MATH 3311, FALL 2025: LECTURE 24, OCTOBER 24

Video: `https://youtu.be/pVYtVdJD6xw`

The sign homomorphism and the alternating group

Theorem 1 (The sign homomorphism)**.** *There is a* unique *surjective homomorphism*

$$\mathrm{sgn} : S_n \to \{\pm 1\}$$

such that $\mathrm{sgn}(\tau) = -1$ *for every transposition* $\tau \in S_n$.

The key points in the proof of the theorem are Proposition 1 and Fact 1 below. The former says that the sign of a permutation that can be written as a product of transpositions is well-defined, regardless of how this product expression is obtained. The latter says that every permutation is in fact a product of transpositions.

Proposition 1. *If* $\sigma \in S_n$ *can be written as*

$$\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l,$$

where $\alpha_i, \beta_j \in S_n$ *are transpositions. Then we have*

$$k \equiv l \pmod 2$$

.

Definition 1. We will say that two cycles $(a_1\ a_2\ \cdots\ a_m)$ and $(b_1\ \cdots\ b_r)$ are **disjoint** if

$$\{a_1, \ldots, a_m\} \cap \{b_1, \ldots, b_r\} = \emptyset.$$

In general, a list of cycles $\alpha_1, \ldots, \alpha_s$ is **disjoint** if all the cycles in the list are pairwise disjoint.

Remark 1.
- The basic property of disjoint cycles is that they act on entirely different parts of the set $\{1, 2, \ldots, n\}$ and hence do not really interact with each other. This means that if $\alpha, \beta \in S_n$ are disjoint cycles, then
$$\alpha\beta = \beta\alpha.$$
- Note that the disjointness is *essential* for the above equality to hold. For example, since $(1\ 2)$ and $(2\ 3)$ are *not* disjoint, we have
$$(1\ 2)(2\ 3) = (1\ 2\ 3) \neq (1\ 3\ 2) = (2\ 3)(1\ 2).$$

Observation 1. Every permutation in S_n can be written as a product of disjoint cycles uniquely up to the order of multiplication. This is the **disjoint cycle decomposition**.

Observation 2. Every m-cycle is a product of $(m-1)$-transpositions.

Proof. In fact, we have We have:

$$(a_1\ a_2)(a_2\ a_3) \cdots (a_{m-1}\ a_m) = (a_1\ a_2\ \cdots\ a_m).$$

□

Combining this with the previous observation shows the fact that we need:

Fact 1. Every permutation is a composition of transpositions.

Proof. Write a given permutation as a product of disjoint cycles and then break each of the cycles down into a product of transpositions. □

Definition 2 (The alternating group)**.** The **alternating group** $A_n \trianglelefteq S_n$ is the kernel of the sign homomorphism: It is a normal subgroup of S_n of index 2 and so has order $\frac{n!}{2}$.

Definition 3 (Odd and even permutations)**.** A permutation $\sigma \in S_n$ is **even** if $\sigma \in A_n$; equivalently, if $\mathrm{sgn}(\sigma) = 1$.[1] Otherwise, it is **odd**.

Example 1. Every transposition is odd and so does *not* belong to A_n

Example 2. More generally, by Observation 2, an m-cycle is even if and only if m is *odd*: So 3 and 5-cycles are even and in A_n, while 4 or 6-cycles are odd and not in A_n.

Definition 4 (Cycle type)**.** Given an element $\sigma \in S_n$, the **cycle type** of σ is an n-tuple $(m_1, m_2, \ldots, m_n)$ of non-negative integers, where for each i, m_i is the number of i-cycles in the disjoint cycle decomposition of σ (including 1-cycles for fixed points!).

Example 3. The identity has cycle type $(n, 0, \ldots, 0)$.

Example 4. A transposition has cycle type $(n-2, 1, \ldots, 0)$.

Example 5. A 3-cycle has cycle type $(n-3, 0, 1, \ldots, 0)$.

Example 6. Let's look at the example of S_3. We have the following possible cycle types:

Cycle type	Example α	Number of elements with the type
$(3,0,0)$	e	1
$(1,1,0)$	(1 2)	3
$(0,0,1)$	(1 2 3)	2

Example 7. Now let's consider S_4.

Cycle type	Example α	Number of elements with the type
$(4,0,0,0)$	e	1
$(2,1,0,0)$	(1 2)	6
$(1,0,1,0)$	(1 2 3)	8
$(0,0,0,1)$	(1 2 3 4)	6
$(0,2,0,0)$	(1 2)(3 4)	3

Here, for computing the number of 3-cycles for instance, note that we can calculate as follows:

- First, we look at the number of ways of choosing 3 elements out of 4: This gives us a factor of 4;
- Next, for each such set, we see that the number of *distinct* 3-cycles one can construct is 2: This is the total number of permutations of 3 elements, $3! = 6$, divided by 3 to account for the fact that each 3-cycle can be represented in 3 ways depending on where one chooses to start. For instance, $(1\ 2\ 3) = (3\ 1\ 2) = (2\ 3\ 1)$.

Conjugacy in S_n

Observation 3. If $\alpha = (a_1\ \cdot\ a_m)$ is an m-cycle and $\sigma \in S_n$ is any permutation, then $\sigma\alpha\sigma^{-1}$ is also an m-cycle, and we in fact have

$$\sigma\alpha\sigma^{-1} = (\sigma(a_1)\ \cdots\ \sigma(a_m)).$$

Remark 2. This should be thought of as an analogy with change of basis: If A is an invertible matrix and B is any square matrix of the same dimension, then ABA^{-1} can be thought of as still describing the linear transformation corresponding to B, but with respect to a different basis. Similarly, $\sigma\alpha\sigma^{-1}$ is doing the same thing as α, except that we have changed our labeling from $\{1, 2, \ldots, n\}$ to $\{\sigma(1), \ldots, \sigma(n)\}$.

Example 8. If $\alpha = (2\ 3\ 4)$ and $\sigma = (1\ 2)$, then

$$\sigma\alpha\sigma^{-1} = (\sigma(2)\ \sigma(3)\ \sigma(4)) = (1\ 3\ 4).$$

[1] The group $\{\pm 1\} = \{1, -1\}$ has 1 as its identity element under multiplication.

Remark 3. If

$$\sigma = \alpha_1 \alpha_2 \cdots \alpha_r$$

is the decomposition into disjoint cycles, then

$$\tau\sigma\tau^{-1} = \tau(\alpha_1 \cdots \alpha_r)\tau^{-1} = (\tau\alpha_1\tau^{-1})(\tau\alpha_2\tau^{-1}) \cdots (\tau\alpha_r\tau^{-1}).$$

What this means is that σ and $\tau\sigma\tau^{-1}$ have the *same* cycle type.

Conversely, if σ and β have the same cycle type, then we can find a τ such that $\tau\sigma\tau^{-1} = \beta$. For example, if

$$\sigma = (1\ 2\ 3)(4\ 5)\ ,\ \beta = (a\ b\ c)(d\ e),$$

then any permutation τ that satisfies $\tau(1) = a, \tau(2) = b, \tau(3) = c, \tau(4) = d, \tau(5) = e$ will work for the equality

$$\tau\sigma\tau^{-1} = (\tau(1)\ \tau(2)\ \tau(3))(\tau(4)\ \tau(5)) = \beta.$$

This gives us the following observation which you saw on Homework 5:

Observation 4. Two permutations $\sigma, \beta \in S_n$ are conjugate to each other (that is, there exists $\tau \in S_n$ such that $\tau\sigma\tau^{-1} = \beta$) *if and only if* they have the same cycle type. In other words, we have a bijection

$$\{\text{conjugacy classes in } S_n\} \leftrightarrow \{\text{cycle types}\}.$$

The tables in Examples 6 and 7 are therefore telling us exactly what the conjugacy classes in S_3 and S_4 are.