Permutations, $S_n$, and the sign of a permutation

Math 481/525, Fall 2009

Let $S_n$ be the set of all bijections (= permutations) of the set $S := \{1, \ldots, n\}$. This is a group under composition of functions; the identity is the identity function on $S$, and if $\sigma \in S_n$, then it is a 1-1 and onto function, and so it has an inverse function $\sigma^{-1}$, which is also a permutation of $S$. In this note we define the sign function on $S_n$, prove its main properties. This function is important in the theory of determinants. However, it is also important in other areas of mathematics. In fact, the proof below of the well-definition of the sign function actually arises in the study of discriminants of polynomials.

A key to define the sign function is the representation of elements of $S_n$ in terms of special permutations. A transposition is an element $\tau \in S_n$ such that there are distinct $i, j \in S$ such that $\tau(i) = j, \tau(j) = i$, and $\tau(k) = k$ for all $k \in S$ with $k \neq i, j$. We denote by $(ij)$ the permutation which maps $i$ to $j$ and vice-versa, and fixes all other $k \in S$.

**Lemma 1.** Let $\sigma \in S_n$. Then $\sigma$ is a product of transpositions.

**Proof.** Let $\sigma \in S_n$. We prove the result by induction on the number $r$ of elements of $S := \{1, \ldots, n\}$ moved by $\sigma$. If $r = 0$, then $\sigma$ is the identity, and is equal to the product $(12)(12)$ of two transpositions. Now, assume that $r > 1$ and that the result holds for permutations moving fewer than $r$ numbers. Let $k$ be the largest integer in $S$ moved by $\sigma$, and suppose that $\sigma(k) = l$. Let $\rho := (kl) \circ \sigma$. Then $\rho(k) = k$. Note that $\sigma(l) \neq l$ since $\sigma(k) = l$ and $\sigma$ is 1-1. The integers moved by $\rho$ are contained in the set of integers moved by $\sigma$ because $(kl)$ only moves $k, l$, which are moved by $\sigma$, so if $i$ is not moved by $\sigma$, then it is not moved by $\rho$. Furthermore, there are integers moved by $\sigma$ but not by $\rho$, notably $k$. So, by induction, $\tau$ is a product of transpositions. Since $\sigma = (kl) \circ \tau$, we conclude that $\sigma$ is also a product of transpositions.

**Theorem 2.** Let $\sigma \in S_n$. If $\sigma$ can be written as a product of $r$ and of $s$ transpositions, then $r \equiv s \pmod{2}$.

**Proof.** Let $h(x) = \prod_{i<j}(x_i - x_j)$, a polynomial in $n$ variables $x_1, \ldots, x_n$ with integer coefficients. Suppose that $\sigma \in S_n$ is a transposition, say $\sigma = (ij)$ with $i < j$. Then $\sigma$ affects only
those factors of \( h \) that involve \( i \) or \( j \). We break up these factors into four groups:

\[
x_i - x_j \\
x_k - x_i, \ x_k - x_j \quad \text{for} \quad k < i, \\
x_i - x_l, \ x_j - x_l \quad \text{for} \quad j < l, \\
x_i - x_m, \ x_m - x_j \quad \text{for} \quad i < m < j.
\]

For \( k < i \), the permutation \( \sigma = (ij) \) maps \( x_k - x_i \) to \( x_k - x_j \) and vice versa, and \( \sigma \) maps \( x_i - x_l \) to \( x_j - x_l \) and vice versa for \( j < l \). If \( i < m < j \), then

\[
\sigma(x_i - x_m) = x_j - x_m = -(x_m - x_j)
\]

and

\[
\sigma(x_m - x_j) = x_m - x_i = -(x_i - x_m).
\]

Finally,

\[
\sigma(x_i - x_j) = x_j - x_i = -(x_i - x_j).
\]

Multiplying all the terms together gives \( \sigma(h) = -h \). Thus, we see for an arbitrary \( \sigma \in S_n \) that \( \sigma(h) = h \) if and only if \( \sigma \) is a product of an even number of permutations, and \( \sigma(h) = -h \) if and only if \( \sigma \) is a product of an odd number of permutations. By substituting the roots \( \alpha_i \) of \( f \) for the \( x_i \), we obtain the desired conclusion.

\[\square\]

We call a permutation \( \sigma \) even if it is the product of an even number of transpositions, and odd otherwise. The theorem shows that this terminology is well-defined, in that no permutation can be both even and odd.

While this is not relevant to the study of the sign function, we mention the connection with discriminants. Let \( f(x) \in F[x] \) be a polynomial over a field \( F \), and suppose \( a_1, \ldots, a_n \) are the roots of \( f(x) \). The discriminant of \( f(x) \) is the element \( \left( \prod_{i<j} (a_i - a_j) \right)^2 \) of \( F \). For example, the discriminant of \( f(x) = x^2 + bx + c \) is \( b^2 - 4c \).

Recall that \( \{\pm 1\} \) is a group under multiplication.

**Proposition 3.** The function \( \text{sgn} : S_n \to \{\pm 1\} \) given by \( \text{sgn}(\sigma) = 1 \) if \( \sigma \) is even, and \(-1\) otherwise, is a group homomorphism.

**Proof.** Let \( \sigma \in S_n \). We note that if \( \sigma \) is a product of \( r \) transpositions, then \( \text{sgn}(\sigma) = (-1)^r \). Using this, suppose that \( \sigma = s_1 \cdots s_u \) and \( \tau = t_1 \cdots t_v \) with the \( s_i, t_j \) transpositions. Then \( \text{sgn}(\sigma) = (-1)^u \) and \( \text{sgn}(\tau) = (-1)^v \). Moreover, \( \sigma \tau = s_1 \cdots s_u t_1 \cdots t_v \) is a product of \( u + v \) transpositions. Therefore,

\[
\text{sgn}(\sigma \tau) = (-1)^{u+v} = (-1)^u (-1)^v = \text{sgn}(\sigma) \text{sgn}(\tau).
\]

\[\square\]