V63.0005.002, Spring 2002
Mathematical Thinking
Chris Wendl

Take-home quiz 4.5: Mappings and Inverses

This is a homework assignment to be handed in on Monday, March 4. It consists of two parts:

1. Do problems in the book on Page 584, #1, 3, 5, 35, 37, 41.

2. Read through the following notes and do Exercises 1–6 on a separate piece of paper.

For the problems in the book, you may find it helpful to read Section 7.2, but it might also be confusing since the book sometimes uses slightly different notation and/or terminology than we've used in class. Don't fret too much about the precise definitions, just so long as you get the general concepts.

Generality

In class we defined what it means to take the composition of two functions that map $\mathbb{R}$ to $\mathbb{R}$, and what it means for such a function to be invertible. In fact, these concepts can be defined in a more general context: given any set S, the composition of two functions $f : S \to S$ and $g : S \to S$ is a new function $f \circ g : S \to S$, defined by

$$(f \circ g)(x) = f(g(x)),$$

where we use the variable x to represent an arbitrary element of the domain S. This is really the same definition as before, only now we're allowing for the possibility that the domain S could be something other than a subset of the real numbers (e.g. it could be a set of ordered pairs, or as in the examples below, a set of letters). Similarly we say that f is *invertible* if there is another function called f^{-1} ("f inverse"), which also maps S to S, such that $(f^{-1} \circ f)(x) = x$ for all $x \in S$. As before, the inverse function f^{-1} can be thought of as a "machine" that reverses the action of the f-machine. Always remember: the -1 in f^{-1} is never to be understood as an exponent, it's merely part of the standard notation for inverse functions. If you prefer, think of it as a component in an alternative style of writing the letter f.

As with the simpler case, it turns out that a mapping is invertible if and only if it is *one-to-one*, which means each element y in the range of f has one and only one counterpart x in the domain which is mapped to it by f, i.e. given y, there's only one x such that $f(x) = y$. It then becomes clear how to define the inverse mapping: f^{-1} must reverse the process of f by mapping y back to x, so $f^{-1}(y) = x$. If there were more than one value of x that could make this work for a given value of y, then we'd have to say that $f^{-1}(y)$ has more than one value, in which case f^{-1} would not be a function.

Application

We discussed in class the following example which could in principle be used as a tool to encode messages. Let $S = \{\mathrm{A}, \mathrm{B}, \mathrm{C}, \cdots, \mathrm{Z}\}$, i.e. the set S contains 26 elements, which are precisely the capital letters of the alphabet (remember, these aren't meant as variables in this case, they're just letters as objects unto themselves). We defined the function $f : S \to S$ as follows:

$$f(x) = \begin{cases} x & \text{if } x \text{ is a consonant, including Y} \\ \mathrm{U} & \text{if } x = \mathrm{A} \text{ or E} \\ \mathrm{E} & \text{if } x = \mathrm{I} \\ \mathrm{A} & \text{if } x = \mathrm{O} \\ \mathrm{I} & \text{if } x = \mathrm{U} \end{cases}$$

Note that of all the letters in this definition, the only one honestly being used as a *variable* is the lowercase x; everything else is just a letter. It's customary to print variables in *italics*, so as to distinguish them from other letters that are meant more literally. We should also be clear on just how we're using this variable: unlike the usual situation in algebra, here we're not using x to represent some unknown number. In fact we're not talking about numbers at all—the relevant objects here are the letters from A to Z, so if we ever have to say that x "equals" something, we would say $x = \mathrm{A}$, or B or C, and so forth.

To get an intuitive feel for what this function really is, it's worthwhile to compute it in a few specific cases. So for example, if we plug in $x = \mathrm{C}$, the fact that C is a consonant tells us $f(\mathrm{C}) = \mathrm{C}$. Similarly $f(\mathrm{K}) = \mathrm{K}$ and $f(\mathrm{Q}) = \mathrm{Q}$. To find $f(\mathrm{A})$ we pay attention to the second line, where it says "if $x = \mathrm{A}$"; thus $f(\mathrm{A}) = \mathrm{U}$. Similarly $f(\mathrm{E}) = \mathrm{U}$, $f(\mathrm{I}) = \mathrm{E}$, $f(\mathrm{O}) = \mathrm{A}$ and $f(\mathrm{U}) = \mathrm{I}$.

Exercise 1. *The domain of f is the set S of all capital letters, but the range of this function contains only 25 letters. Which letter is* not *in the range of f?*

The idea of using this function to encode a message would be to take every letter in the message and replace it with a different letter as dictated by f, for instance

$$\begin{aligned} \mathrm{IODINE} &\mapsto f(\mathrm{I})f(\mathrm{O})f(\mathrm{D})f(\mathrm{I})f(\mathrm{N})f(\mathrm{E}) = \mathrm{EADENU} \\ \mathrm{MEET} &\mapsto f(\mathrm{M})f(\mathrm{E})f(\mathrm{E})f(\mathrm{T}) = \mathrm{MUUT} \\ \mathrm{MEAT} &\mapsto f(\mathrm{M})f(\mathrm{E})f(\mathrm{A})f(\mathrm{T}) = \mathrm{MUUT} \end{aligned}$$

With these last two examples we can see a significant problem: a code is only useful if it can be decoded, and this one cannot be. In particular, if someone sends you a message encoded by this method and the encoded version contains the word "MUUT", even if you know everything there is to know about the code, you have no way of telling (except maybe from context, which is not very reliable) whether this word is supposed to represent "MEET" or "MEAT". The problem lies in the fact that f maps both A and E to the same letter: *f is not one-to-one.* In order to decode the message, we need an inverse for the function f, but f is not invertible.

With relatively little effort however, we can change f to obtain a new function that *is* invertible:

$$g(x) = \begin{cases} x & \text{if } x \text{ is a consonant, including Y} \\ \mathrm{U} & \text{if } x = \mathrm{A} \\ \mathrm{O} & \text{if } x = \mathrm{E} \\ \mathrm{E} & \text{if } x = \mathrm{I} \\ \mathrm{A} & \text{if } x = \mathrm{O} \\ \mathrm{I} & \text{if } x = \mathrm{U} \end{cases}$$

Exercise 2. *Encode the word "IODINE" using this new function g.*

Now there's no ambiguity: if an encoded message contains the letter U, it could only mean that the unencoded letter is A, since $g(\mathrm{A}) = \mathrm{U}$ and no other letter is mapped to U. Equivalently, seeing that g is one-to-one and therefore has an inverse function (called g^{-1}), we can say $g^{-1}(\mathrm{U}) = \mathrm{A}$. Going through the same argument for all letters yields a definition of the inverse function:

$$g^{-1}(x) = \begin{cases} x & \text{if } x \text{ is a consonant, including Y} \\ \mathrm{A} & \text{if } x = \mathrm{U} \\ \mathrm{E} & \text{if } x = \mathrm{O} \\ \mathrm{I} & \text{if } x = \mathrm{E} \\ \mathrm{O} & \text{if } x = \mathrm{A} \\ \mathrm{U} & \text{if } x = \mathrm{I} \end{cases}$$

All we've done here is interchange the letters in each corresponding pair of vowels. The two formerly troublesome examples now present no problem:

$$\begin{aligned} \mathrm{MEET} &\mapsto g(\mathrm{M})g(\mathrm{E})g(\mathrm{E})g(\mathrm{T}) = \mathrm{MOOT} \\ \mathrm{MEAT} &\mapsto g(\mathrm{M})g(\mathrm{E})g(\mathrm{A})g(\mathrm{T}) = \mathrm{MOUT} \end{aligned}$$

Since g is one-to-one, it always encodes different words differently, and we can use the inverse function to decode them:

$$\text{MOOT} \mapsto g^{-1}(\text{M})g^{-1}(\text{O})g^{-1}(\text{O})g^{-1}(\text{T}) = \text{MEET}$$
$$\text{MOUT} \mapsto g^{-1}(\text{M})g^{-1}(\text{O})g^{-1}(\text{U})g^{-1}(\text{T}) = \text{MEAT}$$

Now that we have explicit definitions of the functions g and g^{-1}, it's easy to consider their composition function $g^{-1} \circ g : S \to S$. For instance,

$$(g^{-1} \circ g)(\text{A}) = g^{-1}(g(\text{A})) = g^{-1}(\text{U}) = \text{A}$$
$$(g^{-1} \circ g)(\text{C}) = g^{-1}(g(\text{C})) = g^{-1}(\text{C}) = \text{C}$$
$$(g^{-1} \circ g)(\text{I}) = g^{-1}(g(\text{I})) = g^{-1}(\text{E}) = \text{I}$$

Notice that in all of these cases, $(g^{-1} \circ g)(x) = x$. In fact, by the definition of what an inverse function is, this had better be true for *all* $x \in S$! Take a moment now to convince yourself that it is.

For the following exercises, consider the functions h and j defined as follows:

$$h(x) = \begin{cases} \text{the next consonant in the alphabet} & \text{if } x \text{ is a consonant other than Z (including Y)} \\ \text{B} & \text{if } x = \text{Z} \\ x & \text{if } x \text{ is A, E, I, O or U} \end{cases}$$

$$j(x) = \begin{cases} \text{Z} & \text{if } x = \text{A} \\ \text{A} & \text{if } x = \text{Z} \\ x & \text{if } x \text{ is not A or Z} \end{cases}$$

Exercise 3. *What is the inverse of j?*

Exercise 4. *Is h invertible?*

Exercise 5. *Consider the composite function $p = j \circ h$. Use it to encode the phrase "COLORLESS GREEN IDEAS".*

Exercise 6. *Assume a phrase has been encoded using the function $p = j \circ h$, and the result is "TMEEQ GUSIOUTMA". Decode this.*