

SET CONCEPTS V

PAUL L. BAILEY

ABSTRACT. We continue our endeavor to grasp the basic ideas about sets which underlie mathematics. This time we pursue the fundamental objects which give us algebra. These objects are binary operators.

1. BINARY OPERATORS

Let A be a set. A *binary operator* on A is a function

$$* : A \times A \rightarrow A.$$

A binary operator is simply something that takes two elements of a set and gives back a third element of the same set.

Example 1. Let \mathbb{R} be the set of real numbers. Then $+$: $\mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$, given by $+(x, y) = x + y$, is a binary operator. Also \cdot : $\mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$, given by $\cdot(x, y) = xy$, is a binary operator.

In general, in the sets \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} , and \mathbb{C} , addition and multiplication are binary operators. \square

Example 2. Let X be a set and let $\mathcal{P}(X)$ be the power set of X . Then union and intersection are binary operators on $\mathcal{P}(X)$; for example

$$\cap : \mathcal{P}(X) \times \mathcal{P}(X) \rightarrow \mathcal{P}(X)$$

is defined by $\cap(A, B) = A \cap B$, where $A, B \subset X$. \square

Example 3. Let X be a set and let $\text{Sym}(X)$ be the set of all permutations of X . Then \circ is a binary operator on $\text{Sym}(X)$:

$$\circ : \text{Sym}(X) \times \text{Sym}(X) \rightarrow \text{Sym}(X)$$

is defined by $\circ(\phi, \psi) = \phi \circ \psi$. \square

Let A be a set and let $* : A \times A \rightarrow A$ be a binary operator. As in the above examples, it is customary to write $a * b$ instead of $*(a, b)$, where $a, b \in A$. However, we keep in mind that $*$ is a function and that $a * b \in A$.

2. CLOSURE

Let $*$: $A \times A \rightarrow A$ be a binary operator on a set A and let $B \subset A$. We say that B is *closed* under the operation of $*$ if for every $b_1, b_2 \in B$, we have $b_1 * b_2 \in B$.

Example 4. Let E be the set of even integers. Then E is closed under the operations of addition and multiplication of integers. Indeed, the sum of even integers is even, and the product of even integers is even.

Let O be the set of odd integers. Then O is closed under multiplication. However, O is not closed under addition, because the sum of two odd integers is even. \square

Example 5. Let $B = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$. Then B is closed under addition and multiplication of real numbers. For example, if $a_1 + b_1\sqrt{2}$ and $a_2 + b_2\sqrt{2}$ are two element of B , then

$$(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in B$$

and

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in B.$$

Note that these results are in B because \mathbb{Q} itself is closed under addition and multiplication. Therefore $a_1a_2 + 2b_1b_2 \in \mathbb{Q}$, and so forth. \square

Example 6. Let X be a set and let $Y \subset X$. Then $\mathcal{P}(Y) \subset \mathcal{P}(X)$, and the subset $\mathcal{P}(Y)$ is closed under the operations of intersection and union of subset of X . \square

3. STANDARD NOTATION

It is very common that binary operations be named addition or multiplication, even if the elements of the set are not numbers in the common sense.

If the operation on A is named addition and denoted $+$, then it is standard that the identity element be named zero and denoted 0 and that the inverse of a is denoted $-a$. By convention, one may assume that an operation denoted by $+$ is commutative and associative. If n is a natural number and $a \in A$, then na means a added to itself n times.

If the operation on A is denoted \cdot , it is usually but not always called multiplication and the \cdot is dropped, so that ab means $a \cdot b$. The identity element in this notation is usually called one and written 1 . The inverse of a , if it exists, is denoted a^{-1} . If n is a natural number and $a \in A$, the a^n means a multiplied by itself n times.

When people refer to general binary operations, usually multiplicative notation is used, since it is the simplest. We also use $*$ to mean a “generic” binary operation.

4. PROPERTIES OF BINARY OPERATORS

Let A be a set and let $*$: $A \times A \rightarrow A$ be a binary operator on A .

We say that $*$ is *commutative* if for every $a, b \in A$ we have

$$a * b = b * a.$$

We say that $*$ is *associative* if for every $a, b \in A$ we have

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

We say that $e \in A$ is an *identity element* for $*$ if for every $a \in A$ we have

$$e * a = a * e = a.$$

We note that if $*$ has an identity element, then it is necessarily unique. For suppose that e and f are both identity elements for the operation $*$. Then $e * f = f$ since e is an identity, but also $e * f = e$ since f is an identity. Thus $e = f$.

Suppose that e is an identity for $*$. We say that $b \in A$ is an *inverse* for $a \in A$ if

$$a * b = b * a = e.$$

We note that when $*$ is associative, then inverses are unique. Indeed, if b and c are both inverses for a , then $a * b = e$, and applying c on the left gives $c * (a * b) = c * e = c$. But if $*$ is associative, $c * (a * b) = (c * a) * b = e * b = b$, so $c = b$. If $a \in A$ has an inverse, we say that a is *invertible*.

If $*$ has an identity and every element has an inverse, we say that $*$ is an *invertible operation*.

Example 7. The real numbers have two binary operations, addition and multiplication. Each is commutative and associative. The additive identity is 0, and the multiplicative identity is 1. Every element a has an additive inverse $-a$, and if $a \neq 0$, it has a multiplicative inverse $a^{-1} = \frac{1}{a}$.

The subset \mathbb{Q} , \mathbb{Z} , and \mathbb{N} of \mathbb{R} each contain 0 and 1, and these act as additive and multiplicative identities in these sets. Every nonzero rational number has an additive and multiplicative inverse. The integers have additive inverses but not multiplicative inverses. The natural numbers do not contain additive inverses.

□

Example 8. Let X be a set and consider intersection and union of subsets of X . These are operations on $\mathcal{P}(X)$ which are commutative and associative. Intersection has an identity element, which is the entire set X , since for $A \subset X$, we have $A \cap X = A$. Union also has an identity element, which is \emptyset . Neither of these operations supports inverses.

However, the operation of symmetric difference on $\mathcal{P}(X)$, defined by

$$A \triangle B = (A \cup B) \setminus (A \cap B),$$

is commutative, associative, and invertible. The identity element is \emptyset , and the inverse of $A \in \mathcal{P}(X)$ is itself. □

Example 9. Let X be a set and consider composition of permutations of X . This operation on $\text{Sym}(X)$ is associative, because composition of functions is always associative. It is also invertible. The identity element for this operation is the identity function id_X . The inverse of a permutation exists because bijective functions are always invertible.

However, composition of permutations is not commutative. For example, let $X = \{1, 2, 3\}$. Let $\phi \in \text{Sym}(X)$ be given by $(1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1)$ and let $\psi \in \text{Sym}(X)$ be given by $(1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 3)$. Then $\phi \circ \psi = (1 \mapsto 3, 2 \mapsto 2, 3 \mapsto 1)$ but $\psi \circ \phi = (1 \mapsto 1, 2 \mapsto 3, 3 \mapsto 2)$. Thus $\phi \circ \psi \neq \psi \circ \phi$. \square

Example 10. The standard *dot product* on \mathbb{R}^n is defined by

$$\vec{v} \cdot \vec{w} = v_1 w_1 + \cdots + v_n w_n,$$

where $\vec{v} = (v_1, \dots, v_n)$ and $\vec{w} = (w_1, \dots, w_n)$. Note that for $n > 1$, this is NOT a binary operator, since it is a function

$$\mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R};$$

to be a binary operator on \mathbb{R}^n , the codomain has to be \mathbb{R}^n .

Example 11. Let X be a set and let $\mathcal{F}(X, X)$ be the set of all functions, not necessarily bijective, from X into itself. Composition is a binary operator on $\mathcal{F}(X, X)$, and $\text{Sym}(X)$ is a closed under this operation. The same identity element id_X exists in this set. However, not every element is invertible; in fact, $\text{Sym}(X)$ is the subset of invertible elements.

Let $h \in \mathcal{F}(X, X)$. This is the same as saying $h : X \rightarrow X$. For each $n \in \mathbb{N}$, define the function $h^n : X \rightarrow X$ in the natural way. For $n = 0$, $h^0 = \text{id}_X$. For $n = 1$, $h^1 = h$. However, $h^2 = h \circ h$, $h^3 = h \circ h \circ h$, and in general,

$$h^n = h \circ \cdots \circ h \text{ (} n \text{ times)}.$$

Example 12. An $m \times n$ *matrix* with entries in \mathbb{R} is an array of elements of \mathbb{R} with m rows and n columns. The entries of a matrix are often labeled a_{ij} , where this is the entry in the i^{th} row and j^{th} column. We may write such a matrix with the notation (a_{ij}) .

An $m \times n$ matrix $A = (a_{ij})$ may be added to an $m \times n$ matrix $B = (b_{ij})$ to give an $m \times n$ matrix $AB = C = (c_{ij})$ by the formula

$$c_{ij} = a_{ij} + b_{ij}.$$

An $m \times n$ matrix $A = (a_{ij})$ may be multiplied by an $n \times p$ matrix $B = (b_{jk})$ to give an $m \times p$ matrix $AB = C = (c_{ik})$ by the formula

$$c_{ik} = \sum_{j=1}^n a_{ij} b_{jk};$$

thus the ik^{th} entry of C is the dot product of the i^{th} row of A with the k^{th} column of B .

Let $\mathbf{M}_n(\mathbb{R})$ be the set of all $n \times n$ matrices over \mathbb{R} . Then addition of matrices is a binary operation on $\mathbf{M}_n(\mathbb{R})$ which is commutative, associative, and invertible. Also, multiplication of matrices is a binary operation on $\mathbf{M}_n(\mathbb{R})$ which is associative and has an identity. The identity is simply the matrix given by $a_{ij} = 1$ if $i = j$ and $a_{ij} = 0$ otherwise. However, this operation is not commutative, and there are many elements which do not have inverses.

5. EXERCISES V

Exercise 1. In each case, we define a binary operation $*$ on \mathbb{R} . Determine if $*$ is commutative and/or associative, find an identity if it exists, and find any invertible elements.

(a) $x * y = xy + 1$;

(b) $x * y = \frac{1}{2}xy$;

(c) $x * y = |x|^y$.

Exercise 2. Consider the plane \mathbb{R}^2 . Define a binary operation $*$ on \mathbb{R}^2 by

$$(x_1, y_1) * (x_2, y_2) = \left(\frac{x_1 + x_2}{2}, \frac{y_1 + y_2}{2} \right).$$

Thus the “product” of two points under this operation is the point which is midway between them. Determine if $*$ is commutative and/or associative, find an identity if it exists, and find any invertible elements.

Exercise 3. Let \mathcal{J} be the collection of all open intervals of real numbers. We consider the empty set to be an open interval.

(a) Show that \mathcal{J} is closed under the operation of \cap on $\mathcal{P}(\mathbb{R})$.

(b) Show that \mathcal{J} is not closed under the operation of \cup on $\mathcal{P}(\mathbb{R})$.

Exercise 4. Let X and Y be sets and let $*$: $Y \times Y \rightarrow Y$ be a binary operation on Y which is commutative, associative, and invertible. Let $f : X \rightarrow Y$ be a bijective function. Define an operation \square on X by

$$x_1 \square x_2 = f^{-1}(f(x_1) * f(x_2)).$$

Show that \square is commutative, associative, and invertible.

Exercise 5. Let X and Y be sets and let $*$: $Y \times Y \rightarrow Y$ be a binary operation on Y . Let $\mathcal{F}(X, Y)$ be the set of all functions from X to Y . Show that $*$ induces a binary operation, which may also be called $*$, on $\mathcal{F}(X, Y)$.

Exercise 6. Let X be a set and let $*$: $X \times X \rightarrow X$ be a binary operation on X which is associative and invertible. Show that $*$ induces a binary operation, which may also be called $*$, on $\mathcal{P}(X)$. Is it associative? Does it have an identity? Is it invertible?