Binary operations on sets

Peter Rowlett

1 Definition

If x and y are ordinary numbers, there are various ways of combining them to give another number. For example, we might form their sum $x + y$, their difference $x - y$ or their product xy. These are *binary operations*, being 'binary' in the sense that they operate on two numbers (not having anything to do with base 2 binary numbers).

In general, a binary operation ω on a set A is simply a map from $A \times A = A^2$ into A, so that ω maps each pair $(x, y) \in A^2$ to some element $\omega(x, y) \in A$.

For example, ordinary addition is the map $\alpha : \mathbb{R}^2 \to \mathbb{R}$ which maps $(x, y) \in \mathbb{R}^2$ to the element $\alpha(x, y) = x + y \in \mathbb{R}$.

Similarly, ordinary subtraction is the map $\beta : \mathbb{R}^2 \to \mathbb{R}$ defined by the rule $\beta(x, y) = x - y$. Ordinary multiplication is the map $\gamma(x, y) : \mathbb{R}^2 \to \mathbb{R}$ defined by the rule $\gamma(x, y) = x \cdot y$.

We tend to write binary operations as a symbol between two elements, rather than as a map. So for a general binary operation, instead of $\omega(x, y)$ we might write $x \circ y$ where $\circ$ represents the binary operation.

Definition. For a set A, a *binary operation* $\circ$ on A is a map of A^2 into A, which maps each pair $(x, y) \in A^2$ to an element $x \circ y \in A$.

There is some confusion in mathematical texts because sometimes the notation $x + y$ and xy is used for an operation which is not addition or subtraction and may not act on numbers. What's more, the notation xy doesn't have a symbol between x and y. We'll try to stick to $\circ$ for a general operation, and use $+$ for ordinary addition, $-$ for ordinary subtraction, and $\cdot$ for ordinary multiplication.

Instead of writing out "a set A and a binary operation acting on that set $\circ$", we will use the shorthand notation $(A, \circ)$.

1.1 Closure

Note that the definition of $(A, \circ)$ required that $\forall x, y \in A\ (x \circ y \in A)$, that is a combination of elements in A under $\circ$ remains within A. This property is called *closure*.

For example, ordinary addition on real numbers, $(\mathbb{R}, +)$, is closed because $\forall x, y \in \mathbb{R}$ we have $x + y \in \mathbb{R}$.

However, if we consider subtraction $-$ on $\mathbb{N}$, this is not closed. For example, take $1, 2 \in \mathbb{N}$ and note that $1 - 2 = -1 \notin \mathbb{N}$. Therefore subtraction is not a binary operation on $\mathbb{N}$. (However, subtraction *is* a binary operation on other sets, for example $(\mathbb{Z}, -)$ is defined.)

1.2 Example

Let $A = \{a, b, c\}$ and let $(A, \circ)$ be defined by the following table.

	a	b	c
a	b	c	b
b	b	a	c
c	a	c	c

Then we can find values for this operation from this table, for example $a \circ a = b$, $a \circ b = c$, $a \circ c = b$, $b \circ a = b$, and so on.

We see this operation is closed because pairs of elements always result in one of the letters a, b or c.

2 Commutative operations

Definition. For $(A, \circ)$, if $x, y \in A$, we say x and y *commute* (with respect to $\circ$) if $x \circ y = y \circ x$.

$(A, \circ)$ is called *commutative* if

$$\forall x, y \in A \ (x \circ y = y \circ x),$$

i.e. if every pair of elements of A commute.

2.1 Examples

Addition $(\mathbb{R}, +)$ and multiplication $(\mathbb{R}, \cdot)$ are commutative, since $\forall x, y \in \mathbb{R}$,

$$x + y = y + x$$
$$x \cdot y = y \cdot x.$$

Meanwhile, $(\mathbb{R}, -)$ is not commutative, since $\exists x, y \in \mathbb{R}$

$$x - y \neq y - x.$$

The example operation given in section 1.2 is not commutative, for example from the table we see $a \circ c = b$ and $c \circ a = a$. If it was commutative, the table would be symmetrical above and below the main (top left to bottom right) diagonal.

3 Associative operations

Definition. $(A, \circ)$ is called *associative* if $\forall x, y, z \in A$ it satisfies

$$(x \circ y) \circ z = x \circ (y \circ z).$$

3.1 Examples

Addition $(\mathbb{R}, +)$ and multiplication $(\mathbb{R}, \cdot)$ are associative, since $\forall x, y, z \in \mathbb{R}$ we have

$$(x + y) + z = x + (y + z)$$
$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

$(\mathbb{R}, -)$ is not associative, since $\exists x, y, z \in \mathbb{R}$

$$(x - y) - z \neq x - (y - z).$$

The example operation given in section 1.2 is not associative. To see this consider, for example, $(a \circ a) \circ b$ and $a \circ (a \circ b)$.

The first of these is

$$(a \circ a) \circ b = b \circ b = a$$

and the second is

$$a \circ (a \circ b) = a \circ c = b.$$

Therefore we see that

$$(a \circ a) \circ b \neq a \circ (a \circ b).$$

4 Identity element

Definition. For $(A, \circ)$, any element $e \in A$ which satisfies, $\forall x \in A$,

$$e \circ x = x \circ e = x,$$

is called an *identity element* for the operation $\circ$.

4.1 Examples

For addition $(\mathbb{R}, +)$, $e = 0$ since $\forall x \in \mathbb{R}$ $(x + 0 = 0 + x = x)$.

For multiplication $(\mathbb{R}, \cdot)$, $e = 1$ since $\forall x \in \mathbb{R}$ $(x \cdot 1 = 1 \cdot x = x)$.

For subtraction $(\mathbb{R}, -)$, there is no identity element. For this to be possible, we would require $\exists e \in \mathbb{R}\ \forall x \in \mathbb{R}\ (e - x = x - e = x)$, which is impossible.

The example operation given in section 1.2 has no identity element, since none of a, b or c behave as an identity. An identity element would produce a row and a column with the elements a, b and c in order.

5 Inverse

Let e be an identity element on $(A, \circ)$. Then

1. If $x \circ y = e$, then y is called the *right inverse* of x.
2. If $y \circ x = e$, then y is called the *left inverse* of x.
3. If $x \circ y = y \circ x = e$, i.e. y is both right inverse and a left inverse of x, then y is called the *inverse* of x, usually written x^{-1}.

5.1 Examples

Consider addition $(\mathbb{Z}, +)$, for which we have identity element 0. Then $\forall x \in \mathbb{Z}\ \exists y \in \mathbb{Z}$ such that y is the inverse of x. We write $y = -x$ so that $x + (-x) = (-x) + x = 0$.

Consider multiplication $(\mathbb{R}, \cdot)$, for which we have identity element 1. Then we cannot say $\forall x \in \mathbb{R}\ \exists y \in \mathbb{R}\ (x \cdot y = 1)$ because $x = 0$ is a counterexample. That is, there is no y that gives $0 \cdot y = 1$. This means the inverse of multiplication is not defined on $\mathbb{R}$ unless we exclude 0. For $(\mathbb{R} - \{0\}, \cdot)$, we can define the inverse element x^{-1} as the reciprocal of x, that is $\frac{1}{x}$.

The example operation given in section 1.2 has no inverse, since there is no identity element.

6 Annihilator

The identity element 'leaves alone' any element it is combined with. An annihilator (or zero element) 'swallows up' any element.

Definition. For $(A, \circ)$, any $n \in A$ that satisfies $\forall x \in A$

$$n \circ x = x \circ n = n$$

is called an *annihilator* for the operation $\circ$.

6.1 Examples

For multiplication $(\mathbb{R}, \cdot)$, the number 0 is an annihilator, since $\forall x \in \mathbb{R}\ (0 \cdot x = x \cdot 0 = 0)$.

There is no annihilator for addition $(\mathbb{R}, +)$, since that would require $\exists n \in \mathbb{R}\ \forall x \in \mathbb{R}\ (n + x = x + n = n)$, which is impossible.

The example operation given in section 1.2 has no annihilator, which we can see as there is no row or column consisting entirely of the element at the start of the row or column.

7 Example: Boolean algebra

We saw previously that Boolean algebra has laws for communtativity and associativity as well as identity and annihilator elements.

In terms we are now familiar with, let P be a set whose elements are propositions. Then we have binary operators $\wedge$ and $\vee$ acting on P.

The operator $\wedge$ is commutative and associative, since $\forall p, q \in A$

$$p \wedge q = q \wedge p$$
$$p \wedge (q \wedge r) = (p \wedge q) \wedge r.$$

We also have 1 (representing 'true') as the identity element, since $p \wedge 1 = 1 \wedge p = p$, and 0 (representing 'false') as the annihilator, since $p \wedge 0 = 0 \wedge p = 0$.

The operator $\vee$ is commutative and associative, since $\forall p, q \in A$

$$p \vee q = q \vee p$$
$$p \vee (q \vee r) = (p \vee q) \vee r.$$

We also have 0 as the identity element, since $p \vee 0 = 0 \vee p = p$, and 1 as the annihilator, since $p \vee 1 = 1 \vee p = 1$.

8 Example: Set theory

Set union ($\cup$) is a binary operation acting on two sets. For example, let X, Y and Z be any sets. Then $\cup$ is commutative and associative, since

$$X \cup Y = Y \cup X$$
$$X \cup (Y \cup Z) = (X \cup Y) \cup Z.$$

The empty set $\emptyset$ is an identity element for union, since $X \cup \emptyset = \emptyset \cup X = X$. The universal set U is an annihilator element for union, since $X \cup U = U \cup X = U$.

Set intersection ($\cap$) is a binary operation acting on two sets. For example, let X, Y and Z be any sets. Then $\cap$ is commutative and associative, since

$$X \cap Y = Y \cap X$$
$$X \cap (Y \cap Z) = (X \cap Y) \cap Z.$$

The universal set U is an identity element for union, since $X \cap U = U \cap X = X$. The empty set $\emptyset$ is an annihilator element for intersection, since $X \cap \emptyset = \emptyset \cap X = \emptyset$.