MATH 23B SOLUTION SET 1

1.a) This specific case was covered in class and of course follows directly from 1.b. (Note that we can write e as a product of zero simple reflections. Just like the sum of nothing is defined to be 0, the product of nothing is usually taken to mean 1.)

1.b) Proof 1 (by induction): Trivially any permutation in $\mathbf{S}_1$ can be written as a product of simple reflections. (Please note that this is far more elegant than using $\mathbf{S}_3$ as you base case.) We proceed by induction. Suppose every element in $\mathbf{S}_n$ can be written as a composition of simple reflections. Now take any $\sigma \in \mathbf{S}_{n+1}$. $\sigma \circ s_{\sigma^{-1}(n+1)} \circ s_{\sigma^{-1}(n+1)+1} \circ \ldots \circ s_n$ fixes $n + 1$. That is, if σ is

$$\begin{pmatrix} 1 & \ldots & k-1 & k & k+1 & \ldots & n+1 \\ \sigma(1) & \ldots & \sigma(k-1) & n+1 & \sigma(k+1) & \ldots & \sigma(n+1) \end{pmatrix},$$

then $\sigma \circ s_{\sigma^{-1}(n+1)} \circ s_{\sigma^{-1}(n+1)+1} \circ \ldots \circ s_n$ is

$$\begin{pmatrix} 1 & \ldots & k-1 & k & k+1 & \ldots & n & n+1 \\ \sigma(1) & \ldots & \sigma(k-1) & \sigma(k+1) & \sigma(k+2) & \ldots & \sigma(n+1) & n+1 \end{pmatrix}.$$

But since it fixes $n+1$, $\sigma \circ s_{\sigma^{-1}(n+1)} \circ s_{\sigma^{-1}(n+1)+1} \circ \ldots \circ s_n$ can be considered an element of $\mathbf{S}_n$ and hence is a composition of simple reflections, say $\sigma \circ s_{\sigma^{-1}(n+1)} \circ s_{\sigma^{-1}(n+1)+1} \circ \ldots \circ s_n = s_{i_1} \circ \ldots \circ s_{i_m}$. Now multiplying both sides by $s_n \ldots \circ s_{\sigma^{-1}(n+1)+1} \circ s_{\sigma^{-1}(n+1)}$ shows that, $\sigma = s_{i_1} \circ \ldots \circ s_{i_m} \circ s_n \circ s_{n-1} \circ \ldots \circ s_{\sigma^{-1}(n+1)}$. So by induction the statement is true for all n. $\square$

Proof 2 (by an algorithm): Consider an element $\sigma \in \mathbf{S}_n$. If $\sigma \circ s_{i_1} \circ \ldots \circ s_{i_m} = e$ then $\sigma = s_{i_m} \circ \ldots \circ s_{i_1}$. So it is clearly sufficient to show that $\sigma \circ s_{i_1} \circ \ldots \circ s_{i_m} = e$ for the appropriate simple reflections. That is we need to find a way of sorting the list $(\sigma(1)\ldots\sigma(n))$ only by switching consecutive elements of that list. Those of you with programming experience probably realize that this is precisely what a "bubble sort" does. In a bubble sort you go down through the list until you find consecutive numbers where the first is larger than the second and you switch those. Then you repeat this until the process ends.

FOR THIS TO CONSTITUTE A PROOF, HOWEVER, you must show that this algorithm does in fact terminate and that it terminates in a sorted list. These facts are not obvious. One proof uses the fact that this sorting algorithm always decreases the length (in fact by one, but this isn't important to us). Therefore, since any permutation has finite length, after finitely many steps we must get a permutation of length zero and e is the only such permutation, therefore the bubble sort terminates. $\square$

2.a) First notice that the question asks about $\ell(s_i \circ \sigma)$ not $\ell(\sigma \circ s_i)$. Many of you proved the latter, which although it is true is not the same question. Here's a quick sneaky way to show that the one implies the other. First notice that $\ell(\sigma^{-1}) = \ell(\sigma)$ for all σ (the proof of this fact will be left as an exercise to the reader). Now,

$(s_i \circ \sigma)^{-1} = \sigma^{-1} \circ s_i$. Therefore, $\ell(s_i \circ \sigma)) = \ell(s_i \circ \sigma))^{-1} = \ell(\sigma^{-1} \circ s_i)$. From that equality it is easy to show that proving either of these results implies the other.

Let
$$f_\sigma(j,k) = \left\{ \begin{array}{ll} 1 & \text{if } j < k \text{ and } \sigma(j) > \sigma(k), \\ 0 & \text{otherwise.} \end{array} \right. \quad .$$
Clearly, $\ell(\sigma) = \sum_{1 \le j,k \le n} f_\sigma(j,k)$. But, $f_{s_i \circ \sigma}(j,k) = f_\sigma$ unless $(j,k) = (\sigma^{-1}(i), \sigma^{-1}(i+1))$ in which case they have opposite values. This is because if an integer other than i or $i+1$ is bigger (smaller)than i or $i+1$ then it it is clearly also bigger (smaller) than the other. Therefore, summing, we see that $\ell(\sigma) = \ell(s_i \circ \sigma) \pm 1$ where we get a positive sign when $f_\sigma(i, i+1)$ is 1 and a minus sign when it is 0.

2.b) Let $sign(\sigma) = (-1)^{\ell(\sigma)}$. Therefore, $sign(e) = (-1)^0 = 1$ and $sign(s_i \circ \sigma) = (-1)^{\ell(s_i \circ \sigma)} = (-1)^{\ell(\sigma) \pm 1} = (-1)^{\ell(\sigma)}(-1)^{\pm 1} = -sign(\sigma)$.

2.c) Suppose that there were a map f which satisfied both of those properties. By 1.b) any $\sigma = s_{i_1} \circ ... \circ s_{i_m} \circ e$. Then, $f(\sigma) = f(s_{i_1} \circ ... \circ s_{i_m} \circ e) = (-1)^m$ because of the two properties we are assuming that f has. Therefore there can be at most one function f satisfying these properties (that is to say if we have two such functions g and h then $g(\sigma) = (-1)^m = h(\sigma)$). Since $sign$ has these two properties then there is exactly one function satisfying these properties and this unique function is the $sign$ function.

IMPORTANT NOTE: Uniqueness is not an intrinsic property. You can't say sign is unique, only that the sign function is the unique functions with certain properties. The sentence "sign is unique if and only if ℓ is unique" is completely meaningless. A lot of you thought that unique meant "well-defined". If you have some definition it isn't always clear that it actually gives you a function, you show that your definition is "well-defined." This is a completely different idea from unique. I think the reason many of you were confused is that you could state the property of being well-defined as this definition gives a unique answer. But saying sign is the unique function with certain properties means that any function with those properties must be the sign.

2.d) By 1.b) we know that $\sigma' = s_{i_1} \circ ... \circ s_{i_m} \circ e$ and $\sigma'' = s_{j_1} \circ ... \circ s_{j_k} \circ e$. Therefore, $\sigma = s_{i_1} \circ ... \circ s_{i_m} \circ s_{j_1} \circ ... \circ s_{j_k} \circ e$. Hence by 2.b) $sign(\sigma) = (-1)^{(m+k)} = (-1)^m(-1)^k = sign(\sigma')sign(\sigma'')$

3. Suppose $\sigma = s_{i_1} \circ ... \circ s_{i_m} \circ e$. By 2.a) multiplying by a simple reflection can increase the length of a permutation by at most one. Therefore, since the identity has length zero, it takes at least $\ell(\sigma)$ simple reflections. Now we need only show that we can write σ using only $\ell(\sigma)$ simple reflections. Now we need to show that this can in fact be done using only $\ell(\sigma)$ reflections. This is the same as saying that $s_{i_m} \circ ... \circ s_{i_1} \circ \sigma = e$. I claim that unless a permutation is the identity there is some s_k which decreases the length. But this is immediate from the fact that $<$ is transitive (that is $a < b$ and $b < c$ implies $a < c$) so that if every consecutive pair is in the correct order than the entire list is in the correct order. Hence we can decrease the length by one by multiplying by some simple reflection. Hence after $\ell(\sigma)$ of them we have e, the only permutation of length zero. Therefore $\ell(sigma)$ is the minimal number of simple reflections which can be multiplied together to equal σ.