2. BINARY OPERATIONS

A **binary operation** on a set S is defined to be a mapping

$$S \times S \to S$$

The notation is $(a, b) \mapsto a * b$. In words: for every ordered pair of not necessarily distinct elements (a, b) in the set S the binary operation assigns a unique element $a * b \in S$. The key point is that a, b are elements of the same set S and $a * b$ is another element of the same set S. No exceptions are allows.

For example, the binary operation x/y is not defined for $y = 0$. But it is defined for all positive real numbers x, y and the result $x/y = x \div y$ is also positive real. So, in this case the set could be $S = \mathbb{R}^+, * = (\div)$.

The pair $(S, *)$ is called a **binary structure**. In the example $(\mathbb{R}^+, \div)$ is a binary structure. The idea is to study the common properties of all operations. If we say we have a "binary operation" then we are talking simultaneously about addition, multiplication, subtraction, division, raising to powers, etc. This is very general and universally applicable.

The operation $*$ gives a *structure* on S. A set S by itself is homogeneous. All elements are equally important. There is no way to distinguish between them. Once there is a structure, some elements become much more important than others. For example, take $(\mathbb{Z}, \times)$, the set of integers under multiplication. The numbers 0 and 1 become very important.

0 is the "annihilator" since it "kills" all the other elements:

$$0 \times n = n \times 0 = 0.$$

1 is called "unity" since

$$1 \times n = n \times 1 = n$$

It leaves everyone unaltered.

The numbers 0,1 are called *idempotents* since they are two of the solutions of the equation

$$x^2 = x$$

The word "idem-potent" means "self-power" i.e., its powers are itself. (Prove this: $x^n = x$ if x is idempotent.)

A subset $T \subseteq S$ is said to be *closed* under the operation $*$ if $t_1 * t_2 \in T$ for all $t_1, t_2 \in T$. If this is true then $(T, *)$ is another binary structure.

Example 2.1. *Let $S = \mathbb{R}$ with operation $*$ representing subtraction:*

$$a * b = a - b$$

Then the set of integers $\mathbb{Z}$ is closed under this operation. So, $(\mathbb{Z}, -)$ is also a binary structure.

Theorem 2.2. *There is a bijection* $exp : \mathbb{R} \to \mathbb{R}^+$ *which makes subtraction in* $\mathbb{R}$ *correspond to division in* $\mathbb{R}^+$*:*

$$exp(x) = e^x$$

$$exp(x - y) = exp(x) \div exp(y)$$

What is the inverse mapping

$$\mathbb{R}^+ \to \mathbb{R} \quad ?$$

Definition 2.3. *We say that a binary operation* $*$ *on a set* S *is*

(1) **commutative** *if* $x * y = y * x$ *for every* $x, y \in S$
(2) **associative** *if* $(x * y) * z = x * (y * z)$ *for all* $x, y, z \in S$.

Problems:

(1) Let $S = \mathbb{R}$. Is the binary operation $x * y = x - y$ commutative? associative?
(2) Let $S = \mathbb{Z}$. Is the binary operation $a * b = 2ab$ commutative? associative?
(3) Let $S = \mathbb{R}$. Is the binary operation
$$x * y = x + y + xy$$
commutative? associative?

If the binary operation $*$ is not associative then, given three elements of the set
$$(x * y) * z \neq x * (y * z).$$
Given four elements x, y, z, w there are 5 ways to put the parentheses. Find them.

If a binary operation on S is associative but not commutative then there are two ways to "multiply" x, y (Usually we speak of the operation $*$ as "multiplication" or "product". A commutative operation is often called a "addition" or "sum".)

Given four elements $x, y, z, w \in S$ and a binary operation $*$ which is associative but not commutative, how may ways can you multiply x, y, z, w?

Here is a very important example: Suppose that X is any set and S is the set of all mappings
$$f : X \to X$$
The binary operation $\circ$ (composition of functions) is associative but not commutative. Give an example to show it is not commutative.

Prove that an operation $*$ on a set can have at most one annihilator.