Binary operations

1 Binary operations

The essence of algebra is to combine two things and get a third. We make this into a definition:

Definition 1.1. Let X be a set. A *binary operation* on X is a function $F\colon X \times X \to X$.

However, we don't write the value of the function on a pair (a, b) as $F(a, b)$, but rather use some intermediate symbol to denote this value, such as $a + b$ or $a \cdot b$, often simply abbreviated as ab, or $a \circ b$. For the moment, we will often use $a * b$ to denote an arbitrary binary operation.

Definition 1.2. A *binary structure* $(X, *)$ is a pair consisting of a set X and a binary operation on X.

Example 1.3. The examples are almost too numerous to mention. For example, using $+$, we have $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, as well as vector space and matrix examples such as $(\mathbb{R}^n, +)$ or $(\mathbb{M}_{n,m}(\mathbb{R}), +)$. Using subtraction, we have $(\mathbb{Z}, -)$, $(\mathbb{Q}, -)$, $(\mathbb{R}, -)$, $(\mathbb{C}, -)$, $(\mathbb{R}^n, -)$, $(\mathbb{M}_{n,m}(\mathbb{R}), -)$, but **not** $(\mathbb{N}, -)$.

For multiplication, we have $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$. If we define $\mathbb{Q}^* = \{a \in \mathbb{Q} : a \neq 0\}$, $\mathbb{R}^* = \{a \in \mathbb{R} : a \neq 0\}$, $\mathbb{C}^* = \{a \in \mathbb{C} : a \neq 0\}$, then $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ are also binary structures. But, for example, $(\mathbb{Q}^*, +)$ is **not** a binary structure. Likewise, $(U(1), \cdot)$ and $(\mu_n, \cdot)$ are binary structures. In addition there are matrix examples: $(\mathbb{M}_n(\mathbb{R}), \cdot)$, $(GL_n(\mathbb{R}), \cdot)$, $(SL_n(\mathbb{R}), \cdot)$, $(O_n, \cdot)$, $(SO_n, \cdot)$.

Next, there are function composition examples: for a set X, $(X^X, \circ)$ and $(S_X, \circ)$.

We have also seen examples of binary operations on sets of equivalence classes. For example, $(\mathbb{Z}/n\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z}, \cdot)$, and $(\mathbb{R}/2\pi\mathbb{Z}, +)$ are examples of binary structures. (But there is no natural binary operation of multiplication on $\mathbb{R}/2\pi\mathbb{Z}$.)

Finally, there are many more arbitrary seeming examples. For example,, for a set X, we could simply define $a*b = b$ for all $a, b \in X$: to "combine" two elements, you always pick the second one. Another example is a "constant" binary operation: for a nonempty set X, choose once and for all an element $c \in X$, and define $a * b = c$ for all $a, b \in X$.

If X is a finite set with n elements, say we enumerate $X = \{x_1, \dots, x_n\}$, then a binary operation on X can be described by a table:

$*$	x_1	x_2	$\dots$	x_n
x_1	$x_1 * x_1$	$x_1 * x_2$	$\dots$	$x_1 * x_n$
x_2	$x_2 * x_1$	$x_2 * x_2$	$\dots$	$x_2 * x_n$
$\vdots$	$\dots$	$\dots$	$\dots$	$\dots$
x_n	$x_n * x_1$	$x_n * x_2$	$\dots$	$x_n * x_n$

From this, it follows that the number of different binary operations on a finite set X with $\#(X) = n$ is n^{n^2}.

Remark 1.4. In grade school, when discussing binary operations, one often mentions the "closure property," which roughly says that, for $a, b \in X$, $a * b \in X$. For us, this property is built into the definition of a binary operation, which is defined to be a function from $X \times X$ to X.

2 Isomorphisms

A key concept is the notion of when two binary structures are essentially the same.

Definition 2.1. Let $(X_1, *_1)$ and $(X_2, *_2)$ be two binary structures. An *isomorphism* f from $(X_1, *_1)$ to $(X_2, *_2)$ is a bijection $f \colon X_1 \to X_2$ such that, for all $a, b \in X_1$,

$$f(a *_1 b) = f(a) *_2 f(b).$$

In other words, when we use f to "rename" the elements of X_1, the binary operations correspond.

We say that two binary structures $(X_1, *_1)$ and $(X_2, *_2)$ are *isomorphic* if there exists an isomorphism f from $(X_1, *_1)$ to $(X_2, *_2)$, and write this as $(X_1, *_1) \cong (X_2, *_2)$ (congruence sign). Of course, if $(X_1, *_1)$ and $(X_2, *_2)$ are isomorphic, there might be many possible choices of an isomorphism f.

Thus, given two binary structures $(X_1, *_1)$ and $(X_2, *_2)$, to show that a function $f\colon X_1 \to X_2$ is an isomorphism (of the given binary structures), we must (1) show that f is a bijection (recall that this is usually best done by finding an inverse function) and then establishing the "functional equation" or identity $f(a *_1 b) = f(a) *_2 f(b)$ for all $a, b \in X_1$.

Example 2.2. (1) For every binary structure $(X, *)$, $\mathrm{Id}_X\colon X \to X$ is an isomorphism of binary structures since it is a bijection and, for all $a, b \in X$, $\mathrm{Id}_X(a * b) = a * b = \mathrm{Id}_X(a) * \mathrm{Id}_X(b)$.

(2) Define $f\colon \mathbb{Z} \to \mathbb{Z}$ by $f(n) = -n$. Then f is an isomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Z}, +)$: first, f is a bijection since it has an inverse; in fact $f^{-1} = f$. Then, for all $n, m \in \mathbb{Z}$,

$$f(n + m) = -(n + m) = -n - m = (-n) + (-m) = f(n) + f(m).$$

Thus f is an isomorphism.

(3) Similarly, fix a nonzero real number t and define $f\colon \mathbb{R} \to \mathbb{R}$ by $f(x) = tx$. Then f is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}, +)$. First, f is a bijection since it has an inverse; in fact $f^{-1}(x) = t^{-1}x$. For all $x, y \in \mathbb{R}$,

$$f(x + y) = t(x + y) = tx + ty = f(x) + f(y).$$

Thus f is an isomorphism. Similar examples work for $(\mathbb{Q}, +)$ and $(\mathbb{C}, +)$.

(4) Fix an element $A \in GL_n(\mathbb{R})$. Then A defines an isomorphism from $(\mathbb{R}^n, +)$ to $(\mathbb{R}^n, +)$. By definition, A has an inverse and hence is a bijection. Moreover, as a general property of linear functions, for all $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$,

$$A(\mathbf{v} + \mathbf{w}) = A\mathbf{v} + A\mathbf{w},$$

which says that A is an isomorphism.

(5) It is also interesting to look for examples where the binary structures seem to be quite different. For one very basic example, let $\mathbb{R}^{>0}$ denote the set of positive real numbers:

$$\mathbb{R}^{>0} = \{x \in \mathbb{R} : x > 0\}.$$

Then $(\mathbb{R}^{>0}, \cdot)$ is a binary structure. We claim that $(\mathbb{R}, +) \cong (\mathbb{R}^{>0}, \cdot)$. To see this, we need to find a bijection from $\mathbb{R}$ to $\mathbb{R}^+$ which takes addition to multiplication. A familiar example is the exponential function $f(x) = e^x$. As we know from calculus, or before, e^x is injective and its image is $\mathbb{R}^{>0}$.

Thus f is a bijection. Finally, the fact that f is an isomorphism is expressed by the functional equation: for all $x, y \in \mathbb{R}$,

$$e^{x+y} = e^x \cdot e^y.$$

(6) Recall that $\mu_4 = \{1, i, -1, -i\}$. It is easy to verify directly that $(\mathbb{Z}/4\mathbb{Z}, +) \cong (\mu_4, \cdot)$, under the bijection defined by $[0] \mapsto 1$, $[1] \mapsto i$, $[2] \mapsto -1$, $[3] \mapsto -i$. More generally, $(\mathbb{Z}/n\mathbb{Z}, +) \cong (\mu_n, \cdot)$, and we will have a more systematic way to understand this later.

(7) For our last example, note that $U(1)$ is the set of complex numbers of absolute value 1, and every such complex number can be uniquely written in the form $\cos\theta + i\sin\theta$. Similarly, as we have seen in the homework, every element of SO_2 can be uniquely written as $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. It follows easily that $(U(1), \cdot) \cong (SO_2, \cdot)$, where the first multiplication is multiplication of complex numbers and the second is multiplication of 2×2 matrices. Moreover both binary structures are isomorphic to $(\mathbb{R}/2\pi\mathbb{Z}, +)$.

Let us collect some general facts about isomorphisms, which we have implicitly touched on above:

Proposition 2.3. (i) *For every binary structure $(X, *)$, Id_X is an isomorphism of binary structures from $(X, *)$ to $(X, *)$.*

(ii) *Let $(X_1, *_1)$ and $(X_2, *_2)$ be two binary structures. If f is an isomorphism from $(X_1, *_1)$ to $(X_2, *_2)$, then f^{-1}, which exists because f is a bijection, is an isomorphism from $(X_2, *_2)$ to $(X_1, *_1)$.*

(iii) *Let $(X_1, *_1)$, $(X_2, *_2)$, and $(X_3, *_3)$ be three binary structures. If f is an isomorphism from $(X_1, *_1)$ to $(X_2, *_2)$ and g is an isomorphism from $(X_2, *_2)$ to $(X_3, *_3)$, then $g \circ f$ is an isomorphism from $(X_1, *_1)$ to $(X_3, *_3)$.*

Here, we have already noted (i), and (ii) and (iii) are left as homework. The proposition implies in particular that (i) For every binary structure $(X, *)$, $(X, *) \cong (X, *)$; (ii) Given two binary structures $(X_1, *_1)$ and $(X_2, *_2)$, if $(X_1, *_1) \cong (X_2, *_2)$ then $(X_2, *_2) \cong (X_1, *_1)$; (iii) Given three binary structures $(X_1, *_1)$, $(X_2, *_2)$, and $(X_3, *_3)$, if $(X_1, *_1) \cong (X_2, *_2)$ and $(X_2, *_2) \cong (X_3, *_3)$, then $(X_1, *_1) \cong (X_3, *_3)$. Thus the relation $\cong$ is reflexive, symmetric, and transitive.

3 Basic properties of binary operations

From discussing properties of numbers in grade school, we are familiar with certain basic properties.

Associativity: We say a binary structure $(X, *)$ (or the binary operation $*$) is *associative* if, for all $a, b, c \in X$,

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

Associativity is so basic a property that we will almost always assume it; it is very hard to work with non-associative operations. All of the operations we have denoted $+$ or $\cdot$ or $\circ$ are associative. Aside from the case of numbers, this usually comes down to the fact that function composition is associative. One can write down interesting non-associative operations. For example, subtraction, on $\mathbb{Z}$, say, is not associative, because

$$a - (b - c) = a - b + c \neq (a - b) - c$$

unless $c = 0$. For a related example, define the binary operation $*$ on $\mathbb{N}$ by exponentiation: for all $a, b \in \mathbb{N}$, $a * b = a^b$. Then

$$(a * b) * c = (a^b)^c = a^{bc},$$

by the laws of exponents, and in general this is not equal to $a * (b * c) = a^{b^c}$. Note that, for subtraction, the "primary" operation is addition, and this is in fact associative. Similarly, exponentiation is derived from multiplication which is associative, so in both of these non-associative examples, there is an associative operation lurking in the background.

For an associative binary operation $*$, we often omit the parentheses and simply write $a * (b * c) = (a * b) * c$ as $a * b * c$. There are infinitely many other identities which are a consequence of associativity and which we don't write down explicitly. For example,

$$a * (b * (c * d)) = (a * b) * (c * d) = a * ((b * c) * d) = \dots.$$

Commutativity: A binary structure $(X, *)$ (or the binary operation $*$) is *commutative* if, for all $a, b \in X$,

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

All of the operations we have denoted by $+$ are commutative, and by convention a binary operation denoted $+$ is always assumed to be commutative. Operations denoted by multiplication are commutative for **numbers**, so $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ are all commutative. However, matrix multiplication is usually **not** commutative, in fact $(\mathbb{M}_n(\mathbb{R}), \cdot)$, $(GL_n(\mathbb{R}), \cdot)$, $(SL_n(\mathbb{R}), \cdot)$, $(O_n, \cdot)$ are not commutative for $n \geq 2$ and $(SO_n, \cdot)$ is not commutative for $n \geq 3$. For a set X with $\#(X) \geq 2$, $(X^X, \circ)$ is not commutative, and $(S_X, \circ)$ is not commutative for $\#(X) \geq 3$; in particular $(S_n, \circ)$ is not commutative for $n \geq 3$.

A binary operation on a finite set is commutative $\iff$ the table is symmetric about the diagonal running from upper left to lower right. (Note that it would be very hard to decide if a binary operation on a finite set is associative just by looking at the table.)

Because of the many interesting examples of binary operations which are not commutative, we shall usually not make the assumption that a binary operation is commutative.

Identity element: An *identity* for $(X, *)$ is an element $e \in X$ such that, for all $x \in X$, $e * x = x * e = x$. Note that we have to check that e functions as an identity on both the left and right if $*$ is not commutative. Sometimes we call such an e a *two sided identity*, and define a *left identity* to be an element e_L of X such that, for all $x \in X$, $e_L * x = x$. Similarly, a *right identity* is an element e_R of X such that, for all $x \in X$, $x * e_R = x$. It is possible that a right identity exists but not a left identity, and if a right or left identity exists it does not have to be unique. The situation is different if **both** a right and left identity exist:

Proposition 3.1. *Suppose that $(X, *)$ is a binary structure and that a right identity e_R and a left identity e_L both exist. Then $e_L = e_R$, and hence $e_L = e_R$ is an identity for $(X, *)$.*

Proof. By the definition of right and left identities,

$$e_R = e_L * e_R = e_L.$$

$\square$

Corollary 3.2. *Suppose that $(X, *)$ is a binary structure. If an identity exists for $(X, *)$, then it is unique.*

Proof. Suppose that e and e' are both identities for $(X, *)$. Then in particular e is a left identity and e' is a right identity, so that by the proposition $e = e'$. $\square$

If $(X, *)$ is a finite binary structure with identity e, then by convention we let e be the first element of X. Thus, in a table, the first row and column are as follows:

$*$	e	a	b	$\dots$
e	e	a	b	$\dots$
a	a	$\dots$	$\dots$	$\dots$
b	b	$\dots$	$\dots$	$\dots$
$\vdots$	$\dots$	$\dots$	$\dots$	$\dots$

Notation: If the binary operation on X is denoted by $+$, and there is an identity, we shall always denote the identity by 0. If the binary operation on X is denoted by $\cdot$, and there is an identity, we shall often (but not always) denote the identity by 1.

Inverses: Suppose that $(X, *)$ is a binary structure with identity e. Given $x \in X$, an *inverse* for x is an element x' such that $x' * x = x * x' = e$. For example, e has an inverse and in fact $e' = e$. An element with an inverse will be called *invertible*. Clearly, if x is invertible with inverse x', then the equalities $x' * x = x * x' = e$ say that x' is invertible with inverse x, i.e. $(x')' = x$. To say more we need associativity. A *left inverse* for x is an element x'_L such that $x'_L * x = e$, and a *right inverse* for x is an element x'_R such that $x * x'_R = e$.

Proposition 3.3. *Suppose that $(X, *)$ is an associative binary structure.*

(i) *Let $x \in X$. If x'_L is a left inverse for x and x'_R is a right inverse, then $x'_L = x'_R$. Thus inverses, if they exist, are unique.*

(ii) *Suppose that $x, y \in X$ are both invertible. Then $x * y$ is also invertible, and*

$$(x * y)' = y' * x'.$$

Proof. (i) Consider the product $x'_L * x * x'_R$. Using associativity, we see that

$$x'_L * x * x'_R = (x'_L * x) * x'_R = e * x'_R = x'_R.$$

But also

$$x'_L * x * x'_R = x'_L * (x * x'_R) = x'_L * e = x'_L.$$

Thus $x'_L = x'_L$. Uniqueness of inverses follows as in the proof of Corollary **??**.
(ii) We must check that

$$(x * y) * (y' * x') = (y' * x') * x * y = e.$$

We shall just check that $(x * y) * (y' * x') = e$. Using associativity,

$$(x * y) * (y' * x') = x * (y * y') * x' = x * e * x' = (x * e) * x' = x * x' = e.$$

The equality $(y' * x') * x * y = e$ is similar. $\square$

Note that e is always invertible, and in fact $e' = e$. Also, if x is invertible, with inverse x', then the equation $x' * x = x * x' = e$ says that x' is invertible, with inverse x. In other words, $(x')' = x$.