# Math 335, Homework 3

Due Wednesday, February 17

---

1. Let $A$, $B$, and $C$ be sets, and let $f : A \to B$ and $g : B \to C$ be functions.

   (a) Prove that if $f$ and $g$ are injective, then $g \circ f$ is injective.

   *Proof.* Assume $f \colon A \to B$ and $g \colon B \to C$ are injective functions. Then by definition, $\forall a_1, a_2 \in A$,
   $$f(a_1) = f(a_2) \implies a_1 = a_2,$$
   and $\forall b_1, b_2 \in B$,
   $$g(b_1) = g(b_2) \implies b_1 = b_2.$$
   To prove $g \circ f$ is injective, we must show that
   $$(g \circ f)(a_1) = (g \circ f)(a_2) \implies a_1 = a_2.$$
   Assume $g(f(a_1)) = g(f(a_2))$. Notice that by applying $f(a_1) = b_1$ and $f(a_2) = b_2$ to our injective function $g$, we can conclude that $b_1 = b_2 = f(a_1) = f(a_2)$. Since $f$ is also injective, $a_1 = a_2$. Hence $g \circ f$ is injective. $\square$

   (b) Prove that if $f$ and $g$ are surjective, then $g \circ f$ is surjective.

   *Proof.* Assume $f \colon A \to B$ and $g \colon B \to C$ are surjective functions. Then by definition, this means $\forall b \in B$ there exists $a \in A$ such that $f(a) = b$. Similarly, for every $c \in C$, there exists $f(a) = b \in B$ such that $g(b) = g(f(a)) = c$. Hence $g \circ f$ is surjective. $\square$

2. Prove that a function $f : A \to B$ is both injective and surjective if and only if it has an inverse function $f^{-1} : B \to A$.

   *Proof.* For the forward direction, assume $f \colon A \to B$ is bijective. Since $f$ is surjective, $\forall b \in B$, $\exists a \in A$ such that $f(a) = b$. Let $b \in B$ and define a function $f^{-1} \colon B \to A$ such that $f^{-1}(b) = a$. Since $f$ is injective, $f(a_1) = f(a_2) \implies a_1 = a_2$, so each $a \in A$ is unique as is each $b \in B$.

   Notice that $(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b$ and $(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a$, which means that $f^{-1}$ is the inverse of $f$.

   Conversely, assume that $f \colon A \to B$ has an inverse $f^{-1} \colon B \to A$. To prove that $f$ is surjective, we must show that $\forall b \in B$ there exists $a \in A$ such that $f(a) = b$. Let $b \in B$ and $f^{-1}(b) = a$. Then $f(a) = f(f^{-1}(b)) = b$.

   To prove that $f$ is injective, assume $a_1, a_2 \in A$ and $f(a_1) = f(a_2) = b$. We must show that $a_1 = a_2$. Suppose that $f^{-1}(b) = a$. Notice that
   $$\begin{aligned} a_1 &= (f^{-1} \circ f)(a_1) = f^{-1}(f(a_1)) \\ &= f^{-1}(b) = a. \end{aligned}$$

Also,

$$\begin{aligned} a_2 &= (f^{-1} \circ f)(a_2) = f^{-1}(f(a_2)) \\ &= f^{-1}(b) = a. \end{aligned}$$

Hence $a_1 = a = a_2$, which means that $f$ is injective. $\square$

3. Consider the following two elements of $S_8$, written in cycle notation:

$$f = (2, 3, 8, 4, 7)\ (5, 6)$$

$$g = (1, 2, 3, 4, 5)\ (6, 7, 8).$$

(a) Write $f$ in function notation. (That is, write $f(1) = \cdots$ , $f(2) = \cdots$, et cetera.)

Answer:

$f(1) = 1$ $f(3) = 8$ $f(5) = 6$ $f(7) = 2$
$f(2) = 3$ $f(4) = 7$ $f(6) = 5$ $f(8) = 4$

(b) Compute $f^{-1}$. Express your answer in cycle notation.

Answer:

$f^{-1} = (2, 7, 4, 8, 3)(5, 6)$
$f^{-1}(1) = 1$ $f^{-1}(3) = 2$ $f^{-1}(5) = 6$ $f^{-1}(7) = 4$
$f^{-1}(2) = 7$ $f^{-1}(4) = 8$ $f^{-1}(6) = 5$ $f^{-1}(8) = 3$

(c) Compute $f \circ g$. Express your answer in cycle notation, with each number only appearing once.

Answer:

$f \circ g = (1, 3, 7, 4, 6, 2, 8, 5)$

4. A *transposition* is defined as an element of $S_n$ that swaps two numbers but sends every other number to itself; for example, $(2, 5)$ is a transposition in $S_5$ that swaps 2 and 5.

(a) Express the element

$$f = (2, 4, 5)$$

of $S_5$ as a composition of two transpositions.

Answer:

$f \circ g$
$g = (2, 5)$
$f = (4, 5)$

(b) Express the element

$$g = (1, 2, 3, 4)$$

of $S_4$ as a composition of transpositions. (**Hint**: If you want to send 2 to 3, you can first swap 1 and 2 and then swap 1 and 3.)

Answer:

$f \circ g$

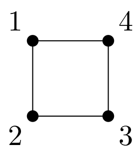
$g = (1, 3)$
$f = (1, 4)(2, 3)$
Also
$g = (1, 2)(3, 4)$
$f = (1, 3)$

In fact, it's a theorem that every element of $S_n$ can be expressed as a composition of transpositions. We won't cover this theorem in class, but you can find a proof in Gallian.

5. Explain in words how the group $D_4$ of symmetries of a square can be viewed as a subset of the symmetric group $S_4$. Are all elements of $S_4$ symmetries of a square?

   Answer:

   Let us consider the symmetries of a square from the diagram below:

   The group $D_4$ can be then described as follows:
   Counterclockwise rotation: $r = (1, 2, 3, 4)$
   Horizontal reflection: $h = (1, 2)(3, 4)$
   Vertical reflection: $v = (1, 4)(2, 3)$
   Diagonal reflection (along the 1 & 3 axis): $d = (2, 4)$
   Diagonal reflection (along the 2 & 4 axis): $d' = (1, 3)$

   Each of these operations on the symmetries of a square are a member of the symmetric group $S_4$. In addition, all symmetries of the square can be produced by a composition of these operations. Nevertheless, not all elements of $S_4$ are symmetries of a square. As a counterexample, $f = (1, 2)$ is not a member of the group $D_4$ as it will not produce a valid square.