Section 2: Binary operations and groups

Our main object of study in this course will be a group. Here is the definition.

Definition 0.1. A **group** $(G, \star)$ is a set G with binary operation $\star$ such that

- $\star$ is associative: $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in G$
- There exists an identity element $e \in G$ such that $e \star a = a \star e = a$ for all $a \in G$.
- There exist inverse elements: for all $a \in G$, there exists $a' \in G$ such that $a \star a' = a' \star a = e$.

This is a lot to unpack at once, so we will just focus on *binary operations* today.

Definition 0.2. A **binary operation** on a set S is a function $\star : S \times S \to S$ that we denote by $(a, b) \mapsto a \star b$.

Example 0.3. The main examples: addition and multiplication (where $S = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \ldots$ i.e. $a \star b = a + b$ or $a \star b = a \cdot b$ where a and b are some type of numbers.

Example 0.4. Let $\mathbb{R}^\times = \{r \in \mathbb{R} | r \neq 0\}$. Multiplication is a valid binary operation but $+$ is not because $1 + (-1) = 0$, and $0 \notin \mathbb{R}^\times$. We use the terminology that $\mathbb{R}^\times$ is not **closed under** $+$ because we can add two entries in the set and get a result that is not in the set.

Example 0.5. Let $H = \{n^2 | n \in \mathbb{Z}\}$: this is not closed under $+$ because $1 = 1^2$ and $4 = 2^2$ but $1 + 4 = 5$ which is not a perfect square. But, this is closed under multiplication because $n^2 \cdot m^2 = (nm)^2$.

Example 0.6. Let $F = \{f : \mathbb{R} \to \mathbb{R}\}$ be the set of all functions from $\mathbb{R} \to \mathbb{R}$. There are many binary operations we could use here: $+, -, \cdot, \circ$.

Example 0.7. Let $\mathbb{Z}_n = \{0, 1, , 2, \ldots, n-1\}$. This is closed under the binary operations $+_n$ and $\cdot_n$ (where the subscript n indicates we are working modulo n).

Example 0.8. Let D_3 be the group of symmetries of the triangle we discussed on Monday. The composition of two symmetries is a binary operation on this set.

Definition 0.9. A binary operation $\star$ on a set S is **commutative** if $a \star b = b \star a$ for all $a, b \in S$.

Example 0.10. $+$ and $\cdot$ are commutative operations on $\mathbb{Z}$. $\circ$ is not a commutative operation on D_3 or F.

Definition 0.11. A binary operation $\star$ on a set S is **associative** if $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in S$.

Example 0.12. Which of the following are associative or commutative?

1. $(\mathbb{Z}, -)$: neither! It is not associative because we do not always have $a - (b - c) = (a - b) - c$; for example, $1 - (0 - 1) \neq (1 - 0) - 1$. It is not commutaive because we do not always have $a - b = b - a$; for example, $1 - 2 \neq 2 - 1$.

2. $(F, \circ)$: This is associative but not commutative. Reason: composition is *always* associative. Proof: we need to show that, given three functions f, g, h, $f \circ (g \circ h) = (f \circ g) \circ h$. We know this is true because

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

and

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

This is not commutative because $f \circ g$ is generally not equal to $g \circ f$.

3. $(D_3, \circ)$: It is associative but not commutative. It is associative because composition is always associative, but it is not commutative because on Monday we saw that $F \circ R \neq R \circ F$.

Definition 0.13. Given a binary operation $\star$ and a finite set S, we can make a **table** representing that operation exactly as we did for the triangle. The ij^{th} entry of the table is i^{th} entry to the left $\star$ j^{th} entry above.

Example 0.14. If $S = \{a, b, c\}$, here's one binary operation.

$\star$	a	b	c
a	b	c	b
b	a	c	b
c	c	a	a

Is this associative or commutative?
Answer: neither! We will come back to this next time.