Day 18: Friday, 3/24/2017
Comments on homework
Collect regular homework 6.4, quiz problem 6.3. Take questions.

New material: 6.5. Inverse Functions

1. Review: Concept of a function from A to B as a subset G of $A \times B$
   a. The function is a set G of ordered pairs
   b. Condition for such a set to be a function from A to B: for each a in A there exists a unique b in B such that (a, b) is in G
   c. Alternate version: Each a in A appears in exactly one ordered pair (a, b) in G
   d. We denote the unique b that is paired with a as $f(a)$.

2. Definition of the inverse of a function using ordered pair concept.
   a. Assume $f : A \to B$ and consider f to be a set ordered pairs
   b. There is a related set obtained by reordering each of the ordered pairs:
      $\{(b,a) \mid (a, b) \in f\} \subseteq B \times A$.
   c. This subset is called the inverse of f. and denoted by f^{-1} .
   d. It is a function from B to A iff f is a bijection. In that case we can call it the inverse *function*. But the inverse *set* is defined in any case.
   e. In fact, if R is *any* subset of $A \times B$, we can define the set $R^{-1} = \{(b,a) \mid (a, b) \in R\} \subseteq B \times A$. We will learn later that R is called a *relation* and R^{-1} is called the *inverse relation*.
   f. Example: Let $H = \{a, b, c, d\}$, $K = \{p, q, r\}$, and $f = \{(a, p), (b, q), \}(c, r), (d, q)\} \subseteq H \times K$. If f a function from H to K? (Yes.) Use the roster method to show the set f^{-1} . (Answer: $f^{-1} = \{(p, a), (q, b), \}(r, c), (q, d)\} \subseteq H \times K$.) Is f^{-1} a function from K to H? (No.)

3. Proof of 2d: For any function $f : A \to B$, f^{-1} is a function from B to A iff f is a bijection.
   Proof: To establish the truth of this biconditional we consider each implication separately. We first assume f^{-1} is a function from B to A and will show that f is a bijection from A to B. Note that f is assumed to be a function from A to B. We shall show this function is both surjective and injective. For the proof of surjectivity, let y be any element of B. Since f^{-1} is a function from B to A, it must contain an ordered pair (y, x) for some x in A. By definition of inverse, that means (x, y) is an element of f. But then we know that $f(x) = y$. Thus we have found an element of A that f takes to the given element y in B. Since y was arbitrary, this shows that f is a surjection.

   Turning next to injectivity, suppose that x_1 and x_2 are elements of A and that $f(x_1) = f(x_2)$. Denote this common element by y, and observe that $y \in B$, $f(x_1) = y$, and $f(x_2) = y$. Thus, thinking of f as a subset of $A \times B$, we see that (x_1, y) and (x_2, y) are both elements of f. Then, by definition of inverse, (y, x_1) and (y, x_2) are both elements of f^{-1}. However, in this part of the proof we have assumed that f^{-1} is a function, and therefore it can contain only *one* ordered pair with first entry y. Thus the pairs (y, x_1) and (y, x_2) must actually be equal, and that implies $x_1 = x_2$. Thus we have shown that $f(x_1) = f(x_2)$ implies $x_1 = x_2$, and that proves that f is an injection. Combining both parts above, we have shown that f is a bijection.

For the converse, we assume that f is a bijection (from A to B) and show that f^{-1} is a function from B to A. By definition, $f^{-1} = \{(b,a) \mid (a, b) \in f\}$, or in the more familiar function notation, $f^{-1} = \{(b,a) \mid b = f(a)\}$. To show that the domain of $f^{-1} = B$, it suffices to demonstrate that every element of B shows up as the first element of some ordered pair in f^{-1}. So, let y be any element of B. We are assuming that f is a surjection, so $y = f(x)$ for some x in A. Thus in the ordered pair (y, x) we have $y = f(x)$, and that shows that (y, x) is an element of f^{-1}. In particular we have shown that for at least one element of f^{-1} the first element of the ordered pair is y. This proves that the domain of $f^{-1} = B$.

Now we have shown that, for every b in B, there is an ordered pair (b, a) in f^{-1}. To prove that f^{-1} is indeed a function, we must show that there can only be one such ordered pair. We argue by contradiction. Suppose there are two different pairs, say (b, a_1) and (b, a_2), both included in f^{-1}. Since these pairs are different, we must have $a_1 \neq a_2$. By definition of f^{-1}, the pairs (a_1, b) and (a_2, b) are both elements of f, and that implies that $f(a_1) = b$ and $f(a_2) = b$. This implies that $a_1 = a_2$ because we also have assumed that f is injective. Thus we have arrived at a contradiction. This shows that there can only be one ordered pair (b, a) in f^{-1} for a given b in B, and proves that f^{-1} is a function.

If $f : A \to B$ is a bijection, so that its inverse is a function, we say that f is invertible. In this case it is common to use the usual function notation, so, for example if $f(3) = 8$ we can also write $f^{-1}(8) = 3$. Note that this is a different meaning to the notation $f^{-1}(\blacksquare)$ that we have already discussed. If $\blacksquare$ is a subset of the codomain, then $f^{-1}(\blacksquare)$ is the set of all the elements in the domain that map into $\blacksquare$. Using that notation, we can take $\blacksquare$ to be the one element set $\{8\}$, and $f^{-1}(\{8\})$ consists of all the elements of the domain that map to 8. But here we are assuming that f is a bijection, so there is only one preimage of 8. If that preimage is 3, then with the earlier notation, we would write $f^{-1}(\{8\}) = \{3\}$. In our new use of the notation, we have simply replace the one element sets $\{8\}$ and $\{3\}$ with their respective elements, 8 and 3. But this is only valid if f is a bijection. Summary: If f is a bijection, both $f^{-1}(\{8\}) = \{3\}$ and $f^{-1}(8) = 3$ are valid statements. If f is not a bijection, only the first of these is valid.

4. Theorem: Let A and B be nonempty sets and let $f : A \to B$ be a bijection. Then f^{-1} is a function from B to A, and both compositions $f^{-1} \circ f : A \to A$ and $f \circ f^{-1} : B \to B$ are defined. Infact, these are both *identity* functions (see page 298). That is, for any a in A and for any b in B,
   $f^{-1} \circ f(a) = a$ and $f \circ f^{-1}(b) = b$. (See proof in the text.)

   Special case: A and B are the same set. Then our bijection is $f : A \to A$, and the inverse is $f^{-1}: A \to A$, both of which map A into A. In this case, the compositions $f^{-1} \circ f$ and $f \circ f^{-1}$ are both equal to I_A, the identity map for A. This justifies writing $f^{-1} \circ f = f \circ f^{-1} = I_A$.

5. Theorem. Let $f : A \to B$ and $g : B \to C$ be bijections. Then the composition $g \circ f$ is a bijection, and its inverse is given by $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. (Proof in book).

6. 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. 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. 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