CHAPTER 1 — FUNDAMENTALS

1 The Principle of Induction

We open this chapter with a discussion of the integers. This topic is typically seen in a course on elementary number theory, but its consequences are important enough to our purposes to warrant including some of it here. In all that follows, we will assume the familiar properties of integer addition and multiplication. It is customary to denote the set of all integers by the symbol $\mathbb{Z}$, a stylized form of the first letter in "*zahlen*," the German word for "numbers.". It is also customary to let $\mathbb{Z}^+$ denote the set of positive integers (the so-called *counting numbers*) and to let $\mathbb{Z}^*$ denote the nonzero integers. There are no universally accepted symbols for the negative integers or the so-called *nonnegative integers* (the set $\mathbb{Z}^+ \cup \{0\}$). In these notes, we will let $\mathbb{Z}^-$ denote the negative integers and will let $\mathbb{W}$ denote the nonnegative integers (which are sometimes called *whole numbers*).

Suppose that $S \subseteq \mathbb{Z}^+$ contains the number 1. Suppose further that, whenever we know $k \in S$, we can somehow *prove* that $k+1 \in S$. What can we conclude about the set S? Since we know $1 \in S$, our assumption tells us that we can prove $2 \in S$. Since we know $2 \in S$, we can prove that $3 \in S$, and so on, progressing through the positive integers. It seems reasonable to claim that S must contain *every* positive integer. Of course, we cannot prove such a claim by the "stepping" method the properties of S provide; we can only show with certainty that S contains every positive integer up to $n+1$. However, we can do this for *any* $n \in \mathbb{Z}^+$; and this does provide compelling evidence that S contains every positive integer. We will choose to *assume* that this is the case by imposing an axiom on the positive integers.

Axiom 1 *(Principle of Induction)*
If $S \subseteq \mathbb{Z}^+$ has the properties that

1. $1 \in S$
2. *If $k \in S$, then $k+1 \in S$*

then $S = \mathbb{Z}^+$.

The Prinicple of Induction is one of the foundational axioms on which the set of integers along with integer addition, multiplication, and subtraction are formally constructed. This process, while interesting in its own right, is not germane to our purposes and will be left for another course. The Principle of Induction provides us with a powerful proof technique called the *method of mathematical induction*. Here is a summary of what the method is and how it works.

Suppose you have a proposition P concerning the positive integers. Let S be the set of all positive integers for which P is true. If you can prove that S satisfies Conditions (1) and (2) of the Principle of Induction, then you may conclude that S contains every positive integer. That is, you may conclude that the proposition P holds true for every positive integer. Let's consider an example of this method in action.

Example 2 *Prove that for any positive integer n, we have*

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$$

Solution. Note that we have a proposition P concerning the positive integers — we claim that for every positive integer n, the equation

$$1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}$$

is true. For a proof by mathematical induction, let S denote the set of all positive integers for which P holds true. We want to prove that $S = \mathbb{Z}^+$. We will do this by proving that S satisfies the two conditions of the Principle of Induction. First, note that, if $n = 1$, then we have

$$\sum_{j=1}^{1} j = 1 = \frac{(1)(1+1)}{2}$$

Thus, P holds true when $n = 1$, and we therefore know that $1 \in S$. The first condition of the Principle of Induction has been met. Next, suppose that $k \in S$. (This assumption is called the *induction hypothesis*.) To meet the second condition, we must somehow prove that this allows us to conclude $k + 1 \in S$. Now, assuming $k \in S$ means that the proposition P holds true for k. In other words, we are assuming that

$$\sum_{j=1}^{k} j = \frac{k(k+1)}{2}$$

We must use this assumption to establish that proposition P also holds true for $k + 1$. Observe that

$$\begin{aligned}
\sum_{j=1}^{k+1} j &= 1 + 2 + ... + k + k + 1 = (1 + 2 + ... + k) + (k + 1) && \text{(Integer addition is associative.)} \\
&= \sum_{j=1}^{k} j + (k + 1) \\
&= \frac{k(k+1)}{2} + (k + 1) && \text{(Proposition } P \text{ holds true for } k.) \\
&= \frac{k(k+1) + 2(k+1)}{2} \\
&= \frac{(k+1)[(k+1)+1]}{2}
\end{aligned}$$

We have established that *assuming* proposition P holds true for k allows us to *prove* proposition P holds true for $k + 1$. We have therefore shown that *IF* $k \in S$, *THEN* $k + 1 \in S$; and Condition (2) of the Principle of Induction has been met. We may conclude that $S = \mathbb{Z}^+$; in other words, we may conclude that proposition P holds true for all positive integers.

****

When we are using the method of mathematical induction, we usually do not take the time to explicitly identify the set S, although there is nothing wrong with doing so. Here is an example of how a seasoned mathematician would go about using the method of induction.

Example 3 *Prove that any nonempty n-element set X has exactly 2^n subsets.*

Solution. We will accomplish this proof by mathematical induction on the number of elements in X. Suppose that X is any set that contains exactly one element. It follows that X is a singleton and therefore has exactly two subsets, namely X and $\varnothing$. Consequently, when X contains exactly one element, we know that X has exactly 2^1 subsets.

Suppose now that any set X containing exactly k elements has exactly 2^k subsets. Let Y be any set containing exactly $k + 1$ elements, and let $a \in Y$. It follows that $X = Y - \{a\}$ contains exactly k elements; hence, we know by assumption that X has exactly 2^k subsets. Suppose that $U \subseteq Y$. Either $a \in U$ or $a \notin U$. If $a \notin U$, then we know that $U \subseteq X$. If $a \in U$, then there is exactly one $V \subseteq X$ such that $U = V \cup \{a\}$ (namely the set $V = U - \{a\}$). Consequently, Y must have exactly 2^k subsets which do not contain a and must have exactly 2^k subsets which do contain a. Therefore, we may conclude that Y has exactly $2^k + 2^k = 2(2^k) = 2^{k+1}$ subsets. We have thus proven the statement by mathematical induction.

****

The specific arguments used in Example 2 differ considerably from those used in Example 1, but the method remains the same. In Example 2, our set S is the collection of all positive integers for which the desired conclusion holds true. That is, $n \in S$ if and only if every set containing exactly n elements has exactly 2^n subsets. We establish that $1 \in S$ in the first paragraph of the proof. We state our induction hypothesis in the first sentence of the second paragraph. The remainder of the second paragraph establishes a link between our induction hypothesis and sets with $k+1$ elements.

There is a useful variation on the Principle of Induction, known as the *Principle of Total Induction*, which is sometimes more convenient to use.

Axiom 4 *(Principle of Total Induction)*
If $S \subseteq \mathbb{Z}^+$ has the properties that

1. $1 \in S$

2. If $1 \leq m \leq n \in S$, *then* $n+1 \in S$

then $S = \mathbb{Z}^+$.

The only difference between the Axiom of Induction and the Axiom of Total Induction lies in the conditional criterion. Under the Axiom of Induction, we must establish that $n \in S$ implies $n+1 \in S$. However, under the Axiom of Total Induction, we must establish that the *collection* $\{1, 2, ..., n-1, n\} \subseteq S$ implies that $n+1 \in S$. This might seem harder to do, but there are circumstances where Total Induction is an easier assumption to work with. Fortunately, the Axiom of Total Induction is *logically equivalent* to the Axiom of Induction. This means that we can *assume* the Axiom of Induction and *prove* the Axiom of Total Induction as a theorem, or we can *assume* the Axiom of Total Induction and *prove* the Axiom of Induction as a theorem. The next two results establish this equivalence.

Theorem 5 *The Principle of Induction implies the Principle of Total Induction.*

We will assume the Axiom of Induction is true and prove the Axiom of Total Induction as a theorem. To this end, assume $S \subseteq \mathbb{Z}^+$ meets the two criteria of the Axiom of Total Induction. We will use our assumption that the Axiom of Induction is true to *prove* that $S = \mathbb{Z}^+$. Now, assuming that S meets the two criteria of the Axiom of Total Induction means

Axiom 6 *1.* $1 \in S$

2. If $1 \leq m \leq n \in S$, *then* $n+1 \in S$

Does S meet the two criteria for the Axiom of Induction? The first criterion ($1 \in S$) is clearly met. What about the second criterion? If we only know that $n \in S$, are we able to deduce that $n+1 \in S$? In order to deduce this, we must first know that the collection $1 \leq m \leq n$ is a subset of S. To this end, suppose that $n \in S$. We know that $1 \in S$; consequently, the collection $1 \leq m \leq 1$ is a subset of S. This allows us to conclude that $2 \in S$. Now, we know that the collection $1 \leq m \leq 2$ is a subset of S; hence, we may conclude that $3 \in S$. Proceeding in this way, we may conclude that the collection $1 \leq m \leq n$ is a subset of S. Consequently, we may deduce that $n \in S$ implies $n+1 \in S$. Thus, the two criteria for the Axiom of Induction are met; and we may conclude that $S = \mathbb{Z}^+$.

QED

Theorem 7 *The Principle of Total Induction implies the Principle of Induction.*

We will assume the Axiom of Total Induction is true and prove the Axiom of Induction as a theorem. To this end, assume $S \subseteq \mathbb{Z}^+$ meets the two criteria of the Axiom of Induction. We will use our assumption that the Axiom of Total Induction is true to *prove* that $S = \mathbb{Z}^+$. Now, assuming that S meets the two criteria of the Axiom of Induction means

Axiom 8 *1.* $1 \in S$

2. If $n \in S$*, then* $n + 1 \in S$

Does S meet the two criteria for the Axiom of Total Induction? The first criterion ($1 \in S$) is clearly met. What about the second criterion? If we know that the collection $1 \leq m \leq n$ is a subset of S, are we able to deduce that $n + 1 \in S$? Well, if this collection is a subset of S, then it is certainly true that $n \in S$. Consequently, we may conclude that $n + 1 \in S$; and the two criteria for the Axiom of Total Induction have been met. We may conclude that $S = \mathbb{Z}^+$.

QED

Many people find the Principle of Induction to be a little fishy since its application requires something of a "leap of faith". There is another axiom frequently associated with the set of positive integers which is more intuitively palatable and quite useful in its own right.

Definition 9 *A nonempty subset X of real numbers is* ***well-ordered*** *provided every nonempty subset of X has a smallest element.*

There are many sets of real numbers which definitely are not well-ordered. For example, the set of negative integers is not well-ordered, since the set itself clearly has no smallest element. Likewise, the interval $[0, 1]$ is not well-ordered, since the subset

$$S = \left\{ \frac{1}{n} : n \in \mathbb{Z}^+ \right\}$$

has no smallest element. It is much harder to prove that a particular subset *is* well-ordered.

Axiom 10 *(Well-Ordering Principle)*
The set of positive integers is well-ordered.

We take the Well-Ordering Principle as an axiom for the positive integers since it is clearly impossible to check every nonempty subset for this property; however, it certainly makes sense. It comes as a shock to many that the Well-Ordering Principle is actually logically equivalent to the Principle of Induction. That is, we can assume the Principle of Induction for the positive integers and prove that the Well-Ordering Principle holds true as a theorem, *or* we can assume the Well-Ordering Principle holds true for the positive integers and prove that the Principle of Induction holds true as a theorem. Let's take a look at how these proofs go. We will present one here and leave the other as an exercise.

Theorem 11 *The Principle of Induction implies the Well-Ordering Principle.*

Proof. We will assume that the Axiom of Induction is true and prove that every nonempty subset of positive integers has a least element. To this end, let S be a subset of positive integers that has no smallest element. We will prove that S must be empty. Let $T = \mathbb{Z}^+ - S$. It will suffice to prove that $T = \mathbb{Z}^+$. Now, either $1 \in S$, or $1 \in T$. Since 1 is the smallest positive integer, it would clearly be the smallest member of S if it were a member of S. We may therefore conclude that $1 \in T$.

As our induction hypothesis, suppose that n is a positive integer and suppose that the collection $1 \leq m \leq n$ is a subset of T. Consider the integer $n + 1$. If $n + 1 \in S$, then our assumption that $\{1, 2, ..., n - 1, n\} \subseteq T$ forces us to conclude that $n + 1$ is the smallest member of S — contrary to our assumption that S has no smallest member. We must therefore conclude that $\{1, 2, ..., n - 1, n\} \subseteq T$ implies $n + 1 \in T$. The Axiom of Total Induction therefore allows us to conclude that $T = \mathbb{Z}^+$, as desired.

Notice that we used the Principle of Total Induction in the last proof rather than the Principle of Induction. Since these axioms are equivalent, there is no problem with this strategy. Furthermore, it is quite a bit harder to prove this theorem using only the Principle of Induction. (Try it yourself.)

EXERCISES FOR SECTION 1

1. Is the interval $[1, 2]$ well-ordered?
2. Is the set of positive prime numbers well-ordered?
3. Is the empty set well-ordered?
4. Suppose that X is a nonempty set of real numbers and let $Y \subseteq X$ be nonempty. Prove that if X is well-ordered, then Y is well-ordered.
5. Is the converse of Problem 4 also true?
6. Use the Principle of Induction to prove that
$$\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}$$
7. Use the Principle of Induction to prove that
$$\sum_{j=1}^{n} j^3 = \frac{n^2(n+1)^2}{4}$$
8. Let r be any real number other than 1. Use the Principle of Induction to prove that, for any positive integer n, we have
$$\sum_{j=0}^{n} r^j = \frac{r^{n+1} - 1}{r - 1}$$
9. Prove that the Well-Ordering Principle implies the Principle of Induction. Hint: Suppose that $T \subseteq \mathbb{Z}^+$ satisfies the two criteria for the Principal of Induction. Assume that $S = \mathbb{Z}^+ - T$ is not empty and use the Well-Ordering Principle to obtain a contradiction.
10. For any fixed integer m, prove that the set $X = \{a \in \mathbb{Z} : m \leq a\}$ is well-ordered. (This is called the *Generalized Well-Ordering Principle.*) Hint: For any nonempty $Y \subseteq X$, consider the set $S = \{b - m : b \in Y\}$.

2 Divisibility

In this section, we will investigate the notion of divisibility in the integers. To begin, we will say that a nonzero integer a *divides* an integer b provided there exists an integer k such that $b = ak$. When this is the case, we will refer to a as a *factor* of b and say that b is a *multiple* of a. It is customary to use the notation $a|b$ to indicate that a divides b.

For example, we know that $6|24$ since $24 = 6 \cdot 4$ and we know that $9|72$ since $72 = 9 \cdot 8$. We know that 8 *does not* divide 12 since there is no integer k such that $12 = 8k$. NOTE: The symbol $a|b$ does *not* have the same meaning as the symbol a/b. When necessary, we will use a/b to represent the *fraction* a divided by b. The symbol $a|b$ represents a statement about a relationship between a and b (namely that a is a factor of b) while the symbol a/b represents a number.The theorem below lists many of the fundamental properties the concept of divisibility brings to the table. We will present proofs for three and leave the rest as exercises.

Theorem 12 *Let a, b, and c be arbitrary integers.*

1. *Every nonzero integer divides itself.*
2. *The integer 1 divides every integer.*
3. *Every nonzero integer divides 0.*
4. *If $a|b$ and $b|c$, then $a|c$.*
5. *We have $a|b$ if and only if $a|(-b)$.*
6. *If $a|b$ and $a|c$, then $a|(bx+cy)$ for any integers x and y.*
7. *We have $a|b$ if and only if $(-a)|b$.*
8. *If $a|b$ and $b|a$, then $a = \pm b$.*

Proof. Let us prove Claim 4. Suppose that $a|b$ and $b|c$. We want to prove that $a|c$. This means that we must find an integer k such that $c = ak$. By assumption, there exist integers m and n such that $b = am$ and $c = bn$. Consequently, we know that

$$c = bn \Longrightarrow c = (am)n \Longrightarrow c = a(mn)$$

since integer multiplication is associative. We can let $k = mn$.

Let us prove Claim 5. Since Claim (5) is an "if and only if" statement, we know that it is actually two conditional statements: IF $a|b$ THEN $a|(-b)$ and IF $a|(-b)$ THEN $a|b$. We must prove both statements. First, suppose that $a|b$. This there exists an integer m such that $b = am$. Consequently, since $-b = (-1)b$, we know that

$$-b = (-1)b \Longrightarrow -b = (-1)(am) \Longrightarrow -b = a(-1)(m) \Longrightarrow -b = a(-m)$$

since integer multiplication is both commutative and associative. Hence, we know that $-b = ak$ for some integer k; and we may conclude that $a|(-b)$. Conversely, suppose that $a|(-b)$. There exists an integer k such that $-b = ak$. Since $b = (-1)(-b)$, we know that

$$b = (-1)(-b) \Longrightarrow b = (-1)(ak) \Longrightarrow b = a(-1)(k) \Longrightarrow b = a(-k)$$

since integer multiplication is both commutative and associative. Hence, we know that $b = am$ for some integer m; and we may conclude that $a|b$.

Let us prove Claim 8. Suppose that $a|b$ and $b|a$. It follows that there exist integers m and n such that $b = am$ and $a = bn$. It follows that $a = a(mn)$. This is certainly true if $a = 0$, but our assumption that $a|b$ precludes this possibility. Since $a \neq 0$, we know that $mn = 1$; and, since both m and n are integers, this tells us that $m = n = \pm 1$. Since $a = bn$, we may conclude that $a = \pm b$, as desired.

QED

The next result, known as the *Division Algorithm* is one of the most important properties of the integers. It verifies an observation we have all used since elementary school — When you divide one integer into another, you get a quotient plus a remainder. For example, when we divide 24 by 9, we get a quotient of 2 and a remainder of 6. In elementary school, we were taught to say that "9 goes into 24 two times, with 6 left over." This sentence translates into symbols as $24 = 2 \cdot 9 + 6$.

The proof of the Division Algorithm is a classic example of another way the Well-Ordering Principle is used in mathematical arguments. (It actually uses the Generalized Well-Ordering Principle appearing in Exercise 1.1.10.)

Theorem 13 *Let $m \in \mathbb{Z}^+$ be fixed. If $x \in \mathbb{Z}$, then there exist unique $q, r \in \mathbb{Z}$ such that $x = qm + r$ and $0 \leq r < m$.*

Proof. Consider the set $S = \{x - nm : n \in \mathbb{Z}\}$. We will first prove that S contains at least one nonnegative integer. If x is itself nonnegative, then this claim is obviously true — just let $n = 0$. If $x < 0$, then let $n = xm$. In this case, we know that $xm < 0$, and we know that

$$x - xm = x(1 - m) \geq 0$$

Since S always contains at least one nonnegative integer, we may consider the collection $T = \{u \in S : u \geq 0\}$. This set is nonempty which means T contains a smallest element by the Generalized Well-Ordering Principle. Call this element r. It is clear that $r = x - qm$ for some integer q, hence, we know that $x = qm + r$. Since $r \in T$, it is clear that $0 \leq r$.

Suppose by way of contradiction that $m \leq r$. Consider the integer $y = r - m$. Since we know $m > 0$, our assumption tells us that $r > y \geq 0$. Furthermore, we know that

$$y = r - m \Longrightarrow y = (x - qm) - m \Longrightarrow y = x - (q + 1)m$$

Therefore, we know that $y \in T$. However, this is impossible, since r is the *smallest* member of T. Consequently, we are forced to conclude that $r < m$.

To complete the proof, we need to show that the integers q and r are unique. To this end, suppose there also exist integers u and v such that $x = um + v$ and $0 \leq v < m$. It will suffice to prove that $q = u$ and $r = v$. Without loss of generality, we may assume that $u \leq q$. Observe that

$$qm + r = um + v \Longrightarrow (q - u)m + (r - v) = 0$$

Since $m > 0$, our assumption that $u \leq q$ forces us to conclude that $(q - u)m \geq 0$. Therefore, the last equation above tells us that $r - v \leq 0$; hence, we may conclude that $r \leq v$. Now, we also know that

$$v < m \Longrightarrow v < m + r \Longrightarrow 0 \leq v - r < m$$

Since the equation $(q - u)m + (r - v) = 0$ tells is that $v - r = (q - u)m$, we are now forced to conclude that $v - r = 0$ and $q - u = 0$. This tells us that $q = u$ and $r = v$, as desired.

QED

The Division Algorithm is, strictly speaking, not an algorithm. An algorithm is actually a step-by-step procedure for carrying out a particular operation or finding a particular result. The so-called division algorithm tells us that we can represent any integer as a quotient times an integer plus a remainder, but it provides no procedure for finding the quotient or remainder. The division algorithm is an example of an *existence theorem* — it tells us that the quotient and remainder exist, but does not directly tell us how to obtain them.

Definition 14 *Let a and m be integers. We say that an integer c is a* ***common factor*** *of a and m provided $c|a$ and $c|m$.*

Common factors are often called common *divisors*. There can be only finitely many common factor for any pair of integers *in which at least one is nonzero*; hence, every such pair of integers must have a *greatest* common factor. Since 1 is a common factor of any pair of integers, it follows that the greatest common factor of two integers (in which at least one is nonzero) is always positive. We will let $\texttt{GCF}(m, n)$ denote the greatest common factor of integers m and n.

Theorem 15 *Let a and m be integers with $m \neq 0$. If b is the greatest common factor of a and m, then there exist integers x and y such that $b = ax + my$.*

Proof. First, let $S = \{ax + my : x, y \in \mathbb{Z}\}$. There exist integers x and y such that $ax + my > 0$ (consider $a + m$ or $-(a + m)$). Consequently, the set $S \cap \mathbb{Z}^+$ is nonempty and therefore has a smallest element by the Well-Ordering Principle. Let $c = ax_0 + my_0$ be the smallest positive integer combination of a and m. We will prove that $c = b$. We first prove that c is a common factor of a and m. The Division Alorithm tells us that there exist unique integers q and r such that $0 \leq r < c$ and $m = qc + r$. Observe that

$$m = qc + r \quad \Longrightarrow \quad m = q(ax_0 + my_0) + r \quad \Longrightarrow \quad r = aqx_0 + m(qy_0 - 1)$$

Now, since $0 \leq r < c$, we know that $aqx_0 + m(qy_0 - 1) < c$. Therefore, since c is the *smallest positive* integer combination of a and m, we may conclude that $r = 0$. Hence, c is a divisor of m. A similar argument shows that c is a divisor of a as well.

Now, suppose that k is any common factor of a and m. We only need to show that k is a factor of c. However, this is easy, since we know there exist integers t and u such that $a = kt$ and $m = ku$. Indeed, this fact tells us that

$$c = ax_0 + my_0 = k(tx_0 + uy_0)$$

We may therefore conclude that $c = b$, as desired.

QED

Observe that $\texttt{GCF}(20, 30) = 10$. The previous theorem tells us that there must exist integers x and y such that $10 = 20x + 30y$. The theorem does not provide a direct way to determine these integers, but we can find some by trial and error. Indeed, observe that

$$10 = 20(-1) + 30(1) \qquad 10 = 20(-4) + 30(3) \qquad 10 = 20(8) + 30(-5)$$

We will conclude this section with a brief introduction to *modular arithmetic*, an application of the Division Algorithm which, first introduced by C.F. Gauss in the early 1800's, will be a great source of examples in the next chapter.

Definition 16 *Let n be a fixed positive integer and let a and b be arbitrary integers. We say that a is **congruent** to b **modulo** n provided $n|(a - b)$. We write $a \equiv b$ $\texttt{MOD}(n)$ if this is the case.*

For $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^*$, we know Theorem 7 above that $n|(a - b)$ if and only if $(-n)|(a - b)$; hence, our assumption that n be positive in the definition above is a matter of custom. As a few examples, note that $2 \equiv 8$ $\texttt{MOD}(3)$ since $3|(2 - 8)$. Likewise, note that $4 \equiv -10$ $\texttt{MOD}(7)$ since $7|(4 - (-10))$. The following result is a direct consequence of Theorem 7; hence, we will leave it as an exercise.

Lemma 17 *Let n be a fixed positive integer. For all integers a, b, and c, we have*

1. $a \equiv a$ $\texttt{MOD}(n)$
2. $a \equiv b$ $\texttt{MOD}(n)$ *if and only if}* $b \equiv a$ $\texttt{MOD}(n)$
3. *If* $a \equiv b$ $\texttt{MOD}(n)$ *and* $b \equiv c$ $\texttt{MOD}(n)$, *then* $a \equiv c$ $\texttt{MOD}(n)$.

Theorem 18 *Let n be a fixed positive integer and let a and b be arbitrary integers. We have $a \equiv b$ $\texttt{MOD}(n)$ if and only if a and b have the same remainder when divided by n.*

Proof. Suppose that $a \equiv b \ \texttt{MOD}(n)$. This implies that there exists an integer k such that $a - b = kn$. Now, by the Division Algorithm, we know that there exist integers q and r such that $a = qn + r$ and there exist integers p and $s$such that $b = pn + s$. It will suffice to prove that $r = s$. We know that

$$kn = a - b \Longrightarrow kn = (q - p)n + (r - s)$$

Now, the Division Algorithm also tells us that there exist integers u and v such that $a - b = un + v$, where $0 \leq v < n$. Furthermore, these integers are *unique*. Therefore, since we know that

$$a - b = kn + 0 \qquad a - b = (q - p)n + (r - s)$$

we may conclude that $r - s = 0$ (and that $q - p = k$ for that matter). This, of course, tells us that $r = s$ as desired.

Conversely, suppose that a and b have the same remainder when divided by n. By the Division Algorithm, this implies that there exist integers q and p and an integer $0 \leq r < n$ such that $a = qn + r$ and $b = pn + r$. Hence, we know

$$a - b = (q - p)n$$

We may therefore conclude that $a \equiv b \ \texttt{MOD}(n)$.

QED

We will use the previous theorem quite a bit in the next chapter. In fact, it gives us the perspective we normally use when working with modular arithmetic. As an example of this theorem in action, we know that $22 = 2 \cdot 8 + 6$ and $78 = 9 \cdot 8 + 6$; hence, we also know automatically that $22 \equiv 78 \ \texttt{MOD}(8)$. Likewise, we know that $218 \equiv 38 \ \texttt{MOD}(20)$, since $218 - 38 = 180$ and $20|180$. Consequently, we know automatically that 218 and 38 leave the same remainder when divided by 20. A quick check shows that the remainder is 18 for both.

In light of the previous theorem, when working with congruences, it is common to reduce the right-hand side to the remainder. For example, instead of writing $218 \equiv 38 \ \texttt{MOD}(20)$, we would usually reduce this to $218 \equiv 18 \ \texttt{MOD}(20)$. It is correct to write either, but reducing to the remainder will have some distinct advantages in the next chapter. The previous theorem also allows us to develop some basic *modular arithmetic* as well.

Corollary 19 *Let n be a fixed positive integer and let a,b, c, and d be integers. If $a \equiv b \ \texttt{MOD}(n)$ and $c \equiv d \ \texttt{MOD}(n)$, then $a + c \equiv b + d \ \texttt{MOD}(n)$ and $ac \equiv bd \ \texttt{MOD}(n)$.*

Proof. Let r be the remainder obtained when a and b are divided by n, and let s be the remainder when c and d are divided by n. There exist integers q and p such that $a = qn + r$ and $b = pn + r$. Likewise, there exist integers u and v such that $c = un + s$ and $d = vn + s$. Now, we know that

$$a + c = (q + u)n + (r + s) \qquad b + d = (p + v)n + (r + s)$$

There exist unique integers x and y such that $r + s = xn + y$, where $0 \leq y < n$. Hence, we know that $a + c$ and $b + d$ have the same remainder (namely y) when divided by n. We may therefore conclude that $a + c \equiv b + d \ \texttt{MOD}(n)$.

The proof for multiplication is similar and will be left as an exercise.

QED

Modular addition and multiplication have a number of uses. We will explore only a few of them here; many more can be found in texts on number theory. We conclude this section by considering two simple examples.

A *Fermat number* is an integer having the form $F_n = 2^{2^n} + 1$ for some positive integer n. Pierre Fermat introduced the Fermat numbers in his attempts to devise a method for generating prime numbers. He noticed that

$$F_1 = 5 \qquad F_2 = 17 \qquad F_3 = 257 \qquad F_4 = 65,537$$

are all prime (no mean feat for a person living in the 1600's). He then claimed that *all* such numbers are prime, but offered no proof. It turns out that he was incorrect. In fact, the very next Fermat number is composite, although it is so large that direct computation makes this almost impossible to determine directly. We will instead use modular arithmetic to help us. We will show that 641 divides this huge number without actually computing it.

Example 20 *Use modular arithmetic to show that* $2^{32} + 1 \equiv 0$ *MOD*(641).

Solution. Observe that $2^8 = 256$ is the largest positive integer power of 2 smaller than 641. Hence, we know that $2^8 \equiv 256$ MOD(641). Consequently, we know

$$2^8 \cdot 2^8 \equiv 256^2 \text{ MOD}(641) \Longrightarrow 2^{16} \equiv 154 \text{ MOD}(641)$$

since a quick computation shows that $256^2 = 102 \cdot 641 + 154$. Therefore, we also know that

$$2^{16} \cdot 2^{16} \equiv 154^2 \text{ MOD}(641) \Longrightarrow 2^{32} \equiv 640 \text{ MOD}(641)$$

since a quick computation shows that $154^2 = 36 \cdot 641 + 640$. It now follows that

$$2^{32} + 1 \equiv 640 + 1 \text{ MOD}(641) \Longrightarrow 2^{32} + 1 \equiv 0 \text{ MOD}(641)$$

****

As another example, let's consider a rule about divisibility we learned in elementary school: A positive integer n is divisible by 3 if and only if the sum of its digits is divisible by 3. For example, we know that 39 is divisible by 3 because $3 + 9 = 12$ is divisible by 3. Why is this rule true? Modular arithmetic provides a quick answer.

Example 21 *Use modular arithmetic to prove that a positive integer is divisible by* 3 *if and only if the sum of its digits is divisible by* 3.

Solution. Let n be a positive integer, and let d_k be the digit in the 10^k position of n ($0 \leq k < m$ for some positive integer m). Then we know that

$$n = d_0 + d_1 \cdot 10 + d_2 \cdot 10^2 + ... + d_{m-1} \cdot 10^{m-1}$$

Now, since $10 \equiv 1$ MOD(3), we know that $d_k \cdot 10^k \equiv d_k$ MOD(3). Therefore, we see that

$$n \equiv \left[d_0 + d_1 \cdot 10 + d_2 \cdot 10^2 + ... + d_{m-1} \cdot 10^{m-1}\right] \text{MOD}(3) \quad \Longrightarrow \quad n \equiv [d_0 + d_1 + d_2 + ... + d_{m-1}] \,\text{MOD}(3)$$

Consequently, n is divisible by 3 if and only if the sum of its digits is divisible by 3.

****

EXERCISES FOR SECTION 2

1. Prove Claims (1), (2), and (3) of Theorem 7.
2. Prove the remaining claims of Theorem 7.

3. Prove Lemma 12.
4. Explain why it is necessary to assume at least one integer is nonzero when discussing the greatest common factor of two integers.
5. Let m be an odd integer. Prove that $4|(m^2-1)$. (Thus, an odd square is always 1 larger than a multiple of 4.)
6. Prove that any positive integer n is divisible by 9 if and only if the sum of its digits is divisible by 9.
7. What conditions on the digits guarantee that a positive integer is divisible by 11?
8. Use modular arithmetic to find the remainder when 3^{40} is divided by 23. Hint: $3^6 \equiv -7$ $\texttt{MOD}(23)$.
9. Prove that $2^{37}-1$ is divisible by 223.
10. Let $n \in \mathbb{Z}^+$ be fixed and let $a, b, c, d \in \mathbb{Z}$ be such that $a \equiv b$ $\texttt{MOD}(n)$ and $c \equiv d$ $\texttt{MOD}(n)$. Prove that $ac \equiv bd$ $\texttt{MOD}(n)$.
11. Two integers m and n are *relatively prime* provided $\texttt{GCF}(m,n) = 1$. Suppose that p and a are relatively prime nonzero integers. Prove that, if $b \in \mathbb{Z}$ is such that $p|(ab)$, then $p|b$. (This result is called *Euclid's Lemma.*)
12. Give an example to show that Euclid's Lemma can fail if p and a are not relatively prime.
13. Let $m \in \mathbb{Z}$. Use Euclid's Lemma to prove that $2|m$ if and only if $2|m^2$.
14. Use Exercise 7 to prove that $\sqrt{2}$ is irrational. Hint: Assume that $\sqrt{2} = p/q$, where $p, q \in \mathbb{Z}$. Square both sides and show that p and q have 2 as a common factor. Cancel the 2 and repeat.
15. It is customary to let $\mathbb{Q}$ denote the set of rational numbers. Use the Division Algorithm to prove that, for any $x \in \mathbb{Q}$, there exist unique $m \in \mathbb{Z}$ and $r \in \mathbb{Q} \cap [0,1)$ such that $x = m + r$. Hint: Let $x = p/q$ where $p, q \in \mathbb{Z}$ and use the Division Alogrithm to divide p by q.
16. Prove the following statements are true:
    (a) If n is even, then $\texttt{GCF}(n, n+2) = 2$.
    (b) If n is odd, then $\texttt{GCF}(n, n+2) = 1$.
17. Let $n \in \mathbb{Z}^+$ be fixed and let $a, b \in \mathbb{Z}$ be such that $a \equiv b$ $\texttt{MOD}(n)$. Prove that any common divisor of a and n also divides b.
18. Let $n \in \mathbb{Z}^+$ be fixed and let $a, b \in \mathbb{Z}$ be such that $a \equiv b$ $\texttt{MOD}(n)$. Prove that $\texttt{GCF}(n, a) = \texttt{GCF}(n, b)$.
19. Let $n \in \mathbb{Z}^+$ be fixed and let $a, b, c \in \mathbb{Z}$. Prove that $a \equiv b$ $\texttt{MOD}(n)$ if and only if $ac \equiv bc$ $\texttt{MOD}(nc)$.
20. Let $n \in \mathbb{Z}^+$ be fixed and let $a, b, c \in \mathbb{Z}$ be such that $ac \equiv bc$ $\texttt{MOD}(n)$. If $d = \texttt{GCF}(n, c)$, then prove that $a \equiv b$ $\texttt{MOD}(n/d)$.

3 Relations

In this section, we will introduce one of the most important fundamental concepts used in abstract algebra — the notion of a *relation.* Relations play a key role in almost everything we will do, although this role is often subtle and easily overlooked. We begin with a definiiton.

Definition 22 *Let X and Y be sets. We define the* ***product*** *$X \times Y$ to be the set of all ordered pairs whose first coordinate comes from X and whose second coordinate comes from Y. In symbols, we write*

$$X \times Y = \{(a, b) : a \in X, b \in Y\}$$

The product $X \times X$ is often denoted by X^2.

As a quick example, suppose that $X = \{a, b, c\}$ and $Y = \{1, 2\}$. There are many products we can form from these two sets. For example, we have

- $X \times Y = \{(a, 1), (b, 1), (c, 1), (a, 2), (b, 2), (c, 2)\}$
- $Y \times X = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$
- $X^2 = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}$
- $Y^2 = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$
- $X \times Y^2 = \{[a, (1, 1)], [a, (1, 2)], [a, (2, 1)], [a, (2, 2)], [b, (1, 1)], [b, (1, 2)], [b, (2, 1)], [b, (2, 2)],$ $[c, (1, 1)], [c, (1, 2)], [c, (2, 1)], [c, (2, 2)]\}$

Since the elements of a product are ordered pairs, we do not consider $X \times Y$ to be equal to $Y \times X$ unless $X = Y$.

Definition 23 *Let X and Y be sets. A **binary relation** on X and Y is any nonempty subset θ of $X \times Y$ or $Y \times X$. The first coordinates of elements in θ form the **domain** of θ; the second coordinates form the **range** of θ.*

Consider the sets $X = \{a, b, c\}$ and $Y = \{1, 2\}$. Since $X \times Y$ and $Y \times X$ both contain six elements, we know there are exactly $2^6 - 1 = 63$ nonempty subsets of each product. Consequently, we know there are a total of 126 binary relations on X and Y. The binary relation

$$\theta = \{(a, 1), (b, 1), (b, 2)\} \subseteq X \times Y$$

has $D_\theta = \{a, b\}$ as its domain and has $R_\theta = \{1, 2\}$ as its range.

Relations play a key role in studying the structure of many mathematical objects. In the sections to follow, we will look closely at two important types of relations, namely equivalence relations and functions. These relations are distinguished by certain key properties they satisfy. In this section, we will introduce these properties.

Definition 24 *Let X be a set, and let $\theta \subseteq X^2$. We say θ is **reflexive** provided $(a, a) \in \theta$ for all $a \in X$.*

Example 25 *Let $Y = \{1, 2\}$. Which of the binary relations on Y is reflexive?*

Solution. We know that $Y \times Y$ contains fifteen nonempty subsets; hence, we know there are fifteen binary relations on Y. Only those relations which contain $(1, 1)$ and $(2, 2)$ will be reflexive. Consequently, the reflexive binary relations are

1. $\theta_1 = \{(1, 1), (2, 2)\}$
2. $\theta_2 = \{(1, 1), (2, 2), (1, 2)\}$
3. $\theta_3 = \{(1, 1), (2, 2), (2, 1)\}$
4. $\theta_2 = \{(1, 1), (2, 2), (1, 2), (2, 1)\}$

****

Example 26 *Let $\mathbb{R}$ denote the set of real numbers and let*

$$\theta = \{(x, y) \in \mathbb{R}^2 : xy > 0\} \qquad \alpha = \{(x, y) \in \mathbb{R}^2 : x - y = 0\}$$

Are either of these binary relations reflexive?

Solution. Notice that the set θ contains (x, x) as long as $x \neq 0$. The fact that $(0, 0) \notin \theta$ is enough to show that θ is not reflexive. On the other hand, since $x - x = 0$ for every real number x, we see that $(x, x) \in \alpha$ for all $x \in \mathbb{R}$. Therefore, we know that α is reflexive.

****

Definition 27 *Let X be a set, and let $\theta \subseteq X^2$. We say θ is **symmetric** provided $(a, b) \in \theta$ always implies $(b, a) \in \theta$.*

Example 28 *What are the symmetric binary relations on $Y = \{1, 2\}$?*

Solution. The condition for symmetry is different in kind from that for reflexivity. Reflexivity is an *unconditional* property in that (a, a) must be a member of the relation *for all* $a \in Y$. Symmetry is a *conditional* property: *IF* a pair (a, b) is a member of the relation, *THEN* (b, a) must be as well. The symmetric relations on Y are

$$\theta_1 = \{(1, 1)\} \qquad \theta_2 = \{(2, 2)\} \qquad \theta_3 = \{(1, 1), (2, 2)\}$$

$$\theta_4 = \{(1, 2), (2, 1)\} \qquad \theta_5 = \{(1, 1), (1, 2), (2, 1)\} \qquad \theta_6 = \{(2, 2), (1, 2), (2, 1)\}$$

$$\theta_7 = \{(1, 1), (2, 2), (1, 2), (2, 1)\}$$

****

Example 29 *Let $\mathbb{R}$ denote the set of real numbers and let*

$$\theta = \{(x, y) \in \mathbb{R}^2 : xy > 0\} \qquad \alpha = \{(x, y) \in \mathbb{R}^2 : x - y = 0\}$$

Are either of these binary relations symmetric?

Solution. Since $xy = yx$ in real number multiplication, IF $xy > 0$, THEN $yx > 0$ as well. Consequently, we know that IF $(x, y) \in \theta$, THEN $(y, x) \in \theta$; and we may conclude that θ is symmetric. Since $x - y = -(y - x)$ in real number subtraction, we know that IF $x - y = 0$, THEN $y - x = 0$ as well. Consequently, we know that IF $(x, y) \in \alpha$, THEN $(y, x) \in \alpha$; and we may conclude that α is symmetric.

****

Example 30 *Let $\mathbb{Z}$ denote the set of integers and let $\theta = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : n = m^2\}$. Is this binary relation reflexive or symmetric?*

Solution. Since $2 \neq 2^2$, we know that $(2, 2) \notin \theta$. Consequently, we know that θ is not reflexive. Now, the pair $(2, 4) \in \theta$ since $4 = 2^2$; however, the pair $(4, 2) \notin \theta$, since $2 \neq 4^2$. Consequently, we know that θ is not symmetric.

****

Definition 31 *Let X be a set, and let $\theta \subseteq X^2$. We say θ is **transitive** provided $(a, b), (b, c) \in \theta$ always implies $(a, c) \in \theta$.*

Like symmetry, transitivity is a conditional property. In elementary arithmetic, transitivity appears in the ordering of the real numbers as the *trichotomy* rule: For all real numbers a, b, c, IF $a \leq b$ and $b \leq c$, THEN $a \leq c$. In general, transitivity, when it holds, provides a way of "linking together" elements in a relation.

Example 32 *What are the transitive binary relations on $Y = \{1, 2\}$?*

Solution. The transitive relations will be

$$\theta_1 = \{(1,1)\} \qquad \theta_2 = \{(2,2)\} \qquad \theta_3 = \{(1,2)\} \qquad \theta_4 = \{(2,1)\}$$

$$\theta_5 = \{(1,1),(2,2)\} \qquad \theta_6 = \{(2,1),(1,1)\} \qquad \theta_7 = \{(1,2),(2,2)\} \qquad \theta_8 = \{(2,1),(2,2)\}$$

$$\theta_9 = \{(1,1),(2,1),(1,2),(2,2)\}$$

****

Example 33 *A group of ten families live along one side of a North-South road with each house exactly one-fifth mile apart. Consider the relation M on this set of ten families defined by $(p, q) \in M$ if and only if Family p lives at most one mile from Family q. Is M reflexive, symmetric, or transitive?*

Solution. This relation is certainly reflexive, since every family livesat most one mile from itself. It is certainly symmetric, because IF Family p lives at most one mile from Family q, THEN we know Family q lives at most one mile from Family p. However, M is not transitive. To see why, number the families consecutively starting with the northern-most one and just consider Family 1, Family 4, and Family 7. By construction, Family 1 lives 3/5 mile from Family 4 and Family 4 lives 3/5 mile from Family 7. Thus, we know that $(1, 4) \in M$ and we know that $(4, 7) \in M$. However, Family 1 lives 6/5 miles from Family 7. Consequently, $(1, 7) \notin M$; and we must conclude that M is not transitive.

****

Example 34 *Let $\mathbb{R}$ denote the set of real numbers and let*

$$\theta = \{(x, y) \in \mathbb{R}^2 : xy > 0\} \qquad \alpha = \{(x, y) \in \mathbb{R}^2 : x - y = 0\}$$

Are either of these binary relations transitive?

Solution. Let's look at the relation θ first. Suppose that $(a, b), (b, c) \in \theta$. Is it necessarily true that $(a, c) \in \theta$ as well? By assuming that $(a, b), (b, c) \in \theta$, we are assuming that $ab > 0$ and we are assuming that $bc > 0$. If $ab > 0$, then clearly $b \neq 0$. Consequently, we know that either $b > 0$ or $b < 0$. Now, if $b > 0$, it must be true that $a > 0$ and $c > 0$ as well since we know that $ab > 0$ and $bc > 0$. In this case, we therefore know that $ac > 0$. On the other hand, if $b < 0$, it must be true that $a < 0$ and $c < 0$ as well since we know that $ab > 0$ and $bc > 0$. In this case, we therefore know that $ac > 0$. Consequently, if $(a, b), (b, c) \in \theta$, we must conclude that $(a, c) \in \theta$ as well. Hence, we know that θ is transitive.

Now let's consider the relation α. Suppose that $(a, b), (b, c) \in \alpha$. Is it necessarily true that $(a, c) \in \alpha$ as well? By assuming that $(a, b), (b, c) \in \alpha$, we are assuming that $a - b = 0$ and we are assuming that $b - c = 0$. Consequently, we know that

$$a - c = (a - b) + (b - c) = 0 + 0 = 0$$

We must therefore conclude that $(a, c) \in \alpha$. Hence, we know that α is transitive.

1. **EXERCISES FOR SECTION 3**
2. Using Definition 1.1 as a guide, formally define $X \times Y \times Z$, where X, Y, and Z are sets.
3. If X, Y, and Z are sets, then is $X \times Y \times Z$ the same set as $(X \times Y) \times Z$? Explain your answer.
4. Let Y be a set. How do you think $\varnothing \times Y$ should be defined? Is this case already covered in Definition 1.1? Explain.
5. Let Y be a nonempty set. What is the difference between $\varnothing \times Y$ and $\{\varnothing\} \times Y$?
6. Let n be any positive integer and let $X_1, ...X_n$ be sets. We use the symbol $\prod_{j=1}^{n} X_j$ to denote the product of these sets (in the order given). Construct a formal definition for this symbol.
7. Let X be any set. Explain why every singleton binary relation $\theta = \{(x, y)\}$ on X is transitive. When is such a relation symmetric? What must be true of X for θ to be reflexive?
8. Let X be any set and let $R = \{(a, b), (c, d)\}$ be any two-element binary relation on X. Under what various conditions will R be transitive?
9. Let $E \subseteq \mathbb{Z} \times \mathbb{Z}$ be defined by $(m, n) \in E$ if and only if $m = kn$ for some $k \in \mathbb{Z}$. Prove that E is reflexive and transitive, but not symmetric.
10. Let $F \subseteq \mathbb{Z} \times \mathbb{Z}$ be defined by $(m, n) \in F$ if and only if $mn \geq 0$. Prove that E is reflexive and symmetric, but not transitive.
11. A student once argued with his instructor that reflexivity is implied by symmetry and transitivity. The argument went as follows: "Suppose that E is a binary relation on X which is symmetric and transitive. If $(x, y) \in E$, then $(y, x) \in E$ by symmetry; hence, $(x, x) \in E$ by transitivity. Thus E is reflexive." What important fact has the student overlooked?
12. Find a binary relation on $\mathbb{Z} \times \mathbb{Z}$ which is symmetric and transitive but not reflexive.
13. Find a binary relation on $\mathbb{Z} \times \mathbb{Z}$ which is reflexive and transitive but not symmetric.
14. Let $\mathbb{Q}$ denote the set of all rational numbers. Define a binary relation R on $\mathbb{Q}$ by $(x, y) \in R$ if and only if $x - y \in \mathbb{Z}$. Prove that R is reflexive, symmetric, and transitive.
15. Let $\mathcal{Q} = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : n \neq 0\}$. Define a binary relation C on $\mathcal{Q}$ by $[(a, b), (c, d)] \in C$ if and only if $ad = bc$. Prove that C is reflexive, symmetric, and transitive.

4 Equivalence Relations

When dealing with elements in a set, we have an intuitive idea of what equality should mean: If x and y represent elements of a set X, then x and y are equal provided they represent the same element. This intuitive idea may seem quite reasonable, but it is not always clear what the phrase "represent the same element" should mean. For example, we can think of the set $\mathcal{Q} = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : n \neq 0\}$ as representing the set of all rational numbers, where an element $(p, q) \in \mathcal{Q}$ represents the rational number p/q. In this set, the pairs $(1, 2)$ and $(2, 4)$ are definitely distinct; yet, we feel they should be "equal" since the rational numbers $1/2$ and $2/4$ are considered "equal.". This suggests that we should have some means at our disposal for equating elements which is more flexible than simple identification.

We will define equality in a typically mathematical fashion. We will take our intuition about what equality between elements in a set *should* mean, isolate certain properties this meaning implies, and then *define* elements to be equal precisely when these properties are met.

Thus, for the moment, suppose that we have a set X and a meaning for equality between elements of X. Let us see what properties our intuition tells us this equality should possess. Speaking formally, under our definition of equality, elements which are identified should be mathematically indistinguishable. Our definition of equality should provide us with rules specifying which elements are to become "indistinguishable". With this in mind, it is clear that, whatever our meaning for equality in X, every element of X should be equal to itself. If x is equal to y, then it should also be true that y should be equal to x. That is, if we cannot distinguish x from y, then we should not be able to distinguish y from x. It should also be clear that, if x is equal to y and y is equal to z, then x should be equal to z. It is upon these properties that we will base our definition of equality.

Definition 35 *A binary relation θ on a set X is called an **equivalence relation** provided θ is reflexive, symmetric, and transitive.*

When we wish formally to define an equality between elements in a set X, we will do so by constructing an equivalence relation θ on X. The ordered pairs which are contained in this relation will denote those elements which we declare to be "equal".

The simplest equivalence relation one can define on a set X is the so-called *identity* relation. The identity relation, normally denoted by ∇_X, or, more simply by "=", is what we normally consider when we think of equality of elements. This

relation is defined formally as follows:

$$\nabla_X = \{(a, a) : a \in X\}$$

In the identity relation, every element is identified with itself and nothing else. The identity relation will be our "defualt" definition of equality. Unless we have specified a different equivalence relation, whenever we speak of equality of elements, we will assume equality is defined by this simple relation.

If we use the identity relation to define equality in $\mathcal{Q}$, then $(1, 2) = (1, 2)$, but $(1, 2) \neq (2, 4)$ since $(1, 2)$ is not the same element as $(2, 4)$.

Another simple equivalence relation which may be defined on any set X is the so-called *entire* relation. Denoted by $\triangle_X$, the entire relation declares everything in X to be equal to everything else. Formally, the entire relation is defined as follows:

$$\triangle_X = \{(a, b) : a, b \in X\}$$

This extreme version of equality essentially collapses the set X to a single element. For example, if we use the entire relation to define equality in $\mathcal{Q}$, then $(1, 2) = (1, 2)$, and $(1, 2) = (2, 4)$. However, we would also have $(1, 2) = (3, 2)$, and $(1, 2) = (5, 6)$. Indeed, we would have $(1, 2)$ equal to *every* element in $\mathcal{Q}$.

It is clear that neither the identity relation nor the entire relation provide a satisfactory definition of equality for $\mathcal{Q}$ if we want this set to represent the rational numbers. In elementary algebra, we are taught to consider two rational numbers a/b and c/d to be equivalent provided $ad = bc$. Notice that this idea is captured by the equivalence relation C defined on $\mathcal{Q}$ in Exercise 1.15. It is this equivalence relation which allows us to identify the set $\mathcal{Q}$ with the set $\mathbb{Q}$ of rational numbers.

Definition 36 *Let X be any nonempty set. A **partition** of X is a collection $\mathcal{F}$ of subsets of X having the property that every element of X is in exactly one member of $\mathcal{F}$. The members of $\mathcal{F}$ are called **equivalence classes** or **cells**.*

Example 37 *If we let $S_e = \{2m : m \in \mathbb{Z}\}$ and $S_o = \{2m + 1 : m \in \mathbb{Z}\}$, then the family $\mathcal{F} = \{S_e, S_o\}$ forms a partition of $\mathbb{Z}$ into two sets, namely the set of even and the set of odd integers. Every integer is a member of exactly one set in $\mathcal{F}$.*

****

Theorem 38 *Let X be a nonempty set. If $\mathcal{F}$ is any partition of X, then the set $\theta \subseteq X \times X$ defined by*

$$(a,b) \in \theta \Longleftrightarrow a,b \in S \text{ for some } S \in \mathcal{F}$$

is an equivalence relation on X.

Proof. We need to prove that the binary relation θ is reflexive, symmetric, and transitive. First, suppose that $a \in X$. Since $\mathcal{F}$ is a partition of X, we know that $a \in S$ for some set $S \in \mathcal{F}$. Consequently, we know that $(a,a) \in \theta$; and we may conclude that θ is reflexive. Second, suppose that $(a,b) \in \theta$. This means that $a,b \in S$ for some $S \in \mathcal{F}$. Of course, if $a,b \in S$, then we know that $b,a \in S$ as well. Hence, we know that $(b,a) \in \theta$; and we may conclude that θ is symmetric. Finally, suppose that $(a,b),(b,c) \in \theta$. This means that $a,b \in S$ and $b,c \in T$ for some $S,T \in \mathcal{F}$. Now, since $\mathcal{F}$ is a partition of X, we know that b is an element of *exactly one* member of $\mathcal{F}$. We must therefore conclude that $S = T$. Consequently, we know that $a,c \in S$; and this tells us that $(a,c) \in \theta$. We may therefore conclude that θ is transitive.

QED

Example 39 *Let $X = \{a,b,c,d,e,f,g,h\}$ and let $\mathcal{F} = \{S_1, S_2, S_3\}$ where*

$$S_1 = \{a,e,f\} \qquad S_2 = \{b,c,g\} \qquad S_3 = \{d,h\}$$

The family $\mathcal{F}$ forms a partition of X. What is the equivalence relation induced by $\mathcal{F}$?

Solution. We know that the equivalence relation induced by $\mathcal{F}$ is defined by

$$(x,y) \in \theta \Longleftrightarrow x,y \in S \text{ for some } S \in \mathcal{F}$$

Consequently, we construct θ simply by taking all pairs of elements which happen to lie in the same member of $\mathcal{F}$. Therefore,

$$\begin{aligned} \theta \;=\; & \{(a,a),(e,e),(f,f),(a,e),(e,a),(a,f),(f,a),(e,f),(f,e),(b,b),(c,c),(g,g) \\ & (b,c),(c,b),(b,g),(g,b),(c,g),(g,c),(d,d),(h,h),(d,h),(h,d)\} \end{aligned}$$

****

Theorem 40 *Let X be any nonempty set. If θ is any equivalence relation on X, then the collection of sets $\mathcal{F} = \{S_a : a \in X\}$ defined by*

$$S_a = \{y \in X : (a,y) \in \theta\}$$

forms a partition of X.

Proof. We need to show that every member of X appears in exactly one member of $\mathcal{F}$. Since we know $(a,a) \in \theta$ for each $a \in X$, it is clear that $a \in S_a$ for each $a \in X$. Hence, we know that every element of X appears in *at least one* member of $\mathcal{F}$. Suppose now that $a \in S_a$ and $a \in S_b$. We will prove that $S_a = S_b$. To this end, suppose that $y \in S_a$. This means that $(a,y) \in \theta$. Since $a \in S_b$, we also know that $(b,a) \in \theta$ as well. The transitivity of θ therefore tells us that $(b,y) \in \theta$, and this implies that $y \in S_b$. We may therefore conclude that $S_a \subseteq S_b$. On the other hand, suppose that $z \in S_b$. This means that $(b,z) \in \theta$. We know that $(b,a) \in \theta$; hence, the symmetry of θ tells us that $(a,b) \in \theta$. Consequently, the transitivity of θ allows us to conclude that $(a,z) \in \theta$. Therefore, we know that $z \in S_a$; and we may conclude that $S_b \subseteq S_a$. Hence, $S_b = S_a$, as desired.

QED

Example 41 *Let $n \in \mathbb{Z}^+$ be fixed and let $\texttt{MOD}_n \subseteq \mathbb{Z} \times \mathbb{Z}$ be defined by $(a,b) \in \texttt{MOD}_n$ if and only if $a \equiv b\texttt{MOD}(n)$. In light of Lemma 12, we know that $\texttt{MOD}_n$ is an equivalence relation. What is the partition induced by $\texttt{MOD}_n$?*

Solution. First, we know there exists a unique integer r_a such that $0 \leq r_a < n$ and $a \equiv r_a\texttt{MOD}(n)$. From the previous theorem and Theorem 13 that the partition $\mathcal{F} = \{S_a : a \in X\}$ induced by $\texttt{MOD}_n$ is comprised of sets having the form

$$\begin{aligned} S_a &= \{y \in \mathbb{Z} : (a,y) \in \texttt{MOD}_n\} \\ &= \{y \in \mathbb{Z} : a \equiv y\texttt{MOD}(n)\} \\ &= \{y \in \mathbb{Z} : a \text{ and } y \text{ have the same remainder when divided by } n\} \\ &= \{y \in \mathbb{Z} : \ y \equiv r_a\texttt{MOD}(n) \ \} \\ &= \{un + r_a : u \in \mathbb{Z}\} \end{aligned}$$

Now, there are only n distinct integers between 0 and $n-1$; hence, the last equality above tells us that the partition $\mathcal{F}$ actually consists of n distinct sets, namely the sets

$$S_0 = \{un : u \in \mathbb{Z}\} \qquad S_1 = \{un+1 : u \in \mathbb{Z}\} \qquad S_2 = \{un+2 : u \in \mathbb{Z}\} \qquad ... \qquad S_{n-1} = \{un+n-1 : u \in \mathbb{Z}\}$$

****

The partition induced on $\mathbb{Z}$ by the equivalence relation $\texttt{MOD}_n$ is often denoted by $\mathbb{Z}_n$. In other words, $\mathbb{Z}_n = \{S_0, ..., S_{n-1}\}$ where the sets S_j are described in the previous example. In number theory, this partition of $\mathbb{Z}$ is traditionally called the family of *residue classes modulo n*. For example, the family of residue classes modulo 4 would be $\mathbb{Z}_4 = \{S_0, S_1, S_2, S_3\}$, where

$$\begin{aligned} S_0 &= \{..., -12, -8, -4, 0, 4, 8, 12, ...\} \quad S_1 = \{..., -11, -7, -3, 1, 5, 9, 13, ...\} \\ S_2 &= \{..., -10, -6, -2, 2, 6, 10, 14, ...\} \quad S_3 = \{..., -9, -5, -1, 3, 7, 11, 15, ...\} \end{aligned}$$

When working with the partition $\mathbb{Z}_n = \{S_0, ..., S_{n-1}\}$, it is common to let $[a]_n = S_j$, where a is any member of S_j. The selected number a is called a *representative* of the equivalence class. It does not matter which member of the set S_j you select to be the representative, since all members of the equivalence class are considered "equal" to one another. For example, in $\mathbb{Z}_4$, we could let

$$S_2 = [-10]_4 \quad \text{or} \quad S_2 = [2]_4 \quad \text{or} \quad S_2 = [14]_4$$

While any member of the equivalence class may be used as its representative, in practice we usually select its smallest positive member. In other words, the default is to let $S_j = [j]_n$. Using this convention, we would write

$$\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$$

EXERCISES FOR SECTION 4

1. What are the elements of the residue class $[9]_{12}$?
2. What are the elements of the residue class $[15]_{30}$?
3. What is the smallest positive member of the residue class $[83]_9$?
4. What are the elements of the residue class $[100]_6$?
5. List the elements in each of the five residue classes modulo 5.
6. List the elements in each of the eight residue classes modulo 8.
7. Let $X = \{a, b, c, d, e, f, g\}$ and let $S_1 = \{a, d, e\}$, $S_2 = \{f, g, c\}$, and $S_3 = \{b\}$. The family $\mathcal{F} = \{S_1, S_2, S_3\}$ forms a partition of X. What is the equivalence relation θ induced by $\mathcal{F}$?

8. Let $X = \{a, b, c, d, e, f, g\}$ and let

$$\theta = \{(a,a),(b,b),(c,c),(d,d),(e,e),(f,f),(g,g),(g,a),(a,g),(a,b),(b,a),(g,b),(b,g)\}$$

The set θ is an equivalence relation on X. What is the partition induced by θ?

9. Let $X = \{a, b, c, d, e, f, g\}$. What is the partition induced on X by the identity relation ∇_X? What is the partition induced by the entire relation $\triangle_X$?

10. Let $\theta \subseteq \mathbb{Z} \times \mathbb{Z}$ be defined by $(m, n) \in \theta$ if and only if $|m| = |n|$.

    (a) Show that θ is an equivalence relation.

    (b) Construct the partition induced by θ.

11. Let $\theta \subseteq \mathbb{Q} \times \mathbb{Q}$ be defined by $(x, y) \in \theta$ if and only if $x - y \in \mathbb{Z}$.

    (a) Show that θ is an equivalence relation.

    (b) Construct the partition induced by θ. Hint: You should use Exercise 2.15.

12. Let X be any nonempty set and let $\mathtt{Su}[X]$ denote the powerset of X (the set of all subsets of X). Let $D \in \mathtt{Su}[X]$ be fixed and let $\theta \subseteq \mathtt{Su}[X] \times \mathtt{Su}[X]$ be defined by $(A, B) \in \theta$ if and onlly if $A \cap D = B \cap D$.

    (a) Show that θ is an equivalence relation on $\mathtt{Su}[X]$.

    (b) What is the partition induced on $\mathtt{Su}[X]$ when $D = \varnothing$?

    (c) Let $X = \{a, b, c, d\}$ and let $D = \{b, c\}$. Construct the relation θ and the partition it induces.

13. Let $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ denote the cartesian plane. For each real number r, let $S_r = \{(a, b) \in \mathbb{R}^2 : a^2 + b^2 = r^2\}$.

    (a) Show that $\mathcal{F} = \{S_r : r \in \mathbb{R}\}$ forms a partition of $\mathbb{R}^2$.

    (b) Construct the equivalence relation induced by $\mathcal{F}$.

5 Functions

In the last two sections, we introduced binary relations on sets and used them to give a formal definition of equality which is more flexible than simply identifying objects with themselves. We will now use binary relations to give a formal definition for the notion of a function — one which is flexible enough to be used outside the familiar contexts of algebra or calculus.

Let X_1, X_2, ..., X_n be a collection of sets. In Exercise 3.6, you defined the *product* of this collection is defined to be the set

$$\prod_{j=1}^{n} X_j = \{(a_1, ..., a_n)\} : a_j \in X_j\}$$

The elements of the product are called *ordered n-tuples* or *vectors*; individual elements of an n-tuple are called *coordinates*. We often use the symbol $X_1 \times X_2 \times ... \times X_n$ to denote the product, especially when we are dealing with a small number of sets. When we refer to the product of n copies of a single set X, we often use the symbol X^n. It is common to let $\boldsymbol{a} = (a_1, ..., a_n)$ when we do not need to specify coordinates.

Definition 42 *Given two sets X and Y, an n-**ary function** from X to Y is a binary relation $f \subseteq X^n \times Y$ satisfying the following conditions:*

1. *If $(a_1, ..., a_n) \in X^n$, there there exist $b \in Y$ such that $([a_1, ..., a_n], b) \in f$.*

2. *If* $([a_1, ..., a_n], b) \in f$ *and* $([a_1, ..., a_n], c) \in f$, *then* $b = c$.

Stated more plainly, we say that an n-ary function f on $X^n \times Y$ is a rule which assigns ever vector in X^n to exactly one member of Y. In keeping with traditional algebra notation, we usually write $f : X^n \longrightarrow Y$ to denote an n-ary function from X to Y, and we often write

$$f(\boldsymbol{a}) = b \qquad \text{or} \qquad f(a_1, ..., a_n) = b$$

in place of the more cumbersome relation notation $([a_1, ..., a_n], b) \in f$. In keeping with relation terminology, we call the set X^n the *domain* of f. The set $R_f = \{b \in Y : f(\boldsymbol{a}) = b \text{ for some } \boldsymbol{a} \in X^n\}$ is called the *range* of f or the *image* of X^n under f. The set Y is called the *codomain* of f. The codomain of an n-ary function is not uniquely determined; indeed, the codomain can be any set which contains the range of the n-ary function.

You encountered n-ary functions in Calculus III, where you called them *multi-variable* functions. Here are a few concrete examples of n-ary functions.

- The function $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ defined by $f(x) = 1/x$.
- The function $g : \mathbb{R}^3 \longrightarrow \mathbb{R}$ defined by $g(x, y, z) = \sin(xy)\cos(yz)$
- The function $h : \mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R}$ defined by $h[(a, b, c), (u, v, w)] = au + bv + cw$

The function f is specifically called a *unary* function, because it acts on 1-tuples. Any single-variable function can be thought of as a unary function on its implied domain. The function g is called a *ternary* function, because it acts on triples. The function h (which happens to be the three-dimensional dot-product from linear algebra) is considered a *binary* function, because it *acts on ordered pairs* — even though the coordinates of the pairs are themselves triples.

Definition 43 *Let* $f : X^n \longrightarrow Y$ *be an* n*-ary function from* X *to* Y. *For all* $y \in Y$, *the set* $\{\boldsymbol{a} \in X^n : f(\boldsymbol{a}) = y\}$ *is called the* ***preimage*** *of* y *under the function* f. *We will use* $\texttt{Pre}_f(y)$ *to denote this set.*

- *We say that* f *is* ***onto*** *(or a* ***surjection****) provided* $\texttt{Pre}_f(y)$ *contains at least one element for all* $y \in Y$.
- *We say that* f *is* ***one-to-one*** *(or an* ***injection****) provided*$\texttt{Pre}_f(y)$ *contains at most one element for all* $y \in Y$.
- *We say that* f *is a* ***bijection*** *provided it is both an injection and a surjection.*

Example 44 *Let* $f(x) = \tan(x)$. *What is* $\texttt{Pre}_f(1)$ *and* $\texttt{Pre}_f(3)$*?*

Solution. We begin with $\texttt{Pre}_f(1)$. We want to find all values of x such that $\tan(x) = 1$. Now, we know from basic trigonometry that

$$1 = \tan(x) \quad \Longrightarrow \quad 1 = \frac{\sin(x)}{\cos(x)} \quad \Longrightarrow \quad \cos(x) = \sin(x)$$

Basic trigonometry also tells us that this occurs when $x = \pi/4$. Furthermore, since the tangent function is periodic with period π, we know that

$$\texttt{Pre}_f(1) = \left\{\frac{\pi}{4} + n\pi : n \in \mathbb{Z}\right\}$$

We now turn attention to $\texttt{Pre}_f(3)$. There are no "special" trigonometric relationships that tell us exactly which values of x yield $\tan(x) = 3$, but a graphing calculator shows that $\tan(1.249\ \texttt{rad}) \approx 3$. Hence, we know that

$$\texttt{Pre}_f(3) \approx \{1.249 + n\pi : n \in \mathbb{Z}\}$$

****

Example 45 *Show that the function $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ defined by $f(x) = 1/x$ is a bijection.*

Solution. We first show that f is onto. To this end, let y be any nonzero real number. We need to show that $\texttt{Pre}_f(y)$ contains *at least* one member. We know that $x = 1/y$ is a nonzero real number, hence

$$f(x) = \frac{1}{x} = \frac{1}{1/y} = y$$

Therefore, we know that $x \in \texttt{Pre}_f(y)$; and we may conclude that f is onto. We now show that f is one-to-one. We need to show that $\texttt{Pre}_f(y)$ contains *at most* one member. To accomplish this, suppose that $a, b \in \texttt{Pre}_f(y)$. It will suffice to prove that $a = b$. Now, assuming that $a, b \in \texttt{Pre}_f(y)$ means $f(a) = y = f(b)$. Therefore, we know

$$f(a) = f(b) \quad \Longrightarrow \quad \frac{1}{a} = \frac{1}{b} \quad \Longrightarrow \quad a = b$$

Therefore, we may conclude that f is one-to-one.

****

Example 46 *Show by counterexample that the function $g : \mathbb{R}^3 \longrightarrow \mathbb{R}$ defined by $g(x, y, z) = \sin(xy)\cos(yz)$ is neither onto nor one-to-one.*

Solution. To prove that g is not onto, we must identify some $u \in \mathbb{R}$ such that $\texttt{Pre}_g(u) = \varnothing$. Recall from basic trigonometry that, by definition, $|\sin(\theta)| \leq 1$ and $|\cos(\theta)| \leq 1$. Consequently, no matter what we choose x, y, and z to be, it is not possible to have $\sin(xy)\cos(yz) > 1$. Therefore, if we let $u = 2$, for example, we must conclude that $\texttt{Pre}_g(2) = \varnothing$. To prove that g is not one-to-one, we must identify some $u \in \mathbb{R}$ such that $\texttt{Pre}_g(u)$ contains more than one element. Since the sine and cosine functions are periodic, we have many choices. Consider, for example, $u = 1$. There are many values of x, y, and z for which $\sin(xy)\cos(yz) = 1$. Indeed,

$$g\left(\frac{\pi}{2}, 1, 0\right) = 1 \quad \text{and } g\left(\frac{\pi}{2}, 1, 2\pi\right) = 1$$

Hence, we know that $(\pi/2, 1, 0), (\pi/2, 1, 2\pi) \in \texttt{Pre}_g(u)$, and we may conclude that g is not one-to-one.

****

Example 47 *Show that $h : \mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R}$ defined by $h[(a, b, c), (u, v, w)] = au + bv + cw$ is onto but is not one-to-one.*

Solution. To see that h is onto, let $u \in \mathbb{R}$. We need to show that $\texttt{Pre}_h(u) \neq \varnothing$. This means we need to find a pair $[(a, b, c), (x, y, z)] \in \mathbb{R}^3 \times \mathbb{R}^3$ such that $h[(a, b, c), (x, y, z)] = u$. One way to do this would be to consider $(u, 0, 0)$ and $(1, 1, 1)$. Observe that

$$h[(u, 0, 0), (1, 1, 1)] = (u)(1) + (0)(1) + (0)(1) = u$$

We therefore know that $[(u, 0, 0), (1, 1, 1)] \in \texttt{Pre}_h(u)$; and we may conclude that h is onto. To prove that h is not one-to-one, we need to identify a specific value of u for which $\texttt{Pre}_h(u)$ contains more than one element. Consider, for example, $u = 2$. We already know that $[(2, 0, 0), (1, 1, 1)] \in \texttt{Pre}_h(2)$. It is easy to see that $[(1, 0, 0), (2, 1, 1)] \in \texttt{Pre}_h(2)$ as well. Hence, we may conclude that h is not one-to-one.

Let $f : X^n \longrightarrow Y$ and $g : X^n \longrightarrow Y$ be n-ary functions. We say that f and g are *equal* provided $f(\boldsymbol{x}) = g(\boldsymbol{x})$ for all $\boldsymbol{x} \in X^n$. We refer to this as the *pointwise* definition of function equality. To show that two functions are equal, you must show they have the same domain, and show they produce the same output for every input in their domain. For example, consider the real-valued functions

$$f(x) = \frac{x^2 - 1}{x + 1} \qquad g(x) = x - 1$$

We can use basic algebra to "simplify" the formula for f. Indeed, we know

$$\frac{x^2 - 1}{x + 1} = \frac{(x - 1)(x + 1)}{x + 1} = x - 1 \qquad (x \neq -1)$$

Does this mean that $f = g$? The answer depends on what we specify the domains of these functions to be. If we assume the largest possible domain (the so-called *implied* domain) for each function, then they are *not* equal because they do not have the same domain. The function g is defined for all real numbers, while the function f is defined for all real numbers *except* $x = -1$. However, if we specify that the domain of each is the set $\mathbb{R}^+$, then the functions would be equal, since they produce the same output for every member of this set. There are many other domains where the functions are equal. (They would, for example, be equal on the domain $\mathbb{W}$.) This is one of the reasons why we are always careful to specify the domain of a function when it is first defined.

We will focus on unary functions for the remainder of this section.

Definition 48 *Let $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$ be unary functions. We define the* ***composition*** *of g* ***after*** *f to be the function $g \circ f : X \longrightarrow Z$ defined pointwise by $(g \circ f)[x] = g(f(x))$.*

Like most mathematical constructions, function composition is interpreted from left to right. If parentheses are involved in the composition then the parenthetic expression is considered as a single function; and what appears immediately to the right of any function is considered input into that function. For example, consider the functions $f : (1, +\infty) \longrightarrow \mathbb{R}^+$, $g : \mathbb{R}^+ \longrightarrow \mathbb{R}$, and $h : \mathbb{R} \longrightarrow \mathbb{Z}^+$ defined by

$$f(x) = \frac{1}{x - 1} \qquad g(x) = x^2 - 10\sqrt{x} - 6 \qquad h(x) = \lceil x \rceil$$

(The function h is called the *least integer function* — $\lceil x \rceil$ is defined to be the smallest integer greater than or equal to x.) We would interpret $(h \circ g) \circ f$ pointwise with $h \circ g$ initially viewed as one function with input from f. In other words, for all $x \in (1, +\infty)$, we have

$$((h \circ g) \circ f)[x] = (h \circ g)[f(x)] = h(g(f(x))) = \left\lceil \frac{1}{(x-1)^2} - 10\sqrt{\frac{1}{x-1}} - 6 \right\rceil$$

Notice that we have $(h \circ g) \circ f : (1, +\infty) \longrightarrow \mathbb{Z}^+$. How would we interpret the function $h \circ (g \circ f)$? In this case, we initially consider $g \circ f$ as a single function which first serves as input into h. We understand $g \circ f : (1, +\infty) \longrightarrow \mathbb{R}$, so for all $x \in (1, +\infty)$, we have

$$(h \circ (g \circ f))[x] = h((g \circ f)[x]) = h(g(f(x))) = \left\lceil \frac{1}{(x-1)^2} - 10\sqrt{\frac{1}{x-1}} - 6 \right\rceil$$

Notice that, according to the pointwise definition of function equality, we have $(h \circ g) \circ f = h \circ (g \circ f)$. It turns out that this is always the case as long as the two compositions are defined.

Theorem 49 *Let $f : X \longrightarrow Y$, $g : Y \longrightarrow Z$, and $h : Z \longrightarrow W$ be unary functions. It is always the case that $(h \circ g) \circ f = h \circ (g \circ f)$.*

Proof. First, note that $(h \circ g) \circ f : X \longrightarrow W$ and $h \circ (g \circ f) : X \longrightarrow W$, so both have the same domain. To show these functions are equal, we must show that they produce the same output for each element of X. Observe that, for all $x \in X$ we have

$$((h \circ g) \circ f)[x] = (h \circ g)[f(x)] = h(g(f(x))) = h((g \circ f)[x]) = (h \circ (g \circ f))[x]$$

QED

Let X be any nonempty set. The unary function $\epsilon_X : X \longrightarrow X$ defined by $\epsilon(x) = x$ is called the *identity function* on the set X. It is so named because it "identifies" every element of X. We often omit the subscript and simply write ϵ to denote this function when no confusion will result. It should be clear that the identity function is always a bijection.

Definition 50 *Let $f : U \longrightarrow V$ be a unary function.*

1. *We say that f has a **left inverse** provided there exists a function $g : V \longrightarrow U$ such that $g \circ f = \epsilon_U$.*
2. *We say that f has a **right inverse** provided there exists a function $h : V \longrightarrow U$ such that $f \circ h = \epsilon_V$.*
3. *We say that f has a **full inverse** provided there exists a function $j : V \longrightarrow U$ such that $j \circ f = \epsilon_U$ and $f \circ j = \epsilon_V$.*

Let U and V be sets and suppose that $f : U \longrightarrow V$ is a unary function. The definition above tells us f has a *left inverse* provided there exists a function $h : V \longrightarrow U$ such that $h(f(u)) = u$ for all $u \in U$. Likewise, the function f has a *right inverse* provided there exists a function $j : V \longrightarrow U$ such that $f(j(v)) = v$ for all $v \in V$. Let's look at some concrete examples of left and right inverses for functions.

Example 51 *Let $f : Y \longrightarrow X$ be the function defined for the sets X and Y shown below. Does f have a left inverse? Does f have a right inverse?*

$$X = \{1, 2, 3, 4\} \qquad Y = \{a, b, c, d, e\}$$

$$f(a) = 1 \qquad f(b) = 2 \qquad f(c) = 4 \qquad f(d) = 3 \qquad f(e) = 3$$

Since there is no formula-based rule defining f, we will answer these questions by trying to construct a left and a right inverse directly for f. We will start with a left inverse. We want a function $h : X \longrightarrow Y$ such that $h(f(y)) = y$ for all $y \in Y$. The strategy is simple — for each $x \in X$, we look to see what element of Y the function f assigns to x. We then let $h(x)$ be that element. Observe

- Since $f(a) = 1$, we will let $h(1) = a$. Then $h(f(a)) = h(1) = a$.
- Since $f(b) = 2$, we will let $h(2) = a$. Then $h(f(b)) = h(2) = b$.
- Since $f(c) = 4$, we will let $h(4) = c$. Then $h(f(c)) = h(4) = c$.
- Since $f(d) = 3$, we wll let $h(3) = d$. Then $h(f(d)) = h(3) = d$.

Unfortunately, we now run into a problem. Since $f(e) = 3$, we must also have $h(3) = e$. This is not possible, since we want h to be a *function*. We must therefore conclude that this particular function f does not have a left inverse.

We will now check to see if f has a right inverse. We want a function $j : X \longrightarrow Y$ such that $f(j(x)) = x$ for all $x \in X$. The strategy is simple — for each $x \in X$, we look to see what element of Y the function f assigns to x. We then let $j(x)$ be that element. Observe

- Since $f(a) = 1$, we will let $j(1) = a$. Then $f(j(1)) = f(a) = 1$.
- Since $f(b) = 2$, we will let $j(2) = b$. Then $f(j(2)) = f(b) = 2$.
- Since $f(c) = 4$, we will let $j(4) = c$. Then $f(j(4)) = f(c) = 4$.
- Since $f(d) = 3$, we wll let $j(3) = d$. Then $f(j(3)) = f(d) = 3$.

So far, the process looks just like the one we used in our failed attempt to construct a left inverse h. Do we run into the same problem with j? Do we also have to have $j(3) = e$? The answer turns out to be "NO." Since we are not trying to return to elements in Y, *we don't have to care about* e this time. The function

$$j(1) = a \qquad j(2) = b \qquad j(3) = d \qquad j(4) = c$$

meets the criterion for a right inverse and therefores serves as one for the function f. As a matter of fact, since *both* e and d are assigned to the element 3 by the function f, we can really construct *two* right inverses for f. The function

$$k(1) = a \qquad k(2) = b \qquad k(3) = e \qquad k(4) = c$$

serves as a right inverse for f as well.

****

When working with unary functions between finite sets, it is common to use *tabular notation* to write down the function, especially when the function has no easily determined rule. Tabular notation represents the function as a kind of matrix, with the top row denoting the domain, and the bottom row denoting the range. For example, the function f from the previous example could be written

$$f : \begin{pmatrix} a & b & c & d & e \\ 1 & 2 & 4 & 3 & 3 \end{pmatrix}$$

1. The columns represent the assignment. In this case, we would interpret the third column as meaning $f(c) = 4$.

Example 52 *Let* $A = \{1, 2, 3, 4\}$ *and let* $B = \{u, v, w, x, y, z\}$ *and consider the function* $g : A \longrightarrow B$ *defined by*

$$g : \begin{pmatrix} 1 & 2 & 3 & 4 \\ v & z & y & u \end{pmatrix}$$

Does this function have a left or a right inverse?

Solution. Let's begin by trying to construct a left inverse for g. The process is exactly the same as in the previous example. Observe

- Since $g(1) = v$, we will let $h(v) = 1$. Then $h(g(1)) = h(v) = 1$.
- Since $g(2) = z$, we will let $h(z) = 2$. Then $h(g(2)) = h(z) = 2$.
- Since $g(3) = y$, we will let $h(y) = 3$. Then $h(g(3)) = h(y) = 3$.
- Since $g(4) = w$, we wll let $h(w) = 4$. Then $h(g(4)) = h(w) = 4$.

The function g does not assign anything to the element x, so we cannot use g to define $h(x)$. Instead, we will just pick something from A and assign it to x. For example, we could let $h(x) = 1$. We now have a function $h : B \longrightarrow A$ with the property that $h(f(t)) = t$ for all $t \in A$. (Since $g(t) \neq x$ for any $t \in A$, the value of $h(x)$ is not important.) Consequently, h is a left inverse for g. Furthermore, we actually have four different functions we could use, since we could let $h(x)$ be any element from A.

Now let's try to construct a right inverse for this function g. Observe

- Since $g(1) = v$, we will let $j(v) = 1$. Then $g(j(v)) = g(1) = v$.
- Since $g(2) = z$, we will let $j(z) = 2$. Then $g(j(z)) = g(2) = z$.
- Since $g(3) = y$, we will let $j(y) = 3$. Then $g(j(y)) = g(3) = y$.
- Since $g(4) = w$, we wll let $j(w) = 4$. Then $g(j(w)) = g(4) = w$.

We now run into another problem — since g does not assign any member of A to the element x, we don't have any value for $j(x)$. Perhaps we could just choose an element at random from A like we did in constructing h. Suppose we let $j(x) = 2$, for example. We would then have a function $j : B \longrightarrow A$. Does the function j satisfy the criterion for right inverse? Well, since $g(2) = z$, observe that

$$g(j(x)) = f(2) = z$$

Consequently, this function *does not* serve as a right inverse for g. There is nothing especially bad about the element 2; we would have the same problem if we let $j(x)$ be any member of A. We must therefore conclude that g does not have a right inverse.

****

What is the difference between the example functions f and g in the last two examples? The function f is onto but is not one-to-one, while the function g is one-to-one but is not onto. It turns out that this distinction makes all the difference.

Let X and Y be sets and let $f : X \longrightarrow Y$ be a function. The function f has a left inverse if and only if it is one-to-one; the function f has a right inverse if and only if it is onto. Furthermore, if f is onto but is not one-to-one, then f will have multiple right inverses. Likewise, if f is one-to-one but not onto, then f will have multiple left inverses. We will provide a proof of these claims shortly; for the moment, let's consider more examples.

Example 53 *The function $f : \mathbb{Z} \longrightarrow \mathbb{W}$ defined by $f(n) = \sqrt{n^2}$ is onto but is not one-to-one. Construct two right inverses for the function f.*

Solution. The key to this problem is to note that, except for 0, the preimage of any whole number contains two elements. For example, $\texttt{Pre}_f(4) = \{-4, 4\}$. With this in mind, it is easy to construct two different right inverses for f. Define $j_1 : \mathbb{W} \longrightarrow \mathbb{Z}$ and $j_2 : \mathbb{W} \longrightarrow \mathbb{Z}$ by

$$j_1(w) = w \qquad j_2(w) = -w$$

Both of these functions serve as right inverses for f. Indeed, observe that

$$f(j_1(w)) = \sqrt{(j_1(w))^2} = \sqrt{w^2} = w \qquad \text{(since } w \geq 0\text{)}$$

$$f(j_2(w)) = \sqrt{(j_2(w))^2} = \sqrt{(-w)^2} = w \qquad \text{(since } w \geq 0\text{)}$$

It is worth noting that neither serves as a left inverse for f. Indeed, observe that

$$j_1(f(-3)) = j_1\left(\sqrt{(-3)^2}\right) = j_1(3) = 3$$

$$j_2(f(3)) = j_2\left(\sqrt{(3)^2}\right) = j_2(3) = -3$$

Consequently, we see that $j_1(f(-3)) \neq -3$ and $j_2(f(3)) \neq 3$.

****

It is also worth noting that the function f in the previous example actually has *infinitely many* right inverses. For example, the function

$$j_3(w) = \begin{cases} w & \text{if} \quad w \neq 4 \\ -4 & \text{if} \quad w = 4 \end{cases}$$

also serves as a right inverse for f.

Example 54 *Consider the function $f : \mathbb{R} \longrightarrow \mathbb{R}^+ \cup \{0\}$ defined by $f(x) = x^2$. Show that $g : \mathbb{R}^+ \cup \{0\} \longrightarrow \mathbb{R}$ and $h : \mathbb{R}^+ \cup \{0\} \longrightarrow \mathbb{R}$ defined by $g(y) = \sqrt{y}$ and $h(y) = -\sqrt{y}$ are both right inverses for f but are not left inverses for f.*

Solution. To see that both are right inverses for f, let $y \in \mathbb{R}^+ \cup \{0\}$ be any nonnegative real number and observe that

$$(f \circ g)[y] = f(g(y)) = [\sqrt{y}]^2 = y = \epsilon_Y(y) \qquad (f \circ h)[y] = f(h(y)) = [-\sqrt{y}]^2 = y = \epsilon_Y(y)$$

Consequently, we see that $f \circ g = \epsilon_Y$ and $f \circ h = \epsilon_Y$; we may therefore conclude that both g and h serve as right inverses for f. To see that g does not serve as a left inverse, we need a counterexample to show that $(g \circ f)[x] \neq x$ for some $x \in \mathbb{R}$. Let $x = -2$ and observe that

$$(g \circ f)[-2] = \sqrt{(-2)^2} = \sqrt{4} = 2$$

This computation shows that $(g \circ f)[-2] \neq -2$; hence, we may conclude that $g \circ f \neq \epsilon_X$. We can use $x = 2$ to show that $h \circ f \neq \epsilon_X$.

****

We had to be careful in choosing the codomain of the function f in the previous example. If we had considered $f : \mathbb{R} \longrightarrow \mathbb{R}$ instead (which we could easily do since $\mathbb{R}^+ \cup \{0\} \subseteq \mathbb{R}$), then f would not have a right inverse. The problem, of course, arises from the fact that squaring any real number always produces a *nonnegative* real number. Consequently, it is simply not possible to define a function $g : \mathbb{R} \longrightarrow \mathbb{R}$ such that $(f \circ g)[y] = (g(y))^2 = y$ when $y < 0$. We must specify the codomain to be the *range* of our function before having any hope of constructing a right inverse.

On the other hand, left inverses are not as picky. Consider the function $g : \mathbb{R}^+ \cup \{0\} \longrightarrow \mathbb{R}$ defined by $g(x) = \sqrt{x}$. Notice that the specified codomian is not the range (since the range is also $\mathbb{R}^+ \cup \{0\}$). The functions $f : \mathbb{R} \longrightarrow \mathbb{R}^+ \cup \{0\}$ and $h : \mathbb{R} \longrightarrow \mathbb{R}^+ \cup \{0\}$ defined by

$$f(y) = y^2 \qquad h(y) = \begin{cases} y^2 & \text{if} \quad y \geq 0 \\ 0 & \text{if} \quad y < 0 \end{cases}$$

are both left inverses for the function g. Indeed, observe that, for all $x \in \mathbb{R}^+ \cup \{0\}$ we have

$$(f \circ g)[x] = f(g(x)) = \left(\sqrt{x}\right)^2 = x = \epsilon_X(x) \qquad (h \circ g)[x] = h(g(x)) = \left(\sqrt{x}\right)^2 = x = \epsilon_X(x)$$

Notice that the branch of h specified for $y < 0$ does not figure into the computation (because g produces only nonnegative output). This means we could use any rule for $y < 0$ that produces nonnegative output. (We need nonnegative output because the range of h must be the domain of g.) Neither f nor h serves as a right inverse for g, as you can check for yourself. (Just consider $y = -2$.)

Theorem 55 *Let $f : X \longrightarrow Y$ be a unary function where X is nonempty.*

1. *The function f has a right inverse if and only if f is onto.*
2. *The function f has a left inverse if and only if f is one-to-one.*
3. *The function f has a full inverse if and only if f is a bijection. Furthermore, this full inverse is unique.*

Proof. To establish Claim (1), first suppose that f has a right inverse g. To prove that f is onto, we must show that $\texttt{Pre}_f(y) \neq \varnothing$ for all $y \in Y$. Since $g : Y \longrightarrow X$, we know that $g(y)$ exists for all $y \in Y$; and, since g is a right inverse for f, we know that $f(g(y)) = y$. Hence, we know that $g(y) \in \texttt{Pre}_f(y)$; and we may conclude that f is onto. Conversely, suppose that f is onto. This means that $\texttt{Pre}_f(y) \neq \varnothing$ for all $y \in Y$. Construct a function $g : Y \longrightarrow X$ by selecting exactly one $x \in \texttt{Pre}_f(y)$ for each $y \in Y$ and letting $g(y) = x$. It follows that $f(g(y)) = f(x) = y$ for all $y \in Y$; consequently, we may conclude that $f \circ g = \epsilon_Y$. Therefore, the function g serves as a right inverse for f.

To establish Claim (2), first suppose that f has a left inverse h. To prove that f is one-to-one, we must show that $\texttt{Pre}_f(y)$ is either empty or is a singleton. Let $y \in Y$ and suppose that $u, v \in \texttt{Pre}_f(y)$. It will suffice to prove that $u = v$. By assumption, we know that $f(u) = y = f(v)$. Consequently, we also know that

$$u = (h \circ f)[u] = h(f(u)) = h(f(v)) = (h \circ f)[v] = v$$

This computation shows that, if $\texttt{Pre}_f(y)$ is nonempty, then it can contain only one element. We may therefore conclude that f is one-to-one. Conversely, suppose that f is one-to-one. Let $U = \{y \in Y : \texttt{Pre}_f(y) \neq \varnothing\}$ and let $V = Y - U$. Since f is assumed to be one-to-ne, we know that for each $y \in U$, the set $\texttt{Pre}_f(y)$ is a singleton. In particular, we know $\texttt{Pre}_f(y) = \{x_y\}$ for some $x_y \in X$. Construct a function $h : Y \longrightarrow X$ in the following way. Let $a \in X$ be fixed and let

$$h(y) = \begin{cases} x_y & \text{if} \quad y \in U \\ a & \text{if} \quad y \in V \end{cases}$$

The function h will serve as a left inverse for f. To see why, suppose $x \in X$ and suppose that $f(x) = b$. Observe that

$$(h \circ f)[x] = h(f(x)) = h(b) = x_b$$

Of course, we know that $x, x_b \in \texttt{Pre}_f(b)$; and, since f is one-to-one, this tells us that $x = x_b$. Consequently, $(h \circ f)[x] = x$ for all $x \in X$; and we may conclude that h is a left inverse for f.

It remains to prove Claim (3). Suppose first that f has a full inverse j. We must prove that f is a bijection. We know that $f \circ j = \epsilon_Y$ and $j \circ f = \epsilon_X$. Consequently, g serves as a right inverse for f which implies f is onto by Claim (1). Also, j serves as a left inverse for f which implies f is one-to-one by Claim (2). Hence, f is a bijection. Conversely, suppose that f is a bijection. We must show that f has a full inverse. In other words, we must find a function $j : Y \longrightarrow X$ such that $j \circ f = \epsilon_X$ and $f \circ j = \epsilon_Y$. The assumption that f is a bijection means that f is onto; hence we know that f has a right inverse $g : Y \longrightarrow X$ by Claim (1). It also means that f is one-to-one; hence we know that f has a left inverse $h : Y \longrightarrow X$ by Claim (2). It will suffice to prove that $g = h$. To this end, let $y \in Y$ and observe that by Theorem 44, we have

$$h(y) = h(\epsilon_Y[y]) = h((f \circ g)[y]) = (h \circ (f \circ g))[y] = ((h \circ f) \circ g)[y] = (\epsilon_X \circ g)[y] = \epsilon_X(g(y)) = g(y)$$

We may now conclude that $g = h$. If we let $j = g = h$, then it follows that j serves as both a right and a left inverse for f and is therefore a full inverse for f.

To complete the proof of Claim (3), we must prove that the full inverse of f is unique. To this end, suppose that j and k are full inverses for f. We must show that $j = k$. However, we have actually already proven this. Since j is a full inverse for f, we know that j is a left inverse for f; and, since k is a full inverse for f, we know that k is a right inverse for f. Consequently, $j = k$ by the previous argument.

The previous result tells us that every function can have *at most* one full inverse (and will have one precisely when it is a bijection). This is certainly not the case for functions which have only left or only right inverses. When it exists, we usually refer to the full inverse of a function f as *the inverse* of f. It is traditional to denote the inverse of a function f by the symbol f^{-1}.

EXERCISES FOR SECTION 5

1. Let $X = \{1, 2, 3, 4\}$ and let $Y = \{a, b, c, d\}$. Determine which, if any, of the following relations is a unary function. For those which are functions, which ones are onto? Which ones are one-to-one? Which ones are bijections?

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

2. Let $X = \{1, 2, 3\}$ and let $Y = \{a, b, c, d\}$. Determine which, if any, of the following relations is a binary function. For those which are functions, which ones are onto? Which ones are one-to-one? Which ones are bijections?

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

3. Consider the unary function $f : \mathbb{R} \longrightarrow \mathbb{R}$ defined by $f(x) = x^4$. What is $\texttt{Pre}_f(9)$?

4. Consider the binary function $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$ defined by $f(x, y) = x^2 \cos(y)$. What is $\texttt{Pre}_f(9)$? What is $\texttt{Pre}_f(-2)$?

5. Consider the binary function $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^+$ defined by $f(x, y) = 1 + x^2 + y^2$. Is this function onto? Is this function one-to-one?

6. Consider the binary function $f : \mathbb{Z}^2 \longrightarrow \mathbb{Z}$ defined by $f(x, y) = 3x + 2y$. Show this function is not one-to-one but is onto. (Use the fact that $\texttt{GCF}(3, 2) = 1$.)

7. Consider the unary function $f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}$ defined by

$$f(n) = \begin{cases} \dfrac{n}{2} & \text{if} \quad n \text{ is even} \\ \dfrac{1 - n}{2} & \text{if} \quad n \text{ is odd} \end{cases}$$

   Show that this function is a bijection.

8. Consider the unary function $f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$ defined by $f(n) = 2n$. Show that the following functions are left inverses for f.

$$g(k) = \begin{cases} \dfrac{k}{2} & \text{if} \quad k \text{ is even} \\ k & \text{if} \quad k \text{ is odd} \end{cases} \qquad h(k) = \begin{cases} \dfrac{k}{2} & \text{if} \quad k \text{ is even} \\ 3k & \text{if} \quad k \text{ is odd} \end{cases}$$

9. Construct two right inverses for the function $f : \mathbb{R} \longrightarrow \mathbb{R}^+ \cup \{0\}$ defined by $f(x) = |x|$.

10. Let $f : X \longrightarrow Y$ be any function. Prove that $\epsilon_Y \circ f = f$ and $f \circ \epsilon_X = f$.

11. Let $f : X^n \longrightarrow Y$ be any function. Show that the family $\mathcal{F} = \{\texttt{Pre}_f(y)\} : y \in Y\}$ forms a partition of X^n. What is the equivalence relation induced by $\mathcal{F}$?

12. If $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$ are both unary functions that are onto, prove that $g \circ f : X \longrightarrow Z$ is onto.

13. If $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$ are both unary functions that are one-to-one, prove that $g \circ f : X \longrightarrow Z$ is one-to-one.

14. Construct two left inverses for the function $f : X \longrightarrow Y$ given by the table below. In this case, assume $Y = \{1, 2, 3, 4, 5, 6\}$. Write your answers using tabular notation.

$$f : \begin{pmatrix} a & b & c & d \\ 1 & 3 & 2 & 5 \end{pmatrix}$$

15. Construct two right inverses for the function $f : X \longrightarrow Y$ given by the table below. In this case, assume $Y = \{1, 2, 3, 4, 5, 6\}$. Write your answers using tabular notation.

$$f : \begin{pmatrix} a & b & c & d & e & f & g & h \\ 6 & 2 & 3 & 2 & 4 & 4 & 5 & 1 \end{pmatrix}$$

16. Construct the inverse for the bijection $f : X \longrightarrow Y$ given by the table below. Write your answer using tabular notation. Why is it unecessary to specify Y this time?

$$f : \begin{pmatrix} a & b & c & d \\ u & x & w & t \end{pmatrix}$$

6 Operations

Most of the arithmetic operations we are familiar with in algebra can be thought of as binary functions. For example, integer addition and integer multiplication "work" on pairs of integers to produce another integer. We conclude this chapter by taking a closer look at what mathematicians mean when they talk about "operations."

Definition 56 *An n-ary function $f : X^n \longrightarrow X$ is often called an n-ary* ***operation*** *on X. An operation must take all possible n-tuples from X and assign them a unique element from X.*

Consider the three functions below that we first encountered in Section 5.

- The function $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ defined by $f(x) = 1/x$.
- The function $g : \mathbb{R}^3 \longrightarrow \mathbb{R}$ defined by $g(x, y, z) = \sin(xy)\cos(yz)$
- The function $h : \mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R}$ defined by $h[(a, b, c), (u, v, w)] = au + bv + cw$

We would consider the function $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ defined by $f(x) = 1/x$ to be a unary operation on the set $\mathbb{R}^*$ of nonzero real numbers. (This rule would *not* be an operation on $\mathbb{R}$ since $f(0)$ is undefined.) The function g defined above is a ternary operation on $\mathbb{R}$. The function h defined above is *not* a binary operation on $\mathbb{R}^3$ because, even though h is defined for all pairs from $\mathbb{R}^3$, it *does not assign these pairs to another member of* $\mathbb{R}^3$. (Instead, h assigns every pair from $\mathbb{R}^3$ to a real number.)

It is very common to use some suggestive symbol like $+$ or $*$ to denote a given binary operation and to write $a * b$ in place of the more formal $f(a, b)$. For example, the function $f : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ defined by

$$f(a, b) = a + \frac{ab}{2} + b$$

defines a binary operation on the real numbers. (All that is required is simply for $f(a, b)$ to be a unique real number for *every* pair of real numbers (a, b).) Consequently, we could use some suggestive symbol like

$$a \boxplus b = a + \frac{ab}{2} + b$$

in place of the more formal and cumbersome function notation. (In this case, since the formula explicitly uses the plus-symbol for real number addition, we would not want to use $+$ to avoid confusion.) There is no corresponding convention for higher order operations.

Example 57 *Let n be a fixed positive integer and let $\mathbb{Z}_n = \{[0]_n, ..., [n-1]_n\}$ denote the family of residue classes modulo n that we introduced in the previous section. Define a binary relation $\theta_n \subseteq [\mathbb{Z}_n]^2 \times \mathbb{Z}_n$ by the formula*

$$([[i]_n, [j]_n], [k]_n) \in \theta_n \quad \Longleftrightarrow \quad k \equiv (i + j)\texttt{MOD}(n)$$

Prove that this relation is a binary operation on $\mathbb{Z}_n$.

Solution. It is clear that θ_n takes every ordered pair from $\mathbb{Z}_n$ and relates it to *at least one* element of $\mathbb{Z}_n$. The real question here is "how many members of $\mathbb{Z}_n$ are related to each pair?" We want to show that θ_n is a *function*, which means we must prove that each ordered pair from $\mathbb{Z}_n$ is related to *exactly one* element of $\mathbb{Z}_n$. Let's look at a concrete example to see where the potential problem lies. Consider the partition

$$\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$$

and in particular consider the residue classes $[3]_6$ and $[5]_6$. Since $2 \equiv (3 + 5)\texttt{MOD}(6)$, we know that $([[3]_6, [5]_6], [2]_6) \in \theta_6$. Is there any other residue class related to the pair $[[3]_6, [5]_6]$? One potential issue arises from the fact that there are many integers equivalent to 3+5 modulo 6. For example, $8 \equiv (3+5)\texttt{MOD}(6)$. The relation θ_6 will not be a function if 2 and 8 lay in different residue classes. Of course, this is not the case, since both leave the same remainder (namely 2) when divided by 6. Another potential issue arises from the fact that there are many representatives for $[3]_6$ and $[5]_6$. For example, $[3]_6 = [15]_6$ and $[5]_6 = [23]_6$. The relation θ_6 will not be a function if it does not pair $[[15]_6, [23]_6]$ with $[2]_6$. However, this also is not a problem, since

$$15 + 23 = 38 \quad \text{and} \quad 38 \equiv 2\texttt{MOD}(6)$$

We have just demonstrated that, at least for $[[3]_6, [5]_6] \in [\mathbb{Z}_6]^2$, the pairing provided by the relation θ_6 is independent of the representatives selected for the residue classes. This is the key to the general proof that θ_n is a binary function.

Suppose that $([[i]_n, [j]_n], [a]_n) \in \theta_n$ and $([[i]_n, [j]_n], [b]_n) \in \theta_n$. To prove that θ_n is a function, we first prove that $[a]_n = [b]_n$. According to the way we have defined θ_n, we know that $a \equiv (i + j)\texttt{MOD}(n)$ and $b \equiv (i + j)\texttt{MOD}(n)$. Of course, this tells us that $a \equiv b\texttt{MOD}(n)$, and this allows us to conclude that $[a]_n = [b]_n$. Ordinarily, this is enough to prove that a relation is a function; but, in this case, we must take into account the fact that there are many different ways to represent the pair $[[i]_n, [j]_n]$. Suppose that $([[i]_n, [j]_n], [a]_n) \in \theta_n$ and suppose further that $[i]_n = [x]_n$ and $[j]_n = [y]_n$. We must show that $([[x]_n, [y]_n], [a]_n) \in \theta_n$. This means we must show that $a \equiv (x + y)\texttt{MOD}(n)$. By assumption, we know $a \equiv (i + j)\texttt{MOD}(n)$. Since Corollary 14 tells us that $x + y \equiv (i + j)\texttt{MOD}(n)$, the desired result follows from transitivity.

****

The previous example shows that the binary relation θ_n defined on $\mathbb{Z}_n$ is actually a binary operation. In keeping with this, we will represent the pairing with an appropriate operation symbol. In particular, for all $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$, we will write

$$[a]_n \boxplus_n [b]_n = [c]_n \iff [a+b]_n = [c]_n \iff c \equiv (a+b)\texttt{MOD}(n) \iff ([[a]_n, [b]_n], [c]_n) \in \theta_n$$

When working with a binary operation on a finite set like $\mathbb{Z}_n$, it is common to summarize the effects of the operation using an *operation table*. An operation table lists the elements of the set in the topmost row and leftmost column (in the same order). The rest of the table entries are the result of performing the operation on the ordered pairs whose first coordinate comes from the leftmost column and whose second coordinate comes from the top row. For example, the table below summarizes the operation $\boxplus_4$ for the set $\mathbb{Z}_4$.

$\boxplus_4$	$[\mathbf{0}]_\mathbf{4}$	$[\mathbf{1}]_\mathbf{4}$	$[\mathbf{2}]_\mathbf{4}$	$[\mathbf{3}]_\mathbf{4}$
$[\mathbf{0}]_\mathbf{4}$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[\mathbf{1}]_\mathbf{4}$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[\mathbf{2}]_\mathbf{4}$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[\mathbf{3}]_\mathbf{4}$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

In an operation table, the element listings comprise the Zero Row and the Zero Column. It is traditional (though not necessary) to list the elements in the same order for both. In the table above, the entry in Row 3, Column 4 is the output obained from $[2]_4 \boxplus_4 [3]_4$. Notice the we used the smallest nonnegative representative for each output. This is not necessary, but it makes the table much easier to interpret.

The binary operation $\boxplus_4$ is defined by a computational rule, and the operation table above simply summarizes the results of applying this rule. Tables can be used to define operations directly with no reference to a computational rule. Consider the table presented below.

$*$	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$
$\boldsymbol{e}$	e	a	b	c
$\boldsymbol{a}$	a	e	c	b
$\boldsymbol{b}$	b	c	e	a
$\boldsymbol{c}$	c	b	a	e

This table directly defines a binary operation (called $*$) on the set $S = \{e, a, b, c\}$. There is no obvious computational formula for computing the output of this operation; all the information about output is contained in the table.

Definition 58 *Let X be a nonempty set and let $f : X^2 \longrightarrow X$ be a binary operation on X. We say that f is **commutative** provided $f(a,b) = f(b,a)$ for all $(a,b) \in X^2$. If we let $a * b = f(a,b)$, then commutativity means $a * b = b * a$ for all $a, b \in X$.*

Example 59 *Consider the binary operation $\diamond$ defined on $\mathbb{Z}$ by the rule $x \diamond y = x + y - 2xy$. Is this operation commutative?*

Solution. We should first point out that it is clear the relation is a *function*, since the output rule is purely integer arithmetic and therefore can only assign one integer number to any pair (x, y) of integers. This is why we did not bother to write the rule using formal relation notation. To determine whether or not the operation is commutative, we either need to prove that $x \diamond y = y \diamond x$ for all integers x and y, or else we need to give a specific counterexample. Since integer addition and multiplication are both commutative, we see that

$$x \diamond y = x + y - 2xy = y + x - 2yx = y \diamond x$$

Hence, this operation is commutative.

****

Example 60 *Consider the binary relation θ on the set $\left[\mathbb{Z}^+\right]^2 \times \mathbb{Q}$ defined by*

$$\left([m.n], k\right) \in \theta \quad \Longleftrightarrow \quad k = \frac{(mn)!}{(m-1)!}$$

1. *Is this relation a binary operation on the positive integers?*
2. *If so, is this operation commutative?*

Solution. As in the previous example, the defining rule in the relation is purley integer arithmetic, so we could have dispensed with the formal relation notation. Recall that the *factorial* is a unary function $()! : \mathbb{W} \longrightarrow \mathbb{Z}^+$ defined by

$$(j)! = \begin{cases} 1 & \text{if} \quad j = 0 \\ 1 \times 2 \times ... \times j & \text{if} \quad j > 0 \end{cases}$$

We know that θ is a binary function. We are therefore justified in writing the relation using function notation:

$$\theta(m, n) = \frac{(mn)!}{(m-1)!}$$

While it is clear from the outset that θ is a binary function from $\left[\mathbb{Z}^+\right]^2$ to $\mathbb{Q}$, it is not clear that θ is an *operation.* Since the domain of θ is specified to be pairs of positive *integers*, we must show that the output of θ is always a positive integer. Observe that the associativity of integer multiplication tells us

$$\begin{aligned} (mn)! &= 1 \times 2 \times 3 \times ... \times (m-1) \times m \times (m+1) \times ... \times (mn) \\ &= [1 \times 2 \times 3 \times ... \times (m-1)] \times m \times (m+1) \times ... \times (mn) \\ &= (m-1)! \times m \times (m+1) \times ... \times (mn) \end{aligned}$$

Consequently, $(m-1)!$ is a factor of $(mn)!$; and this means $\theta(m, n) \in \mathbb{Z}^+$.

We are now justified in writing θ using appropriate operation notation. For example, we could let $m \triangleright n = \theta(m, n)$. If this operation is commutative, then for all $m, n \in \mathbb{Z}^+$ we must have

$$m \triangleright n = \frac{(mn)!}{(m-1)!} = \frac{(nm)!}{(n-1)!} = n \triangleright m$$

This equation looks suspicious, since we know $mn = nm$, but we also know that $m - 1 \neq n - 1$ in general. This suggests that we should look for a counterexample, and it turns out there are many. For example, observe that

$$2 \triangleright 3 = \frac{6!}{1!} = 720 \quad \text{but} \quad 3 \triangleright 2 = \frac{6!}{2!} = 360$$

****

Definition 61 *Let X be a nonempty set and let $f : X^2 \longrightarrow X$ be a binary operation on X. We say that f is **associative** provided $f(f(a, b), c) = f(a, f(b, c))$ for all $a, b, c \in X$. If we let $a * b = f(a, b)$, then associativity means $(a * b) * c = a * (b * c)$ for all $a, b, c \in X$.*

Since binary operations can only operate on pairs of elements, associativity is an important property to have when we need to operate simultaneously on sequences of elements. (Most shortcuts that you learned for adding lists of integers in your head rely on associativity.)

Example 62 *Is either of the operations $\triangleright$ or $\diamond$ defined in the last two examples associative?*

Solution. The operation $\triangleright$ is not associative, since

$$(1 \triangleright 3) \triangleright 2 = \frac{12!}{5!} \qquad 1 \triangleright (3 \triangleright 2) = 360!$$

On the other hand, the operation $\diamond$ is associative. To see why, observe that

$$(a \diamond b) \diamond c = (a + b - 2ab) \diamond c = (a + b - 2ab) + c - 2(a + b - 2ab)c = (a + b + c) - 2(ab + ac + bc) + 4abc$$

$$a \diamond (b \diamond c) = a \diamond (b + c - 2bc) = a + (b + c - 2bc) - 2a(b + c - 2bc) = (a + b + c) - 2(ab + ac + bc) + 4abc$$

****

Example 63 *Let X be any nonempty set and let $[X \longrightarrow X]$ denote the set of all unary functions $f : X \longrightarrow X$. Show that function composition is an operation on $[X \longrightarrow X]$ which is always associative but not always commutative.*

Solution. A binary operation on $[X \longrightarrow X]$ must take every pair of functions (f, g) from X to X and assign to it exactly one function h from X to X. Let $f, g \in [X \longrightarrow X]$ and recall that the composition $f \circ g : X \longrightarrow X$ is the function defined by $(f \circ g)[x] = f(g(x))$. Consequently, by definition, function composition represents a binary operation on $[X \longrightarrow X]$. We will let $\circ$ denote the operation of function composition. The operation $\circ$ is always associative by Theorem 44.

If X is a singleton (that is, if $X = \{a\}$), then $[X \longrightarrow X]$ is only a singleton as well. In particular, $[X \longrightarrow X] = \{\epsilon\}$, where ϵ is the identity function on X. In this extreme case, function composition must be commutative on $[X \longrightarrow X]$. On the other hand, suppose that X contains at least two elements. Let $a, b \in X$ be distinct and let $f, g \in [X \longrightarrow X]$ be defined by

$$f(x) = a \qquad g(x) = b$$

Consider the functions $f \circ g$ and $g \circ f$. Observe that $(f \circ g)[a] = f(g(a)) = f(b) = a$ while $(g \circ f)[a] = g(f(b)) = g(a) = b$. Since $[f \circ g](a) \neq [g \circ f](a)$, we may conclude that $f \circ g \neq g \circ f$. Consequently, function composition is not a commutative operation on $[X \longrightarrow X]$ when X contains at least two elements.

****

Definition 64 *Let X be any nonempty set. A bijection $f : X \longrightarrow X$ is called a **permutation** on X. The family of all permutations on X will be denoted by $\wp_X$.*

Notice that $\wp_X \subseteq [X \longrightarrow X]$. A permutation on a set X is actually a bijective unary operation on that set, but the term "operation" is seldom used when discussing permutations. Theorem 44 along with Exercises 5.12 and 5.13 tell us that function composition forms an associative binary operation on $\wp_X$. Families of permutations under function composition will play a critical role in much of what we do in the next chapter.

Example 65 *If X contains at least three distinct elements, show that function composition is not commutative on $\wp_X$.*

Solution. The counterexample used to show that function composition is not commutative on $[X \longrightarrow X]$ when X contains at least two elements will not work here, because the particular functions chosen are not bijections. In the current example, having three distinct elements will be critical. Let $a, b, c \in X$ be distinct and let $Y = X - \{a, b, c\}$. Define $f : X \longrightarrow X$ and $g : X \longrightarrow X$ as follows

$$f(x) = \begin{cases} x & \text{if} \quad x \in Y \\ c & \text{if} \quad x = a \\ a & \text{if} \quad x = b \\ b & \text{if} \quad x = c \end{cases} \qquad g(x) = \begin{cases} x & \text{if} \quad x \in Y \\ b & \text{if} \quad x = a \\ a & \text{if} \quad x = b \\ c & \text{if} \quad x = c \end{cases}$$

Notice that f and g are simply the identity function on the set Y; hence, it should be clear that both are bijections. Now, observe that

$$(f \circ g)[a] = f(g(a)) = f(b) = a \qquad (g \circ f)[a] = g(f(a)) = g(c) = c$$

Since $(f \circ g)[a] \neq (g \circ f)[a]$, we may conclude that $f \circ g \neq g \circ f$ for these particular functions. This, of course, is enough to prove that function composition is not commutative on $\wp_X$.

****

When X contains exactly n elements, the family $\wp_X$ will contain exactly $n!$ functions. It is common to let $X = \{1, 2, ..., n\}$, and it is common to write $\wp_n$ for the family of permutations on X. It is also common to write the members of $\wp_n$ using tabular notation. For example, the six members of $\wp_3$ will be

$$\epsilon : \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \alpha : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \beta : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\gamma : \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \delta : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \zeta : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Example 66 *Construct the operation table for the family $\wp_3$ under function composition.*

Solution. We need to fill in the following table.

$\circ$	$\boldsymbol{\epsilon}$	$\boldsymbol{\alpha}$	$\boldsymbol{\beta}$	$\boldsymbol{\gamma}$	$\boldsymbol{\delta}$	$\boldsymbol{\zeta}$
$\boldsymbol{\epsilon}$						
$\boldsymbol{\alpha}$						
$\boldsymbol{\beta}$						
$\boldsymbol{\gamma}$						
$\boldsymbol{\delta}$						
$\boldsymbol{\zeta}$						

The first row and first column are easy to fill in, since ϵ is the identity function on $X = \{1, 2, 3\}$ and we know that $\epsilon \circ f = f$ and $f \circ \epsilon = f$ for all $f \in \wp_3$ by Exercise 5.10. Consequently, we know

$\circ$	$\boldsymbol{\epsilon}$	$\boldsymbol{\alpha}$	$\boldsymbol{\beta}$	$\boldsymbol{\gamma}$	$\boldsymbol{\delta}$	$\boldsymbol{\zeta}$
$\boldsymbol{\epsilon}$	ϵ	α	β	γ	δ	ζ
$\boldsymbol{\alpha}$	α					
$\boldsymbol{\beta}$	β					
$\boldsymbol{\gamma}$	γ					
$\boldsymbol{\delta}$	δ					
$\boldsymbol{\zeta}$	ζ					

The remainder of the table will have to be filled in by direct computation, and we can use the tabular notation to make the computations easier to write down. For example, suppose we want to compute $\alpha \circ \gamma$. In tabular notation, we have

$$\alpha \circ \gamma : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

We filled in the final table one column at a time by reading the column assignments from right to left in the composition. For example, we see that γ sends 3 to 2. Since α sends 2 to 1, we know that $\alpha \circ \gamma$ sends 3 to 1. Formally, we have

$$(\alpha \circ \gamma)[3] = \alpha(\gamma(3)) = \alpha(2) = 1$$

but the tabular notation makes this easy to see. Using the same approach, we see that

$$\alpha\circ\beta : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \alpha\circ\delta : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\alpha\circ\alpha : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \alpha\circ\zeta : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

These computations allow us to fill in the second row of the table.

$\circ$	$\boldsymbol{\epsilon}$	$\boldsymbol{\alpha}$	$\boldsymbol{\beta}$	$\boldsymbol{\gamma}$	$\boldsymbol{\delta}$	$\boldsymbol{\zeta}$
$\boldsymbol{\epsilon}$	ϵ	α	β	γ	δ	ζ
$\boldsymbol{\alpha}$	α	ϵ	δ	ζ	β	γ
$\boldsymbol{\beta}$	β					
$\boldsymbol{\gamma}$	γ					
$\boldsymbol{\delta}$	δ					
$\boldsymbol{\zeta}$	ζ					

The remaining rows of the table are filled in using the same approach. The complete table is given below; verification is left as an exercise.

$\circ$	$\boldsymbol{\epsilon}$	$\boldsymbol{\alpha}$	$\boldsymbol{\beta}$	$\boldsymbol{\gamma}$	$\boldsymbol{\delta}$	$\boldsymbol{\zeta}$
$\boldsymbol{\epsilon}$	ϵ	α	β	γ	δ	ζ
$\boldsymbol{\alpha}$	α	ϵ	δ	ζ	β	γ
$\boldsymbol{\beta}$	β	ζ	ϵ	δ	γ	α
$\boldsymbol{\gamma}$	γ	δ	ζ	ϵ	α	β
$\boldsymbol{\delta}$	δ	γ	α	β	ζ	ϵ
$\boldsymbol{\zeta}$	ζ	β	γ	α	ϵ	δ

****

EXERCISES FOR SECTION 5

1. Which of the binary relations below is an operation?

   (a) $\theta \subseteq \left[\mathbb{Z}^+\right]^2 \times \mathbb{Z}^+$ defined by $([b,c],a) \in \theta \iff a = b + c$

   (b) $\beta \subseteq \left[\mathbb{Z}^+\right]^2 \times \mathbb{Z}^+$ defined by $([b,c],a) \in \beta \iff a|(b+c)$

2. Construct the operation table for $\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$ under the operation $\boxplus_6$.

3. When a binary operation is defined by a table, it is relatively easy to check for commutativity — simply check to see if the table is symmetric about the main diagonal. (The elements must be listed in the same order in the zero row and zero column for this trick to work.) Which of the following binary operations on $X = \{a, b, c, d, e\}$ are commutative?

(a)

$\oslash$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$	$\boldsymbol{d}$	$\boldsymbol{e}$
$\boldsymbol{a}$	e	c	a	b	d
$\boldsymbol{b}$	c	e	c	d	a
$\boldsymbol{c}$	a	b	e	c	b
$\boldsymbol{d}$	c	d	a	e	c
$\boldsymbol{e}$	d	c	b	c	e

(b)

$\boxtimes$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{e}$	$\boldsymbol{d}$	$\boldsymbol{c}$
$\boldsymbol{a}$	a	a	a	a	a
$\boldsymbol{b}$	a	b	e	d	c
$\boldsymbol{e}$	a	e	c	b	d
$\boldsymbol{d}$	a	d	b	c	e
$\boldsymbol{c}$	a	c	d	e	b

(c)

$\boxtimes$	$\boldsymbol{b}$	$\boldsymbol{d}$	$\boldsymbol{c}$	$\boldsymbol{a}$	$\boldsymbol{e}$
$\boldsymbol{b}$	b	d	c	a	e
$\boldsymbol{d}$	d	c	a	e	b
$\boldsymbol{c}$	c	a	e	b	d
$\boldsymbol{a}$	a	e	b	d	c
$\boldsymbol{e}$	e	b	d	c	a

4. Explain why the trick used in Exercise 3 works. In other words, explain why symmetry about the main diagonal in an operation table is sufficient to show the operation is commutative.

5. Unfortunately, there is no simple visual trick to determine whether or not a table-defined operation is associative —this can only be done using case-by-case analysis. Verify that the operation below on the set $X = \{e, a, b, c\}$ is associative.

$*$	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$
$\boldsymbol{e}$	e	a	b	c
$\boldsymbol{a}$	a	e	c	b
$\boldsymbol{b}$	b	c	e	a
$\boldsymbol{c}$	c	b	a	e

6. Construct the operation table for $\wp_2$ under function composition and show that composition is commutative on this set.

7. Verify that the operation table for $\wp_3$ given in Example 58 above is correct.

8. Consider the subset $S = \{\epsilon, a, b, c\}$ of $\wp_4$ where

$$\epsilon : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \qquad a : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \qquad b : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \qquad c : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

   Show that function composition is a commutative binary operation on S. (Construct the operation table for S.)

9. Show that $\boxplus_8$ is a binary operation on the subset $T = \{[0]_8, [2]_8, [4]_8, [6]_8\}$ of $\mathbb{Z}_8$. (Construct the operation table for T.)

10. Show that function composition is *not* a binary operation on the subset $U = \{\epsilon, \beta, \zeta\}$ of $\wp_3$. (What happens when you construct the operation table for U?)

11. Show that $\boxplus_6$is *not* a binary operation on the subset $V = \{[1]_6, [3]_6, [5]_6\}$ of $\mathbb{Z}_6$. (What happens when you construct the operation table for V?)

12. Each of the relations below is a binary operation on $\mathbb{R}$. Which ones are associative? Which ones are commutative? (You may assume that real number addition and multiplication are commutative and associative.)

    (a) $x \circledcirc y = x + 2y + 4$
    (b) $x * y = |x + y|$
    (c) $x \circledast y = \texttt{Max}(x, y)$ (That is, $x \circledast y$ is the larger of the two numbers.)

13. Let n be a fixed positive integer and let $\mathbb{Z}_n = \{[0]_n, ..., [n-1]_n\}$ denote the family of residue classes modulo n that we introduced in the previous section. Show that the binary operation $\boxplus_n$on $\mathbb{Z}_n$ is commutative and associative.

14. Show that the binary operation $\maltese$ on $\mathbb{Z}^+$ defined by $m \maltese n = \texttt{GCF}(m, n)$ is commutative and associative.

15. Let n be a fixed positive integer and let $\mathbb{Z}_n = \{[0]_n, ..., [n-1]_n\}$ denote the family of residue classes modulo n that we introduced in the previous section. Define a binary relation $\mu_n \subseteq [\mathbb{Z}_n]^2 \times \mathbb{Z}_n$ by the formula

$$([[i]_n, [j]_n], [k]_n) \in \mu_n \iff k \equiv (ij)\texttt{MOD}(n)$$

    Prove that this relation is a binary operation on $\mathbb{Z}_n$.

16. The binary operation defined in Problem 14 is called *multiplication modulo n*. For $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$, let $\boxtimes_n$ be defined by

$$[a]_n \boxtimes_n [b]_n = [c]_n \iff [ab]_n = [c]_n \iff c \equiv (ab)\texttt{MOD}(n) \iff ([[a]_n, [b]_n], [c]_n) \in \mu_n$$

    Show that multiplication modulo n is commutative and associative.

17. Construction the operation table for $\mathbb{Z}_8$ under multiplication modulo 8.

18. Show that multiplication modulo 8 is a binary operation on the set $S = \{[1]_8, [3]_8, [5]_8, [7]_8\}$.