Algebra 1 Homework 1
Lee Fisher
2017-08-22

- Proposition 0.1: Let $f : A \to B$ be a function. Then:

  1. f is injective iff f has a left inverse.
  2. f is surjective iff f has a right inverse.
  3. f is bijective iff f admits a left and a right inverse. In this case the inverses are equal and the unique. This function is called the inverse of f and is denoted by f^{-1}
  4. If A and B are finite sets of the same order, f is bijective if and only if f is injective if and only if f is surjective.

Proof of 1.
$\to$ Suppose f is injective. By definition this means that for any $b \in f(A)$ there exists a unique a such that $f^{-1}(b) = a$. We define $g(b) = f^{-1}(b)$ if b is in $f(A)$ and if b is not in $f(A)$ then $g(b)$ is arbitrary. In this way $g \circ f = id_A$, because $g \circ f(a) = a$ for all $a \in A$.

$\leftarrow$ Suppose f has a left inverse. This means, by definition, there is a function $g : B \to A$ such that $g \circ f = id_A$. Consider two elements in A, a_1 and a_2 with $a_1 \neq a_2$. (If $|A| = 1$ then f is trivially injective.) $f(a_1) \neq f(a_2)$, otherwise this would mean $g(f(a_1)) = a_1$ and $g(f(a_1)) = a_2$ which contradicts the definition of a function. Therefore $f(a_1) \neq f(a_2)$ and f is injective. $\square$

Proof of 2.
$\to$ Suppose f is surjective this means $f(A) = B$, so for any $b \in B$ there is at least one $a \in A$ such that $f(a) = b$. Consider $g : B \to A$ where for all b we choose $g(b)$ so that $g(b) \in f^{-1}(b)$. In this way $f \circ g = id_B$, because for any $b \in B$, $f \circ g(b) = b$. Thus f has a right inverse.

$\leftarrow$ Suppose for sake of contradiction that f has a right inverse and f is not surjective. This means, by definition, there is a function g such that $f \circ g = id_B$ and that there is also an element b in B such that there is no a in A where $f(a) = b$. Here's the contradiction, in this case $f(g(b)) \neq b$ which contradicts $f \circ g = id_B$. Therefore f is surjective. $\square$

Proof of 3.
Suppose f is bijective. By definition f is both injective and surjective. Since f is injective (from the proof of 1) f has a left inverse, and since f is surjective (from the proof of 2) f has a right inverse. Likewise suppose f has both a left and right inverse. Then from the two previous proofs, f is both injective and surjective, and therefore bijective.

We call the left inverse as f_L^{-1} and the right inverse as f_R^{-1}. Consider for an element $b \in B$, $f_L^{-1} \circ f \circ f_R^{-1}(b)$. Well $f \circ f_R^{-1} = id_B$, so $f_L^{-1} \circ f \circ f_R^{-1}(b) = f_L^{-1}(b)$. Also $f_L^{-1} \circ f = id_A$ so $f_L^{-1} \circ f \circ f_R^{-1}(b) = f_R^{-1}(b)$. Therefore $f_R^{-1}(b) = f_L^{-1}(b)$ and the left and right inverses are equal.

Now we know that if f is bijective then any left inverse will also be a right inverse. Consider two inverses of f, f_1^{-1} and f_2^{-1}. We know that for any $b \in B$, $f \circ f_1^{-1}(b) = f \circ f_2^{-1}(b)$. Therefore $f_1^{-1}(b) = f_2^{-1}(b)$, so the inverses are the same, and thus unique.$\square$

Proof of 4.
Suppose A and B are finite sets of the same size and f is a function from A to B. We want to prove that bijectivity, surjectivity, and injectivity are equivalent. From the definition of bijectivity, it will suffice to prove that a function is surjective if and only if it is injective.

1. Surjectivity $\to$ Injectivity. Suppose $f : A \to B$ is surjective. For sake of contradiction suppose f is not injective. This means there are two distinct numbers a_1 and a_2 such that $f(a_1) = f(a_2)$. Since the since the cardinality of A and B are the same, this means the image of $f(A)$ is a strict subset of B. Which contradicts f being surjective. Therefore f must be injective.
2. Injectivity $\to$ Surjectivity. Suppose $f : A \to B$ is injective. For sake of contradiction suppose f is not surjective. This means $f(A)$ is strictly contained in B, however we know A and B are the same size. This means there must be two elements of A that map to the same thing in B. Thus contradicting injectivity. Thus f must be surjective. $\square$

- Proposition 0.2 Let $\sim$ be an equivalence relation of the set A. For any $a, b \in A$,

  1. $a \sim b$ if and only if $\bar{a} = \bar{b}$
  2. if $\bar{a} \neq \bar{b}$ then $\bar{a} \cap \bar{b} = \emptyset$

  Proof 1.
  $\to$ Suppose $a \sim b$ and consider $\bar{a}$ and $\bar{b}$. Since $a \sim b$ we know that $\bar{a} \subset \bar{b}$ because if any element is equivalent to a it must also be equivalent to b, and likewise that since $b \sim a$ we know that $\bar{b} \subset \bar{a}$. Therefore $\bar{a} = \bar{b}$.
  $\leftarrow$ Suppose $\bar{a} = \bar{b}$. This means $a \in \bar{b}$ and $b \in \bar{a}$. Therefore $a \sim b$.

  Proof 2.
  Suppose $\bar{a} \neq \bar{b}$ and for sake of contradiction, suppose there is an element c that is in $\bar{a} \cap \bar{b}$. This means that $a \sim c$ and $b \sim c$ and that by the previous logic, $\bar{a} = \bar{c}$, $\bar{b} = \bar{c}$, and $\bar{a} = \bar{b}$. Which is a contradiction of $\bar{a} \neq \bar{b}$. Therefore the intersection must be empty. $\square$

- Proposition 0.6 Let n be a fixed positive integer. Then

$$(\mathbb{Z}/n\mathbb{Z})^X = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} | 1 \leq a < n \text{ and } a, n \text{ are relatively prime}\}.$$

  Proof.
  Consider an element a in $(\mathbb{Z}/n\mathbb{Z})^X$. This means there is some number a^{-1} for which $a^{-1}a = 1$ mod n. In other words there is some multiple of n, mn for which $a^{-1}a + mn = 1$ where all numbers are integers. We arrive at the conclusion that a and n are relatively prime. If they had a common divisor then an integer linear combination of a and n would also be divisible by that number; the equation $xa + yn = 1$ would have no solutions. In the other direction suppose a and n are relatively prime. This means $gcd(a, n) = 1$ and since the gcd is a linear combination. There exist solutions x and y such that $xa + yn = 1$. This equation mod$n$ tells us that $a^{-1} = x$ and that a is in $(\mathbb{Z}/n\mathbb{Z})^X$.