Math 411: Honors Algebra I
Problem Set 1
due: September 11, 2019

Emily Riehl

Exercise 1. For each of the following functions determine whether they are injective, surjective, and bijective and construct a left, right, or two-sided inverse whenever these exist.

(i) The function $f\colon \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x^2$.
(ii) The function $f\colon \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$.
(iii) The function $f\colon \mathbb{Z} \times \mathbb{Z}_{>0} \to \mathbb{Q}$ defined by $(a, b) \mapsto \frac{a}{b}$; here $\mathbb{Z}_{>0}$ denotes the set of positive integers.
(iv) The function $\pi_B\colon A \times B \to B$ defined by $\pi_B(a, b) = b$.
(v) The function $\pi\colon A \to A_{/\sim}$ associated to an equivalence relation $\sim$ on A defined by $\pi(a) = [a]_\sim$.
(vi) The function from the set of subsets of $\mathbb{N}$ to the set of countably-infinite binary sequences $(0, 1, 0, 0, 0, 1, \ldots)$ that sends a subset $S \subset \mathbb{N}$ to the sequence that has a 1 in the nth coordinate if and only if $n \in S$.
(vii) Writing $10 = \{0, \ldots, 9\}$ and $[0, 1] = \{x \in \mathbb{R} \mid 0 \le x \le 1\}$, the function $f\colon 10^{\mathbb{N}} \to [0, 1]$ that sends a sequence of decimal digits $(x_n)_{n\in\mathbb{N}}$ to the real number $0.x_1x_2x_3 \ldots$.

Proof. (i) is injective but not surjective (since 2 has no integer square root). A left inverse is defined by sending each perfect square to its positive square root and sending non-square integers to 1.

(ii) is not injective (since 2 and -2 have the same square) and not surjective (since negative reals have no real square root).

(iii) This function is surjective (since every rational can be written as a fraction) but not injective since $(2, 1)$ and $(4, 2)$ have the same image. An inverse function sends each rational number to the pair (n, d) comprised of its numerator n and denominator d in lowest terms.

(iv) The projection function is surjective but not injective (unless A is empty or a singleton). A right inverse is given by fixing any element $a \in A$ and defining $s\colon B \to A \times B$ by $b \mapsto (a, b)$.

(v) The quotient function is surjective but not frequently injective. A right inverse is defined by sending each equivalence class to any representative element.

(v) This function is a bijection. The inverse function sends a sequence $s = (s_i)_{i\in\mathbb{N}}$ to the subset $S = \{i \in \mathbb{N} \mid s_i = 1\}$.

(vi) This function is surjective (since every real number can be written as a decimal) but not injective (since $0.099999 \ldots = 0.1$). A right inverse sends each real number to its "shortest" decimal representation, the one that ends in a 1 rather than in repeating 9s. □

Exercise 2. Write $2 = \{\bot, \top\}$ or $2 = \{0, 1\}$ for the set with two elements. (Your choice which notation you want to use for its elements.)

(i) Let $S \subset A$. Define a function $\chi_S\colon A \to 2$ that is related to S in some natural way.
(ii) Use part (i) to define a natural function $\chi\colon P(A) \to 2^A$.
(iii) Show that the function $\chi\colon P(A) \to 2^A$ that you've defined in part (ii) is a bijection.[1]

Proof. (i) We define the assignment $\chi_S\colon A \to 2$ as follows: $a \mapsto \begin{cases} \top, & a \in S \\ \bot, & a \notin S \end{cases}$

As we can see this does determine a function for every $a \in A$ is assigned an element of 2 and moreover this assignment is unique.

(ii) Now we must define a function assigning $S \in P(A)$ to a *function* $A \to 2$. That means for $S \in P(A)$, or equivalently $S \subseteq A$, we may assigned the *element* $\chi_S \in 2^A$ defined in part (a) – we proved already that χ_S is a function and so it is an element of the set 2^A. We can see that the way in which the assignment is done guarantees that every element $S \in P(A)$ is assigned to some element of 2^A and that this assignment is unique. Thus we have defined a function $\chi\colon P(A) \to 2^A$ via $\chi(S) = \chi_S$.

(iii) To prove that this determines a bijection we will define a function $k\colon 2^A \to P(A)$ and demonstrate that $k\circ\chi = \mathrm{id}_{P(A)}$ and $\chi \circ k = \mathrm{id}_{2^A}$.

[1] If the function you've defined in part (ii) is not a bijection, you might need to redefine the function χ.

Our function k is the assignment $f \in 2^A \mapsto \{a \in A \mid f(a) = \top\}$. We note that $\{a \in A \mid f(a) = \top\} \subseteq A$ by construction and so $\{a \in A \mid f(a) = \top\} \in P(A)$ as desired, and moreover this assignment works for every f and is uniquely determined. Thus $k\colon 2^A \to P(A)$ is a function.

Now we check $k \circ \chi = \mathrm{id}_{P(A)}$. Given $S \in P(A)$ we see that $(k \circ \chi)(S) = k(\chi(S)) = k(\chi_S) = \{a \in A \mid \chi_S(a) = \top\}$. If we unwind the definition of χ_S we see that $\chi_S(a) = \top \leftrightarrow a \in S$ and so we may simplify $\{a \in A \mid \chi_S(a) = \top\} = \{a \in A \mid a \in S\} = S$ – that is, $(k \circ \chi)(S) = S$ as desired.

Finally we check that $\chi \circ k = \mathrm{id}_{2^A}$. Given $f \in 2^A$ we have $(\chi \circ k)(f) = \chi(k(f)) = \chi_{\{a \in A \mid f(a) = \top\}}$. If we want to prove that $\chi(k(f)) = \mathrm{id}_{2^A}(f) = f$ we must now compare the two *functions* $\chi(k(f))$ and f for equality. This means ensuring that they have the same values on every element $a \in A$. Thus we expand

$$\chi_{\{a \in A \mid f(a) = \top\}}(x) = \begin{cases} \top, & x \in \{a \in A \mid f(a) = \top\} \\ \bot, & x \notin \{a \in A \mid f(a) = \top\} \end{cases}$$

Looking at this we notice that $x \in \{a \in A \mid f(a) = \top\} \leftrightarrow f(x) = \top$ and similarly $x \notin \{a \in A \mid f(a) = \top\} \leftrightarrow \neg(f(x) = \top)$. Now we appeal to a decision procedure on 2 to transform $\neg(f(x) = \top)$ into the logically equivalent $f(x) = \bot$. With these simplifications we may rewrite our expanded χ above as

$$\chi_{\{a \in A \mid f(a) = \top\}}(x) = \left\{ \begin{matrix} \top, & f(x) = \top \\ \bot, & f(x) = \bot \end{matrix} \right\} = f(x)$$

Whence $\chi(k(f)) = \mathrm{id}_{2^A}(f)$ and so k, χ witness a bijection between $P(A)$ and 2^A.

□

Exercise 3. Write B^A for the set of functions from A to B.

(i) Express the cardinality of B^A in terms of the cardinalities of A and B, assuming these are finite sets.
(ii) Express the cardinality of the powerset 2^A of A in terms of the cardinality of A, assuming that A is a finite set.
(iii) Explain why (ii) is a special case of (i).

Proof. The cardinality is $|B|^{|A|}$ since for each element of A there are $|B|$ choices for its image.

The cardinality of the powerset is $2^{|A|}$ since for each element of A we have two choices — whether or not it is in the subset — and each choice determines a different subset.

There is a bijection between the powerset and the set of functions from A to the set $2 = \{0, 1\}$, which is why (ii) is a special case of (i). □

Exercise 4. How many functions are there from a set of n elements to itself? How many bijections are there between a set with n elements and itself?

Proof. By part (i) of the previous problem there are n^n functions from the set of n elements to itself. Such a function is a bijection iff there are no repeated outputs.[2] So to define a bijection you have n choices for the image of the 1st element, $n - 1$ for the image of the 2nd, $n - 2$ for the image of the third, etc. Thus there are $n!$ bijections. □

Exercise 5.

(i) Let $f\colon A \to B$ be a function that has a left inverse $g\colon B \to A$ and also a right inverse $h\colon B \to A$. Prove that $h = g$.
(ii) Prove that $f\colon A \to B$ is a bijection if and only if f is an isomorphism without using (i).

Proof. Because g is a left inverse, $g \circ f = 1_A$. Because h is a right inverse $f \circ h = 1_B$. Now since composition is associative and unital we have

$$h = \mathrm{id}_A \circ h = (g \circ f) \circ h = g \circ (f \circ h) = g \circ \mathrm{id}_B = g.$$

If f is a bijection then for each $b \in B$ there exists a unique $a \in A$ so that $f(a) = b$. Define $f^{-1}(b)$ to be this a. Then by construction $f(f^{-1}(b)) = f(a) = b$. We see also that $a = f^{-1}(f(a))$ because both a and $f^{-1}(f(a))$ are defined to be elements of A whose image under f is $f(a)$ and uniqueness of the bijection says that $f(a) \in B$ can have at most one preimage. □

Exercise 6.

(i) For any function $f\colon A \to B$ define an explicit isomorphism between A and the graph $\Gamma_f \subset A \times B$.

[2] This implies automatically that there are no repeated inputs because the sizes of the set of inputs and the set of outputs are both the finite number n.

(ii) Define a natural function $\Gamma_f \to B$. Is it necessarily injective? Is it necessarily surjective?

Proof. Define a function $\phi\colon A \to \Gamma_f$ by $\phi(a) = (a, f(a))$. The inverse isomorphism is $\pi_A\colon \Gamma_f \to A$ defined by projection onto the first coordinate.

The natural function $\Gamma_f \to B$ is projection onto the second coordinate. This is injective if and only if $f\colon A \to B$ is injective and surjective if and only if $f\colon A \to B$ is surjective. □

Exercise 7.

(i) For any non-empty set A, define an isomorphism between the set $A \times A$ and the set A^2 of functions from the set with two elements to the set A.

(ii) For any non-empty set A and positive natural number n, define an isomorphism between the n-fold cartesian product $\prod_n A := A \times \cdots \times A$ and the set A^n of functions from the set with n elements to A.[3]

Proof. (i) Write $2 = \{0, 1\}$ for the two elements of the two-element set. The isomorphism $\phi\colon A \times A \to A^2$ is defined by declaring $\phi(a, b)\colon 2 \to A$ to be the function that sends 0 to a and sends 1 to b. The inverse isomorphism $\psi\colon A^2 \to A \times A$ is defined by declaring that $\psi(f) = (f(0), f(1))$ for each function $f\colon 2 \to A$.

Note that $\psi(\phi(a, b)) = (a, b)$ since $\phi(a, b)$ is the function that sends 0 to a and 1 to b. Also note that $\phi(\psi(f)) = \phi(f(0), f(1))\colon 2 \to A$ is the function that sends 0 to $f(0)$ and sends 1 to $f(1)$. But this is exactly what the function f does. Thus $\phi(\psi(f)) = f$. This proves that ψ and ϕ define an isomorphism

(ii) The construction and the proof are exactly the same as for (i) but with slightly more elaborate notation. Let $n = \{0, 1, \ldots, n-1\}$ and define $\phi\colon A \times \cdots \times A \to A^n$ to be the function that sends $(a_1, \ldots, a_n)$ to the function that sends i to a_{n+i}. Define $\psi\colon A^n \to A \times \cdots A$ to be the function that sends $f\colon n \to A$ to the n-tuple $(f(0), f(1), \ldots, f(n-1))$. The computation above again verifies that these functions define inverse isomorphisms. □

Exercise 8. Explain in your own words why all sets with three elements are isomorphic and speculate why I don't care what we call the elements of a 3-element set.

Proof. Given any two sets of three elements it is always possible to define a bijection between them. Thus, all three element sets are isomorphic. A category theorist generally doesn't distinguish between two isomorphic objects of the same category, which is why I don't care what we call the elements of a 3 element set.[4] □

Exercise 9. Suppose $p\colon A \to B$ is a surjective function. Explain how the fibers of p define an equivalence relation on A and prove that B is isomorphic to the set of equivalence classes for this equivalence relation.

Proof. This is a special case of the canonical decomposition theorem we discussed in class. Define $a \sim_p a'$ if and only if $p(a) = p(a')$. Since p is surjective $B = \mathrm{im}(p)$ and we showed in class that $A_{/\sim_p} \cong \mathrm{im}(p) = B$. Explicitly, $A_{/\sim_p}$ may be identified with the set of fibers for p, i.e.,

$$A_{/\sim_p} \cong \{p^{-1}(b) \subset A \mid b \in B\} \subset 2^A,$$

and there is always a bijection between the set of fibers of a function and the set of elements in its image. □

Dept. of Mathematics, Johns Hopkins Univ., 3400 N Charles St, Baltimore, MD 21218
Email address: eriehl@math.jhu.edu

[3] In fact, it i for any set A and any set I (possible empty and possibly infinite) it is also the case that the product $\prod_I A$ is isomorphic to the set of functions A^I. The proof is by the same argument, but requires somewhat more complicated notation. In fact there is a sense in which the product $\prod_I A$ of the indexed family of sets $(A)_{i\in I}$ is *defined* to be the set of functions A^I.

[4] So if you *do* care, let me know. I'll happily abide by your suggestion!