MATH 3311, FALL 2025: LECTURE 23, OCTOBER 22

Video: `https://youtu.be/lef63OnAAuE`
The sign homomorphism
Recall from last time the following:

Definition 1. (Cycle notation) Given $m \in \{2, \dots, n\}$, an m**-cycle** $\alpha \in S_n$ is an element written in the form

$$(a_1 \; a_2 \; \cdots \; a_m),$$

where $a_1, a_2, \dots, a_m \in \{1, 2, \dots, n\}$ are *distinct* elements, and where, as a permutation of $\{1, 2, \dots, n\}$, α behaves as follows:

- It moves the elements $a_1, \dots, a_m$ like so: $\begin{tikzcd} a_1 \arrow[r, mapsto] & a_2 \arrow[r, mapsto] & \cdots \arrow[r, mapsto] & a_{m-1} \arrow[r, mapsto] & a_m \arrow[llll, mapsto, bend left] \end{tikzcd}$
- It fixes all elements not in the subset $\{a_1, \dots, a_m\}$.

A **cycle** is an element $\alpha \in S_n$ that is an m-cycle for some integer m.

Remark 1. Note that there isn't a unique way to write a cycle: $(a_1 \; a_2 \; \cdots a_m)$ is the same as $(a_m \; a_1 \; \cdots \; a_{m-1})$ or $(a_2 \; a_3 \; \cdots a_m \; a_1)$.

Definition 2. A 2-cycle in S_n will be called a **transposition**.

Definition 3. We will say that two cycles $(a_1 \; a_2 \; \cdots \; a_m)$ and $(b_1 \; \cdots \; b_r)$ are **disjoint** if

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

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

Remark 2.
- The basic property of disjoint cycles is that they act on entirely different parts of the set $\{1, 2, \dots, n\}$ 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**.

Proof. Suppose that we have $\alpha \in S_n$. Then we can look at the cyclic group $H = \langle \alpha \rangle$ acting on the set $\{1, 2, \dots, n\}$. This divides up $\{1, 2, \dots, n\}$ into *disjoint* orbits for the action of H.

$$\{1, 2, \dots, n\} = \bigsqcup_{i=1}^{s} \mathcal{O}_i.$$

The action of α on each orbit $\mathcal{O}_i$ is now described by an m_i-cycle τ_i (why?), where $|\mathcal{O}_i| = m_i$. Now α is the product $\tau_1\tau_2 \cdots \tau_s$ of disjoint cycles. □

Example 1. Let's take $\alpha \in S_9$ to be the permutation given by

$$1 \mapsto 5 \,;\, 2 \mapsto 7 \,;\, 3 \mapsto 2 \,;\, 4 \mapsto 1 \,;\, 5 \mapsto 8 \,;\, 6 \mapsto 9 \,;\, 7 \mapsto 3 \,;\, 8 \mapsto 6; 9 \mapsto 4$$

The orbits for the action of $\langle \alpha \rangle$ are exactly $\{1, 5, 8, 6, 9, 4\}$ and $\{2, 7, 3\}$, and each orbit contributes a cycle that describes what α does to it, so that

$$\alpha = (1\;5\;8\;6\;9\;4)(2\;7\;3) = (2\;7\;3)(1\;5\;8\;6\;9\;4)$$

We would like to prove:

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 main input into this theorem is the following result.

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*

$$k \equiv l \pmod 2$$

.

Proof. we note that the equality

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

translates to

$$e = \alpha_k \alpha_{k-1} \cdots \alpha_1 \beta_1 \cdots \beta_l$$

Therefore, we have expressed e as a product of $k + l$ transpositions. The second part of the proposition is now a consequence of the following fact (note that $k + l \equiv 0 \pmod 2$ is equivalent to $k \equiv l \pmod 2$):

Fact 1. If $e = \tau_1 \ldots \tau_m$ where $\tau_i \in S_n$ are transpositions, them $m \equiv 0 \pmod 2$.

We will show this by induction on m. If $m = 0$, there is nothing to show. It is not possible to have $m = 1$, since then we would have

$$e = (a_1\ b_1),$$

which is absurd, since e cannot move anything while $(a_1\ b_1)$ switches a_1 and b_1.

Now, suppose that we have

$$e = (a_1\ b_1)(a_2\ b_2) \cdots (a_{m-1}\ b_{m-1})(a_m\ b_m).$$

We have the following rules for multiplying transpositions that form the rules of the game:

$$(a\ b)(c\ d) = (c\ d)(a\ b)\ (a\ b)(a\ b) = e\ (a\ c)(a\ b) = (a\ b)(b\ c)\ (b\ c)(a\ b) = (a\ c)(b\ c).$$

Now, look at the last pair of transpositions $(a_{m-1}\ b_{m-1}), (a_m\ b_m)$. Their product has the following possibilities:

$$(a_{m-1}\ b_{m-1})(a_m\ b_m) = \begin{cases} (a_m\ b_m)(a_{m-1}, b_{m-1}), & \text{if the two are disjoint.} \\ e\text{, if the two are equal.} \\ (a_m\ b_m)(b_{m-1}\ b_m), & \text{if } a_m = a_{m-1}, b_m \neq b_{m-1}. \\ (a_m\ b_m)(a_{m-1}\ b_m), & \text{if } a_m = b_{m-1}, b_m \neq a_{m-1}. \\ (a_m\ a_{m-1})(a_{m-1}\ b_m), & \text{if } b_m = b_{m-1}, a_m \neq a_{m-1}. \\ (a_m\ b_{m-1})(b_{m-1}\ b_m), & \text{if } b_m = a_{m-1}, a_m \neq b_{m-1}. \end{cases}$$

In the second situation, we have reduced e to a product of $m - 2$ transpositions

$$e = (a_1\ b_1) \cdots (a_{m-2}\ b_{m-2}).$$

By induction on m, this means that $m - 2$ is even, and hence that m is even.

In all other situations, we have moved a_m over one step to the left while ensuring that it doesn't appear in the last transposition.

Proceeding in this fashion, we will have accomplished one of two things:

- We will have moved a_m all the way to the left, so that it appears in the first transposition in the product and nowhere else. But this is impossible, since the product is supposed to be e which cannot move a_m.
- So what we must have actually accomplished is that, at some point, we reduced the number of transpositions by 2, and concluded by induction that m is even.

□