THE SET OF PERMUTATIONS ON A SET X IS A GROUP UNDER FUNCTION COMPOSITION

Let X be any nonempty set, and let $f : X \longrightarrow X$ and $g : X \longrightarrow X$ and $h : X \longrightarrow X$ be functions. Recall that we define the composition $f \circ g : X \longrightarrow X$ according to the rule

$$(f \circ g)[a] = f(g(a))$$

for all $a \in X$. We say that $f = g$ provided $f(a) = g(a)$ for all $a \in X$.

LEMMA 1: The functions $(f \circ g) \circ h$ and $f \circ (g \circ h)$ are equal. In other words, function composition is associative.

Proof. For simplicity, let $F = f \circ g$ and let $G = g \circ h$. For all $a \in X$, we know

$$[(f \circ g) \circ h](a) = [F \circ h](a) = F(h(a)) = [f \circ g](h(a)) = f(g(h(a)))$$

$$[f \circ (g \circ h)](a) = [f \circ G](a) = f(G(a)) = f([g \circ h](a)) = f(g(h(a)))$$

Consequently, we know that $[(f \circ g) \circ h](a) = [f \circ (g \circ h)](a)$ for all $a \in X$, and we may conclude that $(f \circ g) \circ h = f \circ (g \circ h)$.

QED

Recall that the function f is *one-to-one* provided $f(a) = f(b)$ implies $a = b$ for all $a, b \in X$. The function f is *onto* provided for each $b \in X$, there exists at least one $a \in X$ such that $b = f(a)$. We say the function f is a *bijection* provided it is both one-to-one and onto. In other words, a function f is a bijection provided for each $b \in X$, there is *exactly one* $a \in X$ such that $f(a) = b$. A bijection on the set X is called a *permutation* on X.

LEMMA 2: If f and g are one-to-one, then $f \circ g$ is also one-to-one.

Proof. Suppose that $a, b \in X$ are such that $[f \circ g](a) = [f \circ g](b)$. This tells us that $f(g(a)) = f(g(b))$; and since f is one-to-one, we know that $g(a) = g(b)$. However, since g is also one-to-one, we may conclude that $a = b$. Consequently, $f \circ g$ is also one-to-one.

QED

LEMMA 3: If f and g are onto, then $f \circ g$ is also onto.

Proof. Suppose that $b \in X$. We need to find $a \in X$ such that $[f \circ g](a) = b$. Now, since f is onto, we know there exist $c \in X$ such that $b = f(c)$. Furthermore, since g is onto, there exist $a \in X$ such that $c = g(a)$. Therefore, we know $b = f(c) = f(g(a)) = [f \circ g](a)$. We may conclude that $f \circ g$ is also onto.

QED

THEOREM 4: Let $\wp_X$ represent the set of all permutations on X under the combining rule of function composition. The system $\wp_X$ is a group.

Proof. Note that Lemmas 1, 2, and 3 show us that function composition is an associative operation on the set of permutations. We only need to demonstrate that this set possesses an indentity element under composition, and that every member of the set has an inverse under composition. Note that the identity function $e : X \longrightarrow X$ defined by $e(a) = a$ for all $a \in X$ serves as the identity element. Indeed, observe that for any permutation $f : X \longrightarrow X$ we have

$$[e \circ f](a) = e(f(a)) = f(a) \qquad \text{and} \qquad [f \circ e](a) = f(e(a)) = f(a)$$

Consequently, we know $e \circ f = f = f \circ e$, and we may conclude that e serves as the identity element for $\wp_X$.

Now, suppose that $f : X \longrightarrow X$ is any permutation. For each $b \in X$, there exists *exactly one* $a \in X$ such that $b = f(a)$. We may therefore define a new bijection $g : X \longrightarrow X$ according to the rule $g(b) = a$, where a is the unique member of X such that $f(a) = b$. By construction, g is both one-to-one and onto. Now, observe

$$[f \circ g](b) = f(g(b)) = f(a) = b \qquad \text{and} \qquad [g \circ f](a) = g(f(a)) = g(b) = a$$

Consequently, we know that $f \circ g = e = g \circ f$; and we may conclude that g is the inverse for f under function composition.

QED