MA294 Lecture

Timothy Kohl

Boston University

February 29, 2024

Even vs. Odd Permutations

Last time we learned that any $\sigma \in S_n$ can be decomposed into a product of disjoint cycles:

$$\sigma = \sigma_1 \sigma_2 \ldots \sigma_m$$

and that this decomposition is *unique* except for the order in which we write these cycles since they commute, and the fact that each cycle itself can be written in a number of equivalent ways depending on the first number in the cycle

$$i.e.\ (1,2,3) = (2,3,1) = (3,1,2)$$

so that, for example

$$(1,2,3)(4,5) = (2,3,1)(4,5) = (3,1,2)(4,5) = (4,5)(1,2,3) = ...etc.$$

Beyond the decomposition of a permutation into disjoint cycle, a permutation can be represented in terms of more fundamental building blocks.

Definition

A 2-cycle in S_n is called a <u>transposition</u>.

So for example, $(1,2) \in S_3$ is a transposition.

The significance of these is that one can build up a permutation by viewing it as a sequence of 'swaps', that is, as a sequence of transpositions.

Note that $(a,b) = (b,a)$.

For perspective, consider the the fact that all sorting algorithms one encounters in computer science, are built upon the pairwise comparison of elements in a list (of numbers for example) that one wishes to put into sorted order.

As such, if two elements are out of order, we swap their positions in the list, and repeat this as many times as needed, to restore the list to its correct ordering.

For a permutation, the idea is inverted in the sense that we view a given permutation as the shuffling of the list into a given arrangement by a sequence of swaps, i.e. by a sequence of transpositions.

The one key difference is that in this sequence of transpositions, the same element may be moved several times, i.e. as cycles, these won't generally be disjoint.

Theorem

Every permutation in S_n can be written as a product of (not necessarily disjoint) transpositions.

PROOF: We first start with this (simple yet important) fact about k-cycles:

$$(i_1, i_2, \ldots, i_k) = (i_1, i_k)(i_1, i_{k-1}) \cdots (i_1, i_2)$$

which looks a bit puzzling, but can be understood by looking at an example:

$$(3, 4, 5, 7) = (3, 7)(3, 5)(3, 4)$$

i.e. Follow how each element of $\{3, 4, 5, 7\}$ is moved by the three transpositions.

PROOF (continued):

So if $\sigma = \sigma_1 \cdots \sigma_m$, a product of disjoint cycles, then by the above fact we examined, each of these cycles σ_i can be, in turn, written as a product of transpositions.

So overall, σ can therefore be written as a (possibly large) collection of transpositions. □

For example

$$\underbrace{(1,6)(1,2)}_{(1,2,6)}\underbrace{(3,7)(3,5)(3,4)}_{(3,4,5,7)}$$

We note a number of facts about this theorem.

- $I = ()$ can be written as $(1,2)(1,2)$ so it too is a product of transpositions.
- The decomposition of $\sigma \in S_n$ into a product of transpositions is far from unique.
- For example $(3,4,5,7) = (3,7)(3,5)(3,4) = (1,2)(3,7)(3,5)(3,4)(1,2) = (3,7)(3,6)(3,5)(5,6)(3,4)$.

So the number of ways of writing a permutation as a product of transpositions isn't unique, but the following *is* true.

Theorem

A permutation $\sigma \in S_n$ may be written as a product of an even number of transpositions, or an odd number, but <u>not</u> both.

So the 'even' or 'odd' property is one thing that is characteristic of such a representation.

The proof of this is very interesting and uses a bit of linear algebra.
PROOF: Let $X = \{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n\}$ be the columns of the $n \times n$ (real) identity matrix

$$I = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ldots & 0 \\ 0 & 0 & \ldots & 1 \end{pmatrix} = \begin{pmatrix} \vec{e}_1 & \vec{e}_2 & \ldots & \vec{e}_n \end{pmatrix}$$

As such, $Perm(X) \cong S_n = Perm(\{1, \ldots, n\})$ where $\sigma \in S_n$ acts on the column vectors in $X = \{\vec{e}_1, \ldots, \vec{e}_n\}$ by shuffling the indices, i.e. $\sigma(\vec{e}_i) = \vec{e}_{\sigma(i)}$.

Thus, $\sigma(I)$ is some other $n \times n$ matrix obtained by permutating the columns of I.

PROOF (continued): So if $\tau = (i, j) \in S_n$ then since $det(I) = 1$ then $det(\tau(I)) = -1$ by basic facts we know about how the determinant is affected by column swaps.

As such, if $\sigma = (i_1, j_1)(i_2, j_2)\cdots(i_r, j_r)$ (a product of r transpositions) then $det(\sigma(I)) = (-1)^r$.

If one also writes $\sigma = (i'_1, j'_1)(i'_2, j'_2)\cdots(i'_s, j'_s)$ (a product of s transpositions) then we must have that $det(\sigma(I)) = (-1)^s$.

Thus we must have $(-1)^r = (-1)^s$ which means that r and s must both be even or both odd. □

Definition

For $\sigma \in S_n$ define the signature of σ to be $sgn(\sigma) = (-1)^r$ if σ can be written as product of r transpositions.

We observe that this is well defined no matter what number of transpositions σ can be decomposed into, it's always either an even or odd number.

As such $sgn : S_n \rightarrow \{\pm 1\}$ is a well defined function, but it also has other properties.

First, we can point out that $\{\pm 1\} = \{1, -1\}$ is a group under multiplication. (Exercise!)

Moreover, (although not a critical observation here) $\{\pm 1\} \cong \mathbb{Z}_2$.

We also note the following important fact about *sgn*.

Proposition

$sgn : S_n \to \{\pm 1\}$ is a homomorphism of groups, that is $sgn(\sigma_1\sigma_2) = sgn(\sigma_1)sgn(\sigma_2)$ for all $\sigma_1, \sigma_2 \in S_n$.

Proof.

If σ_1 is a product of r_1 transpositions and σ_2 is a product of r_2 transpositions, then $\sigma_1\sigma_2$ is a product of $r_1 + r_2$ transpositions. (Why?) Thus $sgn(\sigma_1) = (-1)^{r_1}$ and $sgn(\sigma_2) = (-1)^{r_2}$ so

$$sgn(\sigma_1\sigma_2) = (-1)^{r_1+r_2} = (-1)^{r_1}(-1)^{r_2} = sgn(\sigma_1)sgn(\sigma_2)$$

which is the homomorphism property asserted. □

Definition

We call $\sigma \in S_n$ even if $sgn(\sigma) = 1$ or odd if $sgn(\sigma) = -1$.

The even property gives rise to an important class of subgroups.

Definition

For $n > 1$, the n^{th} alternating group is $A_n = \{\sigma \in S_n \mid sgn(\sigma) = 1\}$.

We note that this *is* a subgroup via the homomorphism property stated above, since if $sgn(\sigma_1) = 1$ and $sgn(\sigma_2) = 1$ then $sgn(\sigma_1\sigma_2) = 1$ as well. Moreover, $sgn(\sigma) = 1$ implies that $sgn(\sigma^{-1}) = 1$ too. (Exercise).

How big is A_n?

Proposition

$|A_n| = \frac{n!}{2}$ *for each* $n \geq 2$.

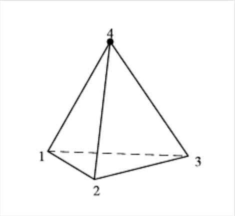
Proof.

Consider $\bar{A}_n = S_n - A_n$ (i.e. the set difference) and, assuming $n > 1$, we have that $(1,2) \in \bar{A}_n$.
If we define $f : A_n \to \bar{A}_n$ by $f(\sigma) = (1,2)\sigma$ where $(1,2)\sigma$ is in $\bar{A}_n$ if $\sigma \in A_n$ since then $sgn((1,2)\sigma) = sgn((1,2))sgn(\sigma) = (-1) \cdot 1 = -1$.
Now, if $(1,2)\sigma = (1,2)\tau$ then $\sigma = \tau$ which implies that f is 1-1.
We can also show that f is onto since if $\mu \in \bar{A}_n$ then
$\mu = (1,2)(1,2)\mu = (1,2)[(1,2)\mu] = f((1,2)\mu)$ where $(1,2)\mu \in A_n$.

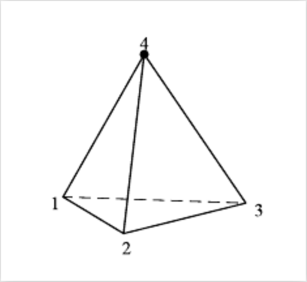
Thus $|A_n| = |\bar{A}_n|$ and since $S_n = A_n \cup \bar{A}_n$ and $A_n \cap \bar{A}_n = \emptyset$ then $|S_n| = 2|A_n|$. □

We saw that D_4 may be viewed as a subgroup of S_4 and that it was exactly those 8 elements that are permissible as plane symmetries of the square.

If we look at figures in space, such as the regular tetrahedron:



then we can consider the symmetries in space which consists of basically any permutations of the figure which don't distort or 'tear' it.



For the tetrahedron, these consist of all the permutations that lie in A_4 as it turns out.

And one of the reasons it's no *larger* is that, for example, $(1,2)$ is not possible since (with the $3-4$ side fixed) the permutation $(1,2)$ would tear it!

And similarly, no other single transposition is permitted, nor is any other odd permutation.

One other observation we can make about even vs. odd permutations (which touches on the proof we gave about a given permutation being representable as only a product or even or odd number of transpositions) is about the formulation of the determinant in terms of the 'parity' of a permutation.

Fact: (Leibniz) For an $n \times n$ matrix $A = (a_{ij})$ one can show that

$$det(A) = \sum_{\sigma \in S_n} sgn(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

which is quite a bit different than the typical formulation (Laplace expansion) in terms of summing over the determinants of the $n-1 \times n-1$ submatrices.

This formula

$$det(A) = \sum_{\sigma \in S_n} sgn(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

is a bit challenging to work with, but does satisfy all the formulas that *a* determinant function should satisfy: alternation, n-linearity, $det(I) = 1$.

One of these is *really* easy to check, and that is the fact that $det(I) = 1$.

To see this, realize that if $A = I$ then $a_{ii} = 1$ while $a_{ij} = 0$ for $i \neq j$ and so $a_{i\sigma(i)} = 1$ only if $\sigma(i) = i$ and so in each term

$$a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

the result will be zero *unless* σ is the identity element, thus $det(I) = sgn(identity) a_{11} a_{22} \cdots a_{nn} = 1$.

Kernels

If we look back to the properties of *sgn* and the definition of A_n we are led to an important class of subgroups of a group.

Definition

A function $f : (G_1, *_1) \rightarrow (G_2, *_2)$ is a group homomorphism if $f(a *_1 b) = f(a) *_2 f(b)$.

which should be familiar from the definition of isomorphism given earlier, but here we are not assuming that f is one-to-one or onto, indeed it need not be.

As we saw earlier, the function $sgn : S_n \rightarrow \{\pm 1\}$ is an example of a homomorphism.

Another fundamental example is $\rho : \mathbb{Z} \rightarrow \mathbb{Z}_m$ (for any $m > 1$) given by $\rho(a) = r$ if $a = qm + r$ for $r \in \{0, \ldots, m-1\}$ coming from the division algorithm.

Yet another example is the determinant $det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$ where $\mathbb{R}^*$ is the group of non-zero real numbers under multiplication.

From a homomorphism between two groups, we can construct a fundamental subgroup one obtains.

Definition

For a group homomorphism $f : (G_1, *_1) \rightarrow (G_2, *_2)$, the kernel is $Ker(f) = \{a \in G_1 \mid f(a) = e_2\}$ where e_2 is the identity of G_2.

The fundamental property to check is this.

Proposition

For a group homomorphism $f : (G_1, *_1) \rightarrow (G_2, *_2)$, the kernel $Ker(f)$ is a subgroup of G_1.

As to examples, consider the one we saw earlier, namely A_n since $\sigma \in A_n$ iff $sgn(\sigma) = 1 \in \{\pm 1\}$ where 1 is the identity of $\{\pm 1\}$.

For the 'remainder' homomorphism $\rho : \mathbb{Z} \rightarrow \mathbb{Z}_m$ we saw earlier, $Ker(\rho) = \{a \in \mathbb{Z} \mid \rho(a) = 0\}$ namely those $a \in \mathbb{Z}$ for which m divides a exactly, ergo $Ker(\rho) = m\mathbb{Z}$.