SOLUTIONS FOR PROBLEM SET NUMBER 1

1. Let $f : B \to C, g : A \to B$ be maps such that the inverse maps $f^{-1} : C \to B, g^{-1} : B \to A$ exist. Prove that the map $f \circ g : A \to C$ is also invertible and show that $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

Solution. Often the easiest way to prove a function is invertible is to produce the inverse. Let $h = g^{-1} \circ f^{-1}$. Then

$$\begin{aligned}
(f \circ g) \circ h &= f \circ (g \circ h) \\
&= f \circ (g \circ (g^{-1} \circ f^{-1})) \\
&= f \circ ((g \circ g^{-1}) \circ f^{-1}) \\
&= f \circ (Id_B \circ f^{-1}) \\
&= f \circ f^{-1} \\
&= Id_C.
\end{aligned}$$

Similarly, we compute

$$\begin{aligned}
h \circ (f \circ g) &= (h \circ f) \circ g \\
&= ((g^{-1} \circ f^{-1}) \circ f) \circ g \\
&= (g^{-1} \circ (f^{-1} \circ f)) \circ g \\
&= (g^{-1} \circ Id_B) \circ g \\
&= g^{-1} \circ g \\
&= Id_A.
\end{aligned}$$

Thus (by the definition of the inverse), $f \circ g$ is invertible and $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

If $f : A \to B$ is a map we say that f has a right inverse if there exists $g : B \to A$ such that $f \circ g = Id_B$. We say that f has a left inverse if there exists a map $g : B \to A$ such that $g \circ f = Id_A$.

2. a) Show that a map $f : A \to B$ is is surjective iff f has a right inverse. Here iff := if and only if.

Solution. If $f : A \to B$ is surjective, then for all $y \in B$ we can choose an $x \in A$ such that $f(x) = y$; do this and label the corresponding choice x_y. Define $g : B \to A$ by $g(y) = x_y$. Then because of the way x_y was choosen we have $f \circ g(y) = f(g(y)) = f(x_y) = y$ for all y. So $f \circ g = Id_B$ and f has a right inverse.

Conversely, if f has a right inverse, say $g : B \to A$, and $y \in B$, then $g(y) \in A$. We have $f(g(y)) = f \circ g(y) = Id_B(y) = y$. So for every $y \in B$ there exists a member of A (namely $g(y)$) that is mapped by f to y. Thus, f is surjective.

b) Show that a map $f : A \to B$ is is injective iff f has a left inverse.

Solution. Assume $f : A \to B$ is injective. Define $g : B \to A$ by $g(f(x)) = x$ on $\{y \in B | \text{there exists } x \in A \text{such that} f(x) = y\}$ and the value of g choosen arbitrarily everywhere else in B. (Note that this arbitrariness is the reason that f doesn't necessarily have a unique left inverse.) For this definition to be valid, there must be a unique x mapped to $f(x)$ by x, which is the case here because f is assumed to be injective. We have $g \circ f(x) = g(f(x)) = x = Id_A(x)$ for all $x \in A$. Thus, $g \circ f = Id_A$ and g is a left inverse of f.

Assume $f : A \to B$ has a left inverse $g : B \to A$. If $f(x) = f(y)$, then $g(f(x)) = g(f(y))$, because g is a left inverse. We have $g(f(x)) = g \circ f(x) = Id_A(x) = x$ and also $g(f(y)) = g \circ f(y) = Id_A(y) = y$. So $x = g(f(x)) = g(f(y)) = y$, and this proves that f is injective (because we've shown that $f(x) = f(y)$ implies $x = y$ for any $x, y \in A$).

c) Let $f : A \to B$ be a map which has both a right inverse $g' : B \to A$ and a left inverse $g'' : B \to A$. Show that f bijective and $g' = g''$.

Solution. We know that $f : A \to B$ has a right inverse, and therefore, by part (a), f is surjective. Also, we know that f has a left inverse, and therefore, by part (b), f is injective. Thus, f is bijective. Using the notation given in the problem, we have $g' = Id_A \circ g' = (g'' \circ f) \circ g' = g'' \circ (f \circ g') = g'' \circ Id_A = g''$, as desired.

Let S_n be the group of permutations of the set $[1, ..., n]$. For any permutation $\sigma \in S_n$ we denote by $l(\sigma)$ the number of pairs $1 \leq i < j \leq n$ such that $\sigma(i) > \sigma(j)$.

3. Show that for any permutation $\sigma \in S_n$ and any elementary transposition $s_k, 1 \leq k \leq n$ we have either
$l(s_k \circ \sigma) = l(\sigma) + 1$ or
$l(s_k \circ \sigma) = l(\sigma) - 1$.

For any permutation $\sigma \in S_n$ we define
$\epsilon(\sigma) := (-1)^{l(\sigma)}$.

Solution. Let $A(\sigma) = (i, j)|i < j\text{and } \sigma(i) > \sigma(j)$. Then $l(\sigma)$ is defined to be the number of elements in $A(\sigma)$. Let $\sigma(i_k) = k$ and $\sigma(i_{k+1}) = k + 1$. Of course, s_k is as given in lecture (simply put, it switches k and $k + 1$ and leaves everything else alone). We have the following two cases.

Case 1: $i_k < i_{k+1}$. This is the same as $(i_k, i_{k+1}) \notin A$. We have $s_k(\sigma(i_k)) = s_k(k) = k+1$ and $s_k(\sigma(i_{k+1})) = s_k(k+1) = k$. Thus $(s_k(\sigma(i_k)), s_k(\sigma(i_{k+1}))) \in A(s_k \circ \sigma)$. Now look at $(i,j) \neq (i_k, i_{k+1})$. We claim that such (i,j) is in $A(\sigma)$ if and only if it is in $A(s_k \circ \sigma)$. In particular, if $i \neq i_k$ and $j \neq i_{k+1}$, then $(s_k \circ \sigma(i), s_k \circ \sigma(j)) = (\sigma(i), \sigma(j))$. If $i \neq i_k$ but $j = i_{k+1}$, then $(s_k \circ \sigma(i), s_k \circ \sigma(j)) = (\sigma(i), \sigma(j) - 1)$. Since $i \neq i_k$, $\sigma(i) < \sigma(j)$ iff $\sigma(j) - \sigma(i) \geq 2$ iff $\sigma(i) < \sigma(j) - 1$. The argument for $i = i_k$, $j \neq i_{k+1}$ is completely analogous. This shows that our claim is correct. Hence $A(s_k \circ \sigma) = A(\sigma) \cup (i_k, i_{k+1})$ (where $(i_k, i_{k+1}) \notin A(\sigma)$). So $A(s_k \circ \sigma)$ has one more element that $A(\sigma)$. Thus $l(s_k \circ \sigma) = l(\sigma) + 1$.

Case 2: $i_{k+1} < i_k$. This is the same as $(i_{k+1}, i_k \in A(\sigma)$. We have that $s_k \circ \sigma(i_{k+1}) = s_k(k+1) = k$ and $s_k \circ \sigma(i_k) = s_k(k) = k+1$, from which we see $(i_{k+1}, i_k) \notin A(s_k \circ \sigma)$. Now look at $(i,j) \neq (i_{k+1}, i_k)$. Again, we claim that such (i,j) is in $A(\sigma)$ if and only if it is in $A(s_k \circ \sigma)$. In particular, if $i \neq i_{k+1}$ and $j \neq i_k$, then $(s_k \circ \sigma(i), s_k \circ \sigma(j)) = (\sigma(i), \sigma(j))$. If $i \neq i_{k+1}$ but $j = i_k$, then $(s_k \circ \sigma(i), s_k \circ \sigma(j)) = (\sigma(i), \sigma(j) + 1)$. Since $i \neq i_{k+1}$, $\sigma(i) > \sigma(j)$ iff $\sigma(i) - \sigma(j) \geq 2$ iff $\sigma(i) > \sigma(j) + 1$. The argument for $i = i_{k+1}$, $j \neq i_k$ is completely analogous. This shows that our claim is correct. Hence $A(s_k \circ \sigma) = A(\sigma) - (i_{k+1}, i_k)$ (where $(i_{k+1}, i_k) \notin A(\sigma)$). So $A(s_k \circ \sigma)$ has one less element that $A(\sigma)$. Thus $l(s_k \circ \sigma) = l(\sigma) - 1$.

Since these cases are the only two possible, we conclude that either $l(s_k \circ \sigma) = l(\sigma) + 1$ or $l(s_k \circ \sigma) = l(\sigma) - 1$, proving the desired result.

4. Prove that for any permutations $\sigma', \sigma'' \in S_n$ we have
$\epsilon(\sigma) = \epsilon(\sigma')\epsilon(\sigma'')$ where
$\sigma := \sigma' \circ \sigma''$.

Solution. The proof will be by induction. Each $\sigma \in S_n$ can be decomposed into the composition of elementray transpositions (by the theorem proved in class). So it suffices to prove the statement for σ' equal to a composition of elementray transpositions. Let $\sigma' = s^n_{k_n} \circ s^{n-1}_{k_{n-1}} \circ \ldots \circ s^1_{k_1}$. We proceed by induction on n.

Case $n = 1$. We have $\epsilon(\sigma' \circ \sigma'') = \epsilon(s_k \circ \sigma'') = (-1)^{l(s_k \circ \sigma'')}$. By problem 3, $l(s_k \circ \sigma) = l(\sigma) + 1$ or $l(s_k \circ \sigma) = l(\sigma) - 1$. So either $\epsilon(\sigma' \circ \sigma'') = (-1)^{l(\sigma'')+1}$ or $\epsilon(\sigma' \circ \sigma'') = (-1)^{l(\sigma'')-1}$. In either case, we get $\epsilon(\sigma' \circ \sigma'') = (-1)(-1)^{l(\sigma'')}$. Since $\epsilon(s_k) = -1$, this gives $\epsilon(\sigma' \circ \sigma'') = \epsilon(s_k)\epsilon(\sigma'')$.

Case n implies $n+1$. Assume $\epsilon(s^n_{k_n} \circ s^{n-1}_{k_{n-1}} \circ \ldots \circ s^1_{k_1} \circ \sigma'') = \epsilon(s^n_{k_n} \circ s^{n-1}_{k_{n-1}} \circ \ldots \circ s^1_{k_1})\epsilon(\sigma'')$. We have $\epsilon(\sigma' \circ \sigma'') = \epsilon((s^{n+1}_{k_{n+1}} \circ s^n_{k_n} \circ \ldots \circ s^1_{k_1}) \circ \sigma'') = \epsilon(s^{n+1}_{k_{n+1}} \circ (s^n_{k_n} \circ \ldots \circ s^1_{k_1} \circ \sigma''))$. By the result of the case $n = 1$, we further have that this equals $\epsilon(s^{n+1}_{k_{n+1}})\epsilon(s^n_{k_n} \circ \ldots \circ s^1_{k_1} \circ \sigma'') = \epsilon(s^{n+1}_{k_{n+1}})\epsilon(s^n_{k_n} \circ \ldots \circ s^1_{k_1})\epsilon(\sigma'')$

by the inductive assumption. This in turn is (by the case $n = 1$) equal to $\epsilon(s^{n+1}_{k_{n+1}} \circ s^n_{k_n} \circ \ldots \circ s^1_{k_1})\epsilon(\sigma'') = \epsilon(\sigma')\epsilon(\sigma'')$. Combining all of these statements gives $\epsilon(\sigma' \circ \sigma'') = \epsilon(\sigma')\epsilon(\sigma'')$. This completes the proof by induction.