4-22-2007

Binary Operations

Definition. A **binary operation** on a set X is a function $f : X \times X \to X$.

In other words, a binary operation takes a *pair* of elements of X and produces an element of X.

It's customary to use **infix notation** for binary operations. Thus, rather than write $f(a, b)$ for the binary operation acting on elements $a, b \in X$, you write afb. Since all those letters can get confusing, it's also customary to use certain symbols — $+$, $\cdot$, $*$ — for binary operations. Thus, $f(a, b)$ becomes (say) $a + b$ or $a \cdot b$ or $a * b$.

Example. Addition is a binary operation on the set $\mathbb{Z}$ of integers: For every pair of integers m, n, there corresponds an integer $m + n$.

Multiplication is also a binary operation on the set $\mathbb{Z}$ of integers: For every pair of integers m, n, there corresponds an integer $m \cdot n$.

However, division is not a binary operation on the set $\mathbb{Z}$ of integers. For example, if I take the pair $(3, 0)$, I can't perform the operation $\dfrac{3}{0}$. *A binary operation on a set must be defined for all pairs of elements from the set.*

Likewise,

$$a * b = (\text{a random number bigger than } a \text{ or } b)$$

does not define a binary operation on $\mathbb{Z}$. In this case, I don't have a *function* $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, since the output is ambiguously defined. (Is $3 * 5$ equal to 6? Or is it 117?) □

When a binary operation occurs in mathematics, it usually has properties that make it useful in constructing abstract structures.

Definition. Let $*$ be a binary operation on a set X.

1. $*$ is **associative** if
$$x * (y * z) = (x * y) * z \quad \text{for all} \quad x, y, z \in X.$$

2. $*$ is **commutative** if
$$x * y = y * x \quad \text{for all} \quad x, y \in X.$$

3. $e \in X$ is an **identity** for $*$ if
$$e * x = x \quad \text{and} \quad x * e = x \quad \text{for all} \quad x \in X.$$

4. If $*$ has an identity and $x \in X$, then x^{-1} is an **inverse** for x if
$$x^{-1} * x = e \quad \text{and} \quad x * x^{-1} = e.$$

For instance, in abstract algebra you will learn about **groups**. A **group** is a set G with a binary operation which is associative, has an identity element, and such that every element has an inverse.

Example. Addition is a binary operation on $\mathbb{R}$.

It is associative, since

$$a + (b + c) = (a + b) + c \quad \text{for all} \quad a, b, c \in \mathbb{R}.$$

It is commutative, since

$$a \cdot b = b \cdot a \quad \text{for all} \quad a, b \in \mathbb{R}.$$

0 is an identity for $+$, since

$$a + 0 = a \quad \text{and} \quad 0 + a = a \quad \text{for all} \quad a \in \mathbb{R}.$$

If $a \in \mathbb{R}$, then $-a$ is an inverse for a with respect to addition:

$$a + (-a) = 0 \quad \text{and} \quad (-a) + a = 0 \quad \text{for all} \quad a \in \mathbb{R}. \quad \square$$

Example. Subtraction is a binary operation on $\mathbb{R}$.

It is *not* associative; for example,

$$3 - (4 - 5) = 3 - (-1) = 4, \quad \text{but} \quad (3 - 4) - 5 = -1 - 5 = -6.$$

It is not commutative; for example,

$$2 - 7 = -5, \quad \text{but} \quad 7 - 2 = 5.$$

There is no identity element for subtraction. Suppose that e was an identity element. Then

$$e - 2 = 2, \quad \text{so} \quad e = 4.$$

But I'd also have

$$e - 13 = 13, \quad \text{so} \quad e = 26.$$

e can't be both 4 and 26, so this contradiction shows that there is no such e.

Since there is no identity element, it makes no sense to ask whether there are inverses. $\square$

Example. Consider the binary operation $*$ on $\mathbb{R}$ given by

$$x * y = x + y - 3.$$

$$(x * y) * z = (x + y - 3) * z = (x + y - 3) + z - 3 = x + y + z - 6,$$
$$x * (y * z) = x * (y + z - 3) = x + (y + z - 3) - 3 = x + y + z - 6.$$

Therefore, $*$ is associative.

Since

$$x * y = x + y - 3 = y + x - 3 = y * x,$$

$*$ is commutative.

To see if $*$ has an identity, I'll work backwards to guess a possible identity. Then I'll check that my guess works.

Suppose e is the identity. Then $e * x = x$ for all x, so $e + x - 3 = x$ for all x. Solving for e, I get $e = 3$. Therefore, I *guess* that 3 is the identity.

Next, I'll confirm my guess by checking the axiom. Let $x \in \mathbb{R}$. Then

$$3 * x = 3 + x - 3 = x \quad \text{and} \quad x * 3 = x + 3 - 3 = x.$$

Therefore, 3 is the identity.

Next, I'll work backwards to guess a formula for the inverse of an element. Let $x \in \mathbb{R}$. Then the inverse x^{-1} must satisfy $x * x^{-1} = 3$, since 3 is the identity. Therefore, $x + x^{-1} - 3 = 3$, so $x^{-1} = 6 - x$. Therefore, I *guess* that $6 - x$ is the inverse of x.

Next, I'll confirm my guess by checking the axiom. Let $x \in \mathbb{R}$. Then

$$x * (6 - x) = x + (6 - x) - 3 = 3 \quad \text{and} \quad (6 - x) * x = (6 - x) + x - 3 = 3.$$

Therefore, $6 - x$ is the inverse of x, and every element has an inverse. □

Many mathematical structures which arise in algebra involve one or two binary operations which satisfy certain axioms.

Definition.

(a) A **monoid** is a set with an associative binary operation.

(b) A **semigroup** is a set with an associative binary operation which has an identity element.

(c) A **group** is a set with an associative binary operation which has an identity element and in which every element has an inverse.

Example. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are groups under the usual addition operations.

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are semigroups under the usual multiplication operations. They aren't groups, because all of them contain 0, which does not have a multiplicative inverse. □

Example. I saw above that the binary operation $*$ on $\mathbb{R}$ given by

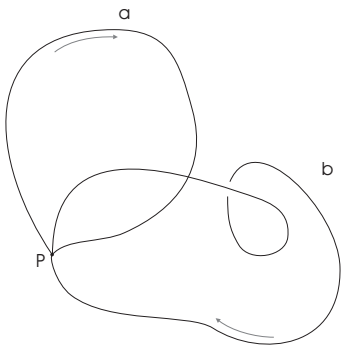
$$x * y = x + y - 3$$

makes $\mathbb{R}$ into a group. Note that this operation is different from the addition operation: A given set can be made into a group in many ways. □

Example. (**A binary operation on loops**) Take a subset X of $\mathbb{R}^n$ and pick a point P as the **basepoint**. Consider the set of **loops** which start and end at P.

To be precise, a **loop** is a continuous function $f : [0, 1] \to X$ such that $f(0) = P$ and $f(1) = P$. Think of the parametrized curves you saw in calculus, for example.

Define an operation on loops by taking loops a and b and letting $a * b$ be the loop formed by going around a, then going around b.



Since both a and b start and end at P, the result is a loop starting and ending at P.

The precise definition of $a * b$ is as follows. If $a, b : [0, 1] \to X$, then

$$(a * b)(t) = \begin{cases} a(2t) & \text{if } 0 \leq t \leq \frac{1}{2} \\ b(2t-1) & \text{if } \frac{1}{2} < t \leq 1 \end{cases} .$$

This traces out a as t goes from 0 to $\frac{1}{2}$, then traces out b as t goes from $\frac{1}{2}$ to 1.

This gives a binary operation on the set of loops. Unfortunately, it isn't quite associative as is. If you have 3 loops a, b, and c, then $(a * b) * c$ will trace out a for $0 \leq t \leq \frac{1}{4}$, b for $\frac{1}{4} \leq t \leq \frac{1}{2}$, and c for $\frac{1}{2} \leq t \leq 1$. On the other hand, $a * (b * c)$ will trace out a for $0 \leq t \leq \frac{1}{2}$, b for $\frac{1}{2} \leq t \leq \frac{3}{4}$, and c for $\frac{3}{4} \leq t \leq 1$.

I could fix this problem by considering **equivalence classes** of loops instead of loops. Define two loops to be equivalent if they have the same *image* — that is, if they "trace out the same curve". The operation above is still defined on equivalence classes of loops, and becomes an associative operation. In fact, it has an identity element, namely the loop which consists of the point P alone.

Thus, the set of equivalence classes of loops with this operation is a semigroup.

In order to make the set into a group, I need a different equivalence relation called **loop homotopy**. Roughly speaking, two loops will be **homotopic** if one can be continuously deformed into the other with X, such that the starting and ending point P doesn't move during the deformation. The resulting group is called the **fundamental group** of X; it is studied in a branch of mathematics called **algebraic topology**. □
