Signature (sign, parity) of a permutation

The sign of a permutation plays an important role in many parts of mathematics. There are many different ways along which one may define the sign of a permutation, show that it is indeed well-defined and that it has the desired properties. (Most notably, it is a nontrivial group homomorphism from the symmetric groups $S_n$ to the multiplicative group $\{\pm 1\}$.) We give one very simple approach, followed by brief synopsis of various alternative proof strategies found in popular textbooks. Many of these require tools from other areas of math.

Definition. A permutation $\sigma \in S_n$ is called even if it can be written as a product of an even number of transpositions. A permutation $\sigma \in S_n$ is called odd if it can be written as a product of an odd number of transpositions. (We understand an empty product, representing the identity permutation, to be even.)

Proposition. Every permutation $\sigma \in S_n$ is either even or odd.

Corollary. The function sign: $S_n \mapsto \{-1, +1\}$ defined by $\text{sign}(\sigma) = +1$ if $\sigma$ is even and $\text{sign}(\sigma) = -1$ if $\sigma$ is odd is well-defined.

Theorem. For $n > 1$, the function sign: $(S_n, \circ) \mapsto \{-1, +1\}$ is a nontrivial group homomorphism.

The proposition follows readily from the following lemma and from the observation that: If $\sigma \in S_n$ and $\tau_1, \mu_1 \in S_n$ are transpositions such that $\sigma = \tau_1 \circ \ldots \circ \tau_1 = \mu_1 \circ \ldots \circ \mu_1$ then $\tau_1 = \tau_1 \circ \ldots \circ \tau_1 \circ \mu_1 \circ \mu_1$ (using that every transposition is its own inverse). The theorem follows readily upon noting that $\text{sign}(1 2) = -1$.

Lemma. For every $n \in \mathbb{Z}^+$ the identity permutation $i_n \in S_n$ is an even, but not an odd permutation.

Proof outline. For $n = 1$ there is nothing to prove. Now assume that $n > 1$ and for all $k < n$ the identity $i_k \in S_k$ is even and not odd. Suppose that $\tau_i = (a_i, b_i) \in S_n$ are transpositions such that $i_n = \tau_i \circ \ldots \circ \tau_i$ (and w.l.o.g. $a_i < b_i$). Strictly speaking we shall analyze and rewrite the sequence $(\tau_i, \ldots, \tau_i)$. If for all $i \leq s$, the transposition $\tau_i$ leaves $n$ fixed, i.e. $a_i, b_i \neq n$, then we may consider each side of the equation as an identity in $S_{n-1}$ and by induction hypothesis $s$ is even. If $i_0$ is the smallest $i$ such that $\tau_i$ moves $n$, i.e. $\tau_0 = (a_i, n)$ for some $a_i \in \{1, \ldots, n\}$, then rewrite the sequence by replacing $(\ldots \tau_{i_0+1}, \tau_{i_0})$ by $(\ldots \tau'_{i_0+1}, \tau'_{i_0}, \ldots)$ where

$$
(\tau'_{i_0+1}, \tau'_{i_0}) = \begin{cases}
(\tau_{i_0}, \tau_{i_0+1}) & \text{if } (\tau_{i_0}, \tau_{i_0+1}) \text{ are disjoint,} \\
((\ell, n), (j \ell)) & \text{if } (\tau_{i_0}, \tau_{i_0+1}) = ((j \ell), (n)) \text{ and } j \neq \ell, \\
((\ell n), (j l)) & \text{if } (\tau_{i_0}, \tau_{i_0+1}) = ((\ell n), (j l)) \text{ and } j \neq \ell, \\
((1 2), (1 2)) & \text{if } \tau_0 = \tau_{i_0+1} = (n, j) \text{.}
\end{cases}
$$

Here we write $(j \ell) = (\ell j)$ regardless of whether $j < \ell$ or $\ell < j$. The rewriting uses that $(j \ell) \circ (j n) = (j n \ell) = (j n) \circ (j \ell)$ and $(\ell n) \circ (j n) = (j \ell n) \circ (j n)$.

Note that the resulting sequence of transpositions is of the same form (and length) as before, but now either all transpositions leave $n$ fixed, or $i'_0$, the smallest $i$ such that $\tau'_i$ moves $n$ is one larger than $i_0$. We claim that by repeating this process we necessarily arrive at a rewritten sequence in which all transpositions leave $n$ fixed. This is because $i'_0$ cannot equal $s$ because in that case the product of transpositions would move $n$ contradicting the assumption that it equals the identity permutation. On the other hand, if some transposition in the rewritten sequence moves $n$, then necessarily $i'_0 \geq i_0 + 1$, but as we have argued above $i'_0$ is bounded by $i'_0 \leq s - 1$.

Some alternative ways to defining the sign of a permutation and verifying that it is well-defined.

- Every permutation can be factored in a unique way into an ordered product of disjoint cycles (e.g. when requiring that the sequence of the smallest members of each cycle is increasing). By considering a few different cases, it is easy to show that multiplying a permutation by a transposition changes the number of cycles in such representation by one. [e.g. Fraleigh]

- There exists a group isomorphism that maps every permutation $\sigma \in S_n$ in the symmetric group to an $n \times n$ permutation matrix $A_\sigma$. Define $\text{sign}(\sigma) = \det A_\sigma$. Of course, to avoid any circular reasoning, this requires that one has defined determinants and established their multiplicativity $\det(AB) = \det(A) \det(B)$ without reference to the signature of a permutation. [e.g. Fraleigh, Artin]

- Analyze the action of the symmetric group $S_n$ on the ring of polynomials $\mathbb{R}[X_1, \ldots, X_n]$ with coefficients in the ring $\mathbb{R} = \mathbb{Z}$ or, more naturally, $\mathbb{R} = \{-1, 0, 1\}$, defined by $(\sigma)p[X_1, \ldots, X_n] = p(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$. Now consider the special polynomial

$$
v[X_1, \ldots, X_n] = \prod_{1 \leq i < j \leq n} (X_j - X_i) \quad \text{ (the determinant of a Vandermonde matrix)}
$$

and define $\text{sign}(\sigma) = \pm 1$ depending on whether $\sigma v = v$. Be very careful when arguing why it is true that $(\text{sign}(\sigma \circ \tau)) v = (\text{sign}(\sigma) \cdot \text{sign}(\tau)) v$. [e.g. Herstein, Dummit-Foote]

- Analyze the action of the symmetric group $S_n$ on the set $\{1, 2, \ldots, n\}$ and define

$$
\text{sign}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{(\sigma(j) - \sigma(i))}{(j - i)}
$$

Again it is easy to see that the quotient, initially assumed to be in $\mathbb{Q}$, actually takes values in $\{-1, +1\}$. One again has to argue carefully why the so defined function is multiplicative. [e.g. Fischer-Sacher].