MTHSC 412 Section 1.5 –Permutations and Inverses

Kevin James

Definition

A bijection from a set A to itself is called a *permutation* on A.

Notation

Suppose that A is nonempty.

- We denote by $\mathcal{S}(A)$ the set of all permutations on A.
- We will denote by $\mathcal{M}(A)$ the set of all mappings form A to A.
- In the special case that the set $A = \{1, 2, \ldots, n\}$, we use the notation $S_n = \mathcal{S}(A)$.

Remark

Suppose that A is a nonempty set. Then composition of functions is an associative binary operation on $\mathcal{M}(A)$. The identity element I_A of $\mathcal{M}(A)$ under composition of functions is given by

$$I_A(x) = x \quad \text{for all } x \in A.$$

Proof.

For any $f \in \mathcal{M}(A)$,
$f \circ I_A(x) = f(I_A(x)) = f(x)$.
Thus $f \circ I_A = f$.
Also, $I_A \circ f(x) = I_A(f(x)) == f(x)$.
Thus, $I_A \circ f = f$.
Thus I_A is the identity element. $\square$

Example

Consider the maps $f, g \in \mathcal{M}(\mathbb{Z})$ defined by

$$\begin{aligned} f(x) &= 2x \\ g(x) &= \begin{cases} \frac{x}{2} & \text{if } x \text{ is even,} \\ 4 & \text{if } x \text{ is odd.} \end{cases} \end{aligned}$$

Then, $g \circ f(x) = g(f(x)) = g(2x) = x$.
Thus $g \circ f = I_{\mathbb{Z}}$.
So, g is a left inverse of f.
However, $f \circ g(x) = f(g(x)) = \begin{cases} f(x/2) \\ f(4) \end{cases} = \begin{cases} x & \text{if } x \text{ is even,} \\ 8 & \text{if } x \text{ is odd.} \end{cases}$
So, $f \circ g \neq I_{\mathbb{Z}}$ and g is not a right inverse of f.

LEMMA

Let A be a nonempty set and let $f : A \longrightarrow A$. Then f is injective if and only if f has a left inverse.

Proof.

(⇐) Suppose first that f has a left inverse g.
The we have,
$f(a) = f(b) \Rightarrow g(f(a)) = g(f(b)) \Rightarrow I_A(a) = I_A(b) \Rightarrow a = b.$
Thus f is injective.
(⇒) Now suppose that f is injective.
Let a_0 be any fixed element of A.
Define $g \in \mathcal{M}(A)$ as follows.

$$g(x) = \begin{cases} y & \text{if there exists } y \in A \text{ such that } f(y) = x, \\ a_0 & \text{otherwise} \end{cases}$$

Note that when such y exists it is unique because f is injective.
So, g is a *well-defined* mapping.
For all $x \in A$ we have $g \circ f(x) = g(f(x)) = x$.
So, $g \circ f = I_A$ and g is a left inverse of f. $\square$

Lemma

Let A be a nonempty set and $f : A \rightarrow A$. Then f is surjective if and only if f has a right inverse.

Proof.

($\Leftarrow$) Suppose first that f has a right inverse g.
Now let $b \in A$.
Put $a = g(b)$.
Then $f(a) = f(g(b)) = f \circ g(b) = I_A(b) = b$.
Since $b \in A$ was arbitrary, it follows that f is surjective.
($\Rightarrow$) Suppose now that f is surjective.
We will construct a right inverse g of f (using the axiom of choice) as follows.
Let $a \in A$.
Since f is surjective, $f^{-1}(\{a\})$ is nonempty.
Choose $x \in f^{-1}(\{a\})$ and put $g(a) = x$.
We must do this for each $a \in A$.
Then, $f \circ g(a) = f(g(a)) = f(x) = a$.
Thus $f \circ g = I_A$ and g is a right inverse of f. $\square$

Theorem

Let $f : A \rightarrow A$. Then f is invertible if and only if f is a permutation on A.

Proof.

(⇒) Suppose first that f is invertible.
Then f has an inverse g.
Since g is a left and right inverse, it follows form the lemmas that f is bijective and therefore is a permutation on A.
(⇐) Now suppose that f is a permutation.
Since f is injective, it has a left inverse g.
Since f is surjective, it has a right inverse h.
So, we have $g = g \circ I_A = g \circ (f \circ h) = (g \circ f) \circ h = I_A \circ h = h$.
Thus f is invertible. □

Note

1. Composition of functions is an associative binary operation on $\mathcal{M}(A)$ with identity element I_A.
2. $f \in \mathcal{M}(A)$ is invertible under composition of functions if and only if $f \in \mathcal{S}(A)$.
3. We will denote the inverse of $f \in \mathcal{S}(A)$ by f^{-1}.
4. $\mathcal{S}(A)$ is closed under composition of functions.
5. That is, if $f, g \in \mathcal{S}(A)$, then $f \circ g \in \mathcal{S}(A)$.
6. Thus, composition of functions is an associative binary operation of $\mathcal{S}(A)$ with identity element I_A.
7. If $f \in \mathcal{S}(A)$ then $f^{-1} \in \mathcal{S}(A)$ also.