5)

a) Show any permutation σ can be written as the composition of transpositions.

Ask?

Let us induct over n, the number of elements in our set.

Base case: $n=1$, no switching of elements is possible in a list of 1, so σ is written as the composition of no transpositions. ✓

Inductive step: If σ is the product of transpos. for n elements, then σ is the product of transpos. for $n+1$ elements.

Take a list $1, 2, 3, \ldots, n, n+1$ where any order $a_1, a_2, \ldots, a_{n+1}$ can be created by transposing elements.

8/28

Our inductive step says we can swap $1, \ldots, n$ to get those elements in the proper order. We are left w/ $n+1$ out of place

$a_1, \ldots \hat{a}_{i_j} \ldots a_{n+1}, n+1$ where $\hat{n}_i$ represents where $n+1$ should go.

Now we swap $n+1$ with only then a_n, then a_{n-1}... until it gets to its proper position. The relative position of all other elements remains unchanged so we get

$a_1, a_2, \ldots, a_n, a_{n+1}$ exactly as we hoped only through the product of transpositions.

5 b) NTS: The parity of N is determined by σ, the sign of $(-1)^N$ is well defined.

We do this by defining a function $r(\sigma)$.
$r(\sigma)$ is the # of pairs of elements (i,j) where $i<j$, but $\sigma(i) > \sigma(j)$. We call these pairs inversions. This function r is dependent on our σ, not on how or σ was created.
Let σ be the product of m transpositions.
We will use induction on m to show that for any value of m, the parity of m and $r(\sigma)$ are equivalent.

Base case: Let $m=0$, σ is the identity and $r=0$
This means the parity of $r(\sigma)$ and m are trivially equivalent.

Induction step: We want to show
if $\frac{r(\sigma)-m}{2} \in \mathbb{Z}$, then $\frac{r(\tau\sigma)-(m+1)}{2} \in \mathbb{Z}$
for some transposition τ.

this is identical to showing
$r(\tau\sigma) - r(\sigma)$ is odd

why? if $\frac{r(\sigma) - r(\tau\sigma) + 1}{2} \in \mathbb{Z}$ and $\frac{r(\sigma) - m}{2} \in \mathbb{Z}$

we subtract:

$\frac{r(\tau\sigma) - m + 1}{2} \in \mathbb{Z}$, which is exactly what we sought to prove.

Now we show $r(\tau\sigma) - r(\sigma)$ is odd.

For a given swap i, j $\quad a_1 a_2 \ldots \overset{\frown}{i} \ldots j \ldots a_n$

we can ignore elements to the left of i and right of j. swapping i and j will not alter the # of inversions.

Next, if a_k is between i and j in our ordering but $a_k > i$ and $a_k > j$ or $a_k < i$ and $a_k < j$, swapping i and j does not change the number of inversions.

But if a_k lies between i and j in the ordering and in value, two inversions occur. If $i < j$, then the pairs (j, a_k) and (a_k, i) are both new inversions.

If $j < i$ then the number of inversions declines by 2 as (i, a_k) and (a_k, j) are no longer inversions.

Ultimately, we get 1 inversion of i and j and an even number of inversions for changed positions relative to our specific a_k's. ✓

The total change is odd
$r(T\sigma) - r(\sigma)$ is odd, so our inductive step is complete.

So, what is the logic behind this proof?
We know that each σ yields only one value for $r(\sigma)$ so, the parity of $r(\sigma)$ is a single determined value.

A σ may be created by different sets of transpositions, but if one set requires an even number and another an odd then for the same σ, $r(\sigma)$ is even and $r(\sigma)$ is odd. That would be a contradiction. So any σ can only be created by either an even or odd number of transpositions. That completes our proof. The parity of N is determined by σ ✓.

This stems from the equivalence of the parity of σ and the parity of m.

4

Well explained

Problem 5

(a) *Proof.* Let S_n be the set of all permutations of $\{1, \ldots, n\}$. Suppose an arbitrary permutation $\sigma \in S_n$. We then wish to show that σ is a composition of transpositions. Let's first show that some composition of transpositions $\tau_1, \ldots, \tau_m$ performed on σ makes σ the ordered set $\{1, \ldots, n\}$; that is, let's show that we can write $\{1, \ldots, n\}$ as

$$\{1, \ldots, n\} = \tau_1 \circ \cdots \circ \tau_m \circ \sigma.$$

This can be done by simply defining each transposition to switch an element out of its original position (in $\{1, \ldots, n\}$) into its original position. At each transposition, we are decreasing the number of elements out of their original position by at least 1 and possibly 2, since we are always switching an element into its original position, and the element that we swapped with could possibly also end up its original position. This holds as long as some element is out of its original position, since if we're not yet at the ordered set, then at least 2 elements must be out of position.

Transposing the same two elements twice does not change a permutation, since this just switches the two elements back and forth. That is, if we have a transposition τ, then $\tau \circ \tau$ does not alter the permutation. If we apply the reverse chain of transpositions in the above equation, we get

$$\tau_m \circ \cdots \circ \tau_1 \circ \{1, \ldots, n\} = \tau_m \circ \cdots \circ \tau_1 \circ \tau_1 \circ \cdots \circ \tau_m \circ \sigma.$$

Notice that we can take the $\tau_1 \circ \tau_1$ out, per the argument above. But this just leaves us with $\tau_2 \circ \tau_2$ in the middle, which can then be removed, and we can continue doing this until the right-hand-side just becomes σ. The above equation can therefore be written as

$$\sigma = \tau_m \circ \cdots \circ \tau_1 \circ \{1, \ldots, n\}.$$

Since we chose σ as an arbitrary permutation, this proves that every permutation is a composition of transpositions. ∎

(b) *Proof.* $\operatorname{sgn}(\sigma)$ is defined as $(-1)^N$, where N is the number of transpositions in the decomposition of σ. Notice that N is not well-defined. For example, the permutation $(2, 1)$ of the set $(1, 2)$ can be gained by swapping the two elements any odd number of times. We wish to show that $\operatorname{sgn}(\sigma)$ is well-defined. This is done by showing that the parity of N is well defined, such that $\operatorname{sgn}(\sigma) = 1$ for all even numbers and $\operatorname{sgn}(\sigma) = -1$ for all odd numbers.

In order to prove this, I will first show that the identity permutation, call it I, is an even permutation (i.e., N for I is even). I will prove this by induction. Per the theorem proved in (a), we can write I as a composition of transpositions:

$$I = \tau_1 \circ \cdots \circ \tau_n.$$

n cannot be 1, since just swapping two elements will not give the identity. For $n = 2$, just swap the same two elements twice. Let then the induction hypothesis be that the theorem holds for compositions of less than n transpositions. Let τ_{ij} denote the transposition swapping elements i and j. Obviously, $\tau_{ij} = \tau_{ji}$. Let then $\tau_n = \tau_{ab}$ for two arbitrary elements a and b. The composition $\tau_{n-1}\tau_n$ must then take one of four forms (depending on what τ_{n-1} swaps):

$$\begin{aligned}
\tau_{ab} \circ \tau_{ab} &= I, \\
\tau_{ac} \circ \tau_{ab} &= \tau_{ab} \circ \tau_{bc}, \\
\tau_{bc} \circ \tau_{ab} &= \tau_{ac} \circ \tau_{bc}, \\
\tau_{cd} \circ \tau_{ab} &= \tau_{ab} \circ \tau_{cd}.
\end{aligned}$$

In the first case, the expression for I can just be written as $I = \tau_1 \circ \cdots \circ \tau_{n-2}$. By the induction hypothesis, $n-2$ is even, and n is therefore also even in this case. In the three other cases, notice that we can write I such that the occurrence of a is in the second right-most transposition. For these cases, write I in this way and repeat the procedure. At each step, we either have the first case (and the induction hypothesis then proves the theorem), or a is moved another transposition to the left. The process must terminate with the first case at some point before a reaches the left-most transposition. If it does not, then we can write I such that a occurs only in the left-most transposition. But this is not the identity permutation, since this composition will switch a from its original position to some other position and then never swap it back. This proves that I is an even permutation.

To prove the theorem, suppose now that we can write a permutation σ as

$$\sigma = \tau_1 \circ \cdots \circ \tau_m \quad \text{and} \quad \sigma = \tau'_1 \circ \cdots \circ \tau'_n,$$

where m is even and n is odd. The inverse permutation σ^{-1} is just the opposite chain of transpositions (since this undoes every transposition), and we may write

$$\sigma^{-1} = \tau_m \circ \cdots \circ \tau_1.$$

Combining this with the definition of σ as an odd permutation, we have

$$I = \sigma\sigma^{-1} = \tau'_1 \circ \cdots \circ \tau'_n \circ \tau_m \circ \cdots \circ \tau_1.$$

Notice that this is an odd permutation. I is an even permutation, however, per the proof above, so this is a contradiction. A permutation that can be written as an even permutation therefore cannot be written as an odd permutation, and vice versa. The parity of N, and consequently $\operatorname{sgn}(\sigma) = (-1)^N$, is therefore well-defined. ■

Solution using cycle decomposition
(cf. Axler pp. 226-227)

(5). (a) Show that any permutation σ can be written as the composition of transpositions

Pf: Suppose $a_1, \dots, a_n$ are elements of a ~~permutation~~ cycle.

$$(a_1 a_2 \cdots a_n) = (a_1 a_n)(a_1 a_{n-1}) \cdots (a_1 a_2)$$

□

(b). I interpret "well-defined" to mean that the same permutation, although it can be written as a product of different permutations, always have the same sign.

Pf. Setup: suppose the permutation π is S_n can be written as the composite of r transpositions, and also as the composite of r' transpositions. WTS either r and r' are both even or both odd.

Let $\pi = \tau_r \tau_{r-1} \cdots \tau_2 \tau_1$, where τ_i $(1 \le i \le r)$ is a transposition. Since τ_1 has one 2-cycle and $n-2$ 1-cycles (1-cycle meaning not swapping an element with another) the count of the number of cycles is $C(\tau_1) = 1 + (n-2) = n-1$

where $\tau_2, \tau_3, \dots, \tau_r$ are combined in turn w/ τ_1 to get the final result π.
At each stage, # of cycles is altered by 1 (Please see proof on the next page)
Suppose it increases by 1 g times and decreases by 1 h times. Then the final # of cycles is $(n-1) + g - h = C(\pi)$ (*)

$r = g + h + 1$, which means $r = 1 + g + h = 1 + g + (n - 1 + g - C(\pi))$ after plugging in (*)

$r = n - C(\pi) + 2g$.

By the same argument, if π is the composite of r' transpositions, there's an integer g' s.t. $r' = n - C(\pi) + 2g'$. Hence $r - r' = 2(g - g')$

RHS is even, hence proved. ✓

To prove that each transposition alter the number of cycles by 1.

Suppose τ switches a and b. $\tau(a)=b$, $\tau(b)=a$, $\tau(k)=k$ for $k \neq a, b$

If a and b are in the same cycle of π, $\pi = (ax \cdots yb \cdots z)$ ... Some other cycles

$\tau\pi = (\overset{b}{\cancel{a}}x \cdots y)(\overset{a}{\cancel{b}} \cdots z)$ ... and the same other cycles.

In this case, the # of cycles increases by 1.

If a and b are not in the same cycle in π. $\pi = (ax \cdots y)(b \cdots z)$ ... and some other cycles

$\tau\pi = (\overset{b}{\cancel{a}}x \cdots y\overset{a}{\cancel{b}} \cdots z)$ ... and the same other cycles.

In this case the # of cycles decreases by 1

Hence applying a transposition always alter the # of cycles in π by 1

4

□

b Show that although the number N of transpositions in the decomposition of σ is not uniquely determined by the permutation, the parity of N is determined by σ so the sign $(-1)^N$ is well defined

Proof:

consider the polynomial in the variables $x_1, \dots x_n$ defined by

$$P = \prod_{1 \le i < j \le n} (x_i - x_j)$$

If the x_i are pairwise distinct then $P(x_1, \dots x_n) \neq 0$ from definition above. For every transposition τ we have that

$P(x_{\tau_1}, \dots x_{\tau_n}) = -P(x_1, \dots x_n)$

Therefore for every composition of transposition $\sigma = \tau_N \circ \dots \circ \tau_1$ we have

$$P(x_{\sigma_1}, \dots x_{\sigma_n}) = (-1)^N P(x_1, \dots x_n)$$

Therefore every permutation σ of list $(x_1, \dots x_n)$, the parity of the number N of transpositions in any decomposition of σ is invariant and only depends on σ i.e $\sigma = \tau_N \circ \dots \circ \tau_1$ hence the sign above is well defined

This is obvious for swapping 2 adjacent elements and not hard to prove in general