Day 15: Tuesday, 3/7/2017
Return Homework. Collect 6.2 hw + 6.1 quiz problem + group exam solutions, taking questions first.

Continue Discussion of 6.3

1. Injections
   a. Terminology: injection, injective function, one-to-one function are all synonyms
   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 **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.

2. 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: $\left\{\begin{array}{c}\text{the range of } f \\ \text{the image of } A \\ f(A)\end{array}\right. = \left\{\begin{array}{c}\text{the codmain of } f \\ B\end{array}\right.$
   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.

3. 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.

4. 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.

Topic 2 (Time permitting) Composition of Functions

1. Definition of composition of Two Functions
   a. If $f : A \to B$ and $g : B \to C$ then we can define $g \circ f : A \to C$ by the equation
      $g \circ f(a) = g(f(a))$
   b. Note reversal of order
   c. Arrow diagram explanation
   d. Definition also makes sense if $g : f(A) \to C$, though our book does not include a definition of this.
2. Theorem 6.20. Let A, B, and C be nonempty sets and f and g functions with $f : A \to B$ and $g : B \to C$.
   a. Part 1: If f and g are both injections, so is $g \circ f : A \to C$.
   b. Part 2: If f and g are both surjections, so is $g \circ f : A \to C$.
   c. Part 3: If f and g are both bijections, so is $g \circ f : A \to C$.
   d. These are not iff statements. Example, if $A = B = C = \mathbb{R}$, $f(x) = x^2$, and $g(x) = x \sin x$, then $g \circ f$ is surjective but f is not. Similarly, if $A = \{1, 2, 3\}$, $B = \{101, 102\}$, and $C = \{0\}$, and f and g are both constant functions, with $f(a) = 101$ for all a and $g(b) = 0$ for all b. (Make an arrow diagram for this example). On the other hand, if $g \circ f$ is surjective then g must definitely be surjective. (Why?) Theorem 6.21 relates to these examples, and the idea that the statements in Theorem 6.20 are not iff statements.

3. Special example: Let n be a given natural number. Define $A = B = C = \{1, 2, 3, \cdots, n\}$. If f and g are any two bijections from A to A then so is their composition. Consider the set of all possible bijections from A to A. These are called permutations of A, and each permutation can be considered as a way to mixup or reorder the elements of A. The set of permutations is denoted S_n and has many interesting properties and applications. Note that the identity function defined by $id(x) = x$ for all x is an element of S_n, and that for any other permutation f, $id \circ f = f$ and $f \circ id = f$. Also, S_n is closed under the operation of composition. This operation is associative, but not commutative. It is also noteworthy that the number of elements in S_n is 2^n. All of these statements can be proved using methods we have discussed in this course. The last is provable by induction.

   End of Day