22. Continuing the idea in the preceding exercise and using Exercises 18 and 19, use exponential notation to fill in the three blanks to give a list of five cardinal numbers, each of which is greater than the preceding one.

$$\aleph_0, |\mathbb{R}|, \_\_, \_\_, \_\_.$$

In Exercises 23 through 27, find the number of different partitions of a set having the given number of elements.

23. 1 element **24.** 2 elements **25.** 3 elements

26. 4 elements **27.** 5 elements

28. Consider a partition of a set S. The paragraph following Definition 0.18 explained why the relation

$$x \mathcal{R} y \text{ if and only if } x \text{ and } y \text{ are in the same cell}$$

satisfies the symmetric condition for an equivalence relation. Write similar explanations of why the reflexive and transitive properties are also satisifed.

In Exercises 29 through 34, determine whether the given relation is an equivalence relation on the set. Describe the partition arising from each equivalence relation.

29. $n \mathcal{R} m$ in $\mathbb{Z}$ if $nm > 0$ **30.** $x \mathcal{R} y$ in $\mathbb{R}$ if $x \geq y$

31. $x \mathcal{R} y$ in $\mathbb{Z}^+$ if the greatest common divisor of x and y is greater than 1

32. $(x_1, y_1) \mathcal{R} (x_2, y_2)$ in $\mathbb{R} \times \mathbb{R}$ if $x_1^2 + y_1^2 = x_2^2 + y_2^2$

33. $n \mathcal{R} m$ in $\mathbb{Z}^+$ if n and m have the same number of digits in the usual base ten notation

34. $n \mathcal{R} m$ in $\mathbb{Z}^+$ if n and m have the same final digit in the usual base ten notation

35. Using set notation of the form $\{\ldots, \#, \#, \#, \cdots\}$, write the residue classes modulo n in $\mathbb{Z}$ as discussed in Example 0.17 for the indicated values of n.

a. 3 **b.** 4 **c.** 5

36. Write each set by listing its elements.

a. $\mathbb{Z}/3\mathbb{Z}$ **b.** $\mathbb{Z}/4\mathbb{Z}$ **c.** $\mathbb{Z}/5\mathbb{Z}$

37. When discussing residue classes, $\overline{1}$ is not well defined until the modulus n is given. Explain.

38. Let $n \in \mathbb{Z}^+$ and let $\sim$ be defined on $\mathbb{Z}$ by $r \sim s$ if and only if $r - s$ is divisible by n, that is, if and only if $r - s = nq$ for some $q \in \mathbb{Z}$.

a. Show that $\sim$ is an equivalence relation on $\mathbb{Z}$.

b. Show that this $\sim$ is the equivalence relation, *congruence modulo n*, of Example 0.20.

39. Let $n \in \mathbb{Z}^+$. Using the relation from Exercise 38, show that if $a_1 \sim a_2$ and $b_1 \sim b_2$, then $(a_1 + b_1) \sim (a_2 + b_2)$.

40. Let $n \in \mathbb{Z}^+$. Using the relation from Exercise 38, show that if $a_1 \sim a_2$ and $b_1 \sim b_2$, then $(a_1 b_1) \sim (a_2 b_2)$.

41. Students often misunderstand the concept of a one-to-one function (mapping). I think I know the reason. You see, a mapping $\phi : A \to B$ has a *direction* associated with it, from A to B. It seems reasonable to expect a one-to-one mapping simply to be a mapping that carries one point of A into one point of B, in the direction indicated by the arrow. But of course, *every* mapping of A into B does this, and Definition 0.12 did not say that at all. With this unfortunate situation in mind, make as good a pedagogical case as you can for calling the functions described in Definition 0.12 *two-to-two functions* instead. (Unfortunately, it is almost impossible to get widely used terminology changed.)

This page is intentionally left blank

PART I

Groups and Subgroups

Section 1 Binary Operations
Section 2 Groups
Section 3 Abelian Examples
Section 4 Nonabelian Examples
Section 5 Subgroups
Section 6 Cyclic Groups
Section 7 Generating Sets and Cayley Digraphs

SECTION 1 BINARY OPERATIONS

The transition from elementary school arithmetic to high school algebra involves using letters to represent unknown numbers and studying the basic properties of equations and expressions. The two main binary operations used in high school algebra are addition and multiplication. Abstract algebra takes the next step in abstraction. Not only are the variables unknown, but the actual operations involved may be unknown! We will study sets that have binary operations with properties similar to those of addition and multiplication of numbers. In Part I, our goal will be to develop some of the basic properties of a group. In this section we start our investigation of groups by defining binary operations, naming properties possessed by some binary operations, and giving examples.

Definitions and Examples

The first step in our journey to understand groups is to give a precise mathematical definition of a binary operation that generalizes the familiar addition and multiplication of numbers. Recall that for any set S, Definition 0.4 defines the set $S \times S$ to contain all ordered pairs (a, b) with $a, b \in S$.

1.1 Definition A **binary operation** $*$ on a set S is a function mapping $S \times S$ into S. For each $(a, b) \in S \times S$, we will denote the element $*((a, b))$ of S by $a * b$. ■

Intuitively, we may regard a binary operation $*$ on S as assigning, to each ordered pair (a, b) of elements of S, an element $a * b$ of S.

Binary refers to the fact that we are mapping *pairs* of elements from S into S. We could also define a ternary operation as a function mapping triples of elements of S to S, but we will have no need for this type of operation. Throughout this book we will often drop the term binary and use the term operation to mean binary operation.

1.2 Example Our usual addition $+$ is an operation on the set $\mathbb{R}$. Our usual multiplication $\cdot$ is a different operation on $\mathbb{R}$. In this example, we could replace $\mathbb{R}$ by any of the sets $\mathbb{C}, \mathbb{Z}$, $\mathbb{R}^+$, or $\mathbb{Z}^+$. ▲

Note that we require an operation on a set S to be defined for *every* ordered pair (a, b) of elements from S.

1.3 Example Let $M(\mathbb{R})$ be the set of all matrices[†] with real entries. The usual matrix addition $+$ is *not* an operation on this set since $A + B$ is not defined for an ordered pair (A, B) of matrices having different numbers of rows or of columns. ▲

Sometimes an operation on S provides an operation on a subset H of S also. We make a formal definition.

1.4 Definition Let $*$ be an operation on S and let H be a subset of S. The subset H is **closed under** $*$ if for all $a, b \in H$ we also have $a * b \in H$. In this case, the operation on H given by restricting $*$ to H is the **induced operation** of $*$ on H. ■

By our very definition of an operation $*$ on S, the set S is closed under $*$, but a subset may not be, as the following example shows.

1.5 Example Our usual addition $+$ on the set $\mathbb{R}$ of real numbers does not induce an operation on the set $\mathbb{R}^*$ of nonzero real numbers because $2 \in \mathbb{R}^*$ and $-2 \in \mathbb{R}^*$, but $2 + (-2) = 0$ and $0 \notin \mathbb{R}^*$. Thus $\mathbb{R}^*$ is not closed under $*$. ▲

In our text, we will often have occasion to decide whether a subset H of S is closed under a binary operation $*$ on S. To arrive at a correct conclusion, *we have to know what it means for an element to be in* H, and to use this fact. Students often have trouble here. Be sure you understand the next example.

1.6 Example Let $+$ and $\cdot$ be the usual operations of addition and multiplication on the set $\mathbb{Z}$, and let $H = \{n^2 | n \in \mathbb{Z}^+\}$. Determine whether H is closed under (a) addition and (b) multiplication.

For part (a), we need only observe that $1^2 = 1$ and $2^2 = 4$ are in H, but that $1 + 4 = 5$ and $5 \notin H$. Thus H is not closed under addition.

For part (b), suppose that $r \in H$ and $s \in H$. Using what it means for r and s to be in H, we see that there must be integers n and m in $\mathbb{Z}^+$ such that $r = n^2$ and $s = m^2$. Consequently, $rs = n^2m^2 = (nm)^2$. By the characterization of elements in H and the fact that $nm \in \mathbb{Z}^+$, this means that $rs \in H$, so H is closed under multiplication. ▲

1.7 Example Let F be the set of all real-valued functions f having as domain the set $\mathbb{R}$ of real numbers. We are familiar from calculus with the operations $+, -, \cdot$, and $\circ$ on F. Namely, for each ordered pair (f, g) of functions in F, we define for each $x \in \mathbb{R}$

$$\begin{array}{rll} f + g \text{ by } (f + g)(x) = f(x) + g(x) & & \text{addition,} \\ f - g \text{ by } (f - g)(x) = f(x) - g(x) & & \text{subtraction,} \\ f \cdot g \text{ by } (f \cdot g)(x) = f(x)g(x) & & \text{multiplication, and} \\ f \circ g \text{ by } (f \circ g)(x) = f(g(x)) & & \text{composition.} \end{array}$$

All four of these functions are again real valued with domain $\mathbb{R}$, so F is closed under all four operations $+, -, \cdot$, and $\circ$. ▲

The operations described in the examples above are very familiar to you. In this text, we want to *abstract* basic structural concepts from our familiar algebra. To empha-

[†] Most students of abstract algebra have studied linear algebra and are familiar with matrices and matrix operations. For the benefit of those students, examples involving matrices are often given. The reader who is not familiar with matrices can either skip all references to them or turn to the Appendix at the back of the text, where there is a short summary.

size this concept of *abstraction* from the familiar, we should illustrate these structural concepts with unfamiliar examples.

The most important method of describing a particular binary operation $*$ on a given set is to characterize the element $a * b$ assigned to each pair (a, b) by some property defined in terms of a and b.

1.8 Example On $\mathbb{Z}^+$, we define an operation $*$ by $a * b$ equals the smaller of a and b, or the common value if $a = b$. Thus $2 * 11 = 2$; $15 * 10 = 10$; and $3 * 3 = 3$. ▲

1.9 Example On $\mathbb{Z}^+$, we define an operation $*'$ by $a *' b = a$. Thus $2 *' 3 = 2; 25 *' 10 = 25$; and $5 *' 5 = 5$. ▲

1.10 Example On $\mathbb{Z}^+$, we define an operation $*''$ by $a *'' b = (a * b) + 2$, where $*$ is defined in Example 1.8. Thus $4 *'' 7 = 6; 25 *'' 9 = 11$; and $6 *'' 6 = 8$. ▲

It may seem that these examples are of no importance, but in fact they are used millions of times each day. For example, consider the GPS navigational system installed in most cars and cell phones. It searches alternative driving routes, computes the travel time, and determines which route takes less time. The operation in Example 1.8 is programmed into modern GPS systems and it plays an essential role.

Examples 1.8 and 1.9 were chosen to demonstrate that an operation may or may not depend on the order of the given pair. Thus in Example 1.8, $a * b = b * a$ for all $a, b \in \mathbb{Z}^+$, and in Example 1.9 this is not the case, for $5 *' 7 = 5$ but $7 *' 5 = 7$.

1.11 Definition An operation $*$ on a set S is **commutative** if (and only if) $a * b = b * a$ for all $a, b \in S$. ■

As was pointed out in Section 0, it is customary in mathematics to omit the words *and only if* from a definition. Definitions are always understood to be if and only if statements. *Theorems are not always if and only if statements, and no such convention is ever used for theorems.*

Now suppose we wish to consider an expression of the form $a * b * c$. A binary operation $*$ enables us to combine only two elements, and here we have three. The obvious attempts to combine the three elements are to form either $(a * b) * c$ or $a * (b * c)$. With $*$ defined as in Example 1.8, $(2 * 5) * 9$ is computed by $2 * 5 = 2$ and then $2 * 9 = 2$. Likewise, $2 * (5 * 9)$ is computed by $5 * 9 = 5$ and then $2 * 5 = 2$. Hence $(2 * 5) * 9 = 2 * (5 * 9)$, and it is not hard to see that for this $*$,

$$(a * b) * c = a * (b * c),$$

so there is no ambiguity in writing $a * b * c$. But for $*''$ of Example 1.10,

$$(2 *'' 5) *'' 9 = 4 *'' 9 = 6,$$

while

$$2 *'' (5 *'' 9) = 2 *'' 7 = 4.$$

Thus $(a *'' b) *'' c$ need not equal $a *'' (b *'' c)$, and the expression $a *'' b *'' c$ is ambiguous.

1.12 Definition An operation on a set S is **associative** if $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$. ■

It can be shown that if $*$ is associative, then longer expressions such as $a * b * c * d$ are not ambiguous. Parentheses may be inserted in any fashion for purposes of computation; the final results of two such computations will be the same.