

Math 642:550 — Summer 2009  
MTTh 6:00–8:30 PM Hill 425  
Prof. Bumby

**Supplement 2, The sign of a permutation**

## 1. Introduction

Proofs will not play a large role in this course. However, any calculation (and, even more so, any program that will be used to perform a calculation on data that will 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 or numerical mathematics, the relevance of the calculation to the problem or its sensitivity to inexact data becomes 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 demonstrate 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.** Using the **linearity property** of the determinant to expand each row as a sum of multiples of rows with 1 in one place and 0 elsewhere gives a **very big** formula for the determinant of a general matrix in terms of the  $n^n$  determinants of matrices that are zero except for one 1 in each row. To find these determinants, try to interchange rows until you wind up with the identity matrix. This fails only for a matrix with two equal rows. The terms with equal rows have determinant zero. Removing them leaves the usual **big** formula with  $n!$  terms.

This shows that 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

$$(1\ 4)(1\ 2)(2\ 3)(3\ 4)(2\ 3)(1\ 2). \quad (*)$$

The progress of the symbol 1 is: the first factor takes 1 to 4; the next two factors don't affect 4 since 4 is not present in  $(1\ 2)$  or  $(2\ 3)$ ; the fourth factor takes 4 to 3; the fifth factor takes 3 to 2; and the last factor takes 2 to 1. A similar process will show that **all** symbols return to their original value, so that the permutation represented by this expression is the identity.

A more typical example is

$$(1\ 2)(2\ 3)(3\ 4)(1\ 2)(2\ 3) \quad (**)$$

Stepping through the action starting from 1: the first term takes 1 to 2; the second takes 2 to 3; the third takes 3 to 4; and 4 is not affected by the last two factors. Similarly, we find that 2 is taken to 3; 3 is taken to 1; and 4 is taken to 2. The **function** described by this action can be written more verbosely by writing the images of 1, 2, 3, 4 in order as we just did. Each new factor **on the right** interchanges the **values** appearing in that term. It is also possible to describe the effect of introducing a new factor **on the left**. In this case, the contents of the positions named in that factor are interchanged. The process of **sorting a list** may be interpreted as introducing factors on the left to produce the identity. Differing interpretations of left and right factors are common. You will often need to choose one interpretation while developing an application of the mathematics, although it will usually not be difficult to re-interpret results.

The idea of sorting introduces new factors in a product to produce the identity permutation. Multiplying the new terms gives the inverse of the given permutation, and forming the product of the same factors in the reverse order gives a possibly different factorization of the original permutation.

The expressions (\*) and (\*\*) are examples 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  $\{1, \dots, n\}$  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 even though this is a convenience in sorting.

**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.

A direct proof of this is fairly tricky. We present it because the method of **mathematical induction** used in the proof is the foundation of the **iterative** computational methods that appear throughout this course. Also, this serves as a reminder that the existence of the determinant, which you have probably accepted without question, requires the parity Proposition. This highlights the importance of changing the sign of the determinant when interchanging the rows of a matrix, and gives a glimpse of the surprising depth of that property.

One application of determinants is a formula for the area of a triangle. The sign of the determinant in that formula indicates the **orientation** of the figure which is usually ignored in elementary geometry, but is fundamental to the modern understanding of the nature of geometric objects.

Emphasizing Property 2 gives the most efficient proof of the existence of the determinant, but it lacks the intuitive appeal of Property 5 that says that the elementary row operations do not change the determinant. However, these two properties are equivalent: you can't have one without the other. This equivalence can be derived by the method sketched in exercise 3 of Section 4.2 of the textbook, which is expressed by the identity

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

in the simplest case.

**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 this as a simplification of the problem.

**4. Rewriting a product** We are now trying to reduce a product of transpositions to an equal one 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 factor 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  $K$  is ignored by earlier transpositions, moved to  $i$  by this transposition, and  $i$  is moved among the quantities different from  $K$  by the later transpositions.

This shows how we can prove that certain permutations are not the identity. Instead of tracing the effect of the permutation on the individual elements of its domain, we can follow the steps of this proof to work with the permutations themselves. Arriving at a point where an element  $K$  appears in only one term signals that we have shown that the permutation is 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. Two factors are removed in this case, so the difference in the number of factors is even, and the permutation represented does not change. This verifies all required properties.

**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 for this induction).

In an 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

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

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

Note that these identities preserve the number of factors.

**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 (as part of the discussion of 4E,p. 225) 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 (i.e., equal to its transpose) 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 any permutation matrix is equal to its transpose. That is, a permutation matrix is an **orthogonal matrix** (defined in section 3.4, p. 167). This is easily seen by considering inner product of the columns of a permutation matrix.

End of Supplement