Day 19: Tuesday, 3/28/2017
Return homework; Take questions on 6.5; Collect 6.5 homework, quiz prob for 6.4.
Announce exam on April 7.

Next Section: 6.6

1. Overview: in homework you have already explored the idea of images and pre-images of sets under a function f. In section 6.6 this idea is covered more systematically

2. Notation and Defs
   a. Assume $f : A \to B$.
   b. For any subset C of A we define the image of C, written $f(C)$, as the set
      $f(C) = \{b \in B \mid b = f(c) \text{ for some } c \text{ in } C\} = \{f(c) \mid c \in C\}$.
   c. Alternate formulation: $b \in f(C)$ iff $(\exists\, c \in C)(b = f(c))$.
   d. Note: $f(\emptyset) = \emptyset$.
   e. Note: in this way we have f acting as a function from $\wp(A)$ to $\wp(B)$.
   f. For any subset D of B we define the preimage of D, written $f^{-1}(D)$, as the set
      $f^{-1}(D) = \{a \in A \mid f(a) \in D\}$.
   g. Note: $f^{-1}(\emptyset) = \emptyset$, and $f^{-1}(D)$ can be empty, even if D is not.
   h. Note: in this way we have f^{-1} acting as a function from $\wp(B)$ to $\wp(A)$.

3. Unions and Intersections
   a. Assume $f : S \to T$.
   b. If A and B are subsets of S we can compute unions and intersections, then apply f, or apply f and then take unions and intersections. That is, we can compute both $f(A \cup B)$ and $f(A) \cup f(B)$, and both $f(A \cap B)$ and $f(A) \cap f(B)$.
   c. Similarly, if C and D are subsets of T we can compute unions and intersections, then find the preimages under f, or find the preimages and then take unions and intersections. That is, we can compute both $f^{-1}(C \cup D)$ and $f^{-1}(C) \cup f^{-1}(D)$, and both $f^{-1}(C \cap D)$ and $f^{-1}(C) \cap f^{-1}(D)$.
   d. In three of the four cases the results in each case are the same. In the remaining case the results are the same provided f is an injection.
   e. Theorem: Let $f : S \to T$, let A and B be subsets of S, and let C and D be subsets of T . Then
      i. $f(A \cup B) = f(A) \cup f(B)$ (seen in exercise 6.3.x1)
      ii. $f(A \cap B) \subseteq f(A) \cap f(B)$ (seen in exercise 6.1.x4)
      iii. $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$ (proved in Thm 6.35(2) in text)
      iv. $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$ (seen in exercise 6.1.x5)
   f. Theorem: Let $f : S \to T$. Then $f(A \cap B) = f(A) \cap f(B)$ for all subsets A and B of S iff f is an injection.
      i. Proof: First, note the correct logical interpretation of the theorem:
         (f is an injection) $\leftrightarrow$ $((\forall\, A, B \subseteq S)(f(A \cap B) = f(A) \cap f(B)))$
      ii. We have seen $\to$ in exercise 6.3.x2

iii. We will prove the contrapositive of $\leftarrow$. That is, we will prove $\neg(f \text{ is an injection}) \rightarrow \neg((\forall A, B \subseteq S)(f(A \cap B) = f(A) \cap f(B)))$
iv. Restating in an equivalent form without using negation, we prove $(f \text{ is not an injection}) \rightarrow ((\exists A, B \subseteq S)(f(A \cap B) \neq f(A) \cap f(B)))$.
v. Argument: suppose that f is not an injection. Then there exist elements s_1 and s_2 in S such that $f(s_1) = f(s_2)$ but $s_1 \neq s_2$. Using these elements, define $A = \{s_1\}$ and $B = \{s_2\}$, and note that $A \cap B = \emptyset$ so $f(A \cap B) = \emptyset$. On the other hand, $f(s_1) \in f(A)$ and $f(s_2) \in f(B)$, so since $f(s_1) = f(s_2)$, it is a common element of both $f(A)$ and $f(B)$. Thus $f(A) \cap f(B) \neq \emptyset = f(A \cap B)$. In this way we have shown that there exist sets A and B for which $f(A \cap B) \neq f(A) \cap f(B)$. This completes the proof.

4. Theorem 6.36.
   a. Statement: Let $f : S \rightarrow T$, let A be a subset of S, and let C be a subset of T. Then
      i. $A \subseteq f^{-1}(f(A))$ and
      ii. $f(f^{-1}(C)) \subseteq C$.
   b. These were proven in the solutions to exercises 6.3.x3 and 6.3.x4, as well as the additional conclusions that
      i. $A = f^{-1}(f(A))$ if f is injective and
      ii. $f(f^{-1}(C)) = C$ if f is surjective.
   c. In each exercise solution, two things are proved. One of them is (i) or (ii) of Theorem 6.36, and the proof of that part makes no assumptions about injectivity or surjectivity. The other part of each exercise is (i) or (ii) of Theorem 6.36 with $\subseteq$ replaced by $\supseteq$. It is in proving these parts that the exercises assume injectivity for (i) and surjectivity in (ii).
   d. Let's look at examples to show that the extra injectivity or surjectivity assumptions in exercise 6.3.x3 and 6.3.x4 are necessary to replace the $\subseteq$'s in Theorem 6.36 with $=$'s.

5. Extra topic, time permitting: permutations
   a. Definition: a permutation of a set A is a bijection from A to A
   b. Special case: A is a finite set. Here a permutation can be thought of as a reordering.
   c. Many applications and interesting properties of these permutations in the finite case.
   d. The complete set of permutations from A to A is called the Symmetric Group on A and written S_A.
   e. This is an algebraic system where the operation is function composition. This operation is associative, but not commutative. Note that S_A is a closed system with respect to composition, so we can compose an number of elements of S_A in any order and the result will always remain within S_A . The identity function defined by $I_A(x) = x$ for all x in A is an element of S_n, and for any other permutation f, $id \circ f = f$ and $f \circ id = f$. Also, every element of S_n is invertible, and the inverse is also in S_n. closed under the operation of composition.

      It is noteworthy that if A has n elements, then S_A has 2^n elements. In particular, S_A is a finite set. It turns out to be interesting to study what happens when you repeatedly compose a permutation with itself. That is, when you consider f , $f \circ f$, $f \circ f \circ f$, $f \circ f \circ f \circ f$, etc. The fact that S_A is a finite set tells us that this chain of self compositions must eventually repeat, which in turn leads to the fact that if you compose f with itself enough times you have to eventually produce the identity function.

f. This is closely related to the sequences we studied earlier of the form x_0, $x_1 = f(x_0)$, $x_2 = f(x_1) = f(f(x_0))$, $x_3 = f(x_2) = f(f(f(x_0)))$, etc. This is called the orbit of x_0. Again, when f is a bijection of a finite set into itself, there are only finitely many possible values that can appear in the orbit of x_0, so at some point a repetition occurs. And since f is invertible, once we know that $x_k = x_j$ for some distinct k and j, we can apply f^{-1} to each term to find $f^{-1}(x_k) = f^{-1}(x_j)$ so $x_{k-1} = x_{j-1}$. Applying this idea repeatedly, we will eventually reach an equation of the form $x_p = x_0$ for some $p > 0$. Choosing the minimum such p, we see that the orbit of x_0 is periodic with period p. That is, the orbit of x_0 cycles endlessly through the distinct values $x_0, x_1, x_2, \ldots, x_{p-1}$. Moreover, if we find the period for every element of A, and then define p^* to be the least common multiple of all the individual periods, then applying f for p^* repetitions will restore every x to its original value. This shows that $f^{(p^*)}$ is the identity function, and that $f^{-1} = f^{(p^*-1)}$.

A consequence is this: the inverse of any permutation f can be expressed as some finite number of compositions of f with itself. Among the applications of this type of discussion are analyses of card shuffling (and other forms of randomization). For example, it tells us this: if you repeat any specific shuffling pattern enough times, a deck of cards will always be restored to its original order. (A 52 card deck will be restored to its original order after 8 perfect “out” riffle shuffles or 52 perfect “in” riffle shuffles.) Another aspect of permutations is explored in a forthcoming article (to appear any day now) about a plot to execute (or rescue) 100 knights held in a dungeon. The action takes place in a setting that parodies the game of thrones, and the story reveals some astonishing facts about permutations.

End of Day