part of abstract algebra, sets are fundamental to all areas of mathematics and we need to establish a precise language for sets. We also explore operations on sets and relations between sets, developing an "algebra of sets" that strongly resembles aspects of the algebra of sentential logic. In addition, as we discussed in chapter 1, a fundamental goal in mathematics is crafting articulate, thorough, convincing, and insightful arguments for the truth of mathematical statements. We continue the development of theorem-proving and proof-writing skills in the context of basic set theory.

After exploring the algebra of sets, we study two number systems denoted $\mathbb{Z}_n$ and $U(n)$ that are closely related to the integers. Our approach is based on a widely used strategy of mathematicians: we work with specific examples and look for general patterns. This study leads to the definition of modified addition and multiplication operations on certain finite subsets of the integers. We isolate key axioms, or properties, that are satisfied by these and many other number systems and then examine number systems that share the "group" properties of the integers. Finally, we consider an application of this mathematics to check digit schemes, which have become increasingly important for the success of business and telecommunications in our technologically based society. Through the study of these topics, we engage in a thorough introduction to abstract algebra from the perspective of the mathematician—working with specific examples to identify key abstract properties common to diverse and interesting mathematical systems.

2.1 The Algebra of Sets

Intuitively, a *set* is a "collection" of objects known as "elements." But in the early 1900's, a radical transformation occurred in mathematicians' understanding of sets when the British philosopher Bertrand Russell identified a fundamental paradox inherent in this intuitive notion of a set (this paradox is discussed in exercises 66–70 at the end of this section). Consequently, in a formal set theory course, a set is defined as a mathematical object satisfying certain axioms. These axioms detail properties of sets and are used to develop an elegant and sophisticated theory of sets. This "axiomatic" approach to describing mathematical objects is relevant to the study of all areas of mathematics, and we begin exploring this approach later in this chapter. For now, we assume the existence of a suitable axiomatic framework for sets and focus on their basic relationships and operations. We first consider some examples.

Example 2.1.1 Each of the following collections of elements is a set.

- $V = \{\text{cat, dog, fish}\}$
- $W = \{1, 2\}$
- $X = \{1, 3, 5\}$
- $Y = \{n : n \text{ is an odd integer}\} = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$

■

In many settings, the upper case letters $A, B, \ldots, Z$ are used to name sets, and a pair of braces {, } is used to specify the elements of a set. In example 2.1.1, V is a finite

set of three English words identifying common household pets. Similarly, W is finite set consisting of the integers 1 and 2, and X is a finite set consisting of the integers 1, 3, and 5. We have written Y using the two most common notations for an infinite set. As finite beings, humans cannot physically list every element of an infinite set one at a time. Therefore, we often use the descriptive set notation $\{n : P(n)\}$, where $P(n)$ is a predicate stating a property that characterizes the elements in the set. Alternatively, enough elements are listed to define implicitly a pattern and ellipses ". . ." are used to denote the infinite, unbounded nature of the set. This second notation must be used carefully, since people vary considerably in their perception of patterns, while clarity and precision are needed in mathematical exposition.

Certain sets are of widespread interest to mathematicians. Most likely, they are already familiar from your previous mathematics courses. The following notation, using "barred" upper case letters, is used to denote these fundamental sets of numbers.

Definition 2.1.1
- $\emptyset$ *denotes the* **empty set** $\{\ \}$*, which does not contain any elements.*
- $\mathbb{N}$ *denotes the set of* **natural numbers** $\{ 1, 2, 3, \ldots \}$.
- $\mathbb{Z}$ *denotes the set of* **integers** $\{ \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots \}$.
- $\mathbb{Q}$ *denotes the set of* **rational numbers** $\{ p/q \ : \ p, q \in \mathbb{Z}$ *with* $q \neq 0 \}$.
- $\mathbb{R}$ *denotes the set of* **real numbers** *consisting of directed distances from a designated point zero on the continuum of the real line.*
- $\mathbb{C}$ *denotes the set of* **complex numbers** $\{ a + bi \ : \ a, b \in \mathbb{R}$ *with* $i = \sqrt{-1} \}$.

In this definition, various names are used for the same collection of numbers. For example, the natural numbers are referred to by the mathematical symbol "$\mathbb{N}$," the English words "the natural numbers," and the set-theoretic notation "$\{1, 2, 3, \ldots\}$." Mathematicians move freely among these different ways of referring to the same number system as the situation warrants. In addition, the mathematical symbols for these sets are "decorated" with the superscripts "$*$," "$+$," and "$-$" to designate the corresponding subcollections of nonzero, positive, and negative numbers, respectively. For example, applying this symbolism to the integers $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, we have

$$\begin{aligned} \mathbb{Z}^* &= \{\ldots, -3, -2, -1, 1, 2, 3, \ldots\}, \\ \mathbb{Z}^+ &= \{1, 2, 3, \ldots\}, \\ \mathbb{Z}^- &= \{-1, -2, -3, \ldots\}. \end{aligned}$$

There is some discussion in the mathematics community concerning whether or not zero is a natural number. Many define the natural numbers in terms of the "counting" numbers $1, 2, 3, \ldots$ (as we have done here) and refer to the set $\{0, 1, 2, 3, \ldots\}$ as the set of *whole numbers*. On the other hand, many mathematicians think of zero as a "natural" number. For example, the axiomatic definition of the natural numbers introduced by the Italian mathematician Giuseppe Peano in the late 1800s includes zero. Throughout this book, we use definition 2.1.1 and refer to the natural numbers as the set $\mathbb{N} = \{ 1, 2, 3, \ldots \}$.

Our study of sets focuses on relations and operations of sets. The most fundamental relation associated with sets is the "element of" relationship that indicates when an object is a member of a set.

Definition 2.1.2 *If a is an element of set A, then $a \in A$ denotes "a is an element of A."*

Example 2.1.2 As in example 2.1.1, let $W = \{1, 2\}$ and recall that $\mathbb{Q}$ is the set of rationals.

- 1 is in W, and so $1 \in W$.
- 3 is not in W, and so $3 \notin W$.
- $\frac{1}{2}$ is rational, and so $\frac{1}{2} \in \mathbb{Q}$.
- $\sqrt{2}$ is not rational (as we prove in section 3.4), and so $\sqrt{2} \notin \mathbb{Q}$.

■

Question 2.1.1 Give an example of a finite set A with $2 \in A$ and an infinite set B with $2 \notin B$.

■

We now consider relationships between sets. We are particularly interested in describing when two sets are identical or equal. As it turns out, the identity relationship on sets is best articulated in terms of a more primitive "subset" relationship describing when all the elements of one set are contained in another set.

Definition 2.1.3 *Let A and B be sets.*

- *A is a* **subset** *of B if every element of A is an element of B. We write $A \subseteq B$ and show $A \subseteq B$ by proving that if $a \in A$, then $a \in B$.*
- *A is* **equal** *to B if A and B contain exactly the same elements. We write $A = B$ and show $A = B$ by proving both $A \subseteq B$ and $B \subseteq A$.*
- *A is a* **proper subset** *of B if A is a subset of B, but A is not equal to B. We write either $A \subset B$ or $A \subsetneq B$ and show $A \subset B$ by proving both $A \subseteq B$ and $B \nsubseteq A$.*

Formally, the notation and the associated proof strategy are not part of the definition of these set relations. However, these facts are fundamental to working with sets and you will want to become adept at transitioning freely among definition, notation, and proof strategy.

Example 2.1.3 As in example 2.1.1, let $W = \{1, 2\}$, $X = \{1, 3, 5\}$, and $Y = \{n : n \text{ is an odd integer}\}$. We first prove $X \subseteq Y$ and then prove $W \nsubseteq Y$.

Proof that $X \subseteq Y$ We prove $X \subseteq Y$ by showing that if $a \in X$, then $a \in Y$. Since $X = \{1, 3, 5\}$ is finite, we prove this implication by exhaustion; that is, we consider every element of X one at a time and verify that each is in Y. Since $1 = 2 \cdot 0 + 1$, $3 = 2 \cdot 1 + 1$, and $5 = 2 \cdot 2 + 1$, each element of X is odd; in particular, each element of X has been expressed as $2k + 1$ for some $k \in \mathbb{Z}$). Thus, if $a \in X$, then $a \in Y$, and so $X \subseteq Y$.

■

Proof that $W \nsubseteq Y$ We prove $W \nsubseteq Y$ by showing that $a \in W$ does not necessarily imply $a \in Y$. Recall that $(p \rightarrow q)$ is false precisely when $[p \wedge (\sim q)]$ is true; in this case, we need to identify a counterexample with $a \in W$ and $a \notin Y$. Consider $2 \in W$. Since $2 = 2 \cdot 1$ is even, we conclude $2 \notin Y$. Therefore, not every element of W is an element of Y.

■

Question 2.1.2 As in example 2.1.1, let $X = \{1, 3, 5\}$ and $Y = \{n : n \text{ is an odd integer }\}$. Prove that X is a proper subset of Y.

■

Example 2.1.4 The fundamental sets of numbers from definition 2.1.1 are contained in one another according to the following proper subset relationships.

$$\emptyset \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

■

When working with relationships among sets, we must be careful to use the notation properly so as to express true mathematical statements. One common misuse of set-theoretic notation is illustrated by working with the set $W = \{1, 2\}$. While it is true that $1 \in W$ since 1 is in W, the assertion that $\{1\} \in W$ is *not* true. In particular, W contains only numbers, not sets, and so the set $\{1\}$ is not in W. In general, some sets do contain sets—W is just not one of these sets. Similarly, we observe that $\{1\} \subseteq W$ since $1 \in \{1, 2\} = W$, but $1 \subseteq W$ is *not* true; indeed, $1 \subseteq W$ is not a sensible mathematical statement since the notation $\subseteq$ is not defined between an element and a set, but only between sets.

Despite these distinctions, there is a strong connection between the "element of" relation $\in$ and the subset relation $\subseteq$, as you are asked to develop in the following question. In this way, we move beyond discussing relationships among specific sets of numbers to exploring more general, abstract properties that hold for every element and every set.

Question 2.1.3 Prove that $a \in A$ if and only if $\{a\} \subseteq A$.
Hint: Use definitions 2.1.2 and 2.1.3 to prove the two implications forming this "if-and-only-if" mathematical statement.

■

We now turn our attention to six fundamental operations on sets. These set operations manipulate a single set or a pair of sets to produce a new set. When applying the first three of these operations, you will want to utilize the close correspondence between the set operations and the connectives of sentential logic.

Definition 2.1.4 *Let A and B be sets.*

- *A^C denotes the* **complement** *of A and consists of all elements not in A, but in some prespecified* **universe** *or* **domain** *of all possible elements including those in A; symbolically, we define $A^C = \{x : x \notin A\}$.*
- *$A \cap B$ denotes the* **intersection** *of A and B and consists of the elements in both A and B; symbolically, we define $A \cap B = \{x : x \in A \text{ and } x \in B\}$.*
- *$A \cup B$ denotes the* **union** *of A and B and consists of the elements in A or in B or in both A and B; symbolically, we define $A \cup B = \{x : x \in A \text{ or } x \in B\}$.*
- *$A \setminus B$ denotes the* **set difference** *of A and B and consists of the elements in A that are not in B; symbolically, we define $A \setminus B = \{x : x \in A \text{ and } x \notin B\}$. We often use the identity $A \setminus B = A \cap B^C$.*

- *$A \times B$ denotes the* **Cartesian product** *of A and B and consists of the set of all ordered pairs with first-coordinate in A and second-coordinate in B; symbolically, we define $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$.*
- *$\mathbb{P}(A)$ denotes the* **power set** *of A and consists of all subsets of A; symbolically, we define $\mathbb{P}(A) = \{X : X \subseteq A\}$. Notice that we always have $\emptyset \in \mathbb{P}(A)$ and $A \in \mathbb{P}(A)$.*

Example 2.1.5 As above, we let $W = \{1, 2\}$, $X = \{1, 3, 5\}$ and $Y = \{n : n \text{ is an odd integer }\}$. In addition, we assume that the set of integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is the universe and we identify the elements of the following sets.

- $W^C = \{\ldots, -2, -1, 0, 3, 4, 5, \ldots\}$
- $Y^C = \{n : n \text{ is an even integer }\}$ by the parity property of the integers
- $W \cap X = \{1\}$, since 1 is the only element in both W and X
- $W \cup X = \{1, 2, 3, 5\}$, since union is defined using the inclusive-or
- $W \setminus X = \{2\}$
- $X \setminus W = \{3, 5\}$
- $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\} = \{\ldots, -3, -2, -1, 1, 2, 3, \ldots\}$
- $W \times X = \{(1, 1), (1, 3), (1, 5), (2, 1), (2, 3), (2, 5)\}$
- $\mathbb{P}(W) = \{\ \emptyset,\ \{1\},\ \{2\},\ \{1, 2\}\ \}$

■

The last two sets given in example 2.1.5 contain mathematical objects other than numbers; the power set is also an example of a set containing other sets. As we continue exploring mathematics, we will study sets of functions, matrices, and other more sophisticated mathematical objects.

Question 2.1.4 Working with W, X, and Y from example 2.1.5, identify the elements in the sets X^C, $W \cap Y$, $W \cup Y$, $W \setminus Y$, $Y \setminus W$, $X \times W$, $W \times W$, $W \times Y$, and $\mathbb{P}(X)$. In addition, state six elements in $\mathbb{P}(Y)$; that is, state six subsets of Y.

■

The use of symbols to represent relationships and operations on mathematical objects is a standard feature of mathematics. Good choices in symbolism can facilitate mathematical understanding and insight, while poor choices can genuinely hinder the study and creation of mathematics. Historically, the symbols $\in$ for "element of," $\cap$ for "intersection," and $\cup$ for "union" were introduced in 1889 by the Italian mathematician Giuseppe Peano. His work in formalizing and axiomatizing set theory and the basic arithmetic of the natural numbers remains of central importance. The Cartesian product $\times$ is named in honor of the French mathematician and philosopher René Descartes, who first formulated "analytic geometry" (an important branch of mathematics discussed in section 4.1).

Although we have presented the Cartesian product $A \times B$ as an operation on pairs of sets, this product extends to any finite number of sets. Mathematicians work with ordered triples $A \times B \times C = \{(a, b, c) : a \in A, b \in B, \text{ and } c \in C\}$, ordered quadruples $A \times B \times C \times D = \{(a, b, c, d) : a \in A, b \in B, c \in C, \text{ and } d \in D\}$, and even ordered n-tuples $A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) : a_i \in A_i \text{ for } 1 \leq i \leq n\}$. While the use of n-tuples may at first seem to be of purely academic interest, models for science

and business with tens (and even hundreds and thousands) of independent variables have become more common as computers have extended our capacity to analyze increasingly sophisticated events.

Along with considering the action of set-theoretic operations on specific sets of numbers, we are also interested in exploring general, abstract properties that hold for all sets. In this way we develop an algebra of sets, comparing various sets to determine when one is a subset of another or when they are equal. In developing this algebra, we adopt the standard approach of confirming informal intuitions and educated guesses with thorough and convincing proofs.

Example 2.1.6 For sets A and B, we prove $A \cap B \subseteq A$.

Proof We prove $A \cap B \subseteq A$ by showing that if $a \in A \cap B$, then $a \in A$. We give a direct proof of this implication; we assume that $a \in A \cap B$ and show that $a \in A$. Since $a \in A \cap B$, both $a \in A$ and $a \in B$ from the definition of intersection. We have thus quickly obtained the goal of showing $a \in A$.

■

In example 2.1.6 we used a direct proof to show that one set is a subset of another. This strategy is very important: we prove $X \subseteq Y$ by assuming $a \in X$ and showing $a \in Y$. In addition, the process of proving $a \in X$ implies $a \in Y$ usually involves "taking apart" the sets X and Y and characterizing their elements based on the appropriate set-theoretic definitions. Once X and Y have been expanded in this way, our insights into sentential logic should enable us to understand the relationship between the two sets and to craft a proof (or disproof) of the claim. We illustrate this approach by verifying another set-theoretic identity.

Example 2.1.7 For sets A and B, we prove $A \setminus B = A \cap B^C$.

Proof In general, we prove two sets are equal by demonstrating that they are subsets of each other. In this case, we must show both $A \setminus B \subseteq A \cap B^C$ and $A \cap B^C \subseteq A \setminus B$.

$A \setminus B \subseteq A \cap B^C$: We assume $a \in A \setminus B$ and show $a \in A \cap B^C$. Since $a \in A \setminus B$, we know $a \in A$ and $a \notin B$. The key observation is that $a \notin B$ is equivalent to $a \in B^C$ from the definition of set complement. Since $a \in A$ and $a \notin B$, we have both $a \in A$ and $a \in B^C$. Therefore, by the definition of intersection, $a \in A \cap B^C$. Thus, we have $A \setminus B \subseteq A \cap B^C$, completing the first half of the proof.

$A \cap B^C \subseteq A \setminus B$: We assume $a \in A \cap B^C$ and show $a \in A \setminus B$. From the definition of intersection, we know $a \in A \cap B^C$ implies both $a \in A$ and $a \in B^C$. Therefore, both $a \in A$ and $a \notin B$ from the definition of complement. This is exactly the definition of set difference, and so $a \in A \setminus B$. Thus, $A \cap B^C \subseteq A \setminus B$, completing the second half of the proof.

The proof of these two subset relationships establishes the desired equality $A \setminus B = A \cap B^C$ for every set A and B.

■

Question 2.1.5 Prove that if A and B are sets with $A \subseteq B$, then $B^C \subseteq A^C$.

■

A whole host of set-theoretic identities can be established using the strategies illustrated in the preceding examples. As we have seen, the ideas and identities of sentential logic play a fundamental role in working with the set-theoretic operations. Recall that De Morgan's laws are among the most important identities from sentential logic; consider the following set-theoretic version of these identities.

Example 2.1.8 De Morgan's laws for sets We prove one of De Morgan's laws for sets: If A and B are sets, then both $(A \cap B)^C = A^C \cup B^C$ and $(A \cup B)^C = A^C \cap B^C$.

Proof We prove the identity $(A \cap B)^C = A^C \cup B^C$ by arguing that each set is a subset of the other based on the following biconditionals:

$a \in (A \cap B)^C$	iff	$a \notin A \cap B$	Definition of complement
	iff	a is not in both A and B	Definition of intersection
	iff	either $a \notin A$ or $a \notin B$	Sentential De Morgan's laws
	iff	either $a \in A^C$ or $a \in B^C$	Definition of complement
	iff	$a \in A^C \cup B^C$	Definition of union

Working through these biconditionals from top to bottom, we have $a \in (A \cap B)^C$ implies $a \in A^C \cup B^C$, and so $(A \cap B)^C \subseteq A^C \cup B^C$. Similarly, working through these biconditionals from bottom to top, we have $a \in A^C \cup B^C$ implies $a \in (A \cap B)^C$, and so $A^C \cup B^C \subseteq (A \cap B)^C$. This proves one of De Morgan's laws for sets, $(A \cap B)^C = A^C \cup B^C$ for every set A and B.

■

Question 2.1.6 Prove the other half of De Morgan's laws for sets; namely, prove that if A and B are sets, then $(A \cup B)^C = A^C \cap B^C$.

■

We end this section by discussing proofs that certain set-theoretic relations and identities do *not* hold. From section 1.7, we know that (supposed) identities can be disproved by finding a counterexample, exhibiting specific sets for which the given equality does not hold. To facilitate the definition of sets A, B, C with the desired properties, we introduce a visual tool for describing sets and set operations known as a *Venn diagram.* In a Venn diagram, the universe is denoted with a rectangle, and sets are drawn inside this rectangle using circles or ellipses. When illustrating two or more sets in a Venn diagram, we draw overlapping circles to indicate the possibility that the sets may share some elements in common. The Venn diagrams for the first four set operations from definition 2.1.4 are given in figure 2.1.

Example 2.1.9 We disprove the *false* claim that if A, B, and C are sets, then $A \cap (B \cup C) = (A \cap B) \cup C$. This demonstrates that union and intersection operations are not associative when used together, and so we must be careful with the order of operation when "mixing" union and intersection.

The Venn diagrams given in figure 2.2 illustrate the sets we are considering in this example. We use three circles to denote the three distinct sets A, B, and C. In addition, the circles overlap in a general way so as to indicate all the various possibilities for sets sharing elements.

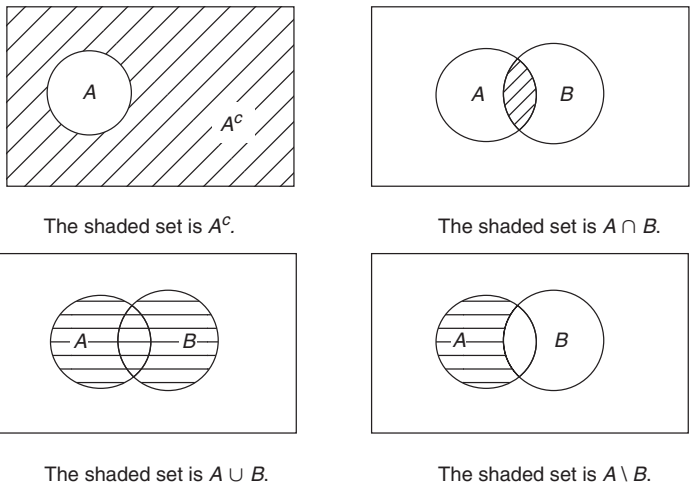

Figure 2.1 Venn diagrams for basic set operations

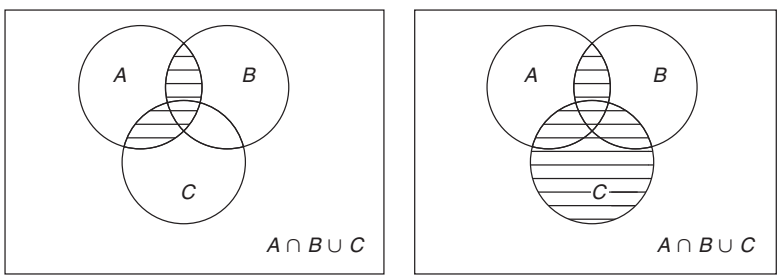

Figure 2.2 The Venn diagram for example 2.1.9 showing $A \cap (B \cup C) \neq (A \cap B) \cup C$

Examining the Venn diagrams, we see that if A, B, C are defined so that C contains an element that is in neither A nor B, the sets $A \cap (B \cup C)$ and $(A \cap B) \cup C$ will be different. Alternatively, we could define A, B, C so that $B \cap C$ contains an element that is not in A. Following the first approach, we choose to define the sets $A = \{1\},\ B = \{1, 2\}$, and $C = \{1, 2, 3\}$ and verify the desired inequality with the following computations.

$$\begin{aligned} A \cap (B \cup C) &= \{1\} \cap \{1, 2, 3\} = \{1\} \\ (A \cap B) \cup C &= \{1\} \cup \{1, 2, 3\} = \{1, 2, 3\} \end{aligned}$$

Therefore these three sets provide a counterexample demonstrating that sometimes $A \cap (B \cup C) \neq (A \cap B) \cup C$.

■

In example 2.1.9, the choice of sets A, B, and C is just one choice among many. We are certainly free to make other choices, and you might even think of

constructing counterexamples as providing an opportunity to express your "mathematical personality."

Question 2.1.7 Guided by example 2.1.9, give another counterexample disproving the *false* claim that $A \cap (B \cup C) = (A \cap B) \cup C$ for all sets A, B, C.

■

We highlight one subtlety that arises in this setting. In example 2.1.9 and question 2.1.7, the counterexamples only disprove the general claim that $A \cap (B \cup C) = (A \cap B) \cup C$ for all sets A, B, C. However, these counterexamples do *not* prove that we have inequality for every choice of sets. In fact, there exist many different cases in which equality does hold. For example, both $A = \emptyset, B = \emptyset, C = \emptyset$ and $A = \{1, 2\}, B = \{1, 3\}, C = \{1\}$ produce the equality $A \cap (B \cup C) = (A \cap B) \cup C$, but only because we are working with these specific sets. We therefore cannot make any general claims about the equality of $A \cap (B \cup C)$ and $(A \cap B) \cup C$, but must consider each possible setting on a case-by-case basis. In short, if we want to prove that a set-theoretic identity does not always hold, then a counterexample accomplishes this goal; if we want to prove that a set-theoretic identity never holds, then we must provide a general proof and not just a specific (counter)example.

Question 2.1.8 Sketch the Venn diagram representing the following sets.

(a) $(A \cup B) \cap C$ (b) $A^C \setminus B$

■

Question 2.1.9 Following the model given in example 2.1.9, disprove the *false* claim that the following identities hold for all sets A, B, C.

(a) $(A \cup B) \cap C = A \cup (B \cap C)$ (b) $A^C \setminus B = (A \setminus B)^C$

■

2.1.1 Reading Questions for Section 2.1

1. What is the intuitive definition of a set?
2. What is the intuitive definition of an element?
3. Describe two approaches to identifying the elements of an infinite set.
4. Name six important sets and the symbolic notation for these sets.
5. Define and give an example of the "element of" relation $a \in A$.
6. Define and give an example of the set relations: $A \subseteq B$, $A = B$, and $A \subset B$.
7. If A and B are sets, what strategy do we use to prove that $A \subseteq B$?
8. If A and B are sets, what strategy do we use to prove that $A = B$?
9. Define and give an example of the set operations: A^C, $A \cap B$, $A \cup B$, $A \setminus B$, $A \times B$, and $\mathbb{P}(A)$.
10. Define and give an example of a generalized Cartesian product $A_1 \times A_2 \times \cdots \times A_n$.
11. State both the sentential logic and the set-theoretic versions of De Morgan's laws.
12. Discuss the use of a Venn diagram for representing sets.