Mathematics Department Stanford University
Math 61CM – Permutations

First, if S is any set, the set G of bijective (i.e. invertible) maps $f : S \to S$ forms a group under composition, as is easy to check; the group theoretic inverse is exactly the set theoretic one, while the identity is the identity map.

With this in mind, a permutation on n elements is a bijection $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$; such permutations form a group, often denoted by S_n (the symmetric group). A reasonable notation for a permutation σ is $(\sigma_1, \sigma_2, \dots, \sigma_n) = (\sigma(1), \sigma(2), \dots, \sigma(n))$ in analogy with the notation for points in $\mathbb{R}^n$ (which are after all maps $\{1, \dots, n\} \to \mathbb{R}$, i.e. somewhat analogous, with the very same domain).

In general, if G is a group, S a subset of G, the subgroup H generated by S is the set of elements of the form $g_1 \dots g_k$, $k \geq 0$ (with the empty product understood as the identity e) where for each j either $g_j \in S$ or $g_j^{-1} \in S$. It is straightforward to check that H is a subgroup of G (i.e. it is a group with the restricted operations).

Now, a special class of elements of S_n is that of transpositions. A transposition is a permutation that fixes all but exactly two elements $k, l \in \{1, \dots, n\}$; thus $\tau_{k,l}(j) = j$ if $j \neq k, l$, $\tau_{k,l}(k) = l$, $\tau_{k,l}(l) = k$ are the permutations as we run over integers $k, l \in \{1, \dots, n\}$, $k \neq l$. (Note that $\tau_{k,l} = \tau_{l,k}$.) Notice that $\tau_{k,l} \circ \tau_{k,l} = e$ (the identity permutation), i.e. a transposition is its own inverse.

Proposition 1 *Every permutation on n elements is a product of transpositions (possibly empty) of the n elements.*

Proof: We proceed by induction on n; this statement is certainly true if $n = 1, 2$. Now, suppose that $n \geq 3$ and the statement is true for all permutations on $n - 1$ elements. Let $\sigma \in S_n$.

There are two cases. Suppose first that $\sigma(n) = n$. Then $\sigma|_{\{1,\dots,n-1\}} \in S_{n-1}$ is a product of transpositions by the inductive hypothesis, and then σ is the product of the very same transpositions, regarded as permutations in S_n, fixing n.

Suppose next that $\sigma(n) \neq n$. As σ is a bijection, $n = \sigma(k)$ for some $k < n$. Now let $\rho \in S_n$ be defined by $\rho(j) = \sigma(j)$ if $j \neq n, k$, $\rho(k) = \sigma(n)$ and $\rho(n) = n$. Then $\rho \in S_n$ indeed, i.e. ρ is bijective, since for maps from a finite set to itself this is equivalent to surjectivity and if $j \neq n, \sigma(n)$, then $j = \sigma(l) = \rho(l)$ for some $l \neq k, n$ while if $j = n$ then $j = \sigma(k) = \rho(n)$, if $j = \sigma(n)$ then $j = \rho(k)$. Since $\rho(n) = n$, we are in the first case, and thus ρ is a product of transpositions. But now note that

$$\sigma = \tau_{\sigma(n),n} \circ \rho,$$

since the equality certainly holds when applied to $j \neq k, n$ while $\tau_{\sigma(n),n} \circ \rho(k) = \tau_{\sigma(n),n}(\sigma(n)) = n$, $\tau_{\sigma(n),n} \circ \rho(n) = \sigma(n)$ as desired. Correspondingly, we conclude that σ is a product of transpositions, proving the proposition. □

Note that a different way of writing σ in the proof above is $\rho \circ \tau_{k,n}$: the equality again holds when applied to $j \neq k, n$, and $\rho \circ \tau_{k,n}(k) = \rho(n) = n = \sigma(k)$, $\rho \circ \tau_{k,n}(n) = \rho(k) = \sigma(n)$. In this perspective we switch whatever maps into n under σ (namely, k) to the correct place, n, by applying the transposition $\tau_{k,n}$, and then leave it alone, while in that of the proof given above, doing a corresponding switch is the last step.

In general, a permutation can be written in many ways as a product of transpositions, e.g. $e = (1, 2)(1, 2)$. However, it turns out that the *parity*, i.e. evenness or oddness, of the number of transpositions is independent of the particular product used (it is even in the example). Namely:

Theorem 1 *Suppose $\sigma \in S_n$ is the product of transpositions $\tau^{(1)} \dots \tau^{(k)}$ as well as $\tilde{\tau}^{(1)} \dots \tilde{\tau}^{(l)}$. Then k and l have the same parity (either both even or both odd).*

It turns out that the argument is simplified if we use transpositions that exchange adjacent numbers, i.e. of the form $\tau_{k,k+1}$. In order to be able to do so, note that for $k < l$

$$\tau_{k,l} = \tau_{l-1,l}\tau_{l-2,l-1} \dots \tau_{k+1,k+2}\tau_{k,k+1}\tau_{k+1,k+2} \dots \tau_{l-2,l-1}\tau_{l-1,l}.$$

To see this, one proceeds inductively on $l-k$, noting that the equality is automatic if $l = k+1$ (namely it says $\tau_{k,k+1} = \tau_{k,k+1}$), and in general, if it is true when l replaced by $l-1$ and k the same, then the right hand side is

$$\tau_{l-1,l}\tau_{l-2,l-1}\cdots\tau_{k+1,k+2}\tau_{k,k+1}\tau_{k+1,k+2}\cdots\tau_{l-2,l-1}\tau_{l-1,l} = \tau_{l,l-1}\tau_{k,l-1}\tau_{l,l-1} = \tau_{k,l}$$

as one easily checks. Note that here both sides have an odd number of factors, consistent with the above theorem. Indeed, we have the following theorem:

Theorem 2 *Suppose $\sigma \in S_n$ is the product of adjacent transpositions $\tau^{(1)}\dots\tau^{(k)}$ as well as $\tilde{\tau}^{(1)}\dots\tilde{\tau}^{(l)}$. Then k and l have the same parity (either both even or both odd).*

This is a special case of the theorem above, Theorem 1, but indeed it proves it, since the transpositions in Theorem 1 can each be written as the product of an odd number of adjacent transpositions, and thus one sees that the parity of the number of factors is the same as the parity of the number of adjacent factors. Thus we are left with proving Theorem 2.

Proof of Theorem 2: Let $N(\sigma)$ denote the number of *inversions* in the permutation σ, i.e. the number of pairs $(k,l) \in \{1,\dots,n\}^2$ such that $k < l$ and $\sigma(k) > \sigma(l)$. Note that $N(\sigma)$ is certainly well-defined for each $\sigma \in S_n$. We show that if $\tau = \tau_{j,j+1}$ is an adjacent transposition then $N(\tau\sigma)$ and $N(\sigma)$ have opposite parities (one odd, the other even). That means that if σ is written as any product of adjacent transpositions, then $N(\sigma)$ has exactly the parity of that of the number of transpositions.

But with $\rho = \tau_{j,j+1}\sigma$, the number of inversions $N(\rho)$ for ρ differs from $N(\sigma)$ by ± 1. Indeed for a pair k,l with $k < l$, $\sigma(l) > \sigma(k)$ and $\rho(l) > \rho(k)$ can be different statements only if one of $\sigma(l), \sigma(k)$ is j and the other is $j+1$ (otherwise the inequalities are preserved: if neither is j or $j+1$ then the σ's are the same as the ρ's, if one is but the other is not, say $\sigma(l) = j$ or $j+1$ then $\sigma(k) = \rho(k)$, and regardless whether $\sigma(l) = j$ or $j+1$, hence $\rho(l) = j+1$ or j, the inequalities $\rho(k) < \rho(l)$ and $\sigma(k) < \sigma(l)$ are equivalent as $k \neq j, j+1$), in which case however $N(\sigma)$ and $N(\rho)$ differ by ± 1. Thus, $N(\rho)$ and $N(\sigma)$ have the opposite parity, which proves the theorem. $\square$

Recall that $\mathbb{Z}/2\mathbb{Z}$ is the integers modulo 2, i.e. can be indentified with a set $\{0,1\}$, with the usual addition. This gives us a map

$$\phi : S_n \to \mathbb{Z}/2\mathbb{Z}$$

with $\phi(\sigma) = 0$ is σ is even (the product of an even number of transpositions), $\phi(\sigma) = 1$ if σ is odd. (Note that we are also using that every permutation *is* a product of transpositions.) Furthermore,

$$\phi(\rho\sigma) = \phi(\rho) + \phi(\sigma)$$

as one sees by going through the various cases of parity for σ, ρ, and $\phi(e) = 0$, $\phi(\sigma^{-1}) = -\phi(\sigma)$. Thus, ϕ is a *group homomorphism* from S_n to the additive group $(\mathbb{Z}/2\mathbb{Z}, +)$. It is often more convenient to identify $(\mathbb{Z}/2\mathbb{Z}, +)$ with the multiplicative group $\{1,-1\}$, namely one identifies $j \in \{0,1\}$ with $(-1)^j \in \{-1,1\}$, then the group homomorphism property

$$\psi : S_n \to \{-1,1\}$$

is

$$\psi(\rho\sigma) = \psi(\rho)\psi(\sigma).$$

Then $\psi(\sigma)$ is called the *sign or index of the permutation* σ, written as $\mathrm{sgn}(\sigma)$.