EXERCISES 1

Computations

Exercises 1 through 4 concern the binary operation $*$ defined on $S = \{a, b, c, d, e\}$ by means of Table 1.31.

1. Compute $b * d$, $c * c$, and $[(a * c) * e] * a$.

2. Compute $(a * b) * c$ and $a * (b * c)$. Can you say on the basis of this computation whether $*$ is associative?

3. Compute $(b * d) * c$ and $b * (d * c)$. Can you say on the basis of this computation whether $*$ is associative?

4. Is $*$ commutative? Why?

5. Complete Table 1.32 so as to define a commutative binary operation $*$ on $S = \{a, b, c, d\}$.

6. Table 1.33 can be completed to define an associative binary operation $*$ on $S = \{a, b, c, d\}$. Assume this is possible and compute the missing entries. Does S have an identity element?

1.31 Table

$*$	a	b	c	d	e
a	a	b	c	b	d
b	b	c	a	e	c
c	c	a	b	b	a
d	b	e	b	e	d
e	d	b	a	d	c

1.32 Table

$*$	a	b	c	d
a	a	b	c	
b	b	d		c
c	c	a	d	b
d	d			a

1.33 Table

$*$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	d	c	d
d				

In Exercises 7 through 11, determine whether the operation $*$ is associative, whether the operation is commutative, and whether the set has an identity element.

7. $*$ defined on $\mathbb{Z}$ by letting $a * b = a - b$

8. $*$ defined on $\mathbb{Q}$ by letting $a * b = 2ab + 3$

9. $*$ defined on $\mathbb{Z}$ by letting $a * b = ab + a + b$

10. $*$ defined on $\mathbb{Z}^+$ by letting $a * b = 2^{ab}$

11. $*$ defined on $\mathbb{Z}^+$ by letting $a * b = a^b$

12. Let S be a set having exactly one element. How many different binary operations can be defined on S? Answer the question if S has exactly 2 elements; exactly 3 elements; exactly n elements.

13. How many different commutative binary operations can be defined on a set of 2 elements? on a set of 3 elements? on a set of n elements?

14. How many different binary operations on a set S with n elements have the property that for all $x \in S$, $x * x = x$?

15. How many different binary operations on a set S with n elements have an identity element?

Concepts

In Exercises 16 through 19, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

16. A binary operation $*$ is *commutative* if and only if $a * b = b * a$.

17. A binary operation $*$ on a set S is *associative* if and only if, for all $a, b, c \in S$, we have $(b * c) * a = b * (c * a)$.

18. A subset H of a set S is *closed* under a binary operation $*$ on S if and only if $(a * b) \in H$ for all $a, b \in S$.

19. An identity in the set S with operation $*$ is an element $e \in S$ such that $a * e = e * a = a$.

20. Is there an example of a set S, a binary operation on S, and two different elements $e_1, e_2 \in S$ such that for all $a \in S$, $e_1 * a = a$ and $a * e_2 = a$? If so, give an example and if not, prove there is not one.

In Exercises 21 through 26, determine whether the definition of $*$ does give a binary operation on the set. In the event that $*$ is not a binary operation, state whether Condition 1, Condition 2, or both conditions regarding defining binary operations are violated.

21. On $\mathbb{Z}^+$, define $a * b = b^a$.

22. On $\mathbb{R}^+$, define $*$ by letting $a * b = 2a - b$.

23. On $\mathbb{R}^+$, define $*$ by $a * b$ to be the minimum of a and $b - 1$ if they are different and their common value if they are the same.

24. On $\mathbb{R}$, define $a * b$ to be the number c so that $c^b = a$.

25. On $\mathbb{Z}^+$, define $*$ by letting $a * b = c$, where c is at least 5 more than $a + b$.

26. On $\mathbb{Z}^+$, define $*$ by letting $a * b = c$, where c is the largest integer less than the product of a and b.

27. Let H be the subset of $M_2(\mathbb{R})$ consisting of all matrices of the form $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ for $a, b \in \mathbb{R}$. Is H closed under

a. matrix addition? **b.** matrix multiplication?

28. Determine whether each of the following is true or false.

a. If $*$ is any binary operation on any set S, then $a * a = a$ for all $a \in S$.
b. If $*$ is any commutative binary operation on any set S, then $a * (b * c) = (b * c) * a$ for all $a, b, c \in S$.
c. If $*$ is any associative binary operation on any set S, then $a * (b * c) = (b * c) * a$ for all $a, b, c \in S$.
d. The only binary operations of any importance are those defined on sets of numbers.
e. A binary operation $*$ on a set S is commutative if there exist $a, b \in S$ such that $a * b = b * a$.
f. Every binary operation defined on a set having exactly one element is both commutative and associative.
g. A binary operation on a set S assigns at least one element of S to each ordered pair of elements of S.
h. A binary operation on a set S assigns at most one element of S to each ordered pair of elements of S.
i. A binary operation on a set S assigns exactly one element of S to each ordered pair of elements of S.
j. A binary operation on a set S may assign more than one element of S to some ordered pair of elements of S.
k. For any binary operation $*$ on the set S, if $a, b, c \in S$ and $a * b = a * c$, then $b = c$.
l. For any binary operation $*$ on the set S, there is an element $e \in S$ such that for all $x \in S$, $x * e = x$.
m. There is an operation on the set $S = \{e_1, e_2, a\}$ so that for all $x \in S$, $e_1 * x = e_2 * x = x$.
n. Identity elements are always called e.

29. Give a set different from any of those described in the examples of the text and not a set of numbers. Define two different binary operations $*$ and $*'$ on this set. Be sure that your set is *well defined*.

Theory

30. Prove that if $*$ is an associative and commutative binary operation on a set S, then

$$(a * b) * (c * d) = [(d * c) * a] * b$$

for all $a, b, c, d \in S$. Assume the associative law only for triples as in the definition, that is, assume only

$$(x * y) * z = x * (y * z)$$

for all $x, y, z \in S$.

In Exercises 31 and 32, either prove the statement or give a counterexample.

31. Every binary operation on a set consisting of a single element is both commutative and associative.

32. Every commutative binary operation on a set having just two elements is associative.

Let F be the set of all real-valued functions having as domain the set $\mathbb{R}$ of all real numbers. Example 1.7 defined the binary operations $+, -, \cdot$, and $\circ$ on F. In Exercises 33 through 41, either prove the given statement or give a counterexample.

33. Function addition $+$ on F is associative.

34. Function subtraction $-$ on F is commutative.

35. Function subtraction $-$ on F is associative.

36. Under function subtraction $-$ F has an identity.

37. Under function multiplication $\cdot$ F has an identity.

38. Function multiplication $\cdot$ on F is commutative.

39. Function multiplication $\cdot$ on F is associative.

40. Function composition $\circ$ on F is commutative.

41. If $*$ and $*'$ are any two binary operations on a set S, then

$$a * (b *' c) = (a * b) *' (a * c) \qquad \text{for all} \quad a, b, c \in S.$$

42. Suppose that $*$ is an *associative binary* operation on a set S. Let $H = \{a \in S \mid a * x = x * a \text{ for all } x \in S\}$. Show that H is closed under $*$. (We think of H as consisting of all elements of S that *commute* with every element in S.)

43. Suppose that $*$ is an associative and commutative binary operation on a set S. Show that $H = \{a \in S \mid a * a = a\}$ is closed under $*$. (The elements of H are **idempotents** of the binary operation $*$.)

44. Let S be a set and let $*$ be a binary operation on S satisfying the two laws

- $x * x = x$ for all $s \in S$, and
- $(x * y) * z = (y * z) * x$ for all $x, y, z \in S$.

Show that $*$ is associative and commutative. (This is problem B-1 on the 1971 Putnam Competition.)

SECTION 2 GROUPS

In high school algebra, one of the key objectives is to learn how to solve equations. Even before learning algebra, students in elementary school are given problems like $5 + \square = 2$ or $2 \times \square = 3$, which become $5 + x = 2$ and $2x = 3$ in high school algebra. Let us closely examine the steps we use to solve these equations:

$$\begin{aligned}
5 + x &= 2, && \text{given,}\\
-5 + (5 + x) &= -5 + 2, && \text{adding } -5,\\
(-5 + 5) + x &= -5 + 2, && \text{associative law,}\\
0 + x &= -5 + 2, && \text{computing } -5 + 5,\\
x &= -5 + 2, && \text{property of } 0,\\
x &= -3, && \text{computing } -5 + 2.
\end{aligned}$$

Strictly speaking, we have not shown here that -3 is a solution, but rather that it is the only possibility for a solution. To show that -3 is a solution, one merely computes $5 + (-3)$. A similar analysis could be made for the equation $2x = 3$ in the rational numbers with the operation of multiplication:

$$\begin{aligned}
2x &= 3, && \text{given,}\\
\tfrac{1}{2}(2x) &= \tfrac{1}{2}(3), && \text{multiplying by } \tfrac{1}{2},\\
(\tfrac{1}{2} \cdot 2)x &= \tfrac{1}{2}3, && \text{associative law,}\\
1 \cdot x &= \tfrac{1}{2}3, && \text{computing } \tfrac{1}{2}2,\\
x &= \tfrac{1}{2}3, && \text{property of } 1,\\
x &= \tfrac{3}{2}, && \text{computing } \tfrac{1}{2}3.
\end{aligned}$$

Now suppose that we have a set with a binary operation $*$. What properties does the operation need to have in order to solve an equation of the form $a * x = b$ where a and b are fixed elements of S? Both equations $5 + x = 2$ and $2x = 3$ have this form; the first uses the operation $+$, and the second uses the operation $\times$. By examining the steps used we can see what properties of the operation $*$ are required as summarized in the table below.

Property	$+$	$\times$
Associative Property	$-5+(5+x)=(-5+5)+x$	$\frac{1}{2}(2x)=(\frac{1}{2}\cdot 2)x$
Identity Element	0: $0+x=x$	1: $1\cdot x=x$
Inverse Element	-5: $-5+5=0$	$\frac{1}{2}$: $\frac{1}{2}\cdot 2=1$

If S is a set with an operation $*$ satisfying these three properties, then an equation of the form $a*x=b$ could be solved for x using exactly the same steps used to solve $5+x=2$ or $2x=3$. These three essential properties are all that is required in order to have a group. We are now ready to present the precise definition.

Definition and Examples

2.1 Definition A **group** $\langle G, *\rangle$ is a set G, closed under a binary operation $*$, such that the following axioms are satisfied:

$\mathscr{G}_1$: For all $a, b, c \in G$, we have

$$(a*b)*c = a*(b*c). \quad \textbf{associativity of } *$$

$\mathscr{G}_2$: There is an element e in G such that for all $x \in G$,

$$e*x = x*e = x. \quad \textbf{identity element } e \text{ for } *$$

$\mathscr{G}_3$: Corresponding to each $a \in G$, there is an element a' in G such that

$$a*a' = a'*a = e. \quad \textbf{inverse } a' \text{ of } a$$ ■

2.2 Example $\langle \mathbb{R}, +\rangle$ is a group with identity element 0 and the inverse of any real number a is $-a$. However, $\langle \mathbb{R}, \cdot\rangle$ is not a group since 0 has no multiplicative inverse. We were still able to solve $2x=3$ in the example above because $\langle \mathbb{R}^*, \cdot\rangle$ is a group since multiplication of real numbers is associative, 1 is an identity, and every real number except 0 has an inverse. ▲

It is often convenient to say that G is a group under the operation $*$ rather than write $\langle G, *\rangle$ is a group. At times, there is only one obvious operation that makes $\langle G, *\rangle$ a group. In this case, we may abuse notation and say that G is a group. For example, if we say that $\mathbb{R}$ is a group, we mean that $\mathbb{R}$ is a group under addition.

2.3 Definition A group G is **abelian** if its binary operation is commutative. ■

Let us give some examples of some sets with binary operations that give groups and also of some that do not give groups.

2.4 Example The set $\mathbb{Z}^+$ under addition is *not* a group. There is no identity element for $+$ in $\mathbb{Z}^+$. ▲

2.5 Example The set of all nonnegative integers (including 0) under addition is still *not* a group. There is an identity element 0, but no inverse for 2. ▲