Binary Operations

Binary operations are important, in part, because they are used in the definitions of groups, rings, and fields.

Def: A **binary operation** $*$ on a set S is a function mapping $S \times S$ into S. For each $(a, b) \in S \times S$, $* (a, b) \in S$.

Ex. Addition and multiplication are both binary operations on $\mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathbb{R}^+, or\ \mathbb{Z}^+$ ($\mathbb{R}^+ = \{x \in \mathbb{R} |\ x > 0\}$, similarly for $\mathbb{Z}^+$).

$+ :\ \mathbb{R} \times \mathbb{R} \to \mathbb{R}$

$$(a, b) \to a + b \quad \text{i.e.} \quad + (a, b) = a + b \in \mathbb{R}$$

$\cdot :\ \mathbb{R} \times \mathbb{R} \to \mathbb{R}$

$$(a, b) \to a \cdot b \quad \text{i.e.} \quad \cdot (a, b) = a \cdot b \in \mathbb{R}.$$

Ex. Division is not a binary operation on $\mathbb{Z}, \mathbb{Z}^+, or\ \mathbb{R}$.

1. It's not a binary operation on $\mathbb{Z}$ because
   $\div :\ \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$
   $$(a, b) \to \frac{a}{b}$$
   $b \neq 0$ thus $\div$ is not defined for all points in $\mathbb{Z} \times \mathbb{Z}$.

2. It's not a binary operation on $\mathbb{Z}^+$ because
   $\div :\ \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$
   $$(a, b) \to \frac{a}{b}$$
   is not defined for points where b doesn't divide a
   (e.g. $a = 2,\ b = 3,\ \frac{2}{3} \notin \mathbb{Z}^+$).

3. It's not a binary operation on $\mathbb{R}$ because

$\div: \quad \mathbb{R} \times \mathbb{R} \to \mathbb{R}$

$(a, b) \to \frac{a}{b}$ is not defined when $b = 0$.

Notice that $\div$ is a binary operation on

$\mathbb{R}^* = \mathbb{R} - \{0\}$, $\mathbb{R}^+$, $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, and $\mathbb{Q}^+$.

Def: Let $*$ be a binary operation on S and let H be a subset of S. The subset H is **closed under** $*$ if for all $a, b \in H$, $a * b \in H$.

Ex. $+$ is a binary operation on $\mathbb{R}$ but $+$ is <u>not</u> a binary operation on

$\mathbb{R}^* = \mathbb{R} - \{0\}$ because

$+: \ \mathbb{R}^* \times \mathbb{R}^* \to \mathbb{R}^*$

$(a, b) \to a + b$

$+(1, -1) = 0 \notin \mathbb{R}^*$.

Ex. $+$ and $\cdot$ are binary operations on $\mathbb{Z}$.

Ex. Let $H = \left\{2n - 1 \mid n \in \mathbb{Z}^+\right\} = \{1, 3, 5, 7, 9, \dots\} \subseteq \mathbb{Z}^+$

Determine whether

a) H is closed under $+$

b) H is closed under $*$.

a) $+: H \times H \to H$

$(a, b) \to a + b$

Is it true if $a = 2n - 1$ and $b = 2m - 1$ that

$a + b = (2n - 1) + (2m - 1) \in H$? **NO!**

$(2n - 1) + (2m - 1) = 2(n + m) - 2 \notin H.$

Thus H is not closed under $+$.

b) $\cdot : H \times H \to H$

$(a, b) \to a \cdot b$

If $a = 2n - 1$ and $b = 2m - 1$ then

$a \cdot b = (2n - 1)(2m - 1) = 4nm - 2n - 2m + 1 \in H$

since an even number plus 1 is an odd number and this number is positive.

So $a \cdot b \in H$ and H is closed under $\cdot$.

Ex. Let F be the set of all real valued functions, f, having $\mathbb{R}$ as a domain.

Define 5 operations: $+,\ -,\ \cdot,\ \div,$ and $\circ$

$+: F \times F \to F$

$(f, g) \to f + g$ i.e. $f + g = f(x) + g(x)$

$-: F \times F \to F$

$(f, g) \to f - g$

$\cdot : F \times F \to F$

$(f, g) \to f \cdot g$ i.e. $f \cdot g = f(x)g(x)$

$\div: F \times F \to F$

$(f, g) \to \frac{f}{g}$

$\circ: F \times F \to F$

$(f, g) \to f \circ g$ i.e. $f \circ g = f\big(g(x)\big).$

Notice $+$, $-$, $\cdot$, and $\circ$ are binary operations but $\div$ is not because if g is a function which has a point $g(x) = 0$ then $\div(f,g) = \frac{f(x)}{g(x)}$ would not be defined for all $x \in \mathbb{R}$.

Ex. Define $*$ on $\mathbb{Z}^+$ by $a * b = a^2 - b^2$. Show $*$ is not a binary operation.

Notice $a * b$ is not necessarily in $\mathbb{Z}^+$.

For example if $a = 2, b = 3$

$2 * 3 = 2^2 - 3^2 = 4 - 9 = -5 \notin \mathbb{Z}^+$. $\Longrightarrow$ $*$ is not a binary operation.

However $*$ is a binary operation on $\mathbb{Z}$.

Def: A binary operation on a set S is **commutative** if $a * b = b * a$ for all $a, b \in S$.

Ex. $+: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by $+(a,b) = a + b$ is commutative because

$+(a,b) = a + b$

$+(b,a) = b + a$ and $a + b = b + a$ for integers

However

$*: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by $*(a,b) = a^2 - b^2$ is not commutative because if, for example, $a = 2, b = 3$

$*(2,3) = 2^2 - 3^2 = -5$

$*(3,2) = 3^2 - 2^2 = 5$

So $a * b \neq b * a$.

Ex. Let $M_n(\mathbb{R}) = n \times n$ matrices with real entries.

Matrix multiplication and matrix addition are binary operations on $M_n(\mathbb{R})$.

$$+: M_n(\mathbb{R}) \times M_n(\mathbb{R}) \to M_n(\mathbb{R})$$

$(A, B) \to A + B$ (add corresponding entries)

$$\cdot : M_n(\mathbb{R}) \times M_n(\mathbb{R}) \to M_n(\mathbb{R})$$

$(A, B) \to A \cdot B$ (matrix multiplication)

However, $+$ is a commutative binary operation.

But $A \cdot B$ is <u>not</u> a commutative binary operation.

Def. A binary operation on a set S is **associative** if:

$(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.

Ex. $+, \cdot$ are both commutative and associative binary operations on

$\mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathbb{Z}^+, \mathbb{R}^+,$ and F (the set a real valued function on $\mathbb{R}$).

Ex. Define $*$ on $\mathbb{Z}^+$ by $(a * b) = 2^{a+b}$. Determine if $*$ is a binary operation.

If so, is it commutative? Associative?

$$*: \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$$

$(a, b) \to a * b = 2^{a+b}$ is defined for all $a, b \in \mathbb{Z}^+$

and $2^{a+b} \in \mathbb{Z}^+$ so it's a binary operation.

Notice $a * b = 2^{a+b}$

$b * a = 2^{b+a} = 2^{a+b}$

So $*$ is commutative.

However $\big((a * b) * c\big) = 2^{a+b} * c = 2^{(2^{(a+b)}+c)}$

$\big(a * (b * c)\big) = 2^{a+(b*c)} = 2^{(a+(2^{b+c}))}$

Let $a = 3,\ b = 1,\ c = 2$ then

$(3 * 1) * 2 = 2^{(2^{(3+1)}+2)} = 2^{18}$

$3 * (1 * 2) = 2^{(3+(2^{(1+2)}))} = 2^{11} \neq 2^{18}$

So $*$ is not associative.

Ex. Compositions of functions is associative since:

$\big(f \circ (g \circ h)\big)(x) = f\Big(g\big(h(x)\big)\Big)$

and $((f \circ g) \circ h))(x) = (f \circ g)\big(h(x)\big) = f(g\big(h(x)\big))$

So composition is an associative binary operation on the set of real valued functions.

However, composition is <u>not</u> commutative.

For example, let $f(x) = x^2$ and $g(x) = x + 1.$

Then, $(f \circ g)(x) = f(x + 1) = (x + 1)^2 = x^2 + 2x + 1$

$(g \circ f)(x) = g(x^2) = x^2 + 1.$

So $(f \circ g) \neq g \circ f.$

Def. $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ where addition is defined as

$a +_n b = (a + b)$ modulo n.

That is, take the remainder when you divide $a + b$ by n.

Ex. $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$2 +_4 3 = 1$ because 5 divided by 4 has a remainder of 1.

Modulo n addition is a commutative and associative binary operation on $\mathbb{Z}_n$.

Given a finite set we can define $*$ through a table.

Ex. Let $S = \{a, b, c\}$

$*$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$
$\boldsymbol{a}$	b	a	b
$\boldsymbol{b}$	c	c	b
$\boldsymbol{c}$	c	b	a

i.e. $a * b = a, \quad a * c = b, \quad b * a = c,$ etc.

$*$ is commutative if the table is symmetric about the major diagonal. For this example, $*$ is not commutative $(a * b = a, \;\; b * a = c)$.

Calculate $(a * b) * c$ and $a * (b * c)$ for this example:

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

$a * (b * c) = a * (b) = a \qquad \Longrightarrow \quad *$ is not associative.