Day 14: Friday, 3/3/2017

Collect hw from section 6.1. Answer any questions.

Continue with 6.2.

5. There are many applications for these number systems. In particular, we often are interested in functions of the form $f : \mathbb{Z}_n \to \mathbb{Z}_n$, or $f : \mathbb{Z}_n \to \mathbb{Z}_m$ with $m \neq n$, or $f : \mathbb{Z}_n \to \mathbb{Z}$, or $f : \mathbb{Z} \to \mathbb{Z}_n$. Here is one example: define $f : \mathbb{Z}_6 \to \mathbb{Z}_6$ by the equation $f(x) = x^2 + 3$. We can compute $f(x)$ for each x in $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ to complete the following table:

x	0	1	2	3	4	5
$f(x)$	3	4	1	0	1	4

Lecture Topic 3. More Examples and properties of Functions (As many as time permits)

1. Equality of two functions
   a. For equality we have to have $f : A \to B$ and $g : A \to B$, and $f(a) = g(a)$ for all a in A.
   b. That is, we do not consider two functions to be identical unless they have the same domain and codomain.
   c. In terms of the alternate definition of function, f and g will each be a subset of $A \times B$ and they are equal functions if they are equal as sets.

2. Linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^m$.
   a. Defined in terms of a constant $m \times n$ matrix A.
   b. The function is defined by $f(\mathbf{x}) = A\mathbf{x}$, where $\mathbf{x}$ is a column vector $[x_1 \;\; x_2 \;\; x_3 \;\cdots\; x_n]^T$ and the result on the right side of the equality is given by matrix multiplication.
   c. This function satisfies the linearity conditions: $f(\mathbf{x} + \mathbf{y}) = f(\mathbf{x}) + f(\mathbf{y})$ for all vectors $\mathbf{x}$ and $\mathbf{y}$; and $f(c\mathbf{x}) = c\, f(\mathbf{x})$ for all vectors $\mathbf{x}$ and all real scalars c.

3. The derivative as a function.
   a. Take the domain A to be the set of differentiable functions on the interval [0,1]
   b. Take the co-domain B to be the set of all real functions on [0,1]
   c. The mapping is depicted visually as $f \to f'$.
   d. If we represent this function by the letter D, then we can write $D : A \to B$ where, for every $f \in A$, $D(f) = f'$.
   e. A similar kind of mapping: Let A = {all functions from $\mathbb{R}$ to $\mathbb{R}$} and define a mapping $T : A \to A$ as follows. For any f in A, let $T(f) = g$ where $g(x)$ is defined to equal $f(x+1)$ for every real x. In this example, if you think of the function f as being identical to its graph in the xy plane, then T has a graphical interpretation: it shifts the graph one unit to the left.

4. Sequences as Functions: a sequence is a function with domain equal to $\mathbb{N}$ or some subset of $\mathbb{Z}$ of the form $\{n, n+1, n+2, \cdots\}$ where n is a fixed element of $\mathbb{Z}$. For example, we could take the domain to be $\{-3, -2, -1, 0, 1, \cdots\}$, and the sequence is then given by the terms $a_{-3}, a_{-2}, a_{-1}, a_0, \cdots$. This is simply using subscript notation a_n in place of the more recognizable function notation $a(n)$.

5. Functions of 2 or more variables
   a. Notation: if we think of the domain as being made up or ordered pairs (x, y), the literal extension of our function notation should be to write $f((x, y))$. But that is needlessly pedantic, so we make the notational convention of writing $f(x, y)$.

   b. Arithmetic operations are actually functions. For example, addition is the mapping $(x, y) \to x + y$.

   c. For functions from $\mathbb{R}^2$ to $\mathbb{R}$, the preimage of a point is often a curve. For example, consider the function $f(x, y) = x^2 - 3y$. We can compute $f(4,2) = 10$. So the image of the point (4,2) is the number 10. On the other hand, the preimage of the number 10 is the set of all the points that f takes to 10. Using the definition of f, we see that (x, y) is such a point if and only if $x^2 - 3y = 10$. This is algebraically equivalent to $y = (x^2 - 10)/3$, and every point on that curve is a preimage of 10.

New Topic: Section 6.3 Injections, Surjections, Bijections

1. Overview
   a. We have a general concept of function – but some functions have special properties such as continuity or differentiability in calc. We will look at special types of functions that can arise in a very general setting.
   b. The two types we care about are called injections and surjections. It is possible for a map to be be both, then it is a bijection.
   c. Injection is one to one – preimage of any y can have at most one x.
   d. Surjection is onto – the range = codmain

2. Injections
   a. Terminology: injection, injective function, one-to-one function are all synomyms
   b. Definition: a function $f : A \to B$ is called an injection if the following holds:
      $$(\forall x, y \in A)(f(x) = f(y) \to x = y)$$
      equivalently,
      $$(\forall x, y \in A)(x \neq y \to f(x) \neq f(y))$$
   c. Another way to say the same thing: for each y in the co-domain, there exists at most one x in the domain with $f(x) = y$.
   d. Another: Every b in B has at most one pre-image
   e. Another: Every b in $f(A)$ has exactly one element
   f. Another: $(\forall b \in f(A))(\exists! a \in A)(f(a) = b)$

g. Relate to horizontal line test for graph
h. To prove f is *not* an injection, exhibit two different a values with the same $f(a)$ values
i. Example: for $f : \mathbb{Z}_6 \to \mathbb{Z}_6$ defined by the equation $f(x) = x^2 + 3$, we know $f(1) = f(5)$, so f is not an injection.
j. To prove f *IS* and injection, use this outline: Assume p and q are elements of A and that $f(p) = f(q)$. Prove that $p = q$.
k. Example: Let A = {differentiable real functions with y intercept 1} and let B = {real functions}. Define the function $D : A \to B$ by the rule $D(f) = (f')$. Prove that D is an injection.

   Proof: Assume f and g are elements of A and that $D(f) = D(g)$. Because f and g are in A, observe that $f(0) = g(0) = 1$. Now by assumption, $f'(x) = g'(x)$ for all real x. That means $f'(x) - g'(x) = 0$ for all real x, and hence $(f - g)'(x) = 0$ for all real x. And we know from calculus that $f - g$ must therefore be a constant function. That is, for some real c, $f(x) - g(x) = c$ for all real x. In particular, when $x = 0$, we have $f(0) - g(0) = c$. On the other hand, we know from the observation above that $f(0) - g(0) = 0$. This shows that $c = 0$, showing that $f(x) - g(x) = 0$ for all real x. But that is the same as saying $f(x) = g(x)$ for all real x. In other words, f and g are equal functions. Thus we have shown that $D(f) = D(g)$ implies $f = g$, proving that D is an injection.

l. Example: using an assumption of injectivity to prove something about a function. Proposition: Let A be an $m \times n$ real matrix and define the function $f : \mathbb{R}^n \to \mathbb{R}^m$ defined by $f(\mathbf{x}) = A\mathbf{x}$. If f is an injection, then the image of an independent set of vectors is independent.

   Proof: We assume that A and f are as in the statement of the problem, and that f is an injection. Let $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \cdots, \mathbf{v}_p\}$ be a linearly independent set of vectors. We want to prove that $\{f(\mathbf{v}_1), f(\mathbf{v}_2), f(\mathbf{v}_3), \cdots, f(\mathbf{v}_p)\}$ is linearly independent. So suppose that some linear combination $c_1 f(\mathbf{v}_1) + c_2 f(\mathbf{v}_2) + c_3 f(\mathbf{v}_3) + \cdots + c_p f(\mathbf{v}_p) = 0$. By definition of f that means $c_1 A(\mathbf{v}_1) + c_2 A(\mathbf{v}_2) + c_3 A(\mathbf{v}_3) + \cdots + c_p A(\mathbf{v}_p) = 0$. Using algebraic properties of matrix and vector operations, we can rewrite the equation as $A(c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + c_3\mathbf{v}_3 + \cdots + c_p\mathbf{v}_p) = 0$. But we also know that $A\mathbf{0} = \mathbf{0}$. Thus, we have $f(c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + c_3\mathbf{v}_3 + \cdots + c_p\mathbf{v}_p) = f(\mathbf{0})$, and since f is an injection, $c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + c_3\mathbf{v}_3 + \cdots + c_p\mathbf{v}_p = \mathbf{0}$. Using this equation, and the fact that $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \cdots, \mathbf{v}_p\}$ is a linearly independent set, we conclude that all the coefficients $c_1, c_2, c_3, \ldots, c_p$ equal 0. Thus we see that a linear combination $c_1 f(\mathbf{v}_1) + c_2 f(\mathbf{v}_2) + c_3 f(\mathbf{v}_3) + \cdots + c_p f(\mathbf{v}_p)$ can only equal $\mathbf{0}$ if all the coefficents equal 0, and that is the definition of an independent set. That is, we have proven that the set $\{f(\mathbf{v}_1), f(\mathbf{v}_2), f(\mathbf{v}_3), \cdots, f(\mathbf{v}_p)\}$ is linearly independent.

   Comment: without the assumption of injectivity, it is not true that a linear transformation preserves independence of sets of vectors. So this is a special property of injections that does not hold in general.

3. Surjections
   a. Terminology: surjection, surjective function, onto function are all synomyms
   b. Definition: a function $f : A \rightarrow B$ is called a surjection if the following holds: every b in B equals $f(a)$ for some a in A
   c. Equivalently: $\begin{cases} \text{the range of } f \\ \text{the image of } A \\ f(A) \end{cases} = \begin{cases} \text{the codmain of } f \\ B \end{cases}$
   d. Logical restatement: $(\forall\, b \in B)(\exists\, a \in A)(f(a) = b)$
      equivalently, $(\forall\, b \in B)(f^{-1}(b) \neq \emptyset)$
   e. To prove that f is *not* a surjection, exhibit one element b of B that has no preimage in A.
   f. Example: $f : \mathbb{Z}_6 \rightarrow \mathbb{Z}_6$ defined by the equation $f(x) = x^2 + 3$ is not surjective because $f(a)$ never equals 5.
   g. To prove that f IS a surjection, follow this outline: Assume that b is an arbitrary element of B and demonstrate that there exists an a in A for which $f(a) = b$.
   h. Example: Let $f : [0,1] \rightarrow [0,1]\times[0,1]$ defined as follows: First, $f(1)$ is defined explicitly to be (1,1). Next. each x in [0,1) has a decimal expansion of the form $x = 0.d_1d_2d_3d_4 \cdots$ which does not end in an infinite string of 9's. (This condition is necessary so that each x has just *one* decimal expansion. For example 1/2 can be expressed as either 0.5 or as $0.49999\cdots$, but we exclude the one that ends in an infinite string of 9's.) Define $f(0.d_1d_2d_3d_4 \cdots) = (0.d_1d_3d_5d_7 \cdots, 0.d_2d_4d_6d_8 \cdots)$. For example, since $0 = 0.0000\cdots$, we see that $f(0) = (0,0)$. Similarly, $f(.192959393939393939\cdots)$ equals $(0.125333\cdots , 0.999999\cdots) = (0.125333\cdots , 1) \in [0,1]\times[0,1]$.
      Now claim that this function is a surjection. To prove this, we let (y,z) be an arbitrary element of $[0.1]\times[0.1]$ and show that $(y,z) = f(x)$ for some x in [0,1]. To do this, we consider four cases: (1) both y and z in [0,1); (2) y in [0,1) and $z = 1$; (3) z in [0,1) and $y = 1$; and (4) $y = z = 1$.

      In case 1, both y and z have decimal expansions so we can write $y = 0.y_1y_2y_3y_4 \cdots$ and $z = 0.z_1z_2z_3z_4 \cdots$ where neither expansion ends in an infinite string of 9's. In this case observe that $f(0.y_1z_1y_2z_2y_3z_3y_4z_4 \cdots) = (y,z)$

      In case 2, write $y = 0.y_1y_2y_3y_4 \cdots$ and observe that
      $f(0.y_19y_29y_39y_49 \cdots) = (y, 0.999\cdots) = (y,1) = (y,z)$.
      Moreover, note that $0.y_19y_29y_39y_49 \cdots$ does not end in an infinite string of 9's, because $y = 0.y_1y_2y_3y_4 \cdots$ does not end in an infinite string of 9's.

      In case 3, write $z = 0.z_1z_2z_3z_4 \cdots$ and observe that
      $f(0.9z_19z_29z_39z_4 \cdots) = (0.999\cdots , z) = (1,z) = (y,z)$.
      As in case 2, we also note that $0.9z_19z_29z_39z_4 \cdots$ does not end in an infinite string of 9's, because $z = 0.z_1z_2z_3z_4 \cdots$ does not end in an infinite string of 9's.

Finally, in case 4, we know by definition that $f(1) = (1,1) = (y,z)$.

Thus, in each case we have exhibited an x for which $f(x) = (y,z)$, showing that f is surjective.

Comment: This function can actually be proven to be continuous. So we have a continuous function from [0,1] onto the rectangle $[0,1]^2$. It is not one-one.

4. Book example: Linear transformation from $\mathbb{R}^2$ to $\mathbb{R}^2$. Example shows how to verify that this function is a bijection. Won't discuss this in detail today.

5. Injections and Surjections for finite domains
   a. If A has n elements, then at most n $f(a)$ values are possible
   b. If A is an injection, then the $f(a)$ values are all distinct so $f(A)$ will have exactly n values. In this case B must have n or more values, and f is a surjection iff B has exactly n values.
   c. Using similar reasoning, if f is a surjection and B has n elements then A has to have n or more elements, and f is an injection iff A has exactly n values.
   d. In fact, any two of the following statements implies the third:
      i. f is an injection
      ii. f is a surjection
      iii. A and B have the same number of elements
   e. A bijection is also called a one-to-one correspondence, and represents an exact pairing of the sets A and B. For finite sets finding a bijection is one way to see that two sets have the same number of elements
   f. Revisit proof that if A has n elements then the power set of A has 2^n elements. We argued by induction, and in the induction step we split the subsets of $\{x_1, x_2, x_2, \cdots, x_{n+1}\}$ into two types: those that include x_{n+1} and those that do not. The sets that do not involve x_{n+1} are simply the elements of the power set of $\{x_1, x_2, x_2, \cdots, x_n\}$ and by the induction hypothesis there are 2^n of those. We want to show that there are also 2^n sets of the other type , accounting for 2^{n+1} overall. For this purpose we define a mapping from the type 1 sets to the type 2 sets and show that this is a bijection. The mapping is simple to define: For every set S of the first type, we define $f(S) = S \cup \{x_{n+1}\}$. To complete the argument we have to show that this mapping is a bijection.

End of Day