Queen Mary University of London

MTH 4104 Introduction to Algebra

Parity of permutations, and the alternating group — Spring 2019

0.1 Transpositions

A *transposition* is a permutation which swaps two elements i and j and fixes all the other elements of $\{1,\dots,n\}$. In disjoint cycle form, a transposition looks like (i,j).

Theorem 0.1. *Any permutation in S_n can be written as a product of transpositions. The number of transpositions occurring in a product equal to a given element f is not always the same, but always has the same parity (even or odd) depending on g.*

Proof. We begin by observing that

$$(1,2,\dots,n) = (1,n)(1,n-1)\cdots(1,3)(1,2).$$

For, in the composition on the right hand side,

- 1 is mapped to 2 by the last factor, and remains there afterwards, as we proceed left along the composition;
- 2 is mapped to 1 by the last factor, then to 3 by the second-to-last, then stays there;
- ...
- $n-1$ is fixed by all factors until the second; it is mapped to 1 by the second factor and then to n by the first;
- n is fixed by all factors except the first, which takes it to 1.

So the two permutations are equal.

Now in exactly the same way, an arbitrary cycle $(a_1,a_2,\dots,a_k)$ can be written as a product of transpositions:

$$(a_1,a_2,\dots,a_k) = (a_1,a_k)\cdots(a_1,a_3)(a_1,a_2).$$

Finally, given an arbitrary permutation, write it in disjoint cycle form, and then write each cycle as a product of transpositions.

The statement about parity is harder to prove, and I have postponed it until the next section (Section 0.2). □

Our standard example can be written

$$f = (1,4,8,6,5)(2,7) = (1,5)(1,6)(1,8)(1,4)(2,7).$$

We call a permutation *even* or *odd* according as it is a product of an even or odd number of transpositions; we call this the *parity* of f. Notice that a cycle of length k is a product of $k-1$ transpositions. So, if the lengths of the cycles of f are $k_1,\ldots,k_r$ (including fixed points), then f is the product of

$$(k_1 - 1) + (k_2 - 1) + \cdots + (k_r - 1) = n - r$$

transpositions (since the cycle lengths add up to n). In other words, if we define $c(f)$ to be the number of cycles in the cycle decomposition of f, then the parity of f is the same as the parity of $n - c(f)$.

Theorem 0.2. *Suppose that $n \geq 2$. Then the set of even permutations in S_n is a subgroup of S_n having order $n!/2$ and index 2.*

Proof. Let A_n be the set of even permutations in S_n. If $f_1, f_2 \in A_n$, then f_2^{-1} has the same cycle lengths as f_2 (since we just reverse all the cycles), so it is also in A_n. Thus, f_1 and f_2^{-1} are each products of an even number of transpositions; and then so, obviously, is $f_1 \circ f_2^{-1}$. By the Subgroup Test, A_n is a subgroup.

Let $\sim$ be the equivalence relation defined by this subgroup; that is, $f_1 \sim f_2$ if and only if $f_1 \circ f_2^{-1} \in A_n$. By considering each of f_1 and f_2 as products of transpositions, we see that $f_1 \sim f_2$ if and only if f_1 and f_2 have the same parity. So there are just two cosets of A_n.

By Lagrange's Theorem,

$$|A_n| = |S_n|/2 = n!/2.$$

□

The subgroup A_n consisting of even permutations is called the *alternating group* of degree n.

Example For $n = 3$, we have $|S_3| = 3! = 6$, so $|A_3| = 3$. The three even permutations are e, $(1,2,3)$ and $(1,3,2)$; the remaining three permutations are the transpositions $(1,2)$, $(1,3)$ and $(2,3)$ form the other coset of A_3 in S_3.

Remark. The formula for a 3×3 determinant can be expressed as follows. For each permutation $f \in S_3$, we do the following. Pick the elements in row i and column if of the matrix, and multiply them together. That is, choose one term from each row and column in all possible ways. Now multiply the product by $+1$ if f is an even permutation, and by -1 if f is an odd permutation. Finally, add up these terms for all the permutations.

For example, if

$$A = \begin{pmatrix} a & b & c \\ l & m & n \\ p & q & r \end{pmatrix},$$

the terms are as follows:

Permutation	Product	Sign
e	amr	$+$
$(1,2,3)$	bnp	$+$
$(1,3,2)$	clq	$+$
$(1,2)$	blr	$-$
$(1,3)$	cmp	$-$
$(2,3)$	anq	$-$

So $\det(A) = amr + bnp + clq - blr - cmp - anq$.

Now exactly the same procedure defines the determinant of an $n\times n$ matrix, for any positive integer n. The drawback is that the number of terms needed for an $n\times n$ determinant is $n!$, a rapidly growing function; so the work required becomes unreasonable very quickly. This is not a practical way to compute determinants; but it is as good a definition as any!

0.2 A permutation is either even or odd

In this appendix, we prove that the parity (even or odd) of a permutation does not depend on the way we write it as a product of transpositions. We will give two entirely different proofs.

First proof

For this proof, we see what happens when we compose a permutation with a transposition. We find that the number of cycles changes by 1, though it may increase or decrease. There are two cases, depending on whether the two points transposed lie in different cycles or the same cycle of the permutation. So let f be a permutation and t a transposition, and examine $t \circ f$.

Case 1: Transposing two points in different cycles. We may suppose that f contains two cycles $(a_1, \ldots, a_k)$ and $(b_1, \ldots, b_l)$, and that $t = (a_1, b_1)$ (this is because we can start each of the cycles at any point). Cycles of f not containing points moved by t will be unaffected. Now we find

$$t \circ f : a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto b_1 \mapsto b_2 \mapsto \cdots \mapsto b_l \mapsto a_1,$$

so the two cycles of f are "stitched together" into a single cycle in $t \circ f$, and the number of cycles decreases by 1.

Case 2: Transposing two points in the same cycle. This time let $(a_1, \ldots, a_m, \ldots, a_k)$ be a cycle of f, and assume that $t = (a_1, a_m)$, where $1 < m \leq k$. This time

$$\begin{array}{rl} t \circ f : & a_1 \mapsto a_2 \mapsto \cdots \mapsto a_{m-1} \mapsto a_1 \\ & a_m \mapsto a_{m+1} \mapsto \cdots \mapsto a_k \mapsto a_m \end{array}$$

so the single cycle of f is "cut apart" into two cycles, and the total number of cycles increases by 1.

Now any permutation f can be written as

$$f = t_1 \circ t_2 \circ \cdots \circ t_s,$$

where $t_1, \ldots, t_s$ are transpositions. Let f_i be the product of the last i of the transpositions, and consider the quantity $n - c(f_i)$, where $c(f)$ denotes the number of cycles of f (including fixed points). We start with $f_0 = e$, having n fixed points, so $n - c(f_0) = 0$. Now, at each step, we compose with a transposition, so we change $c(f_i)$ by one, and hence change $n - c(f_i)$ by one. So the final value $n - c(f)$ is even or odd depending on whether the number s of transpositions is even or odd. But $n - c(f)$ is defined just by the cycle decomposition of f, independent of how we express it as a product of transpositions. So in any such expression, the parity of the number of transpositions will be the same.

Second proof

Let $x_1, \ldots, x_n$ be n indeterminates, and consider the function

$$F(x_1, \ldots, x_n) = \prod_{i<j} (x_j - x_i).$$

For example, for $n = 3$, we have

$$F(x_1,x_2,x_3) = (x_2 - x_1)(x_3 - x_1)(x_3 - x_2).$$

Given a permutation f, we define a new function F^f of the same indeterminates by applying the permutation f to their indices:

$$F^f(x_1,\dots,x_n) = \prod_{i<j}(x_{f(j)} - x_{f(i)}).$$

For example, if $n = 3$ and $f = (2,3)$, then

$$F^{(2,3)}(x_1,x_2,x_3) = (x_3 - x_1)(x_2 - x_1)(x_2 - x_3) = -F(x_1,x_2,x_3).$$

The result of applying f_2 and then f_1 to F is just the result of applying $f_1 \circ f_2$ to F, as you may check. We show that, for any transposition t, we have

$$F^t(x_1,\dots,x_n) = -F(x_1,\dots,x_n).$$

It will follow that, if f is expressed as the product of s transpositions, then

$$F^f(x_1,\dots,x_n) = (-1)^s F(x_1,\dots,x_n).$$

Since the value of F^f does not depend on which expression as a product of transpositions we use, we see that $(-1)^s$ must be the same for all such expressions for f, and hence the number of transpositions in the product must always have the same parity, as required.

To prove our claim, take the transposition $t = (k,l)$, where $k < l$, and see what it does to F. We look at the bracketed terms $(x_j - x_i)$ and see what happens to them. There are several cases.

- If $\{k,l\} \cap \{i,j\} = \emptyset$, then the term is unaffected by the permutation t.
- If $i < k$, then the terms $(x_k - x_i)$ and $(x_l - x_i)$ are interchanged, and there is no effect on F.
- If $k < i < l$, then the term $(x_i - x_k)$ goes to $(x_i - x_l) = -(x_l - x_i)$, and the term $(x_l - x_i)$ goes to $(x_k - x_i) = -(x_i - x_k)$; the two sign changes cancel out.
- If $i > l$, then the terms $(x_i - x_k)$ and $(x_i - x_l)$ are interchanged, and there is no effect on F.
- Finally, the term $(x_j - x_i)$ is mapped to $(x_i - x_j) = -(x_j - x_i)$.

So the overall effect of t is to introduce one minus sign, and we conclude that $F^t = -F$, as required.