Section 7.2: One-to-One, Onto and Inverse Functions

In this section we shall developed the elementary notions of one-to-one, onto and inverse functions, similar to that developed in a basic algebra course. Our approach however will be to present a formal mathematical definition for each of these ideas and then consider different proofs using these formal definitions.

1. One-to-one Functions

We start with a formal definition of a one-to-one function.

Definition 1.1. Let $f\colon X \to Y$ be a function. We say f is one-to-one, or injective, if and only if for all $x_1, x_2 \in X$, if $f(x_1) = f(x_2)$ then $x_1 = x_2$. Or equivalently, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$. Symbolically,

$$f\colon X \to Y \text{ is injective} \iff \forall x_1, x_2 \in X, f(x_1) = f(x_2) \to x_1 = x_2$$

To show that a function is one-to-one when the domain is a finite set is easy - we simply check by hand that every element of X maps to a different element in Y. To show that a function is one-to-one on an infinite set we need to use the formal definition. Specifically, we have the following techniques to prove a function is one-to-one (or not one-to-one):

- to show f is one-to-one, take arbitrary $x_1, x_2 \in X$, suppose that $f(x_1) = f(x_2)$ and try to deduce that this implies $x_1 = x_2$
- to show that f is not one-to-one, find specific $x_1, x_2 \in X$ with $x_1 \neq x_2$ but $f(x_1) = f(x_2)$ (i.e. provide a counter-example)

We illustrate with some examples.

Example 1.2. How many injective functions are there from a set with three elements to a set with four elements? How about a set with four elements to a set with three elements?

Suppose $X = \{a, b, c\}$ and $Y = \{u, v, w, x\}$ and suppose $f\colon X \to Y$ is a function. Then we can define f by simply specifying the images of a, b, and c, and to make it injective, we need to make sure none of the images are the same. But this will simply be equal to the number of 3 permutations from the set Y, and thus there will be a total of $4 \cdot 3 \cdot 2 = 24$ total different injective functions from X to Y.
Next note that if X has four elements and Y has three elements, no function from X to Y will be injective since at least two elements from X must map to the same element in Y.

Example 1.3. Define $f\colon \mathbb{Z} \to \mathbb{Z}$ by $f(n) = 2n + 1$. Show that f is one-to-one.

Suppose that x_1 and x_2 are arbitrary integers and $f(x_1) = f(x_2)$. We need to show that $x_1 = x_2$. Since $f(x_1) = f(x_2)$, it follows that

$$2x_1 + 1 = 2x_2 + 1.$$

Therefore,

$$2x_1 = 2x_2$$

and thus $x_1 = x_2$.

Example 1.4. Define $f\colon \mathbb{Z} \to \mathbb{Z}$ by $f(n) = 3n^2 + 2$. Show that f is not one-to-one.

To show that f is not one-to-one, we need to find $x_1 \neq x_2$ such that $f(x_1) = f(x_2)$. However, this is straight forward - we can take -1 and 1, and we get

$$f(1) = 3 \cdot (1)^2 + 2 = 5 = 3 \cdot (-1)^2 + 2 = f(-1).$$

Thus f is not one-to-one.

2. Onto Functions

We start with a formal definition of an onto function.

Definition 2.1. Let $f\colon X \to Y$ be a function. We say f is onto, or surjective, if and only if for any $y \in Y$, there exists some $x \in X$ such that $y = f(x)$. Symbolically,

$$f\colon X \to Y \text{ is surjective } \iff \forall y \in Y, \exists x \in X f(x) = y$$

To show that a function is onto when the codomain is a finite set is easy - we simply check by hand that every element of Y is mapped to be some element in X. To show that a function is onto when the codomain is infinite, we need to use the formal definition. Specifically, we have the following techniques to prove a function is onto (or not onto):

- to show f is onto, take arbitrary $y \in Y$, and show that there is some $x \in X$ with $f(x) = y$
- to show that f is not onto, find some $y \in Y$ such that for any $x \in X$, we do not have $f(x) = y$ (i.e. provide a counter-example)

We illustrate with some examples.

Example 2.2. How many surjective functions are there from a set with three elements to a set with four elements? How about a set with four elements to a set with three elements?

Suppose $f\colon X \to Y$ is a function. If Y has four elements and X has three elements, then no function from X to Y will be surjective since there are at most three images under f (since there are only three elements in X.

Now suppose $X = \{a, b, c, d\}$ and $Y = \{u, v, w\}$. Then we can define f by simply specifying the images of a, b, c, and d, and to make it surjective, we need to make sure every element in the codomain is mapped to by at least one element. Note that if f is onto, then one of u, v and w will have two elements in its preimage and the others will have a single element. Therefore, we shall break up the set of surjective maps into three subsets - those where $u \in Y$ has two preimages, those where $v \in Y$ has two preimages, and those where $w \in Y$ has two preimages. Note that by symmetry, each of these sets will have the same size, so we shall just consider the first.
Suppose that $f\colon X \to Y$ is a surjective map and $u \in Y$ has two preimages. We can think of all the different ways of constructing f as a counting problem. Specifically, for the first step, to determine $f^{-1}(u)$, we need to choose 2 objects from 4, so there are $\binom{4}{2}$ possibilities. Next, for $f^{-1}(v)$, there are two remaining possibilities, and for $f^{-1}(w)$, one last possibility. Thus the total number of possibilities will be $\binom{4}{2} \cdot 2 \cdot 1 = 12$. Since we will gat equal numbers if we assume either v or w have two preimages, it follows that there are a total of $3 \cdot 12 = 36$ surjective maps.

Example 2.3. Define $f\colon \mathbb{Z} \to \mathbb{Z}$ by $f(n) = 2n + 1$. Show that f is not onto.

To show that f is not onto, we need to find $y \in \mathbb{Z}$ such that there does not exist $x \in X$ with $f(x) = y$. However, this is straight forward - we can take $y = 2$. Then if $f(x) = 2x + 1 = 2$, then $x = 1/2 \notin \mathbb{Z}$.

Example 2.4. Define $f\colon \mathbb{Z} \to \mathbb{Z}$ by $f(n) = n + 5$ Show that f is onto.

Suppose that $y \in \mathbb{Z}$ is an arbitrary integer. We need to show that there exists $x \in \mathbb{Z}$ such that $f(x) = y$. However take $x = y - 5 \in \mathbb{Z}$. Then $f(x) = x + 5 = y - 5 + 5 = y$. It follows that f is onto.

3. One-to-One Correspondence

We have considered functions which are one-to-one and functions which are onto. We next consider functions which share both of these properties.

Definition 3.1. A one-to-one correspondence (or bijection) from a set X to a set Y is a function $F\colon X \to Y$ which is both one-to-one and onto.

To show a function is a bijection, we simply show that it is both one-to-one and onto using the techniques we developed in the previous sections. We illustrate with a couple of examples.

Example 3.2. Define $f\colon \mathbb{Z} \to \mathbb{Z}$ by $f(n) = n + 5$ Show that f is a one-to-one correspondence.

Suppose that $y \in \mathbb{Z}$ is an arbitrary integer. We need to show that there exists $x \in \mathbb{Z}$ such that $f(x) = y$. However take $x = y - 5 \in \mathbb{Z}$. Then $f(x) = x + 5 = y - 5 + 5 = y$. It follows that f is onto.
Now suppose that $x_1, x_2 \in \mathbb{Z}$ and $f(x_1) = f(x_2)$. Then $x_1 + 5 = x_2 + 5$ and thus $x_1 = x_2$. It follows that f is one-to-one. Consequently, f is a bijection.

Notice that if a function $f\colon X \to Y$ is a one-to-one correspondence, then it associates one and only one value of y to each value in x. In particular, it makes sense to define a reverse function from Y to X which reverses this correspondence. Specifically, we can define the following:

Definition 3.3. Suppose $f\colon X \to Y$ is a one-to-one correspondence. Then there is a function $f^{-1}\colon Y \to X$, called the inverse of f defined as follows:

$$f^{-1}(y) = x \iff f(x) = y.$$

Inverse functions are very important both in mathematics and in real world applications (e.g. population modeling, nuclear physics (half life problems) etc). Determining inverse functions is generally an easy problem in algebra.

Example 3.4. Find the inverse function to $f\colon \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = n + 5$.

We have

$$f^{-1}(y) = x \iff f(x) = y \text{ or, } x + 5 = y \text{ or, } x = y - 5$$

i.e.

$$x = f^{-1}(y) = y - 5$$

Example 3.5. Show that the function $f\colon \mathbb{R}^* \to \mathbb{R}\backslash\{1\}$ defined by

$$f(x) = \frac{x+1}{x}$$

is a one-to-one correspondence and determine its inverse function.

Suppose that $y \in \mathbb{R}^*$ is an arbitrary real number. We need to show that there exists $x \in \mathbb{R}$ such that $f(x) = y$ i.e.

$$f(x) = \frac{x+5}{x} = y \text{ or, } yx = x + 5 \text{ or, } yx - x = 5 \text{ or, } x = \frac{5}{y-1}$$

It follows that if we choose $x = 5/(y-1)$, then for any real $y \neq 1$, and thus f is onto.
Now suppose that $x_1, x_2 \in \mathbb{R}^*$ and $f(x_1) = f(x_2)$. Then

$$\frac{x_1+5}{x_1} = \frac{x_2+5}{x_2}$$

and thus $x_1x_2 + 5x_2 = x_1x_2 + 5x_1$, or $5x_2 = 5x_1$ and this $x_1 = x_2$. It follows that f is one-to-one and consequently, f is a bijection.
Next we want to determine a formula for $f^{-1}(y)$. We know

$$f^{-1}(y) = x \iff f(x) = y \text{ or, } \frac{x+5}{x} = y$$

Using a similar argument to when we showed f was onto, we have

$$x = f^{-1}(y) = \frac{5}{y-1}.$$

4. General Inverse Functions and Logarithms

We have seen that given a one-to-one correspondence $f\colon X \to Y$, we can define an inverse function from Y to X. In fact, the conditions for the existence of an inverse functions can be relaxed to restrict to those of a one-to-one function. Specifically, we can define the following:

Definition 4.1. Suppose $f\colon X \to Y$ is a one-to-one function and let $C \subseteq Y$ be the codomain of f. Then there is a function $f^{-1}\colon C \to X$, called the inverse of f defined as follows:

$$f^{-1}(y) = x \iff f(x) = y.$$

One very important function whose definition arises from the notion of an inverse function is a logarithm. To define a logarithm, we first need to recall the definition of an exponential function.

Definition 4.2. The exponential function with base b for $b > 0$ is defined from $\mathbb{R}$ to $\mathbb{R}^+$ as

$$\exp_b(x) = b^x \text{ for any } x \in \mathbb{R}$$

Recall that the exponential function is one-to-one. In particular, we can define an inverse function to an exponential function as follows:

Definition 4.3. The logarithm function with base b is defined from $\mathbb{R}^+$ to $\mathbb{R}$ as

$$\log_b(x) = y \text{ for any } x \in \mathbb{R}^+ \text{ if } x = b^y$$

We illustrate with some examples.

Example 4.4. Determine $\log_3(81)$.

We have $\log_3(81) = 4$ since $3^4 = 81$.

Example 4.5. Prove that for any $b > 0$ and any positive $x, y \in \mathbb{R}$, we have

$$\log_b\left(\frac{x}{y}\right) = \log_b(x) - \log_b(y).$$

We can prove results about logarithms by translating them into results about exponential functions. Let $u = \log_b(x)$ and $v = \log_b(y)$. Then we know $b^u = x$ and $b^v = y$, and so

$$\frac{x}{y} = \frac{b^u}{b^v} = b^{u-v}.$$

It follows that

$$\log_b\left(\frac{x}{y}\right) = u - v = \log_b(x) - \log_b(y).$$

Homework

(i) From the book, pages 417-419: Questions: 1, 3, 5, 8, 9, 10, 13, 14, 18, 21, 24, 27, 30, 34, 35, 40, 41, 42,