3.3 Odd & Even Permutations

Definition

Let σ be a permutation in S_n.

a. If σ can be written as a product of an even number of transpositions, then we say that σ is an <u>even</u> permutation.

b. If σ can be written as a product of an odd number of transpositions, then we say that σ is an <u>odd</u> permutation.

At this point, we cannot yet say whether it is possible for a permutation to be both even <u>and</u> odd. We will have to prove it, but we will see that such an odd situation cannot occur – a permutation must be either even or odd, but cannot be both.

On the other hand, while the number of transpositions used to represent a given permutation must be either even or odd, the <u>number</u> of transpositions needed is not unique. Since any transposition $\alpha = (j\ k)$ satisfies $\alpha^2 = e$, we can always insert transpositions $(j\ k)(j\ k)$ into any representation:

$$(1\ 2) = (1\ 2)(3\ 4)(3\ 4) = (1\ 2)(3\ 4)(3\ 4)(3\ 4)(3\ 4).$$

Still, the number of transpositions used has to be either odd or even.

In order to prove the result, we introduce some notation.

Notation

Let $p(x) = p(x_1, \ldots, x_n)$ be a polynomial in n variables. Then given $\sigma \in S_n$, we define another polynomial p_σ by

$$p_\sigma(x) = p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

Example

Suppose $n = 3$, $p(x_1, x_2, x_3) = 2x_1 + x_1x_3 + 3x_2^2$.

If $\sigma = (1\ 3\ 2)$, then

$$\begin{aligned} p_\sigma(x) &= p(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}) \\ &= p(x_3, x_1, x_2) \\ &= 2x_3 + x_3x_2 + 3x_1^2. \end{aligned}$$

Summary

Let $\sigma \in S_n$ be given. For each polynomial p of n variables, we associate a new polynomial p_σ of n variable. This gives us a mapping $p \longmapsto p_\sigma$ of polynomials to polynomials.

That is, if we let

$$\mathcal{P}_n = \{p : p \text{ is a polynomial in } n \text{ variables}\}$$

Then each $\sigma \in S_n$ determines a mapping

$$\sigma^* : \mathcal{P}_n \longrightarrow \mathcal{P}_n$$

$$\sigma^*(p) = p_\sigma$$

To avoid multiple parentheses, we will often write $\sigma^* p$ instead of $\sigma^*(p)$

We claim that the mapping from σ to σ^* has a homomorphism property, namely:

Claim: $(\sigma\tau)^* = \sigma^*\tau^*$

Since σ^* and τ^* are each functions mapping $Q_n \to Q_n$, to show that $(\sigma\tau)^* = \sigma^*\tau^*$ we must show that their outputs are the same for every input p. That is, we must show that

$$(\sigma\tau)^*(p) = (\sigma^*\tau^*)(p) \quad \text{for every } p \in Q_n.$$

Now,

$$(\sigma\tau)^*(p) = p_{\sigma\tau}$$

← the polynomial p with variables rearranged according to $\sigma\tau$

On the other hand,

$$\tau^*(p) = p_\tau$$

so

$$(\sigma^*\tau^*)(p) = \sigma^*(\tau^*(p)) = \sigma^*(p_\tau) = (p_\tau)_\sigma$$

↑ Composition of σ^* & τ^*

↗ This is the polynomial p with variables rearranged according to τ, followed by a rearrangement according to σ

So, our goal is to prove that $p_{\sigma\tau} = (p_\tau)_\sigma$. These are polynomials, so we must show that they are equal when we evaluate them at x.

Now, $p_{\sigma\tau}(x) = p(x_{\sigma\tau(1)}, x_{\sigma\tau(2)}, \ldots, x_{\sigma\tau(n)})$

p with variables rearranged.

To evaluate $(p_\tau)_\sigma$, let's first introduce some new variables.

Let $q = p_\tau$ and let $y_k = x_{\sigma(k)}$

Then

$$(p_\tau)_\sigma(x) = q_\sigma(x)$$

$$= q(x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(n)})$$ q with variables rearranged by σ

$$= p_\tau(x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(n)})$$

$$= p_\tau(y_1, y_2, \cdots, y_n)$$

$$= p(y_{\tau(1)}, y_{\tau(2)}, \cdots, y_{\tau(n)})$$ p with variables rearranged by τ

$$= p(x_{\sigma(\tau(1))}, x_{\sigma(\tau(2))}, \cdots, x_{\sigma(\tau(n))})$$ $y_k = x_{\sigma(k)}$ so $y_{\tau(k)} = x_{\sigma(\tau(k))}$

$$= p(x_{\sigma\tau(1)}, x_{\sigma\tau(2)}, \cdots, x_{\sigma\tau(n)})$$

Comparing, we see that $p_{\sigma\tau} = (p_\tau)_\sigma$.

Therefore $(\sigma\tau)^*(p) = (\sigma^*\tau^*)(p)$ for every $p \in P_n$

Hence $(\sigma\tau)^* = \sigma^*\tau^*$

Thus, we have proved the "homomorphism property" $(\sigma\tau)^* = \sigma^*\tau^*$. But what is the actual homomorphism that this is a property for?

Recall that σ belongs to $S_n = A(\{1,2,\dots,n\})$. This is the set of all bijections of $\{1,2,\dots,n\}$ onto itself.

Then σ "induces" another mapping $\sigma^* : \mathcal{P}_n \to \mathcal{P}_n$. This σ^* is a bijection that maps polynomials to polynomials. Hence $\sigma^* \in A(\mathcal{P}_n)$, the symmetric group on the set of polynomials $\mathcal{P}_n$. Each permutation σ of $\{1,2,\dots,n\}$ determines a permutation σ^* that maps $\mathcal{P}_n$ to $\mathcal{P}_n$.

Therefore, we can define a "meta-function" that sends σ to σ^*. This is the function

$$T : S_n \longrightarrow A(\mathcal{P}_n)$$
$$T(\sigma) = \sigma^*$$

T maps the group S_n into the group $A(\mathcal{P}_n)$. Since S_n is a finite group while $A(\mathcal{P}_n)$ is an infinite group, this function T cannot be onto. You should think about

whether T is 1-1. One thing that we do know is that T is a homomorphism, because

$$T(\sigma\tau) = (\sigma\tau)^* = \sigma^*\tau^* = T(\sigma)T(\tau)$$

[The group operation in both S_n & $A(\mathcal{P}_n)$ is composition.]

Summary: At the "top level",

$$T : S_n \longrightarrow A(\mathcal{P}_n)$$
$$T(\sigma) = \sigma^*$$

The output σ^* is itself a function:

$$\sigma^* : \mathcal{P}_n \longrightarrow \mathcal{P}_n$$
$$\sigma^*(p) = p_\sigma$$

where p_σ is a polynomial in n variables, which is the function defined by

$$p_\sigma(x) = p(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$$

where $x = (x_1, x_2, \dots, x_n)$. The homomorphism property is that

p with variables rearranged by $\sigma\tau$ = p with variables rearranged by τ following by a rearrangement by σ

Beware: be sure to use notation carefully.

$\sigma^* p$ is a polynomial

$(\sigma^* p)(x)$ is that polynomial evaluated at x

$\sigma^*(p(x))$ has no meaning

$p(x)$ is a number, it does not belong to the domain of σ^*. If $p(x) = 5$, then $\sigma^*(p(x)) = \sigma^*(5) = ??$

Correct: Since $(\sigma\tau)^* = \sigma^* \tau^*$ we have

$$\Big((\sigma\tau)^*(p)\Big)(x) = \Big((\sigma^*\tau^*)(p)\Big)(x)$$

$$= \Big(\sigma^*(\tau^*(p))\Big)(x)$$

A special polynomial

Now we consider a particular polynomial

$$\Delta(x) = (x_1 - x_2)(x_1 - x_3)\cdots(x_1 - x_n)\ (x_2 - x_3)\cdots(x_2 - x_n)(x_{n-1} - x_n)$$

$$= \prod_{1 \le i < j \le n} (x_i - x_j).$$

We want to see how $\tau * \Delta$ relates to Δ when $\tau = (k\ l)$ is a transposition. WLOG, take $k < l$.

WLOG = without loss of generality

Example: $n = 4$

For $n = 4$,

$$\Delta(x) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4).$$

Consider $\tau = (2\ 4)$. We have

$$(\tau * \Delta)(x) = (x_1 - x_4)(x_1 - x_3)(x_1 - x_2)(x_4 - x_3)(x_4 - x_2)(x_3 - x_2)$$

We have the same factors except that some $(x_i - x_j)$ terms have become $(x_j - x_i)$.

Each time $(x_i - x_j)$ is replaced by $(x_j - x_i)$, this changes the sign of the product. Otherwise everything is unchanged. Hence $\tau^* \Delta = \Delta$ if there were an even number of such interchanges, and $\tau^* \Delta = -\Delta$ if there were an odd number.

Can we count how many times this happens?

The term $x_i - x_j$ will only be affected if $i = k$ or $j = l$ or both. Further, the sign changes only when $(x_i - x_j)$ [which has $i < j$] is replaced by $(x_a - x_b)$ with $a > b$. When does this happen? Let us consider the possible cases. These are:

$$i = k,\ j \neq l, \qquad i = k,\ j = l, \qquad i \neq k,\ j = l.$$

Case 1: $i = k$, $j \neq l$.

In this case, $(x_i - x_j) = (x_k - x_j)$

becomes $(x_l - x_j)$.

Since $j > i = k$, the only times when we get a sign change are when $j < l$, i.e., for

$$j = k+1, \ldots, l-1.$$

There are $(l-1) - (k+1) + 1 = l - k - 1$ such terms.

Case 2: $i = k$, $j = l$.

In this case $(x_k - x_l)$ becomes $(x_l - x_k)$

Since $k < l$, this gives one sign change.

Case 3: $i \neq k$, $j = l$.

In this case $(x_i - x_l)$ becomes $(x_i - x_k)$.

Since $i < j = l$, the sign changes correspond to $i > k$, i.e.,

$$i = k+1, \ldots, l-1.$$

$$(\ell-1)-(k+1)+1$$

There are [redacted] $= \ell-k-1$ such terms.

All told

There are

$$(\ell-k-1)+1+(\ell-k-1) = 2\ell-2k-1$$

sign changes. This is an odd number. Hence we have shown that:

if $\tau = (k\ell)$ is a transposition,

then $\tau^* \Delta = -\Delta$.

[redacted]

Now we can prove our theorem about decomposition into decompositions.

Theorem

Every permutation $\sigma \in S_n$ is either odd or even, but cannot be both.

Proof:

We have already seen that every permutation can be written (nonuniquely) as a product of transpositions, so we just have to show that a permutation cannot be both odd & even.

Suppose that $\sigma \in S_n$, and we have both $\sigma = \alpha_1 \cdots \alpha_k$ and $\sigma = \beta_1 \cdots \beta_j$ where each α_i & β_i is a transposition. Let Δ be the polynomial considered before. Then

$$\sigma^*\Delta = (\alpha_1 \cdots \alpha_k)^* \Delta$$

$$= \alpha_1^* \cdots \alpha_k^* \Delta$$

$$= (-1)^k \Delta$$

since $\alpha_i^* \Delta = -\Delta$ for each i. Similarly,

$$\sigma^* \Delta = (\beta_1 \cdots \beta_j)^* \Delta$$

$$= \beta_1^* \cdots \beta_j^* \Delta$$

$$= (-1)^j \Delta .$$

Therefore $(-1)^j = (-1)^k$, which implies so either $j = k \bmod 2$, [redacted] j, k are both even or both odd.

Thus, σ is either even or odd, but not both. ▨

The Alternating Group

Definition

Given $n \in \mathbb{N}$, the alternating group A_n of order n is the set of all even permutations in S_n:

$$A_n = \{\sigma \in S_n : \sigma \text{ is even}\}.$$

Since every permutation is either even or odd, we know that every permutation in S_n is either in A_n or in $S_n \setminus A_n$.

Of course, the name "alternating group" begs the question: Is A_n a group? We answer this with our favorite proof technique.

Exercise

Show that A_n is a subgroup of S_n, i.e., the product of even transpositions is even, and the inverse of an even transposition is even (and A_n is nonempty, since $e \in A_n$ — why?).

In fact, we can say more about products of even and odd permutations.

Exercise
Show that if $\sigma, \tau \in S_n$ then:

σ even, τ even $\Rightarrow$ $\sigma\tau$ even
σ even, τ odd $\Rightarrow$ $\sigma\tau$ odd
σ odd, τ even $\Rightarrow$ $\sigma\tau$ odd
σ odd, τ odd $\Rightarrow$ $\sigma\tau$ even.

Corollary
A_n is a normal subgroup of S_n.

Proof:
Suppose $\sigma \in A_n$, so σ is even, and ρ is any element of S_n. If ρ is even, then so is ρ^{-1}, so $\rho\sigma\rho^{-1}$ is the product of even permutations, hence is even, so belongs to A_n. If ρ is odd, then ρ^{-1} is odd (why?), so $\rho\sigma\rho^{-1}$ is even (why?) In any case $\rho\sigma\rho^{-1} \in A_n$, so A_n is normal. ∎

How big is A_n? Every permutation is either even or odd, so $\{A_n, S_n \setminus A_n\}$ is a partition of S_n. But are the two parts of this partition the same size? Are there as many even permutations as odd? Can we find a bijection from the even permutations to the odd permutations?

Exercise

Let α be a fixed transposition, such as $\alpha = (1\ 2)$.

Define

$$T: A_n \longrightarrow S_n \setminus A_n$$
$$T(\sigma) = \alpha\sigma$$

Verify that T really does map A_n into $S_n \setminus A_n$, i.e., T maps an even permutation to an odd permutation.

Then prove that T is a bijection.

Note: Although A_n is a group, $S_n \setminus A_n$ is not (why?)

We're not asking if T is an isomorphism. We just want to know about the sizes of A_n & $S_n \setminus A_n$, so we just need to prove that T is a bijection.

Once we know that T is a bijection, we know that $|A_n| = |S_n \setminus A_n|$. Hence $A_n, S_n \setminus A_n$ is a partition of S_n into two sets of equal size. Hence each piece must have half of the elements of S_n.

Corollary

$$|A_n| = \frac{n!}{2}.$$

There are $\frac{n!}{2}$ even permutations in S_n, & $\frac{n!}{2}$ odd permutations.

This actually gives us another proof that A_n is normal, because it implies that $[S_n : A_n] = 2$,

and we know that any subgroup that has index 2 must be normal.

A_n is simple for $n \geq 5$

The alternating group A_n have a very special property: For $n \geq 5$, they are simple, i.e., they have no nontrivial normal subgroups (they have lots of subgroups, but only $\{e\}$ and A_n are normal). This is not easy to prove. Even more difficult is the following question: Find all finite simple groups. This has been a major project in abstract algebra, recently completed — hundreds of papers were published to complete the project.