Binary operations on sets
(after Ray Mayer's notes)

Definition: *A* **binary operation** *on a set A is a function $\circ : A \times A \to A$. Binary operations are usually denoted by special symbols such as:*

$$+, -, \cdot, /, \times, \circ, \cap, \cup, \text{ or }, \text{ and }.$$

We often write $a \circ b$ rather than $\circ(a, b)$.

Examples and non-examples:

(1) $+, \cdot$ on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$;
(2) $-$ on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$;
(3) $/$ on $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$;
(4) $-$ is not a binary operation on $\mathbb{N}$.

Definition: *Let $\circ$ be a binary operation on a set A. An element $e \in A$ is an* **identity element for** $\circ$ *if for all $a \in A$, $a \circ e = a = e \circ a$.*

Examples and non-examples:

Theorem: *Let $\circ$ be a binary operation on A. Suppose that e and f are both identities for $\circ$. Then $e = f$. In other words, if an identity exists for a binary operation, it is unique. Hence we talk about the identity for $\circ$.*

Proof: Since for all $a \in A$, $e \circ a = a$, we get in particular that $e \circ f = f$. Also, for every $a \in A$, $a \circ f = a$, hence $e \circ f = e$. Thus $e = e \circ f = f$. $\square$

Note: we used the symmetry and the transitivity of the equality property.

Definition: *Let $\circ$ be a binary operation on A and suppose that e is its identity. Let x be an element of A. An* **inverse** *of x is an element $y \in A$ such that $x \circ y = e = y \circ x$.*

Examples and non-examples:

(1) Let $\circ = +$ on $\mathbb{Z}$. Then 0 is the identity element and every element has an (additive) inverse.
(2) Let $\circ = \cdot$ on $\mathbb{Q} \setminus \{0\}$. Then 1 is the identity element and every element has a multiplicative inverse.
(3) If S is a set and A is the collection of all subsets of S, $\cap$ is a binary operation on S. Find its identity element, and find all elements that have an inverse.

Definition: *A binary operation $\circ$ on A is* **associative** *if for all $a, b, c \in A$, $a \circ (b \circ c) = (a \circ b) \circ c$.*

Examples and non-examples:

(1) $+, \cdot$ and function composition are associative.
(2) $-, /$ are not associative.

Theorem: *Let $\circ$ be an associative binary operation on A with identity e. If x has an inverse, that inverse is unique.*

Proof: Let y and z be inverses of x. Then

$$\begin{aligned} y &= y \circ e \text{ (by property of identity)} \\ &= y \circ (x \circ z) \text{ (since } z \text{ is an inverse of } x) \\ &= (y \circ x) \circ z \text{ (since } \circ \text{ is associative)} \\ &= e \circ z \text{ (since } y \text{ is an inverse of } x) \\ &= z \text{ (by property of identity).} \end{aligned}$$

Thus by the transitivity of equality, $y = z$. □

Definition: *We say that x is* **invertible** *if x has an inverse. The (abstract) inverse is usually denoted x^{-1}.*

Be careful! What is the number 5^{-1} if $\circ = +$?

Theorem: *If x is invertible, then its inverse is also invertible, and the inverse of the inverse is x.*

Proof: By definition of inverses of x, $x^{-1} \circ x = e = x \circ x^{-1}$, which also reads as "the inverse of x^{-1} is x. □

Theorem: Cancellation. *Let $\circ$ be an associative binary operation on a set A, let e be the identity and z an invertible element in A. Then for all $x, y \in A$,*

$$x \circ z = y \circ z \Rightarrow x = y,$$
$$z \circ x = z \circ y \Rightarrow x = y.$$

Proof: We prove only the first implication. If $x \circ z = y \circ z$, then $(x \circ z) \circ z^{-1} = (y \circ z) \circ z^{-1}$, hence by associativity, $x \circ (z \circ z^{-1}) = y \circ (z \circ z^{-1})$. Thus by the definition of inverses and identities, $x = x \circ e = y \circ e = y$. □

If $\circ$ is associative, we will in the future omit parentheses in $a \circ b \circ c \circ d$, as the order of the computation does not matter.

If $\circ$ is not associative, you need to keep parentheses! For example, in $\mathbb{Z}$, $a - b - c - d$ can have parentheses inserted in how many different ways, and five different values can be obtained! Find specific four integers a, b, c, d for which you get 5 values with different placements of parentheses.

Definition: *A binary operation $\circ$ on A is* **commutative** *if for all $a, b \in A$, $a \circ b = b \circ a$.*

Examples and non-examples: