends on a variable x with domain S, then for each element $s \in S$, the truth value of the statement $P(s)$ is well-defined and can be determined.

Example 2.7.1. Consider the following statement about an integer n.

$$P(n): \text{ The integer } n \text{ is even.}$$

We can plainly see that the verity of $P(n)$ depends entirely on the value of n. Each of the following statements in the left-hand column is true, but each statement in the right-hand column is false.

$P(0)$: The integer 0 is even. $P(1)$: The integer 1 is even.

$P(2)$: The integer 2 is even. $P(3)$: The integer 3 is even.

$P(4)$: The integer 4 is even. $P(5)$: The integer 5 is even.

Quantification is another process of converting an open sentence $P(x)$ in the variable x into a statement whose truth value can be determined. **Quantified statements** are expressed using **logical quantifiers**. Primarily, we will study three logical quantifies throughout this course.

We use the **universal quantifier** $\forall$ to symbolically represent the phrases "for all," "for every," or "for each." Consequently, the statement $\forall x \in S,\ P(x)$ can be understood in words to mean "for all elements $x \in S$, we have that $P(x)$." Observe that the quantified statement $\forall x \in S,\ P(x)$ is true if $P(x)$ is true for all elements $x \in S$; otherwise, this statement is false. Put another way, if the statement $P(x_0)$ is false for some element $x_0 \in S$, then the statement $\forall x \in S,\ P(x)$ is false.

Summary 2.7.2. Given any open sentence $P(x)$ with domain S, the quantified statement

$$\forall x \in S,\ P(x): \text{ For every element } x \in S, \text{ we have that } P(x).$$

is true if and only if $P(x)$ is true for all elements $x \in S$. Conversely, this quantified statement is false if and only if there exists an element $x_0 \in S$ such that $P(x_0)$ is false.

Example 2.7.3. Consider the following statement about an integer n.

$$P(n): \text{ The integer } n \text{ is even.}$$

By using the universal quantifier $\forall$ ("for all"), we obtain the following quantified statement.

$$\forall n \in \mathbb{Z},\ P(n): \text{ For every integer } n, \text{ we have that } n \text{ is even.}$$

By Example 2.7.1 and Summary 2.7.2, the above quantified statement is false because $P(1)$ is false.

Example 2.7.4. Consider the following statements about an integer n.

$$P(n): \text{ The integer } n \text{ is even.}$$
$$Q(n): \text{ The integer } n^2 \text{ is even.}$$

By using the universal quantifier $\forall$ ("for all"), we obtain the following quantified statement.

$$\forall n \in \mathbb{Z},\ [P(n) \iff Q(n)]: \text{ For every integer } n, \text{ we have that } n \text{ is even if and only if } n^2 \text{ is even.}$$

By Example 2.3.11, this statement is true because $P(n) \iff Q(n)$ is true for all integers n.

Example 2.7.5. Consider the following statement about a pair of real numbers x and y.

$$P(x, y): \text{ The real number } x^2 + y^2 \text{ is non-negative.}$$

By using the universal quantifier $\forall$ ("for all"), we obtain the following quantified statement.

$$\forall x, y \in \mathbb{R},\ P(x, y): \text{ For every pair of real numbers } x \text{ and } y, \text{ we have that } x^2 + y^2 \geq 0.$$

Considering that $x^2 \geq 0$ for every real number x, it follows that $x^2 + y^2 \geq 0$ for every pair of real numbers x and y. Consequently, the quantified statement $\forall x, y \in \mathbb{R}, P(x, y)$ is true.

Example 2.7.6. Consider the following statements about a real number x.

$$P(x): \text{ The real number } x^2 + 4 \text{ satisfies that } x^2 + 4 \geq 4.$$
$$Q(x): \text{ The real number } x^2 + 4 \text{ satisfies that } x^2 + 4 \leq 4.$$

By using the universal quantifier $\forall$ ("for all"), we obtain the following quantified statements.

$$\forall x \in \mathbb{R},\ P(x): \text{ For all real numbers } x, \text{ we have that } x^2 + 4 \geq 4.$$
$$\forall x \in \mathbb{R},\ Q(x): \text{ For all real numbers } x, \text{ we have that } x^2 + 4 \leq 4.$$

Considering that $x^2 \geq 0$ for every real number x, it follows that $x^2 + 4 \geq 4$ for every real number x. Consequently, the quantified statement $\forall x \in \mathbb{R},\ P(x)$ is true; however, $Q(1)$ is false because the real number $5 = 1^2 + 4$ does not satisfy that $5 \leq 4$. We conclude that $\forall x \in \mathbb{R},\ Q(x)$ is false.

One other indispensable way to view the universally quantified statement $\forall x \in S,\ P(x)$ in words is as either the statement "if x is an element of S, then we have that $P(x)$" or "if $x \in S$, then $P(x)$." Observe that in this manner, any statement involving the universal quantifier is simply a conditional statement. Consequently, Proposition 2.6.1 entails that the quantified statement $\forall x \in S,\ P(x)$ is

logically equivalent to the disjunction $(x \notin S) \vee P(x)$. By De Morgan's Laws, the negation of $\forall x \in S,\ P(x)$ is logically equivalent to the negation of $(x \notin S) \vee P(x)$ — namely, $(x \in S) \wedge \neg P(x)$.

Better yet, the negation of a quantified statement is itself a quantified statement. Explicitly, we use the **existential quantifier** $\exists$ to express the phrases "there exists," "for at least one," or "for some." Consequently, the quantified statement $\exists x \in S,\ P(x)$ can be understood in words as "there exists an element $x \in S$ such that $P(x)$." Observe that the quantified statement $\exists x \in S,\ P(x)$ is true if $P(x_0)$ is true for some element $x_0 \in S$; otherwise, this statement is false. Put another way, if $P(x)$ is false for every element $x \in S$, then the quantified statement $\exists x \in S,\ P(x)$ is false.

Summary 2.7.7. Given any open sentence $P(x)$ with domain S, the quantified statement

$$\exists x \in S,\ P(x):\ \text{There exists an element } x \in S \text{ such that } P(x)$$

is true if and only if $P(x_0)$ is true for some element $x_0 \in S$. Conversely, this quantified statement is false if and only if the statement $P(x)$ is false for all elements $x \in S$.

Example 2.7.8. Consider the following statement about an integer n.

$$P(n):\ \text{The integer } n \text{ is even.}$$

By using the existential quantifier $\exists$ ("there exists"), we obtain the following quantified statement.

$$\exists n \in \mathbb{Z},\ P(n):\ \text{There exists an integer } n \text{ such that } n \text{ is even.}$$

Certainly, the above quantified statement is true because $P(2)$ is true.

Example 2.7.9. Consider the following statement about an integer n.

$$P(n):\ \text{The integer } n^4 + 1 \text{ is prime.}$$

By using the existential quantifier $\exists$ ("there exists"), we obtain the following quantified statement.

$$\exists n \in \mathbb{Z},\ P(n):\ \text{There exists an integer } n \text{ such that } n^4 + 1 \text{ is prime.}$$

Considering that $2 = 1^4 + 1$ is prime, $P(1)$ is true, hence the above quantified statement is true.

Example 2.7.10. Consider the following statement about a pair of real numbers x and y.

$$P(x, y):\ \text{The real numbers } x \text{ and } y \text{ satisfy that } x^2 + y^2 = 4.$$

By using the existential quantifier $\exists$ ("there exists"), we obtain the following quantified statement.

$$\exists x, y \in \mathbb{R},\ P(x, y):\ \text{There exist real numbers } x \text{ and } y \text{ such that } x^2 + y^2 = 4.$$

Considering that the set of ordered pairs (x, y) of real numbers satisfying that $x^2 + y^2 = 4$ is the graph of a circle of radius 2 centered at the origin in the Cartesian plane, it follows that the above quantified statement is true: indeed, both of the statements $P(2, 0)$ and $P(0, 2)$ are true.

Example 2.7.11. Consider the following statements about a real number x.

$$P(x): \text{ The real number } x \text{ satisfies that } x^2 - 2x - 3 = 0.$$
$$Q(x): \text{ The real number } x^3 \text{ satisfies that } x^3 \geq 8.$$

By using the existential quantifier $\exists$ ("there exists"), we obtain the following quantified statements.

$$\exists x \in \mathbb{R},\, [P(x) \implies Q(x)]: \text{ There exists a real number } x \text{ such that if } x^2 - 2x - 3 = 0, \text{ then } x^3 \geq 8.$$
$$\exists x \in \mathbb{R},\, [P(x) \wedge \neg Q(x)]: \text{ There exists a real number } x \text{ such that } x^2 - 2x - 3 = 0 \text{ and } x^3 < 8.$$

Observe that if $P(x)$ is false, then the conditional statement $P(x) \implies Q(x)$ is vacuously true. Consequently, the first quantified statement above is true for any real number x such that $x^2 - 2x - 3$ is nonzero (e.g., suppose that $x = 0$). Likewise, the second quantified statement above is true because the real number $x = -1$ satisfies that $(-1)^2 - 2(-1) - 3 = 0$ and $(-1)^3 = 1 < 8$. Put another way, the real number $x = -1$ satisfies that $P(-1)$ is true and $Q(-1)$ is false.

We provide next the crucial theorem that relates the universal and existential quantifiers.

Theorem 2.7.12. *Consider any open sentence $P(x)$ over the domain S.*

(a.) *We have that* $\neg[\forall x \in S,\, P(x)] \equiv [\exists x \in S,\, \neg P(x)]$.

(b.) *We have that* $\neg[\exists x \in S,\, P(x)] \equiv [\forall x \in S,\, \neg P(x)]$.

Last, if $P(x)$ is any open sentence whose domain is any nonempty set S, then we say that an element $x_0 \in S$ is the **unique** element of S **satisfying the statement** $P(x_0)$ if and only if

1.) the statement $P(x_0)$ is true and

2.) for every element $x \in S$, if $P(x)$ is true, then we must have that $x = x_0$.

We use the **uniqueness quantifier** ! to represent the phrase "unique". Explicitly, we will write $\exists! x \in S,\, P(x)$ to signify that "there exists a unique element $x \in S$ such that $P(x)$."

Example 2.7.13. Consider the following statement about an integer n.

$$P(n): \text{ The integer } n \text{ satisfies that } 3n - 4 = 5.$$

Observe that $P(n)$ is true if and only if $3n - 4 = 5$ if and only if $n = 3$, hence the statement $P(n)$ admits a unique element $n_0 \in \mathbb{Z}$ satisfying that $P(n_0)$ is true: namely, it is the integer $n_0 = 3$. Put another way, the following quantified statement involving the uniqueness quantifier is true.

$$\exists! n \in \mathbb{Z},\, P(n): \text{ There exists a unique integer } n \text{ such that } 3n - 4 = 9.$$

Example 2.7.14. Consider the following statement about a real number x.

$$P(x): \text{ The real number } x \text{ satisfies that } x - 5 + \frac{25}{x+5} = \frac{4x+5}{x+5}.$$

By solving the rational equation that defines $P(x)$, we find that $P(x)$ is true if and only if $x = 1$.

$$\frac{(x-5)(x+5)+25}{x+5} = \frac{4x+5}{x+5}$$

$$(x-5)(x+5)+25 = 4x+5$$

$$x^2 - 25 + 25 = 4x + 5$$

$$x^2 - 4x - 5 = 0$$

$$(x-1)(x+5) = 0$$

Considering that $x + 5$ cannot equal 0, the Zero Product Property yields that $x - 1 = 0$ so that $x = 1$. Put another way, the following statement involving the uniqueness quantifier is true.

$$\exists! x \in \mathbb{R},\ P(x): \text{ There exists a unique real number } x \text{ such that } x - 5 + \frac{25}{x+5} = \frac{4x+5}{x+5}.$$

2.8 Direct Proof

Our primary focus for the remainder of this chapter will be using our solid foundation in the calculus of logic to inform and develop our proof-writing skills. We remark that the primary focus of much of mathematics lies in proving statements of the form "if P, then Q" for some statements (or open sentences) P and Q. Consequently, our attentions will be by-and-large fixed on conditional statements of the form $P \implies Q$. Considering the truth table (Table 2.7) for the implication, if either the statement Q is true or the statement P is false, then the conditional statement $P \implies Q$ is true. Proofs that are carried out by showing that Q is true are called **trivial proofs**. Conversely, proofs that rely on exhibiting that P is false are called **vacuous proofs**. We begin our discussion of direct proofs with this low-hanging fruit, as demonstrated in the following examples.

Example 2.8.1. Prove that if n is an even integer, then $n^2 + 4 \geq 3$.

Solution. Consider the following statements involving an integer n.

$$P(n): \text{ The integer } n \text{ is even.}$$
$$Q(n): \text{ The integer } n \text{ satisfies that } n^2 + 4 \geq 3.$$

We seek to prove that $P(n) \implies Q(n)$ is a true statement. Considering that $n^2 \geq 0$ for any real number (and hence any integer) n, it follows that $n^2 + 4 \geq 4$. Consequently, the statement $Q(n)$ is true for all integers n, hence the conditional statement $P(n) \implies Q(n)$ is trivially true. ◇

Our above work is merely a suggestion of a proof of the statement in Example 2.8.1. Below, we provide an example of what an actual proof of this statement might look like. Crucially, observe that in the following proof, there is no need to provide any symbols for the statements.

Proof. (Example 2.8.1) Considering that $n^2 \geq 0$ for any real number n, it follows that $n^2 + 4 \geq 4$. Consequently, we have that $n^2 + 4 \geq 3$ for every integer n, so the claim holds trivially. □

We point out at this juncture two important features of a mathematical proof. First, it is vitally important for the writer to indicate the beginning of a proof with an italicized "Proof" and a period. Equally as important is the ending of a proof. We will use in this course an empty box □ to signify the conclusion of a proof; however, the reader may alternatively use the acronym "QED" (Latin for "quod erat demonstrandum" or "what was to be shown") depending upon their preference.

Example 2.8.2. Prove that if a real number x satisfies that $x^2 - 2 = 0$, then 7 is an odd integer.

Solution. Like the previous example, the hypothesis that x is a real number satisfying that $x^2 - 2 = 0$ has no bearing on the truth value of the conclusion that 7 is an odd integer: indeed, 7 is an odd integer, so regardless of what hypotheses we make, the if-then statement remains true. ◇

Proof. (Example 2.8.2) Considering that 7 is an odd integer, the statement is trivially true. □

Example 2.8.3. Prove that if the Riemann Hypothesis holds, then $\frac{d}{dx}e^x = e^x$.

Proof. By elementary calculus, it holds that $\frac{d}{dx}e^x = e^x$, hence the statement is trivially true. □

Example 2.8.4. Prove that if -1 is an even integer, then the Riemann Hypothesis holds.

Solution. We are now in the opposite case of a trivial proof: indeed, the hypotheses of the statement are false because -1 is not an even integer, hence the statement is true vacuously. ◇

Proof. (Example 2.8.4) Considering that -1 is an odd integer, the statement is vacuously true. □

Example 2.8.5. Prove that if there exist a pair of real numbers x and y such that $x^2 + y^2 = -4$, then there are only finitely many prime integers.

Proof. Given any real number x, we have that $x^2 \geq 0$. Consequently, we find that $x^2 + y^2 \geq 0$ for all real numbers x and y. Bearing this in mind, it follows that the statement is vacuously true. □

Example 2.8.6. Prove that if $\{(x, y) \mid x, y \in \mathbb{R} \text{ and } y^2 = x\}$ is a function, then $\frac{1}{0} = 1$.

Proof. Observe that if $x = 1$, then the real numbers $y = 1$ and $y = -1$ both satisfy that $y^2 = x$. Consequently, the ordered pairs $(1, -1)$ and $(1, 1)$ both belong to $\{(x, y) \mid x, y \in \mathbb{R} \text{ and } y^2 = x\}$, hence this set is not a function. We conclude that the statement is vacuously true. □

Often, it will not be the case that we will encounter a statement that can be proved by a trivial or vacuous proof; rather, we will typically suppose that the hypotheses of the statement are true, and we will subsequently need to perform some sort of algebraic analysis or manipulation in order to rigorously justify that the conclusion of the statement holds. We refer to this process as a **direct proof**. Explicitly, a direct proof of a conditional statement $P \implies Q$ usually begins with the phrase, "Suppose that P is true" and ends with the phrase, "We conclude that Q is true." Between these two points, the writer is left to fill in the details — how ever complicated they might be.

Crucially, the validity of a direct proof relies on the law of inference called **modus ponens** that asserts that the conditional statement $[(P \implies Q) \wedge P] \implies Q$ is a tautology. Eliminating the

trivial or vacuous cases, in order to establish the verity of a conditional statement $P \implies Q$, we need only assume that P is true and deduce from this that $P \implies Q$ is true (because if P is false, then $P \implies Q$ is true vacuously). Let us construct a truth table to verify the law of modus ponens.

P	Q	$P \implies Q$	$(P \implies Q) \wedge P$	$[(P \implies Q) \wedge P] \implies Q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

Table 2.18: the truth table for modus ponens $[(P \implies Q) \wedge P] \implies Q$

We conclude this section with several examples of direct proofs that require a bit more work than trivial or vacuous proofs. Be sure to note the definitions of an even integer versus an odd integer. Explicitly, an integer n is **even** if and only if there exists an integer k such that $n = 2k$. Conversely, an integer n is **odd** if and only if there exists an integer ℓ such that $n = 2\ell + 1$.

Example 2.8.7. Prove that if n is an even integer, then $4n + 7$ is an odd integer.

Proof. By definition, if n is an even integer, then there exists an integer k such that $n = 2k$. Consequently, we have that $4n + 7 = 4(2k) + 7 = 8k + 7 = 8k + 6 + 1 = 2(4k + 3) + 1$. Considering that $4k + 3$ is also an integer, it follows that $4n + 7$ is an odd integer, as desired. □

Example 2.8.8. Prove that if n is an odd integer, then $3n - 1$ is an even integer.

Proof. By definition, if n is an odd integer, then there exists an integer k such that $n = 2k + 1$. Consequently, we have that $3n - 1 = 3(2k + 1) - 1 = 6k + 2 = 2(3k + 1)$. Considering that $3k + 1$ is also an integer, it follows that $3n - 1$ is an even integer, as desired. □

Example 2.8.9. Prove that if n is an even integer, then $3n^2 + 5n - 3$ is an odd integer.

Proof. By definition, if n is an even integer, then $n = 2k$ for some integer k. Consequently, we have

$$3n^2 + 5n - 3 = 3(2k)^2 + 5(2k) - 3 = 12k^2 + 10k - 3 = 12k^2 + 10k - 4 + 1 = 2(6k^2 + 5k - 2) + 1.$$

Considering that $6k^2 + 5k - 2$ is an integer, it follows that $3n^2 + 5n - 3$ is an odd integer. □

Example 2.8.10. Prove that if a, b, c are integers, then $ab + ac + bc$ is even if a and b are even.

Proof. We will assume that a, b, and c are integers such that a and b are even. By definition, there exist integers k and ℓ such that $a = 2k$ and $b = 2\ell$. Consequently, we have that

$$ab + ac + bc = (2k)(2\ell) + (2k)c + (2\ell)c = 4k\ell + 2(ck) + 2(c\ell) = 2(ck + c\ell + k\ell).$$

Considering that $ck + c\ell + k\ell$ is an integer, it follows that $ab + ac + bc$ is an even integer. □

2.9 Proof by Contrapositive

Let P and Q be any pair of statements. Recall from Section 2.6 that the **contrapositive** of the conditional statement $P \implies Q$ is the conditional statement $\neg Q \implies \neg P$. By the result of Table 2.15 and Proposition 2.6.2, any conditional statement is logically equivalent to its contrapositive. Consequently, the **proof by contrapositive** is a proof technique that exploits this logical equivalence. Explicitly, a proof by contrapositive is used to establish the verity of a conditional statement $P \implies Q$ by instead demonstrating the truth of its contrapositive statement $\neg Q \implies \neg P$ and using the logical equivalence of the two statements to conclude the truth of the original implication $P \implies Q$. Bearing this in mind, a typical proof by contrapositive will begin something along the lines of "Suppose that $\neg Q$ is true" and end with the phrase, "We conclude that $\neg P$ is true."

Before we proceed to illustrate the technique of proof by contrapositive, we turn our attention to a law of inference called **modus tollens** that is closely related to the law of modus ponens and asserts that the conditional statement $[(P \implies Q) \wedge \neg Q] \implies \neg P$; its truth table is as follows.

P	Q	$\neg P$	$\neg Q$	$P \implies Q$	$(P \implies Q) \wedge \neg Q$	$[(P \implies Q) \wedge \neg Q] \implies \neg P$
T	T	F	F	T	F	T
T	F	F	T	F	F	T
F	T	T	F	T	F	T
F	F	T	T	T	T	T

Table 2.19: the truth table for modus tollens $[(P \implies Q) \wedge \neg Q] \implies \neg P$

Proof by contrapositive is a powerful technique that is most useful when either the verity of Q is difficult to deduce from the verity of P or $\neg Q$ is a stronger hypothesis than P itself. We illustrate the importance and usefulness of the proof by contrapositive in the following examples. Be sure to make note of where a direct proof might falter or what difficulties arise from weak assumptions.

Example 2.9.1. Prove that the integer n is even if and only if the integer n^2 is even.

Solution. Consider the following statements involving an integer n.

$$P(n): \text{ The integer } n \text{ is even.}$$
$$Q(n): \text{ The integer } n^2 \text{ is even.}$$

We seek to prove that the biconditional statement $P(n) \iff Q(n)$ is true. Consequently, we must establish that both the implication $P(n) \implies Q(n)$ and its converse $Q(n) \implies P(n)$ are true statements. One direction is fairly straightforward: if the integer n is even, then there exists an integer k such that $n = 2k$. By squaring both sides of this equation, we conclude that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$ is even because $2k^2$ is an integer. Conversely, if we assume that n^2 is an even integer, then there exists an integer k such that $n^2 = 2k$. Unfortunately, this assumption does not buy us much in the way of deductive power: it is unclear to the author (and likely to the reader) at this point why the equation $n^2 = 2k$ entails that n must be even. (Later, we will learn about division by prime numbers, but for now, we make no assumption that the reader is familiar with this technique.) Consequently, the hypothesis of $Q(n)$ is relatively "weak."

We may therefore seek to prove the conditional statement $Q(n) \implies P(n)$ by contrapositive We will see that we fare immediately better with this proof technique because the assumption $\neg P(n)$ that n is an odd integer is "stronger" than the assumption that n^2 is an even integer: indeed, if n is an odd integer, then $n = 2k + 1$ for some integer k. By squaring both sides of this equation, we find that $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Considering that $2k^2 + 2k$ is an integer, we conclude that n^2 is an odd integer; thus, our proof by contrapositive is complete. ◇

Proof. (Example 2.9.1) We will assume first that n is an even integer. By definition of an even integer, there exists an integer k such that $n = 2k$. By squaring both sides of this equation, we find that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Considering that $2k^2$ is an integer, it follows that n^2 is even.

Conversely, we will prove the converse by contrapositive. We must assume to this end that n is an odd integer. By definition of an odd integer, there exists an integer k such that $n = 2k + 1$. By squaring both sides of this equation, we find that $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Considering that $2k^2 + 2k$ is an integer, it follows that n^2 is an odd integer, as desired. □

Example 2.9.2. Prove that if n is an integer and $7n + 6$ is even, then the integer n is even.

Solution. We might first attempt a direct proof. Observe that if $7n+6$ is even, then $7n+6 = 2k$ for some integer k. By subtracting 6 from both sides, we find that $7n = 2k-6 = 2(k-3)$; however, it is here that things become unclear without a solid understanding of how prime numbers behave with respect to divisibility. Consequently, a direct proof is unsatisfactory; on the other hand, we might fare better with a proof by contrapositive. Observe that if n is odd, then there exists an integer k such that $n = 2k + 1$ and $7n + 6 = 7(2k + 1) + 6 = 14k + 13 = 14k + 12 + 1 = 2(7k + 6) + 1$. We conclude therefore that if n is odd, then $7n + 6$ is odd, hence the contrapositive is true. ◇

Proof. (Example 2.9.2) We will prove the contrapositive of the statement. We must assume to this end that n is an odd integer. By definition of an odd integer, there exists an integer k such that $n = 2k + 1$. Observe that $7n + 6 = 7(2k + 1) + 6 = 14k + 13 = 14k + 12 + 1 = 2(7k + 6) + 1$. Considering that $7k + 6$ is an integer, it follows that $7n + 6$ is an odd integer, as desired. □

Example 2.9.3. Prove that if n is an integer and $7n - 3$ is odd, then the integer $11n + 6$ is even.

Solution. Let us attempt a direct proof. We will assume along these lines that $7n - 3 = 2k + 1$ for some integer k. By adding $4n + 9$ to both sides of this equation, we find that

$$11n + 6 = (2k + 1) + (4n + 9) = 2k + 4n + 10 = 2(k + 2n + 5)$$

so that $11n+6$ is an even integer because $k+2n+5$ is an integer. But perhaps it seems miraculous to the reader that we were able to add $4n+9$ to both sides of the equation to obtain a direct proof. Bearing this in mind, we might seek a proof by contrapositive; this would entail that $11n+6 = 2k+1$ for some integer k so that $11n = 2k - 5$. We are at this point stuck because it is not clear how to extract any meaning from this equation. Our intuition might suggest that if $7n - 3$ is odd, then n must be even: indeed, an odd integer times an odd integer is an odd integer, and the difference of two odd integers is an odd integer, so n cannot (ostensibly) be odd. We are therefore brought to the potential midpoint in the present problem to prove that if $7n - 3$ is odd, then n is even. ◇

Often, the proof of an assertion could benefit from (or even more requires) an ostensibly more powerful observation. Conventionally, such a helping proposition is referred to as a **lemma**. Let us state and prove a lemma that will make the proof of the previous example follow more efficiently.

Lemma 2.9.4. *Let n be an integer. If $7n-3$ is an odd integer, then n is an even integer.*

Solution. We might first attempt a direct proof: indeed, suppose that $7n-3=2k+1$ for some integer k. We have that $7n=2k+4=2(k+2)$. But again, without further knowledge of divisibility of prime numbers, this equation is rather useless; we will therefore attempt a proof by contrapositive for this lemma. Observe that if n is odd, then there exists an integer k such that $n=2k+1$. Consequently, we have that $7n-3=7(2k+1)-3=14k+4=2(7k+2)$ is even, as desired. ◇

Proof. (Lemma 2.9.4) We will prove the contrapositive of the statement of the lemma. We must assume to this end that n is an odd integer. By definition of an odd integer, there exists an integer k such that $n=2k+1$. Observe that $7n-3=7(2k+1)-3=14k+4=2(7k+2)$. Considering that $7k+2$ is an integer, it follows that $7n+6$ is an even integer, as desired. □

Proof. (Example 2.9.3) By Lemma 2.9.4, if n is an integer and $7n-3$ is odd, then n is even. Consequently, there exists an integer k such that $n=2k$. Even more, we have that

$$11n+6=11(2k)+6=22k+6=2(11k+3).$$

Considering that $11k+3$ is an integer, we conclude that $11n+6$ is an even integer. □

Example 2.9.5. Prove that if n is any integer, then $2n^2+n$ is odd if and only if $\cos\left(\frac{n\pi}{2}\right)=0$.

Solution. Glancing at this proposition, it might seem quite unwieldy — after all, we are comparing the parity of an integer $2n^2+n$ with the roots of the cosine function — but if one takes a moment to recognize the values this cosine sequences takes, the proof strategy becomes clear: indeed, computing $\cos\left(\frac{n\pi}{2}\right)=0$ for some integers n, the reader will have a much better handle of the situation.

$$\cos(-2\pi)=1 \qquad \cos\left(\frac{-\pi}{2}\right)=0 \qquad \cos(\pi)=-1$$

$$\cos\left(\frac{-3\pi}{2}\right)=0 \qquad \cos(0)=1 \qquad \cos\left(\frac{3\pi}{2}\right)=0$$

$$\cos(-\pi)=-1 \qquad \cos\left(\frac{\pi}{2}\right)=0 \qquad \cos(2\pi)=1$$

Consequently, we deduce that $\cos\left(\frac{n\pi}{2}\right)=0$ if and only if n is odd. We are lead to the following. ◇

Lemma 2.9.6. *Let n be an integer. We have that $\cos\left(\frac{n\pi}{2}\right)=0$ if and only if n is odd.*

Proof. By elementary trigonometry, we have that $\cos\left(\frac{n\pi}{2}\right)=0$ if and only if $\frac{n\pi}{2}=\frac{(2k+1)\pi}{2}$ for some integer k if and only if $n=2k+1$ for some integer k if and only if n is an odd integer. □

Proof. (Example 2.9.5) By Lemma 2.9.6, it suffices to prove that $2n^2 + n$ is odd if and only if n is odd. We will assume first that n is an odd integer. By definition of an odd integer, there exists an integer k such that $n = 2k + 1$. Consequently, we have that

$$2n^2 + n = 2(2k + 1)^2 + (2k + 1) = 2(4k^2 + 4k + 1) + (2k + 1) = 2(4k^2 + 5k + 1) + 1.$$

Considering that $4k^2 + 5k + 1$ is an integer, it follows that $2n^2 + n$ is odd.

Conversely, we will prove the contrapositive of the converse. We must assume to this end that n is an even integer. By definition of an even integer, we have that $n = 2k$ for some integer k. Consequently, we find that $2n^2 + n = 2(2k)^2 + (2k) = 8k^2 + 2k = 2(4k^2 + k)$. Considering that $4k^2 + k$ is an integer, it follows that $2n^2 + n$ is an even integer, as desired. □

Example 2.9.7. Prove that if x and y are real numbers such that $x^3 + xy^2 \leq y^3 + x^2y$, then $x \leq y$.

Proof. We will prove the contrapositive statement. We must assume to this end that x and y are real numbers such that $x > y$. By multiplying this inequality by the non-negative real number y^2, we find that $xy^2 \geq y^3$. Likewise, by multiplying this inequality by the non-negative real number x^2, we find that $x^3 \geq x^2y$. By adding these two inequalities, we conclude that $x^3 + xy^2 \geq y^3 + x^2y$. Considering that $x > y$, one of the real numbers x or y must be nonzero, hence one of the inequalities $xy^2 \geq y^3$ or $x^3 \geq x^2y$ must be strict. Consequently, we conclude that $x^3 + xy^2 > y^3 + x^2y$, as desired. □

2.10 Proof by Cases

Let $P(x)$ be an open sentence involving a variable x (or possibly several variables) whose domain is some nonempty set S. **Proof by cases** is an exhaustive proof technique that exploits some finiteness property of the nonempty S. Potential reasons to attempt a proof by cases include that

(a.) S is finite (in which case it might be possible to prove $P(x)$ for each element $x \in S$) or

(b.) S admits a finite partition $S = S_1 \cup S_2 \cup \cdots \cup S_n$ (in which case it might be possible to prove the statement $P(x)$ for each element $x \in S_i$ for each integer $1 \leq i \leq n$).

Concretely, we will illustrate the proof by cases by completing the following typical examples.

Example 2.10.1. Consider the finite set $S = \left\{1, \sqrt{2}, 2\sqrt{2}\right\}$. Prove that for every element $x \in S$, there exists an element $y \in S$ such that $x - y \leq 0$ and $x^2 + y^2$ is a perfect square.

Proof. We may consider the following three cases.

1.) If $x = 1$, then observe that for $y = 2\sqrt{2}$, we have that $x < y$ so that $x - y \leq 0$ and

$$x^2 + y^2 = (1)^2 + \left(2\sqrt{2}\right)^2 = 1 + 8 = 9 = 3^2.$$

2.) If $x = \sqrt{2}$, then observe that for $y = \sqrt{2}$, we have that $x = y$ so that $x - y \leq 0$ and

$$x^2 + y^2 = \left(\sqrt{2}\right)^2 + \left(2\sqrt{2}\right)^2 = 2 + 2 = 4 = 2^2.$$

3.) If $x = 2\sqrt{2}$, then observe that for $y = 2\sqrt{2}$, we have that $x = y$ so that $x - y \leq 0$ and

$$x^2 + y^2 = \left(2\sqrt{2}\right)^2 + \left(2\sqrt{2}\right)^2 = 8 + 8 = 16 = 4^2.$$

We have exhausted all possibilities for an element $x \in S$, hence our proof is complete. □

Example 2.10.2. Consider the finite subset $S = \{2, 3, 4\}$. Prove that for every element $x \in S$ such that $x^2(x-1)^2/4$ is even, we have that $x^2(x+1)^2/4$ is even.

Proof. We may consider the following four cases.

1.) If $x = 2$, then $x^2(x-1)^2/4 = 2^2(2-1)^2/4 = 1$ is not even, so we proceed to the next case.

2.) If $x = 3$, then $x^2(x-1)^2/4 = 3^2(3-1)^2/4 = 9$ is not even, so we proceed to the next case.

3.) If $x = 4$, then each of $x^2(x-1)^2/4$ and $x^2(x+1)^2/4$ have a factor of 4, so they are even.

We have exhausted all possibilities for an element $x \in S$, hence our proof is complete. □

Essentially, a proof by cases for a finite set is simply a matter of verifying the statement in question for each of the possible elements of the set. We turn our attention next to proofs involving integers and other sets. Recall that an integer is either even or odd; the quality that an integer is even or odd is called the **parity** of the integer. Consequently, if we encounter a statement involving an integer, it is possible to construct a proof by cases by checking the case that n is even and the case that n is odd separately. We illustrate this idea in the following three examples.

Example 2.10.3. Prove that for every integer n, the integer $n^2 + 3n - 4$ is even.

Proof. We may consider the following two cases.

1.) By definition, if n is even, then there exists an integer k such that $n = 2k$. Consequently, we have that $n^2 + 3n - 4 = (2k)^2 + 3(2k) - 4 = 4k^2 + 6k - 4 = 2(2k^2 + 3k - 2)$. Considering that $2k^2 + 3k - 2$ is an integer, we conclude that $n^2 + 3n - 4$ is an even integer.

2.) By definition, if n is odd, then there exists an integer k such that $n = 2k+1$. Consequently, we have that $n^2 + 3n - 4 = (2k+1)^2 + 3(2k+1) - 4 = (4k^2 + 4k + 1) + (6k + 3) - 4 = 2(2k^2 + 5k)$. Considering that $2k^2 + 10k$ is an integer, we conclude that $n^2 + 3n - 4$ is an even integer.

We have exhausted all possibilities for the parity of the integer n, hence our proof is complete. □

Example 2.10.4. Prove that any integers x and y have the same parity if and only if $x + y$ is even.

Proof. We will first prove the statement that if x and y are any integers of the same parity, then $x + y$ is even. Consider toward this end the following two cases.

1.) By definition, if the integers x and y are both even, then there exist integers k and ℓ such that $x = 2k$ and $y = 2\ell$. Consequently, we have that $x + y = 2k + 2\ell = 2(k + \ell)$. Considering that $k + \ell$ is an integer, we conclude that $x + y$ is even.

2.) By definition, if the integers x and y are both odd, then there exist integers k and ℓ such that $x = 2k+1$ and $y = 2\ell+1$. Consequently, we have that $x+y = (2k+1)+(2\ell+1) = 2(k+\ell+1)$. Considering that $k+\ell+1$ is an integer, we conclude that $x+y$ is even.

We have exhausted all possibilities for the parity of the integers x and y, hence the statement holds.

Conversely, we will prove the contrapositive of the statement that if $x+y$ is even, then the integers x and y have the same parity. Explicitly, we will demonstrate that if x and y have opposite parity, then the integer $x+y$ is odd. We may assume **without loss of generality** that x is even and y is odd. Consequently, there exist integers k and ℓ such that $x = 2k$ and $y = 2\ell+1$. Observe that $x+y = 2k+(2\ell+1) = 2(k+\ell)+1$. Because $k+\ell$ is an integer, the integer $x+y$ is odd. □

Remark 2.10.5. We reflect here on two important features of the proof of Example 2.10.4.

1.) First, it is important to note that the biconditional ("if and only if") statement was proved by using a proof by cases for one direction of the biconditional (the "only if" direction) and using a proof by contrapositive for the other direction (the "if" direction). Often, we will be required to use multiple proof techniques in tandem to write a satisfactory proof of a proposition.

2.) We have introduced in the body of the proof of Example 2.10.4 an important phrase in the trade of mathematical writing: "without loss of generality." Essentially, what this means is that the author is asserting to the reader that there is no need to distinguish between the two variables x and y in the above proof: indeed, it does not matter if x is even and y is odd or vice-versa; the result would work the same if the names (or roles) of x and y were swapped. One way to think about the phrase "without loss of generality" is that it can be useful to save the author and the reader precious time if the same (or at least a similar) proof could be used for the other cases that would be necessary to consider in the proof by cases; therefore, one might instead use the phrase, "A similar proof can be used to establish the result."

Example 2.10.6. Prove that $3x+5y+7z$ is odd if exactly two of the integers x, y, z are even.

Proof. Observe that $3x+5y+7z = 2(x+2y+3z)+x+y+z$. Consequently, it suffices to prove that $x+y+z$ is odd by Example 2.10.4: indeed, if $x+y+z$ were even, then $3x+5y+7z$ would be even. Consequently, we may assume without loss of generality that x and y are even and z is odd. Explicitly, suppose that there exist integers k, ℓ, and m such that $x = 2k$, $y = 2\ell$, and $z = 2m+1$. We have that $x+y+z = 2k+2\ell+(2m+1) = 2(k+\ell+m)+1$, hence $x+y+z$ is odd. □

Remark 2.10.7. Observe that the proof of Example 2.10.6 is quite clever and drastically reduces the amount of work required to prove the statement. We immediately used the result of Example 2.10.4 to reduce the problem at hand to simply demonstrating that $x+y+z$ is odd whenever exactly two of the integers x, y, and z are even; then, because each of the integers x, y, and z appeared as terms of the sum, there was no need to distinguish between them, so we could appeal to the phrase "without loss of generality" to reduce a proof potentially involving three cases to just one case. Compare this with the amount required to write a proof for Example 2.10.4 with three cases.

Last, a proof by cases can sometimes be used to handle statements involving the union of sets.

Example 2.10.8. Prove that if A, B, and C are sets with $x \in A \cup B$, then $x \in A \cup C$ or $x \in B \cup C$.

Proof. By definition of the set union, we have that $x \in A \cup B$ if and only if $x \in A$ or $x \in B$. Consequently, we may consider the following two cases.

1.) If $x \in A$, then $x \in A \cup C$ by definition of the set union.

2.) If $x \in B$, then $x \in B \cup C$ by definition of the set union.

Either way, we conclude that $x \in A \cup C$ or $x \in B \cup C$, as desired. □

2.11 Counterexamples

Before we are able to prove a statement, we must first deduce that it is true. Often, this amounts to computing several examples to convince ourselves that the statement is valid. Best case scenario, either this practice reveals the nature of a potential proof, or a **counterexample** is revealed to us. By counterexample, we mean an explicit instance for which the statement in question is false.

Example 2.11.1. Consider the following statement.

$$P(n): \text{ If } n \text{ is an integer, then the integer } 5n+4 \text{ is even.}$$

Considering that $5(1)+4 = 9$ is an odd integer, the statement $P(1)$ is false. Consequently, the integer $n_0 = 1$ provides a counterexample and illustrates that $P(n)$ is not a true statement.

Example 2.11.2. Consider the following statement.

$$P(x): \text{ If } x \text{ is a real number, then } x - e^x > 0.$$

Considering that $0 - e^0 = 0 - 1 = -1 < 0$, the statement $P(0)$ is false. Consequently, the real number $x_0 = 0$ provides a counterexample and illustrates that $P(x)$ is not a true statement.

Example 2.11.3. Consider the following statement.

$$P(x): \text{ If } x \text{ is a real number, then } \cot^2(x) + 1 = \csc^2(x).$$

Considering that neither $\cot(0)$ nor $\csc(0)$ are defined, the statement $P(0)$ is false. Consequently, the real number $x_0 = 0$ provides a counterexample and illustrates that $P(x)$ is not a true statement.

Counterexamples can be quite difficult to determine in some cases; in fact, it is an active area of mathematical research to find counterexamples to certain statements of particular interest. Explicitly, the desire for a counterexample is illuminated by the following observation. Consider an open sentence $P(x)$ in a variable x with domain S. Recall that the quantified statement $\forall x \in S,\ P(x)$ is true if and only if $P(x)$ is true for all elements $x \in S$. By Theorem 2.7.12, if we wish to **disprove** the statement $\forall x \in S,\ P(x)$ (or show that this statement is false), it suffices to exhibit an element $x_0 \in S$ such that $P(x_0)$ is false. By name, this element x_0 is a counterexample to $\forall x \in S,\ P(x)$.

Example 2.11.4. Disprove the following statement.

$$P(x): \text{ If } x \text{ is a real number, then } \frac{x^3+1}{x^3-1} = \frac{x^2-x+1}{x^2+x+1}.$$

Solution. Observe that if $x = 1$, then $x^3 - 1 = 0$, hence the fraction in the statement of $P(x)$ is undefined. Consequently, $x = 1$ is a counterexample to the statement $P(x)$. $\diamond$

Example 2.11.5. Disprove the following statement.

$$P(x, y): \text{ If } x \text{ and } y \text{ are real numbers, then } x^2 - 4xy + y^2 > 0.$$

Solution. Observe that if $x = 1$ and $y = 1$, then $x^2 - 4xy + y^2 = 1 - 4 + 1 = -2 < 0$. Consequently, the ordered pair $(x, y) = (1, 1)$ is a counterexample to the statement $P(x, y)$. $\diamond$

Example 2.11.6. Disprove the following statement.

$$P(x, y, z): \text{ If } x, y, \text{ and } z \text{ are positive real numbers, then } (x^y)(x^z) = x^{yz}.$$

Solution. Observe that if $x = 2$, $y = 1$, and $z = 3$, then $(x^y)(x^z) = (2^1)(2^3) = 16$ and $x^{yz} = 8$, hence the ordered triple $(x, y, z) = (2, 1, 3)$ is a counterexample to the statement $P(x, y, z)$. $\diamond$

Be sure to make note of the form we use when solving a problem that asks us to disprove something: we begin with an italicized "Solution" and a period; we exhibit an explicit counterexample to the statement; and we conclude with an empty diamond $\diamond$ to signify the conclusion of our solution.

2.12 Proof by Contradiction

Last but certainly not least, **proof by contradiction** (or **reductio ad absurdum**) rounds out the tools that we will most often use in mathematical proofs. Essentially, the proof by contradiction constitutes a valid proof technique by a combination of the Law of the Excluded Middle, the Law of Non-Contradiction, and Table 2.14. We bear out the details in two cases of particular interest. We will first assume toward this end that P is a statement that we wish to prove is true.

1.) By the Law of the Excluded Middle, either P is true or P is false.

2.) By the Law of Non-Contradiction, if P is not false, then it must be true.

3.) Consequently, it suffices to prove that P cannot be false. We assume toward this end that P is in fact false, i.e., we assume that $\neg P$ is true.

4.) By some properties of $\neg P$, it might be possible to derive a contradiction C, i.e., a statement C that is false with respect to all possible truth inputs. Crucially, the contradiction C could reveal itself as a direct consequence of the assumption $\neg P$, or it might be possible to derive a contradiction C from some other known facts (e.g., definitions, propositions, and theorems).

5.) We have illustrated thus that $(\neg P) \implies C$ is true. But C is false, so $\neg P$ must be false; therefore, our initial assumption that P is false is untenable, so P must be true.

Often, a proof by contradiction is desirable to prove a conditional statement $P \implies Q$. We outline how a proof by contradiction for such a statement could be carried out and why it is valid.

1.) By the Law of the Excluded Middle, either $P \implies Q$ is true or $P \implies Q$ is false.

2.) By the Law of Non-Contradiction, if $P \implies Q$ is not false, then it must be true.

3.) Consequently, it suffices to prove that $P \implies Q$ cannot be false. By Table 2.7, we must show that if Q is false, then P is false. We assume toward this end that Q is false and P is true.

4.) Like in the other case of proof by contradiction, it might be possible to derive from some properties of $\neg Q$ a contradiction C; this would entail that $\neg Q \implies C$ is true.

5.) Observe that if C is false and $\neg Q \implies C$ is true, then $\neg Q$ must be false; therefore, our assumption that Q is false is untenable, so Q must be true.

We should always take care to mention in the first line of our proof our intentions to use a proof by contradiction (if that is indeed our plan). Best practices dictate that this can be achieved by indicating something to the effect of "suppose on the contrary that P is true and Q is false" or "we will assume toward a contradiction that P is true and Q is false." Even more, we should take care to point out exactly what contradiction we have derived in our proof by contradiction.

Example 2.12.1. Prove that there is no smallest integer.

Proof. Suppose on the contrary that there n is the smallest integer. Observe that $n - 1$ is an integer. By adding n to both sides of the inequality $-1 < 0$, we find that $n - 1 < n$. But this is a contradiction: if n is the smallest integer, there can be no integer less than n. Our assumption that there exists a smallest integer is untenable, hence we conclude that there is no smallest integer. □

Example 2.12.2. Prove that no integer is both even and odd.

Proof. Suppose on the contrary that n is an even integer and an odd integer. By definition of an even integer, there exists an integer k such that $n = 2k$. By definition of an odd integer, there exists an integer ℓ such that $n = 2\ell + 1$. Considering that $n = n$, it follows that $2k = 2\ell + 1$ so that $1 = 2k - 2\ell = 2(k - \ell)$. By dividing both sides of this equation by 2, we find that $k - \ell = \frac{1}{2}$. But this is a contradiction: the difference of two integers is an integer, but the rational number $\frac{1}{2}$ is not an integer. Our assumption that there exists an integer that is both even and odd is untenable, hence we conclude that no integer is both even and odd. □

Example 2.12.3. Prove that no even integer is the sum of three odd integers.

Proof. Suppose on the contrary that n is an even integer that is the sum of three odd integers a, b, and c. By definition of an odd integer, we have that $a = 2k + 1$, $b = 2\ell + 1$, and $c = 2m + 1$ for some integers k, ℓ, and m. Considering that $n = a + b + c$, it follows that

$$n = (2k + 1) + (2\ell + 1) + (2m + 1) = 2(k + \ell + m + 1) + 1,$$

hence n is odd. But this is a contradiction: by Example 2.12.2, we have that no integer is both even and odd. Our assumption that there exists an even integer that is the sum of three odd integers is untenable, hence we conclude that no even integer is the sum of three odd integers. □

Example 2.12.4. Prove that if a, b, and c are integers such that $a^2 + b^2 = c^2$, then a or b is even.

Proof. Suppose on the contrary that a and b are both odd integers. By definition of an odd integer, we have that $a = 2k + 1$ and $b = 2\ell + 1$ for some integers k and ℓ. Consequently, we find that

$$c^2 = a^2 + b^2 = (2k+1)^2 + (2\ell+1)^2 = (4k^2 + 4k + 1) + (4\ell^2 + 4\ell + 1) = 2(2k^2 + 2k + 2\ell^2 + 2\ell + 1).$$

Considering that $2k^2 + 2k + 2\ell^2 + 2\ell + 1$ is an integer, we conclude that c^2 is even so that c is even. By definition of an even integer, we have that $c = 2m$ for some integer m so that

$$4m^2 = (2m)^2 = c^2 = 2(2k^2 + 2k + 2\ell^2 + 2\ell + 1).$$

Cancelling one factor of 2 from both sides of this equation yields that

$$2m^2 = 2k^2 + 2k + 2\ell^2 + 2\ell + 1 = 2(k^2 + k + \ell^2 + \ell) + 1.$$

But this is a contradiction: the left-hand side shows an even integer, but the right-hand side shows an odd integer. Our assumption that a and b are odd is untenable, hence a or b is even. □

Example 2.12.5. Prove that if x is even and y is odd, then $x^2 + 2y^2$ is not divisible by 4.

Proof. Suppose on the contrary that x is an even integer and y is an odd integer such that $x^2 + 2y^2$ is divisible by 4. By definition of the parity of an integer, we have that $x = 2k$ and $y = 2\ell + 1$ for some integers k and ℓ. Consequently, we may simplify the expression $x^2 + 2y^2$ to find that

$$x^2 + 2y^2 = (2k)^2 + (2\ell+1)^2 = 4k^2 + 2(4\ell^2 + 4\ell + 1) = 4(k^2 + 2\ell^2 + 2\ell) + 2.$$

By assumption that $x^2 + 2y^2$ is divisible by 4, there exists an integer m such that $x^2 + 2y^2 = 4m$. Combined with our previous displayed equation, this yields that

$$4m = 4(k^2 + 2\ell^2 + 2\ell) + 2,$$

from which we deduce that $2 = 4m - 4(k^2 + 2\ell^2 + 2\ell) = 4(m - k^2 - 2\ell^2 - 2\ell)$. By cancelling a factor of 2 from both sides, we find that $1 = 2(m - k^2 - 2\ell^2 - 2\ell)$. But this is a contradiction: the integer 1 is odd, so it cannot be divisible by 2 by Example 2.12.2. Our assumption that x is an even integer and y is an odd integer such that $x^2 + 2y^2$ is divisible by 4 is untenable, hence we conclude that if x is an even integer and y is an odd integer, then $x^2 + 2y^2$ is not divisible by 4. □

Example 2.12.6. Prove that $\sqrt{2}$ is irrational.

Proof. Suppose on the contrary that $\sqrt{2}$ is rational. By definition of a rational number, there exists integers a and b such that b is nonzero; a and b possess no common factors other than ± 1; and

$$\sqrt{2} = \frac{a}{b}.$$

By squaring both sides of this equation and clearing the denominator, we find that

$$a^2 = 2b^2.$$

Consequently, the integer a^2 is even. Considering that the square of an integer is even if and only if that integer is even, it follows that a is even so that $a = 2k$ for some integer k. By substituting this identity back into our above displayed equation, we find that

$$4k^2 = (2k)^2 = a^2 = 2b^2.$$

Cancelling a factor of 2 from both sides yields that b^2 is an even integer since

$$b^2 = 2k^2.$$

By the same rationale as before, we conclude that b is even so that $b = 2\ell$ for some integer ℓ. But this is a contradiction: we had originally assumed that a and b possess no common factors other than ± 1, but if a and b are both even, then they have a common factor of 2. Our assumption that $\sqrt{2}$ is rational is untenable, hence we conclude that $\sqrt{2}$ is irrational. □

2.13 Existence Proofs

Complementary to counterexamples, proving the existence of certain mathematical objects or structures with desirable properties is also a foremost concern throughout mathematics. We remind the reader at this point that an existence statement is a quantified statement of the form

$$\exists x \in S,\ P(x):\ \text{There exists an element } x \in S \text{ such that } P(x).$$

for some open sentence $P(x)$ in a variable x with domain S. Consequently, in order to determine the verity of an existence statement, it suffices to provide an explicit example of an element $x_0 \in S$ such that $P(x_0)$ is true; if this is possible, then the resulting proof of the attendant existence statement is called a **constructive proof** because the element is often "constructed" or produced by explicitly performing some algebraic manipulation or computation. We provide some examples below.

Example 2.13.1. Prove that there exists an integer whose cube is equal to its square.

Solution. Before we prove this existence statement, it will benefit us to express the statement in symbols. Observe that if n is an integer, then n^3 is its cube and n^2 is its square. Consequently,

$$P(n):\ \text{The integer } n \text{ satisfies that } n^3 = n^2.$$

is the open sentence that n is an integer whose cube is equal to its square. Ultimately, we are trying to prove the following existential statement in the variable n over the domain $\mathbb{Z}$.

$$\exists n \in \mathbb{Z},\ P(n):\ \text{There exists an integer } n \text{ such that } n^3 = n^2.$$

Observe that if $n^3 = n^2$, then $n^3 - n^2 = 0$ so that $n^2(n-1) = 0$. By the Zero Product Property, it follows that $n = 0$ or $n = 1$. Either one of these integers provides an explicit solution to the integer equation $n^3 = n^2$, hence we have the ingredients to write a constructive proof for the statement. ⋄

Proof. Observe that the integer $n = 1$ satisfies that $n^3 = 1^3 = 1 = 1^2 = n^2$, and the claim holds. □

Example 2.13.2. Prove that there exist real numbers x and y such that $(x+y)^2 = x^2 + y^2$.

Solution. Before we determine a proof of the statement, we note that we seek to establish the verity of the following existential statement in the variables x and y over the domain $\mathbb{R}$.

$$\exists x, y \in \mathbb{R},\ P(x,y):\ \text{There exist real numbers } x \text{ and } y \text{ such that } (x+y)^2 = x^2 + y^2.$$

Observe that if $(x+y)^2 = x^2 + y^2$, then $x^2 + 2xy + y^2 = x^2 + y^2$ so that $2xy = 0$. By the Zero Product Property, it follows that $x = 0$ or $y = 0$. Either way, the statement that $(x+y)^2 = x^2 + y^2$ will be true for any value of the variables x and y so long as one of them is zero: indeed, if $y = 0$, then $(x+y)^2 = (x+0)^2 = x^2 = x^2 + 0^2 = x^2 + y^2$. We have the makings of a constructive proof. ◇

Proof. Observe that the real numbers $x = 1$ and $y = 0$ satisfy that

$$(x+y)^2 = (1+0)^2 = 1^2 = 1^2 + 0^2 = x^2 + y^2.$$

Consequently, the statement in question holds. □

Example 2.13.3. Prove that $f(x) = x^5 + x^4 + x^3 + x^2 + x + 1$ has at least one real root.

Solution. By definition of a root of a function, the statement we are tasked to prove is as follows.

$$\exists x \in \mathbb{R},\ P(x):\ \text{There exists a real number } x \text{ such that } f(x) = 0.$$

Observe that $f(-1) = (-1)^5 + (-1)^4 + (-1)^3 + (-1)^2 + (-1) + 1 = -3 + 3 = 0$, hence a direct proof is possible because we have found an explicit example of a real root of $f(x)$. ◇

Proof. Observe that the real numbers $x = -1$ is a root of $f(x)$ since we have that

$$f(-1) = (-1)^5 + (-1)^4 + (-1)^3 + (-1)^2 + (-1) + 1 = -3 + 3 = 0.$$ □

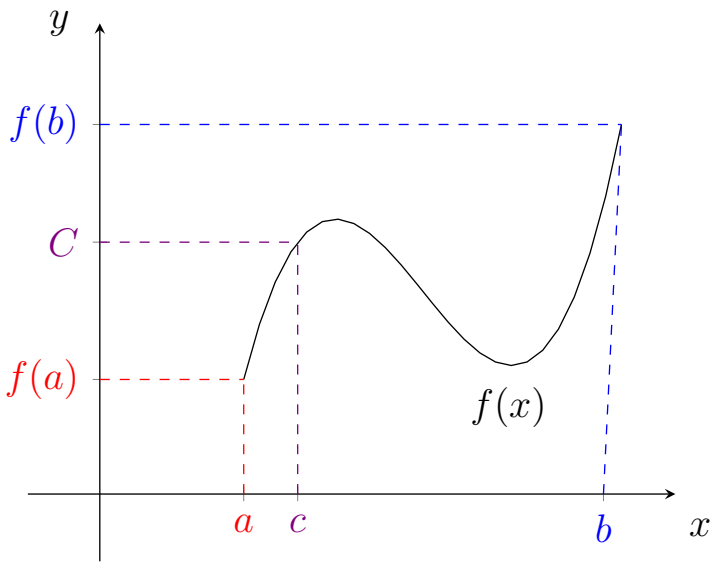
Remark 2.13.4. We make an important note at this point about the serendipitous nature of the existence proof provided in Example 2.13.3. Exactly how did we stumble upon the real number $x = -1$, and why did we suspect that it was a root of the polynomial $f(x) = x^5 + x^4 + x^3 + x^2 + x + 1$? Unfortunately, this was simply a lucky coincidence — the product of years of schema and knowing where to look. One natural starting point in the aforementioned example is simply to begin by plugging in integer values of x near zero. Plugging in $x = 0$ yields that $f(0) = 0$, and plugging in $x = 1$ yields that $f(1) = 6$. We were exceedingly lucky that our next guess of $x = -1$ worked.

Generally, the roots of a real function $f(x)$ are quite difficult to determine. By the Quadratic Formula, the roots of any real function of the form $f(x) = ax^2 + bx + c$ with a nonzero are known; there are also the Cubic Formula and the Quartic Formula, but these are typically not taught, and students are not expected to know them (the author freely admits to not knowing them, either). Beyond that, it is a landmark result of Galois Theory that there is no closed form expression for the roots of a real polynomial of degree at least five. Consequently, there is little hope for deducing the roots of a polynomial of degree five or larger — let alone trying to find the roots of a real function that is not a polynomial (other than certain trigonometric, inverse trigonometric, or logarithmic functions) — for students in this course without specialized knowledge (such as the Newton-Raphson Method or other recursive numerical methods for finding roots of differentiable functions).

Even still, there is a way to prove the existence of roots of continuous functions without ever knowing exactly what those roots are. Before we provide such a proof along these lines, we must first recall the following important fact about continuous functions from Calculus I.

Theorem 2.13.5 (Intermediate Value Theorem)**.** *Every real function $f : \mathbb{R} \to \mathbb{R}$ that is continuous on a closed and bounded interval $[a, b]$ satisfies the property that for every real number C between $f(a)$ and $f(b)$, there exists a real number c such that $a \leq c \leq b$ and $f(c) = C$.*

Essentially, the Intermediate Value Theorem states that every real function $f(x)$ that is continuous on a closed and bounded interval $[a, b]$ achieves every possible y-value between $f(a)$ and $f(b)$ for some x-value between a and b. Graphically, the intuition is that the graph of a continuous function can be drawn without lifting one's pencil, hence as the curve $y = f(x)$ is traced out from the point $x = a$ to the point $x = b$ along the x-axis, every point on the y-axis between $f(a)$ and $f(b)$ must correspond to some point on the x-axis. Consider the picture below for the idea.



Consequently, the idea is that in order to prove the existence of roots of a continuous function $f(x)$, we may find real numbers a and b such that $f(a)$ and $f(b)$ have opposite sign (e.g., $f(a) < 0$ and $f(b) > 0$ or vice-versa); then, because $f(x)$ is a continuous function such that $f(a)$ and $f(b)$ have opposite sign, there must exist a real number c such that $a \leq c \leq b$ and $f(c) = 0$. We refer to such a proof of the existence of the roots of a continuous function as a **non-constructive proof** because we are not explicitly exhibiting the roots of the function; we are simply relying on the Intermediate Value Theorem to conclude that some root must exist. Generally, a non-constructive proof must rely on some known fact, theorem, or definition and might not always be direct.

We conclude this section with several examples of non-constructive proofs.

Example 2.13.6. Prove that $f(x) = x^5 + x^4 + x^3 + x^2 + x + 1$ has at least one real root.

Proof. Observe that the polynomial $f(x)$ is a continuous function. Considering that $f(-2) = -21$ and $f(0) = 1$, by the Intermediate Value Theorem, there exists a real number c such that $-2 < c < 0$ and $f(c) = 0$. By definition, the real number c is a root of the polynomial $f(x)$, as desired. □

Example 2.13.7. Prove that $f(x) = e^x - 3x$ has at least one real root.

Proof. Observe that $f(x)$ is a continuous function since it is the difference of the continuous functions e^x and $3x$. Considering that $f(1) = e - 3 < 0$ and $f(0) = 1 > 0$, by the Intermediate Value Theorem, there exists a real number c such that $0 < c < 1$ and $f(c) = 0$, as desired. □

Example 2.13.8. Prove that $\cos(x) - \sin(x) = \frac{1}{2}$ for some real number x such that $0 \leq x \leq \frac{\pi}{4}$.

Proof. Consider the function $f(x) = \cos(x) - \sin(x)$. Observe that $f(x)$ is continuous because it is a difference of the continuous functions $\cos(x)$ and $\sin(x)$. Considering that

$$f(0) = 1 - 0 = 1 \text{ and } f\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} = 0,$$

by the Intermediate Value Theorem, there exists a real number $0 \leq c \leq \frac{\pi}{4}$ and $f(c) = \frac{1}{2}$. □

Example 2.13.9. Prove that some digit appears infinitely often in the decimal expansion of π.

Solution. Before we proceed to outline a proof strategy, we first note the distinct nature of the statement from the previous three non-constructive examples. We cannot rely on the Intermediate Value Theorem because the statement does not involve a continuous function. Even worse, we are not in a position to verify directly that some digit appears infinitely often in the decimal expansion of π because there is no way to check the infinitely many digits in the decimal expansion of π. Consequently, there is no hope for a constructive proof. We are not proving an implication, so there is no contrapositive. We turn our attention at last to a proof by contradiction. Observe that the negation of the existence statement in question is, "No digit appears infinitely often in the decimal expansion of π," or better yet, "Every digit in the decimal expansion of π appears finitely many times." Considering that π is irrational, this statement cannot be true, so the existence statement we sought to prove must be true by the Law of the Excluded Middle and the Law of Non-Contradiction. Because we never had to verify any digits of π, this is a non-constructive proof. ◇

Proof. On the contrary, suppose that every digit in the decimal expansion of π appears finitely many times. Considering that the only possible digits in the decimal expansion of any real number are the integers $0, 1, 2, \ldots, 9$, it follows that the decimal expansion of π contains at most ten digits. But this is a contradiction: if the decimal expansion of π is finite, then π is a rational number; however, it is well-known that π is irrational. Consequently, our assumption that every digit in the decimal expansion of π appears finitely many times is untenable, hence we conclude as desired that some digit in the decimal expansion of π appears infinitely many times. □

2.14 Chapter 2 Overview

We say that a complete sentence P is a **statement** if it asserts something that can be unambiguously measured as true or false. Examples of statements include "the integer 3 is an odd" and "the integer 17 is larger than the integer 38"; the first statement is true, but the second statement is false. Using logical connectives, we can form new statements from given statements P and Q. Explicitly, the **implication** $P \implies Q$ is the statement that "P implies Q" (or equivalently, "If P, then Q"); the implication is false if and only if P is true and Q is false. Regardless of the verity of the statement Q, if the statement P is false, then the statement $P \implies Q$ is **vacuously** true. We define the

disjunction $P \vee Q$ ("P or Q"), the **conjunction** $P \wedge Q$ ("P and Q"), and the **negation** $\neg P$ ("not P"). Observe that the disjunction $P \vee Q$ is true if and only if P is true or Q is true; the conjunction $P \vee Q$ is true if and only if P is true and Q is true; and the negation $\neg P$ is true if and only if P is false. Given any statement P, the Law of the Excluded Middle states that the disjunction $P \vee \neg P$ is true, and the Law of Non-Contradiction asserts that the conjunction $P \wedge \neg P$ is false.

We use **truth tables** to deduce the verity of a statement $S(P, Q)$ depending upon two statements P and Q. One can construct a truth table for $S(P, Q)$ by writing all possible **truth values** of P in one column; all possible truth values of Q in a subsequent column; and the resultant truth values of the statement $S(P, Q)$ in a third column. Considering that the statements P and Q could themselves depend upon other statements $P_1, \ldots, P_n$, truth tables may become quite large when the attendant statements are complicated. Generally, we need $2^n + 1$ rows and $n + 1$ columns to construct the truth table of a statement $S(P_1, \ldots, P_n)$ depending upon n distinct statements $P_1, \ldots, P_n$.

We say that two statements S_1 and S_2 are **logically equivalent** if and only if they induce the same truth table; in particular, the truth values of S_1 are exactly the same as the truth values of S_2 for all possible truth inputs, hence the verity of the statement S_1 is exactly the same as the verity of the statement S_2. Even more, if the truth values for a statement S are all true, then S is a **tautology**; if the truth values for S are all false, then S is a **contradiction**.

De Morgan's Laws are two rules of inference that relate the conjunction, disjunction, and negation to assert that the statements (a.) $\neg(P \vee Q)$ ("it is not the case that either P or Q") and $\neg P \wedge \neg Q$ ("neither P nor Q") are logically equivalent and (b.) $\neg(P \wedge Q)$ ("it is not the case that P and Q") and $\neg P \vee \neg Q$ ("either it is the case that not P or not Q") are logically equivalent.

Logical quantifiers allow us to symbolically handle statements involving quantities. We use the **universal quantifier** $\forall$ to express that an open sentence $P(x)$ is true "for all" possible values of x in its domain, and we use the **existential quantifier** $\exists$ to express that "there exists" a value of x in the domain of $P(x)$ such that $P(x)$ is true. We say that an element x_0 in the domain of the open sentence $P(x)$ is **unique** if it is the only value in the domain of $P(x)$ such that $P(x_0)$ is true. We use the **uniqueness quantifier** $\exists!$ to express the existence ($\exists$) and uniqueness ($!$) of x_0.

Given any conditional statement $P \implies Q$, we obtain the **contrapositive** $\neg Q \implies \neg P$ by taking the implication of the negations of Q and P, respectively. Observe that the contrapositive $\neg Q \implies \neg P$ is the statement that "not Q implies not P" (or equivalently, "If Q does not hold, then P does not hold"). **Proof by contraposition** is a proof technique that exploits the fact that the contrapositive is logically equivalent to the implication, i.e., the statements $P \implies Q$ and $\neg Q \implies \neg P$ induce the same truth table (see Table 2.15 and the subsequent Proposition 2.6.2).

Proof by contradiction is a proof technique that can be deduced from the Law of the Excluded Middle, the Law of Non-Contradiction, and the logical equivalence of the statements $\neg(P \implies Q)$ and $P \wedge \neg Q$ (see Table 2.14). We carry out a proof by contradiction by assuming that P is true and that Q is false; then, we arrive at a contradiction (i.e., a statement that is false for all possible truth inputs). Contradictions can be derived from any assumption made in the context of the proof, from definitions, or from any known fact. We note that if $\neg P$ can be deduced from $\neg Q$, then a proof by contrapositive may be simpler than a proof by contradiction; on the other hand, if Q can be deduced from P, then a **direct proof** may be simpler than a proof by contradiction.

2.15 Chapter 2 Exercises

Exercise 2.15.1. Consider the following statements.

P : The sun is shining in Kansas City.
Q : Bob rides his bike to work.

Use the letters P and Q and logical connectives such as the biconditional $\iff$, conjunction $\wedge$, disjunction $\vee$, implication $\implies$, and negation $\neg$ to convert each of the following statements into symbols; then, identify all logically equivalent statements, tautologies, and contradictions.

(a.) If the sun is shining in Kansas City, then Bob rides his bike to work.

(b.) Bob rides his bike to work only if the sun is shining in Kansas City.

(c.) Either the sun is not shining in Kansas City or Bob rides his bike to work.

(d.) The sun is shining in Kansas City, and Bob does not ride his bike to work.

(e.) If the sun is not shining in Kansas City, then Bob does not ride his bike to work.

(f.) If Bob does not ride his bike to work, then the sun is not shining in Kansas City.

(g.) Neither the sun is shining in Kansas City nor Bob rides his bike to work.

(h.) Either the sun is not shining in Kansas City or Bob does not ride his bike to work.

(i.) The sun is not shining in Kansas City, and Bob does not ride his bike to work.

(j.) Either Bob rides his bike to work or Bob does not ride his bike to work.

(k.) The sun is shining in Kansas City, and the sun is not shining in Kansas City.

(l.) Bob rides his bike to work if and only if the sun is shining in Kansas City.

(m.) The sun is not shining in Kansas City if and only if Bob does not ride his bike to work.

Exercise 2.15.2. Let P, Q, and R be any statements. Construct an appropriate truth table to prove that the statements "If P, then Q or R" and "If P and not Q, then R" are logically equivalent.

Exercise 2.15.3. Use Example 2.11 to prove that if Bob placed in the top two in a cycling race on Saturday, but he did not place second, then Bob must have placed first.

Exercise 2.15.4. Use a proof by contradiction to prove that if Bob placed in the top two in a cycling race on Saturday, but he did not place second, then Bob must have placed first. Cite any theorems or laws of inference (by name) that you use in your proof.

Chapter 3

Proofs in the Wild

3.1 Divisibility Properties of Integers

Recall that if a and b are any integers such that a is nonzero, we say that a **divides** b provided that there exists an integer q such that $b = aq$, and we write $a \mid b$. Consequently, the **divisors** of b are the nonzero integers a that divide b. We are already familiar with this notion, but for illustrative purposes, we note that the divisors of 12 are 1, 2, 3, 4, 6, and 12 because $12 = 12 \cdot 1 = 2 \cdot 6 = 3 \cdot 4$. We say that an integer $p \geq 2$ is **prime** if its only positive integer divisors are 1 and p. Conversely, any integer $n \geq 2$ that possesses positive integer divisors other than 1 and n is called **composite**.

Proposition 3.1.1. *Given any integer $n \geq 2$, we have that n is composite if and only if there exist positive integers a and b such that $n = ab$ and $1 < a < n$, i.e., neither a nor b equals n.*

Proof. By definition, if $n \geq 2$ is composite, then there exists a positive integer a other than 1 and n that divides n. Consequently, we may write $n = ab$ for some positive integer b. We must have that $n = ab \geq a$ because b is a positive integer. Equality cannot hold because that entails $a = n$, hence we conclude that $1 < a < n$. Conversely, if $n \geq 2$ is prime, then its only positive integer divisors are 1 and n. Explicitly, if $n = ab$ for some positive integers a and b, then either a or b is n. □

We will soon see that primes form the "building blocks" for all integers. Explicitly, every integer $n \geq 2$ can be written as a product of primes. We refer to such an expression of an integer as a product of its prime factors as the **prime factorization** of the integer. Observe that $12 = 4 \cdot 3 = 2^2 \cdot 3$ is the prime factorization of 12 and $30 = 2 \cdot 15 = 2 \cdot 3 \cdot 5$ is the prime factorization of 30. Before we are able to prove that every integer $n \geq 2$ admits a unique prime factorization, we set out to develop some basic tools for dealing with divisibility of integers. Our first task is to verify the following.

Proposition 3.1.2. *Consider any nonzero integers a and b and any integers c and d.*

1.) *If $a \mid c$ or $a \mid d$, then $a \mid cd$.*

2.) *If $a \mid b$ and $b \mid c$, then $a \mid c$.*

3.) *If $a \mid c$ and $b \mid d$, then $ab \mid cd$.*

4.) *If $a \mid c$ and $a \mid d$, then $a \mid cx + dy$ for any integers x and y.*

Proof. Each statement can be proved directly by appealing to the definition of divisibility.

1.) We may assume without loss of generality that $a \mid c$. By definition, if a divides c, then there exists an integer q such that $c = aq$. Consequently, we have that $cd = (aq)d = (dq)a$. Considering that dq is an integer because d and q are integers, we conclude that a divides cd.

2.) By definition, if $a \mid b$ and $b \mid c$, then there exist integers q and r such that $b = aq$ and $c = br$. We conclude that $c = br = (aq)r = (qr)a$ is divisible by a because qr is an integer.

3.) By definition, if $a \mid c$ and $b \mid d$, then $c = aq$ and $d = br$ for some integers q and r. We conclude that $cd = (aq)(br) = (qr)(ab)$ is divisible by ab because qr is an integer.

4.) By definition, if $a \mid c$ and $a \mid d$, then there exist integers q and r such that $c = aq$ and $d = ar$. Given any integers x and y, we have that

$$cx + dy = (aq)x + (ar)y = (qx)a + (ry)a = (qx + ry)a.$$

Considering that qx and ry are integers, we conclude that $a \mid cx + dy$. □

Proposition 3.1.3. *Consider any pair of nonzero integers a and b.*

1.) *If $a \mid b$, then $|a| \leq |b|$.*

2.) *If $a \mid b$ and $b \mid a$, then $|a| = |b|$.*

Proof. We will prove the first statement; the second statement then follows from the first statement because if $a \mid b$ and $b \mid a$, then $|a| \leq |b|$ and $|b| \leq |a|$. By definition, if $a \mid b$, then there exists an integer q such that $b = aq$. Even more, by assumption that b is nonzero, it follows that $|q| \geq 1$. Consequently, we conclude that $|b| = |aq| = |a||q| \geq |a|$, as desired. □

Even with this very basic notion of divisibility, there are many interesting examples to consider.

Example 3.1.4. Prove that if a, b, c are integers, a and b are nonzero, $a^2 \mid b$, and $b^3 \mid c$, then $a^6 \mid c$.

Proof. By definition, if $a^2 \mid b$, then there exists an integer q such that $b = a^2q$. Likewise, there exists an integer r such that $c = b^3r$. Considering that $b = a^2q$, we find that $b^3 = (a^2q)^3 = a^6q^3$ so that $c = b^3r = (a^6q^3)r = (q^3r)a^6$. We conclude that $a^6 \mid c$ because q^3r is an integer. □

Example 3.1.5. Prove that for any integers a and b, if $2 \mid ab$, then $2 \mid a$ or $2 \mid b$.

Proof. We will prove the contrapositive. We must assume to this end that $2 \nmid a$ and $2 \nmid b$. Consequently, the integers a and b are odd, hence there exist integers k and ℓ such that $a = 2k + 1$ and $b = 2\ell + 1$. We find that $ab = (2k + 1)(2\ell + 1) = 4k\ell + 2k + 2\ell + 1 = 2(2k\ell + k + \ell) + 1$. Considering that $2k\ell + k + \ell$ is an integer, we conclude that ab is odd so that $2 \nmid ab$. □

Example 3.1.6. Prove that if n is an integer such that $7 \mid 4n$, then $7 \mid n$.

Proof. By definition of divides, if $7 \mid 4n$, then there exists an integer q such that $4n = 7q$. Considering that $4n = 2(2n)$ is even, we must have that q is even; otherwise, if q is odd, then $q = 2k + 1$ for some integer k, and we find that $4n = 7q = 7(2k + 1) = 2(7k + 3) + 1$ is odd — a contradiction. Consequently, there exists an integer k such that $q = 2k$ and $4n = 7q = 14k$. Cancelling one factor of 2 from each side of this equation yields that $2n = 7k$ so that $2 \mid 7k$. By Example 3.1.5, we conclude that $2 \mid k$ because 7 is not divisible by 2. Consequently, there exists an integer ℓ such that $k = 2\ell$ and $q = 2k = 4\ell$. Going back once more to our identity $4n = 7q$ yields that $4n = 7(4\ell)$. Cancelling one factor of 4 from both sides yields that $n = 7\ell$ so that $7 \mid n$, as desired. □

Exercise 3.9.5 asserts that Examples 3.1.4 and 3.1.5 can be generalized to demonstrate that for any integers a and b and any prime p, we have that $p \mid ab$ if and only if $p \mid a$ or $p \mid b$.

Example 3.1.7. Prove that if n if an integer such that $2 \mid (n^2 + 3)$, then $4 \mid (n^2 + 3)$.

Proof. By definition of divides, if $2 \mid (n^2 + 3)$, then $n^2 + 3 = 2k$ for some integer k. Consequently, we have that $n^2 = 2k - 3 = 2(k - 2) + 1$ is an odd integer so that n is odd. By definition of an odd integer, there exists an integer ℓ such that $n = 2\ell + 1$ and

$$n^2 + 3 = (2\ell + 1)^2 + 3 = (4\ell^2 + 4\ell + 1) + 3 = 4(\ell^2 + \ell + 1).$$

Considering that $\ell^2 + \ell + 1$ is an integer, we conclude that $4 \mid (n^2 + 3)$. □

We will henceforth adopt the notation that $a \mid b$ to assert that a nonzero integer a divides an integer b. Given any nonzero integer c such that $c \mid a$ and $c \mid b$, we say that c is a **common divisor** of a and b; the **greatest common divisor** of a and b is the unique integer $d = \gcd(a, b)$ such that

(1.) $d \mid a$ and $d \mid b$, i.e., d is a common divisor of a and b and

(2.) if c is any common divisor of a and b, then $c \mid d$.

Example 3.1.8. Consider the integers $a = 12$ and $b = 30$. By writing down the prime factorizations of a and b, their greatest common divisor can be easily determined. Observe that $12 = 2^2 \cdot 3$ and $30 = 2 \cdot 3 \cdot 5$. Consequently, the greatest common divisor of 12 and 30 is $2 \cdot 3$, i.e., $\gcd(12, 30) = 6$.

Example 3.1.9. Consider the integers $a = 24$ and $b = 16$. By writing down the prime factorizations of a and b, their greatest common divisor can easily be read off. Observe that $24 = 4 \cdot 6 = 2^3 \cdot 3$ and $16 = 4^2 = 2^4$. Consequently, the greatest common divisor of 24 and 16 is 2^3, i.e., $\gcd(24, 16) = 8$.

Generally, for any nonzero integers a and b, we may determine $\gcd(a, b)$ from the prime factorizations of a and b in the same manner as in Examples 3.1.8 and 3.1.9. Certainly, it is possible that $\gcd(a, b) = 1$. One immediate instance of this is that both a and b are prime. Generalizing this notion, we say that positive integers a and b are **relatively prime** if and only if $\gcd(a, b) = 1$.

Example 3.1.10. Observe that 2 and 3 are relatively prime because they are distinct primes, hence they have no prime factors in common. Particularly, we have that $\gcd(2, 3) = 1$.

Example 3.1.11. We claim that 30 and 77 are relatively prime. Observe that the prime factorization of 30 is $30 = 2 \cdot 3 \cdot 5$, and the prime factorization of 77 is $77 = 7 \cdot 11$. Because they have no prime factors in common, we conclude that $\gcd(30, 77) = 1$, hence 30 and 77 are relatively prime.

3.2 The Principle of Mathematical Induction

One of the most useful proof techniques is the **proof by induction** that appeals to one of the three incarnations of the **Principle of Mathematical Induction**. We say that a nonempty subset S of real numbers is **hereditary** if it holds that $x+1 \in S$ whenever we have that $x \in S$. Basically, the Principle of Mathematical Induction is a property of nonempty subsets of integers that asserts that if S is any hereditary subset of integers that admits a smallest element n_0 satisfying an open sentence $P(n)$ whose domain is the integers, then every element $n \in S$ satisfies the statement $P(n)$. Before we proceed to the definition of the Principle of Mathematical Induction, let us see some examples of properties of integers for which a proof by induction is appropriate.

Example 3.2.1. Consider the sum of the first n consecutive odd positive integers.

$$o(n) = 1 + 3 + 5 + \cdots + (2n-1) = \sum_{k=0}^{n-1} (2k+1)$$

Computing the value of $o(n)$ for the first four positive integers $1 \leq n \leq 4$ yields that $o(1) = 1$, $o(2) = 1+3 = 4$, $o(3) = 1+3+5 = 9$, $o(4) = 1+3+5+7 = 16$, and so on.

n	1	2	3	4
$o(n)$	1	4	9	16

Table 3.1: the sum of first n consecutive odd positive integers

Observe that $o(n) = n^2$ for each integer $1 \leq n \leq 5$. Continuing with the table, we would find that $o(n) = n^2$ for all integers $1 \leq n \leq k$ for any positive integer k. Consequently, we have the following.

Conjecture 3.2.2. We have that $o(n) = n^2$ for all integers $n \geq 1$ for $o(n)$ as in Example 3.2.1.

Observe that $o(1) = 1 = 1^2$ and $o(n) + (2n+1) = o(n+1)$, hence if we could assume that $o(n) = n^2$, then we could conclude that $o(n+1) = n^2 + 2n + 1 = (n+1)^2$. We will soon return to validate this idea: it is precisely one of the tenants of the Principle of Mathematical Induction!

Example 3.2.3. Consider the sum of the first n consecutive positive integers.

$$c(n) = \sum_{k=1}^{n} k = 1 + 2 + 3 + \cdots + n$$

Computing the value of $c(n)$ for the first four positive integers $1 \leq n \leq 4$ yields that $c(1) = 1$, $c(2) = 1+2 = 3$, $c(3) = 1+2+3 = 6$, and $c(4) = 1+2+3+4 = 10$, and so on.

n	1	2	3	4	5
$c(n)$	1	3	6	10	15

Table 3.2: the sum of the first n consecutive positive integers

Unfortunately, the pattern here is not obvious; however, due to a young Gauss, the following strategy can be employed. Briefly put, the idea is to write down the sum $1 + 2 + 3 + \cdots + n$ forwards and

backwards, adding each column of the sum to determine the value of $2(1+2+3+\cdots+n)$.

$$\begin{array}{cccccccccc} & 1 & + & 2 & + & 3 & + & \cdots & + & n \\ + & n & + & (n-1) & + & (n-2) & + & \cdots & + & 1 \\ \hline & (n+1) & + & (n+1) & + & (n+1) & + & \cdots & + & (n+1) \end{array}$$

Considering that there are n columns and the sum of each column is $n+1$, we conclude that $2(1+2+3+\cdots+n) = n(n+1)$. Consequently, we have the following.

Conjecture 3.2.4. We have that $c(n) = \frac{n(n+1)}{2}$ for all integers $n \geq 1$ for $c(n)$ as in Example 3.2.3.

Like before, we can verify the formula for $n = 1$ as $c(1) = 1 = \frac{1\cdot 2}{2}$ and $c(n) + (n+1) = c(n+1)$, hence if we could assume that $c(n) = \frac{n(n+1)}{2}$, then we could conclude that

$$c(n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}.$$

Definition 3.2.5 (Principle of Ordinary Induction)**.** Let $P(n)$ be any open sentence defined for all integers $n \geq n_0$. If the following conditions hold, then $P(n)$ holds for all integers $n \geq n_0$.

(i.) $P(n_0)$ is a true statement.

(ii.) $P(n+1)$ is a true statement whenever $P(n)$ is a true statement for some integer $n \geq n_0$.

Remark 3.2.6. Be cognizant that we have taken the Principle of Ordinary Induction as an axiom in our set theory; however, some authors prefer to prove it as a corollary by first *defining* the non-negative integers $\mathbb{Z}_{\geq 0}$ as the intersection of all hereditary subsets of $\mathbb{R}$ that contain 0 (cf. [DW00, Definition 3.5]). Put another way, we may define $\mathbb{Z}_{\geq 0}$ as the intersection of all sets $S \subseteq \mathbb{R}$ such that

(a.) $0 \in S$ and

(b.) if $s \in S$, then $s+1 \in S$.

Using this axiom, the Principle of Ordinary Induction can be established by proving that the set $S = \{n \in \mathbb{Z}_{\geq 0} \mid P(n) \text{ is a true statement}\}$ is simply $\mathbb{Z}_{\geq 0}$. But this is clear: by definition of S, if $P(0)$ is a true statement, then $0 \in S$; likewise, if $n \in S$, then $P(n)$ is a true statement, hence $P(n+1)$ is a true statement, i.e., $n+1 \in S$. Combined, these observations illustrate that S is a hereditary subset of $\mathbb{R}$ that contains 0, i.e., $S \supseteq \mathbb{Z}_{\geq 0}$. By definition of S, we have also that $S \subseteq \mathbb{Z}_{\geq 0}$.

By the Principle of Ordinary Induction, we can return to prove Conjectures 3.2.2 and 3.2.4.

Proof. (Conjecture 3.2.2) Consider the following open sentence involving an integer $n \geq 1$.

$$P(n): \text{ We have that } 1+3+5+\cdots+(2n-1) = n^2.$$

We will prove that $P(n)$ is true for all integers $n \geq 1$, i.e., we will prove that $\forall n \in \mathbb{Z}_{\geq 1}$, $P(n)$ is true. We proceed by the Principle of Ordinary Induction. We must verify the following two conditions.

(i.) Observe that $P(1)$ is a true statement because it holds that $1 = 1^2$.

(ii.) We will assume that $P(n)$ is true for some integer $n \geq 1$. Consequently, we have that

$$1+3+5+\cdots+(2n+1) = 1+3+5+\cdots+(2n-1)+(2n+1) = n^2+2n+1 = (n+1)^2.$$

Considering that (i.) $P(1)$ is a true statement and (ii.) $P(n+1)$ is true whenever $P(n)$ is true for some integer $n \geq 1$, our proof is complete by the Principle of Ordinary Induction. □

Proof. (Conjecture 3.2.4) Consider the following open sentence involving an integer $n \geq 1$.

$$P(n): \text{ We have that } 1+2+3+\cdots+n = \frac{n(n+1)}{2}.$$

We will prove that $P(n)$ is true for all integers $n \geq 1$, i.e., we will prove that $\forall n \in \mathbb{Z}_{\geq 1}$, $P(n)$ is true. We proceed by the Principle of Ordinary Induction. We must verify the following two conditions.

(i.) Observe that $P(1)$ is a true statement because it holds that $1 = \frac{1 \cdot 2}{2}$.

(ii.) We will assume that $P(n)$ is true for some integer $n \geq 1$. Consequently, we have that

$$\begin{aligned} 1+2+3+\cdots+(n+1) &= 1+2+3+\cdots+n+(n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1)+2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

Considering that (i.) $P(1)$ is a true statement and (ii.) $P(n+1)$ is true whenever $P(n)$ is true for some integer $n \geq 1$, our proof is complete by the Principle of Ordinary Induction. □

Going forward, we will begin any inductive proof by simply stating our intention to use a proof by induction; however, we will not typically make any explicit reference to the statement $P(n)$ that we intend to prove, and we will somewhat abbreviate the steps in the proof with the assumption that the reader is familiar with induction. We illustrate a typical proof by induction as follows.

Example 3.2.7. Prove that $2^n > n^2$ for all integers $n \geq 5$.

Proof. We proceed by induction. Observe that $2^5 = 32 > 25 = 5^2$, hence the claim holds for $n = 5$. We will assume inductively that $2^n > n^2$ for some integer $n \geq 5$. By hypothesis, we have that

$$2^{n+1} = 2 \cdot 2^n > 2n^2,$$

so it suffices to prove that $2n^2 \geq (n+1)^2$. Considering that $n \geq 5$ by our inductive hypothesis, we have that $n^2 \geq 5n$ and $5n \geq 4n+5 \geq 2n+1$ so that

$$2n^2 = n^2 + n^2 \geq n^2 + 5n \geq n^2 + 2n + 1 = (n+1)^2.$$

We conclude by induction that $2^n > n^2$ for all integers $n \geq 5$. □

Occasionally, it is desirable to strengthen the hypotheses of the Principle of Ordinary Induction in order to simplify proofs involving induction. Currently, we may view induction as a property of falling dominoes: (i.) if the n_0th domino falls and (ii.) the nth domino falling causes the $(n+1)$th domino to fall, then as the n_0th domino falls, all consecutive dominoes after it will fall. But suppose that we could knock down all dominoes from the n_0th to the nth domino: this would provide even more power with which to knock down the $(n+1)$th domino! We introduce this as the following.

Definition 3.2.8 (Principle of Complete Induction)**.** Let $P(n)$ be any open sentence defined for all integers $n \geq n_0$. If the following conditions hold, then $P(n)$ holds for all integers $n \geq n_0$.

(i.) $P(n_0)$ is a true statement.

(ii.) $P(n+1)$ is a true statement whenever $P(k)$ is a true statement for all integers $1 \leq k \leq n$.

Even though the hypotheses of the Principle of Complete Induction ostensibly appear to be stronger than the Principle of Ordinary Induction, the two principles are in fact equivalent to one another. Last, we obtain another ubiquitous tool that will prove crucial in our future endeavors.

Theorem 3.2.9 (Well-Ordering Principle)**.** *Every nonempty set of non-negative integers admits a smallest element with respect to the total order $\leq$. Put another way, if $S \subseteq \mathbb{Z}_{\geq 0}$ is a nonempty set, then there exists an element $s_0 \in S$ such that $s_0 \leq s$ for all elements $s \in S$.*

Proof. We will establish the contrapositive, i.e., we will prove that if $S \subseteq \mathbb{Z}_{\geq 0}$ has the property that for every element $s \in S$, there exists an element $s_0 \in S$ such that $s_0 < s$, then S must be empty. Let $P(n)$ be the statement that $n \notin S$. We claim that $P(n)$ holds for all integers $n \geq 0$. We proceed by the Principle of Complete Induction. Observe that if $0 \in S$, then there exists an element $s_0 \in S$ such that $s_0 < 0$. But this is not possible because S consists of non-negative integers. Consequently, we must have that $0 \notin S$, hence $P(0)$ is true. We will assume according to the Principle of Complete Induction that $P(k)$ holds for each integer $1 \leq k \leq n$. By definition, this means that $k \notin S$ for any integer $1 \leq k \leq n$. Observe that if $n+1 \in S$, then there exists an integer $s_0 \in S$ such that $1 \leq s_0 \leq n$. But this is not possible by the hypothesis of our induction. Consequently, we must have that $n+1 \notin S$, i.e., $P(n+1)$ is a true statement whenever $P(k)$ is a true statement for each integer $1 \leq k \leq n$. By the Principle of Complete Mathematical Induction, our proof is complete. □

Conversely, the Well-Ordering Principle implies the Principle of Ordinary Induction, hence it is equivalent to both ordinary induction and complete induction (cf. Exercise 3.9.4). Combined, the Principle of Ordinary Induction, the Principle of Complete Induction, and the Well-Ordering Principle constitute the triumvirate that is the Principle of Mathematical Induction.

3.3 The Division Algorithm

Even as early as grade school, we learn the process of dividing one integer by another. Each time we divide an integer a by a nonzero integer b, we obtain an integer q and a non-negative integer r that is strictly smaller than $|b|$ such that $a = qb + r$. Explicitly, we say that a is the **dividend**; b is the **divisor**; q is the **quotient**; and r is the **remainder** of the division. Our aim throughout this section is to establish that this process is well-founded, i.e., the process of division of an integer a by

a nonzero integer b unambiguously results in integers q and r such that $a = qb + r$ and $0 \leq r < |b|$. We will also establish an algorithm that will allow us to efficiently find the integers q and r.

Example 3.3.1. Consider the case that $a = 11$ and $b = 2$. One can easily see that $11 = 5 \cdot 2 + 1$, hence the integers $q = 5$ and $r = 1$ satisfy the requirements that $a = qb + r$ and $0 \leq r < |b|$.

Example 3.3.2. Consider the case that $a = -17$ and $b = 6$. One can easily see that $-17 = -3 \cdot 6 + 1$, hence the integers $q = -3$ and $r = 1$ satisfy the requirements that $a = qb + r$ and $0 \leq r < |b|$.

Example 3.3.3. Consider the case that $a = -8$ and $b = -9$. One can easily see that $-8 = 1(-9) + 1$, hence the integers $q = 1$ and $r = 1$ satisfy the requirements that $a = qb + r$ and $0 \leq r < |b|$.

Each of the previous examples can be completed by noticing that the integer multiples of b are completely determined by b. Consequently, we may consider all integer multiples of b that do not exceed a, i.e., we may consider the collection $R(a, b) = \{a - qb \mid q \text{ is an integer and } a \geq qb\}$. Our idea is to find the largest (in absolute value) integer q such that $a \geq qb$; then, the difference $a - qb$ must be non-negative (by assumption) and strictly smaller than b (otherwise, we could increase q). Using this intuition as our guide, let us return to find $R(a, b)$ in our previous examples.

Example 3.3.4. By definition, we have that $R(11, 2) = \{11 - 2q \mid q \text{ is an integer and } 11 \geq 2q\}$. Observe that $11 \geq 2q$ if and only if $q \leq 11/2$, hence the only valid values of q in $R(11, 2)$ are $q \leq 5$. Consequently, we have that $-2q \geq -10$ so that $11 - 2q \geq 1$. By consecutively decreasing the value of $q \leq 5$, we find that $R(11, 2) = \{1, 3, 5, 7, \dots\}$ consists of all odd positive integers.

Example 3.3.5. We have that $R(-17, 6) = \{-17 - 6q \mid q \text{ is an integer and } -17 \geq 6q\}$. Observe that $-17 \geq 6q$ if and only if $q \leq -17/6$, hence the only valid values of q in $R(-17, 6)$ are $q \leq -3$. Consequently, we conclude that $R(-17, 6) = \{-17 - 6q \mid q \leq -3 \text{ is an integer}\} = \{1, 7, 13, 19, \dots\}$.

Example 3.3.6. We have that $R(-8, -9) = \{-8 + 9q \mid q \text{ is an integer and } -8 \geq -9q\}$. Observe that $-8 \geq -9q$ if and only if $q \geq 8/9$, hence the only valid values of q in $R(-8, -9)$ are $q \geq 1$. Consequently, we conclude that $R(-8, -9) = \{-8 + 9q \mid q \geq 1 \text{ is an integer}\} = \{1, 10, 19, 28, \dots\}$.

Generalizing the collection $R(a, b)$ and using the Well-Ordering Principle yields the following.

Theorem 3.3.7 (Division Algorithm)**.** *Given any integer a and any nonzero integer b, there exist unique integers q and r such that $a = qb + r$ and $0 \leq r < |b|$.*

Proof. Consider the collection $R(a, b) = \{a - qb \mid q \text{ is an integer and } a \geq qb\}$. By definition, $R(a, b)$ consists of non-negative integers. Observe that if $a \geq 0$, then $R(a, b)$ is nonempty because we may take $q = 0$ to conclude that $R(a, b)$ contains a. On the other hand, if $a < 0$, then if $b \geq 1$, we conclude that $R(a, b)$ is nonempty because we may take $q = a - 1$ to find that $R(a, b)$ contains $a - qb$ because $a \geq a - 1 \geq (a - 1)b = qb$. Last, if $a < 0$ and $b \leq -1$, then $R(a, b)$ must once again be nonempty because we may take $q = -(a - 1)$ to find that $R(a, b)$ contains $a - qb$ because $a \geq a - 1 \geq -(a - 1)b = qb$. Ultimately, this shows that $R(a, b)$ is a nonempty subset of non-negative integers, hence the Well-Ordering Principle implies that there exists a smallest element $r(a, b) = a - qb$ with respect to the total order $\leq$. Rearranging this identity and rewriting $r(a, b)$ as r yields that $a = qb + r$. Clearly, it follows that $r \geq 0$, hence it suffices to see that $r < |b|$. On the contrary, suppose that $a - bq = r \geq |b|$. Observe that if $b \geq 1$, then $|b| = b$ yields that $a - qb \geq b$ and $a - (q + 1)b \geq 0$. Considering that $a - (q + 1)b$ is smaller than the smallest element $r(a, b) = a - qb$ of $R(a, b)$, we obtain a contradiction. Likewise, if $b \leq -1$, then $|b| = -b$ implies that $a - qb \geq b$ and

$a-(q-1)b \geq 0$. Considering that $b \leq -1$, we find that $a-(q-1)b = a-qb+b < a-qb = r(a,b)$. Once again, this contradicts the fact that $r(a,b)$ is the smallest element of $R(a,b)$. Ultimately, we conclude that there exist integers q and r such that $a = qb+r$ and $0 \leq r < |b|$.

We must prove next that these integers are unique. We accomplish this by assuming that there exist integers q' and r' such that $a = q'b+r'$ and $0 \leq r' < |b|$. Considering that $a = qb+r$ by the previous paragraph, we conclude that $qb+r = q'b+r'$ so that $b(q-q') = r'-r$. Observe that if $q' = q$, then it is clear that $r' = r$, hence our proof is complete. Consequently, we may assume on the contrary that $q-q'$ is nonzero, hence we must have that $|b| \leq |r'-r|$. Observe that if $r' > r$, then $|r'-r| = r'-r$ implies that $r' \geq |b|+r \geq |b|$ — a contradiction. Likewise, if $r' < r$, then $|r'-r| = r-r'$ implies that $r \geq |b|+r' \geq |b|$ — a contradiction. Either way, we conclude that $r' = r$ so that $b(q-q') = 0$. By hypothesis that b is nonzero, we conclude that $q-q' = 0$ or $q' = q$. □

We have therefore rigorously verified the method of division that we have taken for granted since elementary school! Even though the Division Algorithm does not explicitly provide the steps to compute the unique integers q and r such that $a = qb+r$ and $0 \leq r < |b|$, we note that the proof is constructive in the sense that the unique integers q and $0 \leq r < |b|$ can be deduced from the collection $R(a,b) = \{a-qb \mid q \text{ is an integer and } a \geq qb\}$, as we have done in previous examples.

One of the most fruitful applications of the Division Algorithm is that it gives us access to a finite number of cases for divisibility proofs involving any positive integer. Explicitly, if we wish to prove that a positive integer $a \geq 2$ divides an integer b, then by the Division Algorithm, we may write $b = aq+r$ for some integers q and r such that $0 \leq r < |b|$. Consequently, it suffices to check each of the $|b|$ cases that $0 \leq r \leq |b|-1$. We have already tacitly used this kind of proof by cases: in fact, every integer is either even or odd because the remainder an integer modulo 2 is either 0 or 1. Concretely, we illustrate this more general idea for divisibility proofs involving the integer 3.

Example 3.3.8. Prove that if n is an integer, then $3 \mid (2n^2+1)$ if and only if $3 \nmid n$.

Proof. We will assume first that $3 \nmid n$. By the Division Algorithm, there are two cases.

(a.) Observe that if $n = 3q+1$ for some integer q, then

$$2n^2+1 = 2(3q+1)^2+1 = 2(9q^2+6q+1)+1. = 3(6q^2+4q+1).$$

Considering that $6q^2+4q+1$ is an integer, we conclude that $3 \mid (2n^2+1)$.

(b.) Observe that if $n = 3q+2$ for some integer q, then

$$2n^2+1 = 2(3q+2)^2+1 = 2(9q^2+12q+4)+1. = 3(6q^2+8q+3).$$

Considering that $6q^2+8q+3$ is an integer, we conclude that $3 \mid (2n^2+1)$.

Conversely, we will prove the contrapositive. We must assume to this end that $3 \mid n$. By definition of divides, there exists an integer q such that $n = 3q$. Consequently, we have that

$$2n^2+1 = 2(3q)^2+1 = 18q^2+1.$$

Certainly, this is not divisible by 3 because 1 is not divisible by 3, i.e., $3 \nmid (2n^2+1)$. □

Example 3.3.9. Prove that if n is an odd integer such that $3 \nmid n$, then $24 \mid (n^2 - 1)$.

Proof. We will assume that n is an odd integer. By definition of an odd integer, we have that $n = 2k + 1$ for some integer k. By the Division Algorithm, if $3 \nmid n$, then there are two cases.

(a.) Observe that if $n = 3q + 1$ for some integer q, then $2k + 1 = 3q + 1$ yields that $2k = 3q$. By Example 3.1.5, we must have that $2 \mid q$ so that $q = 2\ell$ for some integer ℓ and

$$n^2 - 1 = (6\ell + 1)^2 - 1 = (36\ell^2 + 12\ell + 1) - 1 = 12(3\ell^2 + \ell).$$

We claim that ℓ is even. On the contrary, if ℓ were odd, then we would have that $\ell = 2m + 1$ for some integer m. Combining this identity with our previous identity that $n = 6\ell + 1$ yields that $n = 6(2m + 1) + 1 = 12m + 2 = 2(6m + 1)$ — a contradiction. Consequently, there exists an integer m such that $\ell = 2m$ and $n^2 - 1 = 12[3(2m)^2 + 2m] = 24(6m^2 + m)$.

(b.) Observe that if $n = 3q + 2$ for some integer q, then $2k + 1 = 3q + 2$ yields that $2k = 3q + 1$. Consequently, we must have that q is odd; otherwise, if it were the case that $q = 2\ell$ for some integer ℓ, then $2k = 3(2\ell) + 1 = 2(3\ell) + 1$ is odd — a contradiction. We conclude that there exists an integer ℓ such that $q = 2\ell + 1$ and $n = 3q + 2 = 3(2\ell + 1) + 2 = 6\ell + 5$. Observe that

$$n^2 - 1 = (6\ell + 5)^2 - 1 = (36\ell^2 + 60\ell + 25) - 1 = 12(3\ell^2 + 5\ell + 2).$$

We claim that $3\ell^2 + 5\ell + 2$ is even. Certainly, this holds if ℓ is even because the sum of three even integers is even; on the other hand, if $\ell = 2m + 1$ for some integer m, then

$$3\ell^2 + 5\ell + 2 = 3(2m + 1)^2 + 5(2m + 1) + 2 = 3(4m^2 + 4m + 1) + 10m + 7 = 2(6m^2 + 11m + 5).$$

Either way, we conclude that $2 \mid (3\ell^2 + 5\ell + 2)$ so that $24 \mid (n^2 - 1)$, as desired. □

We note that if the Division Algorithm produces a remainder of $r = 0$, then $a = qb$ so that b divides a, and we write that $b \mid a$. Before we state our next theorem, we remind the reader that if c is any nonzero integer such that $c \mid a$ and $c \mid b$, then we say that c is a common divisor of a and b; the greatest common divisor of a and b is the unique integer $d = \gcd(a, b)$ such that

(1.) $d \mid a$ and $d \mid b$, i.e., d is a common divisor of a and b and

(2.) if c is any common divisor of a and b, then $c \mid d$.

We say that a pair of nonzero integers a and b are relatively prime if and only if $\gcd(a, b) = 1$. Our next theorem states that $\gcd(a, b)$ can be realized as an integer-linear combination of a and b.

Theorem 3.3.10 (Bézout's Identity)**.** *If a and b are nonzero integers, then there exist integers x and y such that $\gcd(a, b) = ax + by$. Even more, $\gcd(a, b)$ divides $av + bw$ for all integers v and w.*

Proof. Consider the collection $L(a, b) = \{ax + by \mid x, y \text{ are integers and } ax + by \geq 1\}$ of positive $\mathbb{Z}$-linear combinations of a and b. Observe that one of the elements $a + b$, $a - b$, $-a + b$, or $-a - b$ lies in $L(a, b)$, hence it is nonempty. By the Well-Ordering Principle, there exists a smallest element $d(a, b) = ax + by$ with respect to the total order $\leq$. We will establish that $\gcd(a, b) = d(a, b)$.

By the Division Algorithm, there exist unique integers q_a and r_a such that $a = q_a d(a,b) + r_a$ and $0 \leq r_a < d(a,b)$. By rearranging this identity and using that $d(a,b) = ax + by$, we find that

$$r_a = a - q_a d(a,b) = a - q_a(ax + by) = (1 - q_a x)a - (q_a y)b.$$

Observe that if r_a were nonzero, then it would lie in $L(a,b)$ and satisfy $1 \leq r_a < d(a,b)$, but this is impossible because $d(a,b)$ is the smallest element of $L(a,b)$. Consequently, it must be the case that $r_a = 0$. Likewise, the Division Algorithm with b in place of a yields that $d(a,b)$ divides b. Ultimately, this proves that $d(a,b) \mid a$ and $d(a,b) \mid b$, hence $d(a,b)$ is a common divisor of both a and b.

Consider another common divisor c of a and b. We must prove that $c \mid d(a,b)$. By assumption, there exist integers q_a and q_b such that $a = q_a c$ and $b = q_b c$, from which it follows that

$$d(a,b) = ax + by = (q_a c)x + (q_b c)y = (q_a x + q_b y)c.$$

By definition, this implies that c divides $d(a,b)$ so that $\gcd(a,b) = d(a,b) = ax + by$, as desired.

Last, let v and w be any integers. By the previous two paragraphs, there exist integers q_a and q_b such that $a = q_a \gcd(a,b)$ and $b = q_b \gcd(a,b)$, hence $\gcd(a,b)$ divides $av + bw$. □

Corollary 3.3.11. *If a and b are relatively prime, then $ax + by = 1$ for some integers x and y.*

Corollary 3.3.12. *If a and b are any nonzero integers, then $\gcd(a,b)$ is unique.*

Proof. By the proof of Bézout's Identity, $\gcd(a,b)$ is unique because it is by construction the smallest (with respect to the total order $\leq$) positive integer satisfying some property. □

Even though Bézout's Identity guarantees the existence of integers x and y such that we may write $\gcd(a,b) = ax + by$, it does not provide any tools for explicitly finding these integers x and y.

Example 3.3.13. Consider the case that $a = 24$ and $b = 16$. We know already that $\gcd(a,b) = 8$, and it is not difficult to see that $8 = 24 \cdot 1 + 16(-1)$; however, this can also be seen as follows. By the Division Algorithm, we have that $24 = 1 \cdot 16 + 8$, hence we have that $8 = 24 \cdot 1 + 16(-1)$.

Example 3.3.14. Consider the case that $a = 110$ and $b = 24$. Observe that the unique prime factorizations of 110 and 15 are $110 = 10 \cdot 11 = 2 \cdot 5 \cdot 11$ and $24 = 2^3 \cdot 3$, respectively. By Exercise 3.9.10, it follows that $\gcd(110, 15) = 2$. By successively implementing the Division Algorithm, we may find the integers x and y such that $110x + 24y = 2$, as guaranteed to us by Bézout's Identity. Explicitly, we begin by running the Division Algorithm with $a = 110$ and $b = 24$ to find the unique integers q_1 and $0 \leq r_1 < 24$ such that $110 = 24q_1 + r_1$; then, we run the Division Algorithm with 24 and r_1 to produce the unique integers q_2 and $0 \leq r_2 < r_1$ such that $24 = q_2 r_1 + r_2$. Continuing in this manner produces a strictly decreasing sequence $r_1 > r_2 > \cdots > r_n$ of non-negative integers at the nth step; by the Well-Ordering Principle, this sequence must have a least element, hence the process must eventually terminate. Putting this process to the test, we find that

$$\begin{aligned} 110 &= 4 \cdot 24 + 14, \\ 24 &= 1 \cdot 14 + 10, \\ 14 &= 1 \cdot 10 + 4, \text{ and} \\ 10 &= 2 \cdot 4 + 2. \end{aligned}$$

We find the integers x and y such that $110x + 24y = 2$ by unravelling this process in reverse. Explicitly, our last identity yields that $10-2\cdot 4 = 2$; the identity before that yields that $4 = 14-1\cdot 10$, hence we have that $-2 \cdot 14 + 3 \cdot 10 = 10 - 2 \cdot (14 - 1 \cdot 10) = 2$; the identity before $14 = 1 \cdot 10 + 4$ yields that $10 = 24 - 1 \cdot 14$, hence we have that $3 \cdot 24 - 5 \cdot 14 = -2 \cdot 14 + 3 \cdot (24 - 1 \cdot 14) = 2$; and at last, the identity before $24 = 1 \cdot 14 + 10$ yields that $14 = 110 - 4 \cdot 24$, hence we have that

$$110(-5) + 24(23) = 3 \cdot 24 - 5 \cdot (110 - 4 \cdot 24) = 2.$$

Algorithm 3.3.15 (Euclidean Algorithm)**.** Let a and b be any nonzero integers such that $a \geq b$.

1.) Use the Division Algorithm to find integers q_1 and r_1 such that $a = q_1 b + r_1$ and $0 \leq r_1 < |b|$.

2.) Use the Division Algorithm to find integers q_2 and r_2 such that $b = q_2 r_1 + r_2$ and $0 \leq r_2 < r_1$.

3.) Use the Division Algorithm to find integers q_3 and r_3 such that $r_1 = q_3 r_2 + r_3$ and $0 \leq r_3 < r_2$.

4.) Continue in this manner until r_{n+1} divides r_n. By the Well-Ordering Principle, this must eventually occur, and moreover, it must occur in a finite number of steps.

5.) Use the fact that $r_{n-1} = q_{n+1} r_n + r_{n+1}$ to express that $r_{n+1} = r_{n-1} - q_{n+1} r_n$.

6.) Use the fact that $r_{n-2} = q_n r_{n-1} + r_n$ to express that $r_n = r_{n-2} - q_n r_{n-1}$; then, use the fact that $r_{n+1} = r_{n-1} - q_{n+1} r_n$ to express that $r_{n+1} = r_{n-1} - q_{n+1}(r_{n-2} - q_n r_{n-1})$ so that

$$r_{n+1} = (q_n q_{n+1} + 1) r_{n-1} - q_{n+1} r_{n-2}.$$

7.) Continue in this manner to produce integers x and y such that $r_{n+1} = ax + by$.

By Bézout's Identity, we must have that $\gcd(a, b) \leq r_{n+1}$. Conversely, because r_{n+1} divides r_n by step four, it must divide r_k for all integers $1 \leq k \leq n$ by the fifth through seventh steps above. Consequently, by the second step above, we conclude that r_{n+1} must divide b, and by the first step above, we conclude that r_{n+1} must divide a. Ultimately, this shows that r_{n+1} is a common divisor of a and b, hence we must have that r_{n+1} divides $\gcd(a, b)$; in particular, we have that $r_{n+1} = \gcd(a, b)$.

3.4 Congruence Modulo n, Revisited

We will assume throughout this section that n is a fixed nonzero integer. By the Division Algorithm, for every integer a, there exist unique integers q_a and r_a such that $a = q_a n + r_a$ and $0 \leq r_a < |n|$. Considering that the remainder r_a of a divided by n is always a non-negative integer, we may assume without loss of generality that n is a positive integer. We will refer to the unique integer r_a as the remainder of a **modulo** n. Our naming convention is justified by the next proposition.

Proposition 3.4.1. *We have that $R_n = \{(a, r) \mid a = qn + r$ for some integer $q\}$ is an equivalence relation on $\mathbb{Z}$ with distinct equivalence classes $\{qn + r \mid q \in \mathbb{Z}\}$ for each integer $0 \leq r \leq n - 1$. Explicitly, the equivalence class of a modulo R_n is given by $[a] = \{qn + r_a \mid q \in \mathbb{Z}\}$.*

Proof. By definition, we must justify that R_n is (i.) reflexive, (ii.) symmetric, and (iii.) transitive.

(i.) Clearly, the pair (a, a) lies in R_n because we may always write $a = 0 \cdot n + a$ for any integer a.

(ii.) We must next show that if $(a, r) \in R_n$, then $(r, a) \in R_n$. By definition of R_n, if we assume that $(a, r) \in R_n$, then there exists an integer q such that $a = qn + r$. Consequently, the integer $-q$ satisfies that $r = -qn + a = (-q)n + a$, and we conclude that $(r, a) \in R_n$.

(iii.) Last, we will assume that $(a, r) \in R_n$ and $(r, s) \in R_n$. By definition of R_n, there exist integers q and q' such that $a = qn + r$ and $r = q'n + s$. Consequently, we have that $(a, s) \in R_n$ because

$$a = qn + r = qn + (q'n + s) = (q + q')n + s,$$

and the sum $q + q'$ of the two integers q and q' is itself an integer.

We have therefore established that R_n is an equivalence relation on $\mathbb{Z}$; the equivalence class of an arbitrary integer a modulo R_n is defined by $[a] = \{r \in \mathbb{Z} \mid a = qn + r \text{ for some integer } q\}$. By the Division Algorithm, for every integer a, there exist unique integers q_a and r_a such that $a = q_a n + r_a$ and $0 \leq r_a \leq n - 1$. Consequently, we have that $r_a \in [a]$. By Proposition 1.10.2, we conclude that $[a] = [r_a] = \{r \in \mathbb{Z} \mid r = -qn + r_a \text{ for some integer } q \in \mathbb{Z}\} = \{qn + r_a \mid q \in \mathbb{Z}\}$, as desired. □

Example 3.4.2. Observe that R_2 is an equivalence relation on $\mathbb{Z}$ whose distinct equivalence classes consist of the even integers $\mathbb{E} = \{2q \mid q \in \mathbb{Z}\}$ and the odd integers $\mathbb{O} = \{2q + 1 \mid q \in \mathbb{Z}\}$.

3.5 The Integers Modulo n

We will henceforth refer to the collection $\mathbb{Z}_n$ of equivalence classes of $\mathbb{Z}$ modulo R_n as the equivalence classes of $\mathbb{Z}$ **modulo** n. By Proposition 3.4.1, $\mathbb{Z}_n$ consists of exactly n distinct elements. Even more, for any two integers a and b, we have that $[a] = [b]$ if and only if the remainder of a modulo n is equal to the remainder of b modulo n if and only if there exist unique integers q_a, q_b, and r such that $a = q_a n + r$ and $b = q_b + r$ and $0 \leq r \leq n - 1$ if and only if $b - a = (q_b - q_a)n$. Put another way, two integers lie in the same equivalence class modulo n if and only if their difference is divisible by n. Generally, an equivalence relation is merely a set whose elements possess no arithmetic; however, the above observation allows us to deduce that $\mathbb{Z}_n$ (i.e., the set of equivalence classes of $\mathbb{Z}$ modulo n) admits a notion of addition and multiplication, as we demonstrate next.

Proposition 3.5.1. *Let $\mathbb{Z}_n$ denote the set of equivalence classes of the integers modulo n.*

1.) *If a and b are arbitrary integers, then $[a] + [b] = [a + b]$ is a well-defined operation. Even more, this addition is associative, commutative, and satisfies that $[a] + [0] = [a] = [0] + [a]$.*

2.) *Every equivalence class $[a]$ of the integers modulo n admits an additive inverse $[-a]$.*

3.) *If a and b are arbitrary integers, then $[a][b] = [ab]$ is a well-defined operation. Even more, this multiplication is associative, commutative, distributive, and satisfies that $[a][1] = [a] = [1][a]$.*

4.) *If a is an arbitrary integer, then $[a]$ admits a multiplicative inverse if and only if $\gcd(a, n) = 1$.*

Proof. (1.) We must demonstrate that if $[a_1] = [a_2]$ and $[b_1] = [b_2]$, then $[a_1 + b_1] = [a_2 + b_2]$. By the previous paragraph, if we assume that $[a_1] = [a_2]$ and $[b_1] = [b_2]$, then there exist integers q_a and q_b such that $a_1 - a_2 = q_a n$ and $b_1 - b_2 = q_b n$. Consequently, we have that

$$(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) = q_a n + q_b n = (q_a + q_b)n,$$

from which we conclude that $[a_1 + b_1] = [a_2 + b_2]$. Considering that integer addition is associative and commutative, our addition defined here is associative and commutative.

(3.) We must demonstrate that if $[a_1] = [a_2]$ and $[b_1] = [b_2]$, then $[a_1 b_1] = [a_2 b_2]$. By the paragraph preceding the proposition statement, if we assume that $[a_1] = [a_2]$ and $[b_1] = [b_2]$, then there exist integers q_a and q_b such that $a_1 - a_2 = q_a n$ and $b_1 - b_2 = q_b n$. Consequently, we have that

$$a_1 b_1 - a_2 b_2 = a_1 b_1 - a_1 b_2 + a_1 b_2 - a_2 b_2 = a_1(b_1 - b_2) + b_2(a_1 - a_2) = q_b a_1 n + q_a b_2 n = (q_b a_1 + q_a b_2)n,$$

from which we conclude that $[a_1 b_1] = [a_2 b_2]$. Considering that integer multiplication is associative and commutative, our multiplication defined here is associative and commutative. Even more, this multiplication is distributive because the first and third parts of the proposition that we have proved thus far establish that $[a]([b] + [c]) = [a][b + c] = [ab + ac] = [ab] + [ac] = [a][b] + [a][c]$.

(4.) By definition of our multiplication, the equivalence class $[a]$ admits a multiplicative inverse $[b]$ if and only if $[a][b] = [1]$ if and only if $[ab] = [1]$ if and only if $ab - 1 = qn$ for some integer q if and only if $ab - qn = 1$ for some integer q if and only if $\gcd(a, n) = 1$ by Bézout's Identity. Consequently, $[a]$ admits a multiplicative inverse if and only if $\gcd(a, n) = 1$, as desired. □

Combined, the operations of addition and multiplication on $\mathbb{Z}_n$ form the **modular arithmetic**.

Remark 3.5.2. Going forward, we will adopt the standard notation $b \equiv a \pmod{n}$ ("b is equivalent to a modulo n") in place of our current notation that $[b] = [a]$. Explicitly, we will set $b \equiv a \pmod{n}$ if and only if $n \mid (b - a)$ if and only if $b - a = qn$ for some integer q. Under this identification, observe that $[a] = \{r \in \mathbb{Z} \mid a \equiv r \pmod{n}\}$. One immediate advantage of this notation is that we can perform addition and multiplication modulo n in a natural way: indeed, if $b \equiv a \pmod{n}$, then we have that $b + c \equiv a + c \pmod{n}$ and $bc \equiv ac \pmod{n}$ for all integers c because it holds that $(b+c)-(a+c) = b-a = qn$ and $bc-ac = (b-a)c = (qc)n$ in this case. Even more, Proposition 3.5.1 implies that if $b \equiv a \pmod{n}$ and $d \equiv c \pmod{n}$, then $b+d \equiv a+c \pmod{n}$ and $bd \equiv ac \pmod{n}$.

3.6 Proofs Involving Sets

Using the calculus of logic, we may deduce further properties of sets and set operations. Before proceeding to any new material, we provide first a reinterpretation of Chapter 1 in the language of Chapter 2. We will assume to this end that X and Y are arbitrary (possibly empty) sets.

- We may view the **set membership** $x \in X$ as the statement $P(x) : x$ is an element of X; its negation is the statement $\neg P(x) : x$ is not an element of X (or $x \notin X$ in symbols).
- We have that $X \subseteq Y$ ("X is a **subset** of Y") if and only if for every element $x \in X$, it is true that $x \in Y$, i.e., if and only if it is true that "$\forall x \in X,\ x \in Y$." Consequently, the empty set $\varnothing$ is a subset of every set: there are no elements in $\varnothing$, hence "$\forall x \in \varnothing,\ x \in X$" is vacuously true!

- Provided that both $X \subseteq Y$ and "$\exists y \in Y$, $y \notin X$" ("there exists an element $y \in Y$ such that $y \notin X$") are true, we say that X is a **proper subset** of Y, and we write $X \subsetneq Y$; otherwise, it must be the case that $Y \subseteq X$, hence X and Y are **equal**, i.e., we must have that $X = Y$. Put another way, we have that $X = Y$ if and only if "$(\forall x \in X,\, x \in Y) \wedge (\forall y \in Y,\, y \in X)$" holds.

- Elements of either X or Y comprise the **union** $X \cup Y$ of X and Y. Put another way, we have that $X \cup Y$ is the superset of both X and Y for which "$(w \in X) \vee (w \in Y)$" is true.

- Elements of both X and Y comprise the **intersection** $X \cap Y$ of X and Y. Put another way, we have that $X \cap Y$ is the subset of both X and Y for which "$(w \in X) \wedge (w \in Y)$" is true.

- Elements in Y but not in X comprise the **relative complement** $Y \setminus X$ of X in Y. Put another way, we have that $Y \setminus X$ is the subset of Y for which "$(y \in Y) \wedge (y \notin X)$" is true.

- We may view the **Cartesian product** $X \times Y$ of the sets X and Y as the collection of all ordered pairs (x, y) for which the statement "$(x \in X) \wedge (y \in Y)$" is true.

By using the above dictionary between set theory and logic, we can prove facts about sets.

Example 3.6.1. Prove that for any sets X, Y, and W such that $X \subseteq W$ and $Y \subseteq W$, we have that

$$X \setminus Y = X \cap (W \setminus Y).$$

Proof. By the above definition of set equality, we must demonstrate that $X \setminus Y \subseteq X \cap (W \setminus Y)$ and $X \cap (W \setminus Y) \subseteq X \setminus Y$. By definition of $X \setminus Y$, if $x \in X \setminus Y$, then $x \in X$ and $x \notin Y$. By assumption that $X \subseteq W$, we find that $x \in W$ and $x \notin Y$ so that $x \in X$ and $x \in W \setminus Y$. We conclude that $x \in X \cap (W \setminus Y)$, from which it follows that $X \setminus Y \subseteq X \cap (W \setminus Y)$. Conversely, if $x \in X \cap (W \setminus Y)$, then $x \in X$ and $x \in W \setminus Y$. By definition of $W \setminus Y$, we have that $x \in W$ and $x \notin Y$. We conclude that $x \in X \setminus Y$ since $x \in X$ and $x \notin Y$, from which it follows that $X \cap (W \setminus Y) \subseteq X \setminus Y$. □

Example 3.6.2. Prove that for any sets X and Y, we have that $X = (X \cap Y) \cup (X \setminus Y)$.

Proof. By the above definition of set equality, we must demonstrate that $X \subseteq (X \cap Y) \cup (X \setminus Y)$ and $(X \cap Y) \cup (X \setminus Y) \subseteq X$. Given any element $x \in X$, either $x \in Y$ or $x \notin Y$: if the former holds, then $x \in X \cap Y$; if the latter holds, then $x \in X \setminus Y$. Either way, it follows that $x \in (X \cap Y) \cup (X \setminus Y)$. Conversely, suppose that $x \in (X \cap Y) \cup (X \setminus Y)$. Each of the sets $X \cap Y$ and $X \setminus Y$ is by definition a subset of X, hence if either $x \in X \cap Y$ or $x \in X \setminus Y$, we have that $x \in X$. □

Example 3.6.3. Prove that for any sets X and Y, we have that $X \cup Y = X$ if and only if $Y \subseteq X$.

Proof. By the above definition of set equality, we must demonstrate that if $Y \subseteq X$, then $X \cup Y \subseteq X$ and $X \subseteq X \cup Y$. Observe that the latter inclusion is true by definition of the union, hence it suffices to prove that if $Y \subseteq X$, we have that $X \cup Y \subseteq X$. We will assume to this end that $Y \subseteq X$ and $w \in X \cup Y$. By definition of the union, we have that $w \in X$ or $w \in Y$. Either way, by hypothesis that $Y \subseteq X$, it follows that $w \in X$, hence we conclude that $X \cup Y \subseteq X$.

Conversely, we will assume that $X \cup Y = X$. Given any element $y \in Y$, we have that $y \in X \cup Y$ so that $y \in X$ by assumption that $X \cup Y = X$. We conclude that $Y \subseteq X$. □

3.7 Fundamental Properties of Set Operations

We will suppose throughout this section that X, Y, and W are arbitrary (possibly empty) sets for which the inclusions $X \subseteq W$ and $Y \subseteq W$ hold. We remind the reader that in this case, we refer to W as our **universe** (or as the **universal set**), and we may view all elements of X and Y as elements of W via the aforementioned inclusions. We obtain the following membership laws.

Theorem 3.7.1 (Law of the Excluded Middle for Sets)**.** *Given any element $w \in W$, we must have that either $w \in X$ or $w \notin X$; the analogous statement holds for the set Y in place of X.*

Theorem 3.7.2 (Law of Non-Contradiction for Sets)**.** *Given any element $w \in W$, we cannot have that both $w \in X$ and $w \notin X$; the analogous statement holds for the set Y in place of X.*

We omit the proofs of the aforementioned facts because they follow immediately from the Law of the Excluded Middle and the Law of Non-Contradiction for the statement $P(w) : w \in X$. Even more, we have De Morgan's Laws for the relative complements of $X \cup Y$ and $X \cap Y$ in W.

Theorem 3.7.3 (De Morgan's Laws for Sets)**.** *Let $X \subseteq W$ and $Y \subseteq W$ be arbitrary sets.*

1.) *We have that $W \setminus (X \cup Y) = (W \setminus X) \cap (W \setminus Y)$.*

2.) *We have that $W \setminus (X \cap Y) = (W \setminus X) \cup (W \setminus Y)$.*

Proof. (1.) We will first establish the inclusion $W \setminus (X \cup Y) \subseteq (W \setminus X) \cap (W \setminus Y)$. Given any element $w \in W \setminus (X \cup Y)$, we have that $w \in W$ and $w \notin X \cup Y$ by definition of the relative complement. Consequently, we must have that $w \notin X$ and $w \notin Y$. But this implies that $w \in W \setminus X$ and $w \in W \setminus Y$ so that $w \in (W \setminus X) \cap (W \setminus Y)$. Conversely, suppose that $w \in (W \setminus X) \cap (W \setminus Y)$. By definition of the intersection, we have that $w \in W \setminus X$ and $w \in W \setminus Y$. By definition of the relative complement, we have that $w \in W$ and $w \notin X$ and $w \notin Y$ so that $w \in W$ and $w \notin X \cup Y$.

(2.) We will first establish the inclusion $W \setminus (X \cap Y) \subseteq (W \setminus X) \cup (W \setminus Y)$. Given any element $w \in W \setminus (X \cap Y)$, we have that $w \in W$ and $w \notin X \cap Y$ by definition of the relative complement. Consequently, we must have that either $w \notin X$ or $w \notin Y$. But this implies that $w \in W \setminus X$ or $w \in W \setminus Y$ so that $w \in (W \setminus X) \cup (W \setminus Y)$. Conversely, suppose that $w \in (W \setminus X) \cup (W \setminus Y)$. By definition of the union, we have that $w \in W \setminus X$ or $w \in W \setminus Y$. Consequently, we have that $w \in W$ and either $w \notin X$ or $w \notin Y$. Either way, it follows that $w \notin X \cap Y$ so that $w \in W \setminus (X \cap Y)$. □

Often, we will simultaneously handle more sets than simply a pair; in this case, it is easiest to adopt the following notation. Let $X_1, X_2, \ldots, X_n$ be arbitrary sets such that $X_i \subseteq W$ for each integer $1 \leq i \leq n$. Each set X_i is **indexed** by an integer subscript $0 \leq i \leq n$. Consider the union

$$\bigcup_{i=1}^{n} X_i = X_1 \cup X_2 \cup \cdots \cup X_n = \{w \mid w \in X_i \text{ for some integer } 1 \leq i \leq n\}.$$

Once again, we note that the subscript i indicates the set X_i under consideration; the identification $i = 1$ beneath the union symbol indicates that we begin with $i = 1$; and the superscript n above the union symbol indicates that we end with $i = n$. Put another way, the elements of $\cup_{i=1}^{n} X_i$ are

precisely those elements $w \in W$ such that $w \in X_i$ for some integer $1 \leq i \leq n$, i.e., $w \in \cup_{i=1}^{n} X_i$ if and only if the quantified statement "$\exists i \in \{1, 2, \ldots, n\}$, $w \in X_i$" holds. Consider the intersection

$$\bigcap_{i=1}^{n} X_i = X_1 \cap X_2 \cap \cdots \cap X_n = \{w \mid w \in X_i \text{ for all integers } 1 \leq i \leq n\}.$$

Observe that $w \in \cap_{i=1}^{n} X_i$ if and only if the quantified statement "$\forall i \in \{1, 2, \ldots, n\}$, $w \in X_i$" holds.

Generally, De Morgan's Laws for Sets hold for finite unions and intersections of sets as follows.

Proposition 3.7.4. *Let $X_1, X_2, \ldots, X_n \subseteq W$ be arbitrary sets.*

1.) *We have that $W \setminus (X_1 \cup X_2 \cup \cdots \cup X_n) = (W \setminus X_1) \cap (W \setminus X_2) \cap \cdots \cap (W \setminus X_n)$.*

2.) *We have that $W \setminus (X_1 \cap X_2 \cap \cdots \cap X_n) = (W \setminus X_1) \cup (W \setminus X_2) \cup \cdots \cup (W \setminus X_n)$.*

By appealing to our dictionary between logic and set theory, we may also prove many important properties of functions. We remind the reader that a function $f : X \to Y$ is a subset of the Cartesian product $X \times Y$ with the additional property that for each element $x \in X$, there exists one and only one element $f(x) = y \in Y$ such that $(x, f(x)) \in f$. Each function $f : X \to Y$ gives rise to a set $\text{range}(f) = \{f(x) \mid x \in X\}$ of all **images** of elements of X under f. We refer to the function $f : X \to Y$ as **injective** provided that the condition $f(x) = f(y)$ implies that $x = y$ for all elements $f(x) \in \text{range}(f)$. Likewise, we refer to the function $f : X \to Y$ as **surjective** provided that $Y = \text{range}(f)$, i.e., for every element $y \in Y$, there exists an element $x \in X$ such that $y = f(x)$.

Proposition 3.7.5. *Let $f : X \to Y$ be any function between any two sets X and Y.*

(a.) *If f is injective, then $f^{-1}(f(V)) = V$ for any set $V \subseteq X$.*

(b.) *If f is surjective, then $f(f^{-1}(W)) = W$ for any set $W \subseteq Y$.*

Proof. 1.) By Exercise 3.9.16, it suffices to prove that $f^{-1}(f(V)) \subseteq V$. Let x be an arbitrary element of $f^{-1}(f(V))$. By definition of the inverse image $f^{-1}(f(V))$ of $f(V)$, this means that $f(x) \in f(V)$. By definition of the image $f(V)$, we have that $f(x) = f(v)$ for some element $v \in V$. Last, by assumption that f is injective and $V \subseteq X$, we conclude that $x = v$, hence x is an element of V.

(2.) By Exercise 3.9.16, it suffices to prove that $W \subseteq f(f^{-1}(W))$. Let w be any element of W. By assumption that f is surjective and $W \subseteq Y$, there exists an element $x \in X$ such that $w = f(x)$. By definition of the inverse image $f^{-1}(W)$, it follows that $x \in f^{-1}(W)$. By definition of the image $f(f^{-1}(W))$, we conclude that $w = f(x)$ for some element $x \in f^{-1}(W)$ so that $w \in f(f^{-1}(W))$. □

Conversely, if $f^{-1}(f(V)) = V$ holds for any set $V \subseteq X$, then $f : X \to Y$ must be injective; likewise, if $f(f^{-1}(W)) = W$ for any set $W \subseteq Y$, then f must be surjective (cf. Exercise 3.9.17).

3.8 Chapter 3 Overview

One of the most useful tools in mathematics is the **Principle of Mathematical Induction**. Collectively, the Principle of Mathematical Induction contains the (equivalent) Principle of Ordinary Induction and the Principle of Complete Induction. Explicitly, the Principle of Ordinary Induction asserts that if $P(n)$ is any statement about a non-negative integer n such that

(1.) $P(0)$ is a true statement and

(2.) $P(k+1)$ is a true statement whenever $P(k)$ is a true statement,

then $P(n)$ is a true statement for all non-negative integers n; the Principle of Complete Induction asserts that if $P(n)$ is any statement about a non-negative integer n such that

(1.) $P(0)$ is a true statement and

(2.) $P(k+1)$ is a true statement whenever $P(1), P(2), \ldots, P(k)$ are all true statements,

then $P(n)$ is a true statement for all non-negative integers n. One of the benefits of using complete induction is that its stronger hypotheses allow us more information with which to conveniently write proofs that might otherwise be awkward with ordinary induction (cf. Exercise 3.9.2). Even more, the Principle of Mathematical Induction appears also in the guise of the Well-Ordering Principle for the non-negative integers; this powerful tool guarantees that every nonempty set of non-negative integers admits a smallest element with respect to the total order $\leq$. Put another way, if $S \subseteq \mathbb{Z}_{\geq 0}$ is a nonempty set, then there exists an element $s_0 \in S$ such that $s_0 \leq s$ for all elements $s \in S$.

Using the Well-Ordering Principle, we may rigorously establish that for any integer a and nonzero integer b, there exist unique integers q and r such that $a = qb + r$ and $0 \leq r < |b|$; this fact is known as the Division Algorithm. We refer to the integer a as the **dividend**; b is the **divisor**; q is the **quotient**; and r is the **remainder**. Conventionally, if we obtain a remainder of zero when we divide an integer a by a nonzero integer b, then we say that b **divides** a; in this case, there exists a unique integer q such that $a = qb$, and we use the notation $b \mid a$. If a and b are any integers, then a nonzero integer c is called a **common divisor** of a and b if it holds that $c \mid a$ and $c \mid b$; the **greatest common divisor** of a and b is the unique integer $d = \gcd(a, b)$ such that

(a.) $d \mid a$ and $d \mid b$, i.e., d is a common divisor of a and b and

(b.) if c is any common divisor of a and b, then $c \mid d$.

We say that a and b are **relatively prime** if and only if $\gcd(a, b) = 1$. Bézout's Identity asserts that there exist integers x and y such that $\gcd(a, b) = ax + by$; the Euclidean Algorithm is one method from which the integers x and y guaranteed by Bézout's Identity can be obtained.

By the Division Algorithm, for any positive integer n, we may partition the integers $\mathbb{Z}$ into distinct equivalence classes determined by the unique remainder of an integer **modulo** n. Explicitly, we say that two integers a and b are **equivalent modulo** n if and only if $b - a$ is divisible by n; if this is the case, then we write $b \equiv a \pmod{n}$. One can verify that equivalence modulo n induces an equivalence relation R_n on the integers defined by $(a, b) \in R_n$ if and only if $b \equiv a \pmod{n}$; the distinct equivalence classes of $\mathbb{Z}$ modulo R_n are given by $\{qn + r \mid q \in \mathbb{Z}\}$ for each integer $0 \leq r \leq n - 1$; and the collection $\mathbb{Z}_n$ of equivalence classes of $\mathbb{Z}$ modulo n admits operations of addition and multiplication that together comprise the so-called **modular arithmetic**. Explicitly, if $b \equiv a \pmod{n}$ and $d \equiv c \pmod{n}$, then we have that $b + d \equiv a + c \pmod{n}$ and $bd \equiv ac \pmod{n}$.

3.9 Chapter 3 Exercises

The Principle of Mathematical Induction

If X is an arbitrary set, then the **power set** of X is the set $P(X) = \{Y \mid Y \subseteq X\}$, i.e., it is the collection of all subsets of X. Explicitly, if $X = \{x, y\}$, then $P(X) = \{\varnothing, \{x\}, \{y\}, \{x, y\}\}$.

Exercise 3.9.1. Let X be an arbitrary finite set with power set $P(X)$.

(a.) Use ordinary induction on $n = |X|$ to prove that $|P(X)| = 2^{|X|}$.

(b.) Let 2^X denote the collection of all functions $f : X \to X$. Exhibit an explicit bijection between $P(X)$ and 2^X; then, conclude from part (a.) above that $|2^X| = 2^{|X|}$.

One of the most curious objects in mathematics is the sequence $(F_n)_{n\geq 0}$ of **Fibonacci numbers** that are defined recursively by $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$. We refer to F_n as the nth Fibonacci number. Quite astoundingly, the Fibonacci numbers appear abundantly in nature.

Exercise 3.9.2. Let F_n denote the nth Fibonacci number.

(a.) Prove that $F_n < 2^n$ for each integer $n \geq 0$.

(b.) Prove that $F_{n+1}F_{n-1} = F_n^2 + (-1)^n$ for each integer $n \geq 2$.

(c.) Prove that $\gcd(F_n, F_{n+1}) = 1$ for all integers $n \geq 0$.

Exercise 3.9.3. Prove that the Principle of Ordinary Induction and the Principle of Complete Induction are equivalent to one another by completing the following two steps.

(1.) Given any statement $P(n)$ involving a non-negative integer n, let $Q(n)$ be the statement that $P(k)$ holds for all integers $1 \leq k \leq n$. Use the Principle of Ordinary Induction to prove that the statement $Q(n)$ is true for all integers $n \geq 0$, hence $P(n)$ is true for all integers $n \geq 0$. Unravelling this shows that ordinary induction implies complete induction.

(**Hint:** Observe that $Q(0)$ is vacuously true, hence we may assume that $Q(n)$ is true. By definition, this means that $P(k)$ is true for all integers $1 \leq k \leq n$. What about $P(n+1)$?)

(2.) Given any statement $P(n)$ involving a non-negative integer n, let $Q(n)$ be the statement that $P(k)$ holds for some integer $1 \leq k \leq n$. Use the Principle of Complete Induction to prove that the statement $Q(n)$ is true for all integers $n \geq 0$, hence $P(n)$ is true for all integers $n \geq 0$. Unravelling this shows that complete induction implies strong induction.

(**Hint:** Observe that $Q(0)$ is vacuously true, hence we may assume that $Q(k)$ is true for all integers $1 \leq k \leq n$; in particular, $P(1)$ is true. What does this say about $Q(n+1)$?)

Exercise 3.9.4. Prove that the Well-Ordering Principle and the Principle of Ordinary Induction are equivalent to one another by completing the following three steps.

(1.) Prove that 0 is the smallest non-negative integer with respect to $\leq$.

(2.) Prove that if $S \subseteq \mathbb{Z}_{\geq 0}$ satisfies $0 \in S$ and $n + 1 \in S$ whenever $n \in S$, then $\mathbb{Z}_{\geq 0} \subseteq S$.

(3.) Conclude that the Well-Ordering Principle implies the Principle of Ordinary Induction; then, use Exercise 3.9.3 and the proof of the Well-Ordering Principle to conclude that the Principle of Ordinary Induction implies the Well-Ordering Principle.

The Division Algorithm

Exercise 3.9.5. Recall that a positive integer p is **prime** if and only if the only integers that divide p are $\pm p$ and 1. Prove that if a and b are any integers such that $p \mid ab$, then $p \mid a$ or $p \mid b$.

(**Hint:** We may assume that $p \nmid a$ and show that $p \mid b$; now, use Bézout's Identity.)

Exercise 3.9.6. Let a, b, and c be any integers. Prove that if $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Exercise 3.9.7 (Fundamental Theorem of Arithmetic)**.** Let a be a positive integer. Prove that

(a.) there exist (not necessarily distinct) prime numbers $p_1, \ldots, p_k$ such that $a = p_1 \cdots p_k$ and

(b.) the primes $p_1, \ldots, p_k$ are unique in the sense that if $a = q_1 \ldots q_\ell$, then we must have that $\ell = k$ and $\{p_1, \ldots, p_k\} = \{q_1, \ldots, q_k\}$ (i.e., $q_1, \ldots, q_k$ are simply a rearrangement of $p_1, \ldots, p_k$).

(**Hint:** Consider the collection N of positive integers that do *not* possess such a prime factorization. Use the Well-Ordering Principle to show that if N is nonempty, then there exists a smallest element n with respect to $\leq$. What can be said about the factors of n? Conclude that N must be empty, hence the existence is established. On the matter of uniqueness, proceed by induction on k.)

Exercise 3.9.8. Prove that every nonzero integer a can be written as $a = \pm p_1^{e_1} \ldots p_n^{e_n}$ for some distinct prime numbers $p_1, \ldots, p_n$ and unique non-negative integers $e_1, \ldots, e_n$ such that

Given any integers a and b, the **least common multiple** $\operatorname{lcm}(a, b)$ of a and b can be defined in a manner analogous to the greatest common divisor of a and b. Explicitly, we say that an integer m is a **multiple** of a if and only if $a \mid m$. Consequently, m is a **common multiple** of a and b if and only if $a \mid m$ and $b \mid m$; a least common multiple of a and b is an integer $\ell = \operatorname{lcm}(a, b)$ such that

(1.) $a \mid \ell$ and $b \mid \ell$, i.e., ℓ is a common multiple of a and b and

(2.) if ℓ' is any common multiple of a and b, then $\ell \mid \ell'$.

Exercise 3.9.9. Prove that the least common multiple $\operatorname{lcm}(a, b)$ is unique up to sign.

By the Fundamental Theorem of Arithmetic, for any positive integers a and b, there exist prime numbers $p_1, \ldots, p_k$ and unique non-negative integers $e_1, \ldots, e_k, f_1, \ldots, f_k$ such that $a = p_1^{e_1} \cdots p_k^{e_k}$ and $b = p_1^{f_1} \cdots p_k^{f_k}$. Consider these prime factorizations of a and b for the next three exercises.

Exercise 3.9.10. Prove that $\gcd(a, b) = p_1^{\min\{e_1, f_1\}} \cdots p_k^{\min\{e_k, f_k\}}$.

Exercise 3.9.11. Prove that $\operatorname{lcm}(a, b) = p_1^{\max\{e_1, f_1\}} \cdots p_k^{\max\{e_k, f_k\}}$.

Exercise 3.9.12. Conclude from Exercises 3.9.10 and 3.9.11 that $ab = \gcd(a, b) \operatorname{lcm}(a, b)$.

Fundamental Properties of Set Operations

Exercise 3.9.13. Let W be an arbitrary set. Let $X \subseteq W$ and $Y \subseteq W$ be arbitrary subsets of W.

(a.) Prove that for any subset $Z \subseteq W$ such that $Z \supseteq X$ and $Z \supseteq Y$, it follows that $Z \supseteq X \cup Y$. Conclude that $U = X \cup Y$ is the "smallest" subset of W containing both X and Y.

(b.) Prove that for any subset $Z \subseteq W$ such that $Z \subseteq X$ and $Z \subseteq Y$, it follows that $Z \subseteq X \cap Y$. Conclude that $I = X \cap Y$ is the "largest" subset of W contained in both X and Y.

Consider the relative complement $X' = W \setminus X$ of X in W. We may sometimes refer to X' simply as the **complement** of X if we are dealing only with subsets of W, i.e., if W is our universe.

(c.) Prove that $Y \setminus X = Y \cap X'$. Use part (b.) above to conclude that $C = Y \cap X'$ is the "largest" subset of W that is contained in Y and disjoint from X.

Exercise 3.9.14. Consider any function $f : X \to Y$ from a set X to a set Y.

(a.) Prove that $f(U \cup V) = f(U) \cup f(V)$ for any sets $U, V \subseteq X$.

(b.) Prove that $f(\cup_{i \in I} V_i) = \cup_{i \in I} f(V_i)$ for any index set I and any sets $V_i \subseteq X$.

(c.) Prove that $f(U \cap V) = f(U) \cap f(V)$ for any sets $U, V \subseteq X$.

(d.) Prove that $f(\cap_{i \in I} V_i) = \cap_{i \in I} f(V_i)$ for any index set I and any sets $V_i \subseteq X$.

(e.) Prove that $f^{-1}(V \cup W) = f^{-1}(V) \cup f^{-1}(W)$ for any sets $V, W \subseteq Y$.

(f.) Prove that $f^{-1}(\cup_{i \in I} W_i) = \cup_{i \in I} f^{-1}(W_i)$ for any index set I and any sets $W_i \subseteq Y$.

(g.) Prove that $f^{-1}(V \cap W) = f^{-1}(V) \cap f^{-1}(W)$ for any sets $V, W \subseteq Y$.

(h.) Prove that $f^{-1}(\cap_{i \in I} W_i) = \cap_{i \in I} f^{-1}(W_i)$ for any index set I and any sets $W_i \subseteq Y$.

Exercise 3.9.15. Let X be any set. Consider the diagonal function $\delta_X : X \to X \times X$ defined by $\delta_X(x) = (x, x)$ and the diagonal $\Delta_X = \{(x, x) \mid x \in X\}$ relation on X. Prove that $\Delta_X = \delta_X(X)$.

Exercise 3.9.16. Let $f : X \to Y$ be any function between any two sets X and Y.

(a.) Prove that $V \subseteq f^{-1}(f(V))$ for any set $V \subseteq X$.

(b.) Exhibit sets $V \subseteq X$ and Y and a function $f : X \to Y$ such that $f^{-1}(f(V)) \not\subseteq V$.
(**Hint:** By Proposition 3.7.5, $f : X \to Y$ cannot be injective.)

(c.) Prove that $f(f^{-1}(W)) \subseteq W$ for any set $W \subseteq Y$.

(d.) Exhibit sets X and $W \subseteq Y$ and a function $f : X \to Y$ such that $W \not\subseteq f(f^{-1}(W))$.
(**Hint:** By Proposition 3.7.5, $f : X \to Y$ cannot be surjective.)

Exercise 3.9.17. Let $f : X \to Y$ be any function between any two sets X and Y.

(a.) Prove that if $f^{-1}(f(V)) = V$ for any set $V \subseteq X$, then f is injective.
(**Hint:** If $f(x_1) = f(x_2)$, then consider the set $V = \{x_1\}$.)

(b.) Prove that if $f(f^{-1}(W)) = W$ for any set $W \subseteq Y$, then f is surjective.
(**Hint:** Consider the set $W = Y$; then, use the definition of $f(f^{-1}(W))$.)

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.