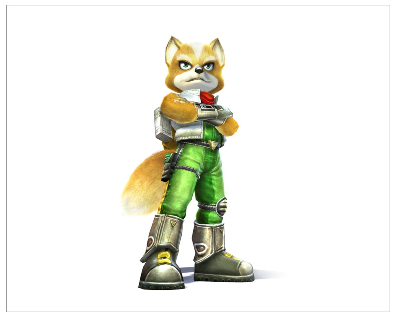
A proof that Corey finally understands

By: Star Fox

February 13, 2008



Greetings, young cadets! Below is a proof that the identity permutation must be even. In fact, Corey gives two proofs. Corey challenged Dr. Hasan to find a proof before he could. The result? We both came up with similar proofs, and Corey admits that Dr. Hasan's proof is more elegant. But hey, Corey is used to Dr. Hasan beating him at tennis, too. ROCK ON!

Lemma. The identity permutation $e \in S_n$ must be even. That is, any time e is written as a product of r transpositions, then r must be even.

Proof. (By Dr. Hasan) Define the polynomial in the variables $x_1, \ldots, x_n$ as follows:

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

(The Π notation does the same thing as $\sum$, but returns the *product*, rather than the *sum*. Also, it is implicit that i, j range from 1 to n.) Suppose you have a permutation $\sigma \in S_n$. Then one may use σ to produce a new polynomial by permuting the indices of the x's. For instance, for S_3 and the permutation $\sigma = (12)$, we can have σ act on p by changing the index 1 to 2, and 2 back to 1, while leaving the index 3 fixed:

$$p(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \longrightarrow (12) \cdot p(x_2, x_1, x_3) = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3).$$

Notice above that the transposition changed p to $(12) \cdot p = -p$, changing the sign of the polynomial. In general, notice that any transposition changes p to its negative, and that if you have a product of r transpositions that each act one by one on p, then you will change

p to $(-1)^r p$. The identity permutation leaves p alone, and if the identity were written as a product of r transpositions, then we would have to conclude that $p = (-1)^r p$, or that $(-1)^r = 1$, or that r is even.

Proof. (By Dr. Dunn) Consider the transposition (ab). One can use the transposition to construct a matrix which is the identity matrix with the ath row and bth row interchanged. Suppose the identity permutation is written as the product of r transpositions. For each of the permutations in the product, form the matrix described above, and consider the product of all of these matrices in the same order as the product of the transpositions that is equal to the identity. The resulting product of all of the matrices must be the identity matrix since each represents a swap of rows and the overall combination of all of these permutations is the identity. But the determinant of each of these matrices individually is -1, since they are the identity matrix (of determinant $+1$) with a row swap (changing the sign of the determinant to -1). Thus the determinant of the identity (which is 1) must be equal to the determinant of the product of these r matrices (which is $(-1)^r$). So $1 = (-1)^r$ and again, r must be even.

Corollary. No permutation can be written as both an odd number of permutations and an even number of permutations.

Proof. (By the math Gods) Suppose $\alpha = \beta_1 \cdots \beta_r$ and $\alpha = \gamma_1 \cdots \gamma_s$, where the β_i and γ_j are transpositions. Note also that $\gamma_j^{-1} = \gamma_j$ (the point is that the γ_j^{-1} are transpositions). Then

$$\alpha = \beta_1 \cdots \beta_r = \gamma_1 \cdots \gamma_s,$$

and so

$$\begin{aligned} e &= \beta_1 \cdots \beta_r \gamma_s^{-1} \gamma_{s-1}^{-1} \cdots \gamma_1 \\ &= \beta_1 \cdots \beta_r \gamma_s \gamma_{s-1} \cdots \gamma_1. \end{aligned}$$

We observe that the identity has been written as the product of $r + s$ transpositions. By the above Lemma, we must have $r + s$ is even, and so it is not possible for one of r or s to be even, and that the other be odd.