Homework 2

Ryan Coyne

February 10, 2024

Theorem 1: Let $(G, \circ)$ be a group, and let $g, h \in G$. Then

$$(g \circ h)^{-1} = h^{-1} \circ g^{-1}.$$

PROOF: First, we compose $(g \circ h)^{-1}$ with $(g \circ h)$. This gives us,

$$(g \circ h)^{-1} \circ (g \circ h) = e.$$

Next compose $g^{-1} \circ h^{-1}$ with $(g \circ h)$. This gives us

$$\begin{aligned}(h^{-1} \circ g^{-1}) \circ (g \circ h) &= h^{-1} \circ (g^{-1} \circ g) \circ h \\ &= h^{-1} \circ h \\ &= e.\end{aligned}$$

Now, since $(g \circ h)^{-1} \circ (g \circ h) = (h^{-1} \circ g^{-1}) \circ (g \circ h)$, it follows that $(g \circ h)^{-1} = h^{-1} \circ g^{-1}$. ■

Theorem 2: Let $\mathbb{Z}_N = 0, 1, 2, \cdots, N-1$. Show that the operation $\circ : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N$ defined by

$$a \circ b := \begin{cases} a + b, & a + b < N \\ a + b - N, & a + b \geq N \end{cases}$$

is associative. i.e. Show that for any $a, b, c \in \mathbb{Z}_N$, we have

$$(a \circ b) \circ c = a \circ (b \circ c)$$

PROOF: Case 1: ■