Intro to Abstract Algebra

Irvin Avalos

1 Introduction

Definition. A **operation**, $\star$, over a set S is a mapping,

$$\star : S \times S \to S$$

that assigns to each $(a, b) \in S$ a unique element $c = a \star b \in S$.

Example. Take the set $\mathbb{R}$ where the operations $+$ and $\cdot$ are well defined over $\mathbb{R}$, i.e., $+$ is defined as $a + b$ for $a, b \in \mathbb{R}$ and $\cdot$ as $a \cdot b$. Therefore, each pair $(a, b) \in \mathbb{R}$ is given an element $a + b$ and $a \cdot b$.

Example. An example of a set where the operation $+$ fails is the set of all matrices with real-valued entries, $M(\mathbb{R})$. This is because, matrix addition only works when two matrices have the same number number of rows and columns.

- Say that $\star$ is a valid operation on S, then S is said to be closed under $\star$ but a subset of S may not be, e.g., the set of nonzero real numbers $\mathbb{R}^\star$. This can be seen easily with the fact that $1 \in \mathbb{R}^\star$ and $-1 \in \mathbb{R}^\star$ but $1 + (-1) = 0 \notin \mathbb{R}^\star$.
- Formally, we call this an **induced operation** where $\star$ is an operation on S and $H \subseteq S$. Here H is closed under $\star$ only if for all $a, b \in H,\ a \star b \in H$.

Example. Let $H = \{n^2 \mid n \in \mathbb{Z}^+\}$.

1. Addition: Take $n_1 = 1 \in \mathbb{Z}^+$ and $n_2 = 5 \in \mathbb{Z}^+$, then it is obvious that $1 \in H$ and $25 \in H$ but $1 + 26 \notin H$. Therefore, addition fails on H.
2. Multiplication: Take two integers $p, q \in H$ which are defined as $p = n^2$ and $q = m^2$ where $n, m \in \mathbb{Z}^+$. The product $p \cdot q = (n^2) \cdot (m^2) = (n \cdot m)^2 \in H$ since $n \cdot m \in \mathbb{Z}^2$. Therefore, H is closed under $\cdot$.

Definition. An operation $\star$ on S is **commutative** if $a \star b = b \star a$ for all $a, b \in S$.

Definition. An operation $\star$ on S is **associative** if $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in S$.

- If $\star$ is not associative then expressions like $a \star b \star c$ are said to be *ambiguous* as the result of $a \star b \star c$ depends on the grouping order, i.e., $(a \star b) \star c$ and $a \star (b \star c)$ yield different results from each other.

Definition. For any set S and functions f, g that map S into S, the composition $f \circ g$ is defined as the function mapping S into S such that $(f \circ g)(x) = f(g(x))$ for all $x \in S$.

Theorem (Associativity of Composition)**.** Let S be a set and let $f, g,$ and h be functions mapping S into S, then $f \circ (g \circ h) = (f \circ g) \circ h$.
Proof. Given a set S where $x \in S$ let $f, g,$ and h be functions that map S into S. Solving the left side of $(f \circ g)(x) = f(g(x))$ results in

$$(f \circ (g \circ h))(x) = f \circ ((g \circ h)(x)) = f(g(h(x))).$$

Similarly, solving the right side yields

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))).$$

Thus, the composition of functions is associative.