# 642:550, Summer 2004, Supplement 2

# The sign of a permutation

# Summer 2004

## 1. Introduction

Proofs will not play a large role in this course. However, any calculation (and, even more so, any program that will perform a calculation on data to be supplied later) is a proof that a certain question is answered by the result (barring computational slips) of the calculation. When your habits for doing mathematical work were formed in elementary mathematics, there was usually one accepted algorithm, and the use of that algorithm was taken as evidence that the student has understood the question. This is no longer the case in advanced mathematics. There may be several valid approaches; and in applied mathematics, the relevance of the calculation to the problem is the main issue. The student is then expected to include a justification of the method used and to include a clear statement that a certain quantity is what was sought. A verification (i.e., a proof) that the result satisfies the required conditions always improves the presentation.

There are usually pressures to be brief on those presenting mathematics in a textbook or a lecture. Since the assumption is that the writer or lecturer knows the subject, this means that one usually sees only outlines of proofs that call attention to a few main points while leaving details to the reader. On the other hand, the student is required to demonstrated that he hasn't missed anything, so that high grades are reserved for those who can produce complete proofs without ever having seen one. To illustrate what is involved, I will fill in the details of a proof sketched in lecture.

## 2. Statement of the problem.

The key step in showing the existence of a function satisfying the desired properties of a determinant is to show that the requirement that interchange of distinct rows **always** changes the sign of the determinant does not contradict that the requirement that the identity matrix have determinant $+1$.

### 2.1 Permutations

Stripping away from the notation all that is not essential, we denote the operation that interchanges row $i$ and row $j$ by $(i\ j)$ (using a slight space to separate the two symbols). We insist that the permutation actually do something, i.e., that $i \neq j$. Performing several such operations will be indicated by writing them in a row with the convention (opposite to the usual convention for composition of functions, but convenient in this case since it marks the progress of symbols through the permutation as the line is normally read) that the operations are to be performed from left to right. For example, consider

$$(1\,4)(1\,2)(2\,3)(3\,4)(2\,3)(1\,2). \tag{$*$}$$

The permutation represented by this expression is easily seen to be the identity. For example, if you start with 1, the first term takes it to 4, the next two terms do not affect 4, but the fourth term takes 4 to 3, the fifth takes 3 to 2 and the last term takes 2 back to 1. The effect on 2, 3 and 4 can be found in the same manner. The expression $(*)$ is an example of a general process for expressing a general interchange as a succession of interchanges of adjacent elements. Indeed, it extends to a process (known as the **bubble sort**) for expressing an arbitrary permutation as a succession of interchanges of adjacent pairs (see Donald E. Knuth, *The Art of Computer Programming, Volume 3: Searching and Sorting*, Addison-Wesley, 1973, section 5.2.2, p. 106, for a description of the process and its basic properties). The fact that all of the $n!$ permutations of $\{1, \ldots, n\}$ can be written as products of transpositions shows that the determinant of a permutation matrix can be found using only row interchanges to relate the matrix to the identity. There was no attempt to restrict to interchanges of adjacent rows. There may be some interest in showing that a smaller number of conditions suffice to characterize the determinant, but a proof of a stronger result would be more difficult.

### 2.2 The statement

An operation interchanging a pair of numbers (or whatever symbols you are using as labels) is called a **transposition**. What we need is

**Parity Proposition.** *If a product of transpositions represents the identity permutation, then it has an even number of transpositions.*

For example, $(*)$ contains $6 = 2 \cdot 3$ transpositions.

## 3. The main organization of the proof

This proof is an attempt to simplify the one in Charles C. Pinter, *A book of Abstract Algebra*, McGraw-Hill, 1982. Use the set of integers between 1 and $K$, for $K \geq 1$, to name the quantities being permuted. The proof is essentially an induction on $K$, although we use the **well-ordering** version of induction in which the object being considered is replaced by an equivalent one that has a smaller value of the induction parameter. A **basis** is provided to describe the case where the parameter takes its smallest value.

### 3.1 Basis of the induction

The basis will be $K = 1$. In this case, there is no way to form any transpositions, so the only expression that is allowed is an empty product which represent the identity. The number of terms is zero — an even number.

### 3.2 The induction step

The induction step consists of showing that a product of transpositions involving the numbers between 1 and $K$ that represents the identity determines another such product of transpositions representing the identity for which: (1) the number $K$ does not actually appear; and (2) the difference between the number of terms in the two expressions is even.

Now, the induction step on $K$ is trivially satisfied if $K$ does not appear in the expression being considered. The main role of the induction on $K$ will be to allow us to stop the operation about to be described by employing the inductive hypothesis on $K$.

## 4. Rewriting a product

We are trying to reduce to a case in which $K$ does not appear. Repeating a permutation simply restores the order before the first permutation was applied, so the **two** permutations can be removed **without changing the product** and **without changing whether the number of terms is even or odd**. However, this **only** applies when these equal permutations are **adjacent**. For example, if the two $(1\,2)$ terms were dropped from $(*)$, the resulting permutation would take 1 to 2, 2 to 4, and 4 to 1, leaving 3 fixed. **It is no longer the identity permutation**. To allow terms to cancel, we need to find a way **change the individual permutations without changing their product** to **create the effect** moving a term to a place where it can be canceled.

### 4.1 Another induction

Let the first transposition containing $K$ be $(K\, i)$. If this is the only transposition containing $K$, the product **cannot be the identity**, since the $K$ is ignored by earlier transpositions, moved to $i$ by this transposition, and $i$ is moved among the other quantities by the later transpositions.

This shows how we can prove that certain permutations are not the identity. In our proof, we assume that we **are given the identity**, so **this will never happen**. In particular, there will be at least one term after $(K\, i)$. The next part of the proof can be organized as an induction on the number $m$ of terms **after** the first term containing $K$.

### 4.2 Basis of the induction

If $m = 1$, the last two terms of the product are the only ones that can contain $K$. If $K$ is to be fixed by the product, the last term must also be $(K\, i)$, but **this repeats the previous transposition**, allowing cancellation.

### 4.3 The induction step

The induction step is a construction that rewrites the product of transpositions as another product in which **either** $m$ is smaller **or** $K$ disappears from the expression (as it did in the basis). If $K$ remains in the product, its first appearance will be among the $m-1$ remaining terms, so the number of terms following it has been decreased.

In another easy case, the next transposition does not involve either $K$ or $i$. Then, if it is $(a\,b)$, we have

$$(i\ K)(a\,b) = (a\,b)(i\ K).$$

Replacing the given terms by the equivalent product on the right decreases $m$ by 1.

The remaining cases are dealt with in the same way using one of the identities

$$(i\ K)(i\ a) = (i\ a)(a\ K)$$
$$(i\ K)(a\ K) = (i\ a)(i\ K)$$

## 5. Conclusion

We have already noted that the proof includes a procedure that distinguishes between identity and non-identity permutations. By itself, this is not significant since direct computation of the effect of the permutation on all quantities establishes this distinction with equal ease. Its main virtues are: (1) it is an independent calculation, so it can be used for checking; (2) it proves the Parity Proposition which appears to be outside the scope of direct computation.

The textbook contains a slick proof of the Parity Proposition, but it is less constructive.

## 6. A corollary

Every transposition is its own inverse. The general rule for constructing inverses of products is to by take the product, in the reverse order, of the inverses of the terms. Thus the inverse of a product of transpositions is the product of the same transpositions in the reverse order. If the same permutation can be written as a product of $n_1$ transpositions and as a product of $n_2$ transpositions, then following one of these representations by the reverse of the other gives a representation of the identity as a product of $n_1 + n_2$ transpositions.

Now, $n_1 + n_2$ is even if and only if $n_1 - n_2$ is even, since the difference of these quantities is even. We collect the results of these observations.

**Corollary.** *If a permutation has one representation as a product of an even number of transpositions, then every representation of that permutation as a product of transpositions has an even number of factors. Such permutations are called even permutations. If a permutation has one representation as a product of an odd number of transpositions, then every representation of that permutation as a product of transpositions has an odd number of factors. Such permutations are called odd permutations. The inverse of an even permutation is an even permutation and the inverse of an odd permutation is an odd permutation. Also the product of two permutations is even unless one is odd and one is even. Finally, a matrix representing a permutation has determinant* $+1$ *if the permutation is even, and determinant* $-1$ *if the permutation is odd.*

Each row interchange is given by left multiplication by a matrix $P$ that depends only on the location of the rows being interchanged and not on the matrix being manipulated. In particular, acting on the identity matrix shows that $P$ must be the matrix obtained by interchanging these rows of an identity matrix. The same approach gives a description of the matrices associated with the other elementary row operations. The matrix representing a transposition is both symmetric and equal to its inverse. Since the order of factors is reversed by both operations **transpose** and **inverse**, the correct generalization of this observation to arbitrary permutation matrices is that the inverse of a permutation matrix is equal to its transpose. That is, a permutation matrix is an **orthogonal matrix** (defined in section 3.4, p. 167).

**7. Exercise 4.3 A** Apply the method of Section 4 of this supplement to either find all symbols that are moved by the permutation or show that the permutation reduces to the empty permutation. (In both cases, one may assume that $K = 5$).

(i) $(1\,2)(1\,5)(3\,4)(2\,5)(1\,3)(3\,4)$.

(ii) $(1\,2)(1\,5)(3\,4)(2\,5)(1\,5)(3\,4)$.

End of Supplement