AM 106/206: Applied Algebra **Madhu Sudan**[1]

Lecture Notes 7

September 26, 2016

- **Reading:** Gallian Chapter 5

1 Permutation Groups: Basics

- **Def:** A *permutation group* on a set A is a subgroup of $Sym(A)$ (the set of permutations of A under composition).
- **Examples:**
  - S_n
  - D_n (two choices for A)
  - $GL_n(\mathbb{R})$

  [Technically, D_n and $GL_n(\mathbb{R})$ are only "isomorphic" to permutation groups on $[n]$ and $\mathbb{R}^n$, respectively.]
- Today we'll focus on $A = [n] = \{1, \ldots, n\}$, ie S_n and its subgroups.
- Running examples: $\sigma, \tau \in S_7$ defined by

$$\sigma(1) = 5, \sigma(2) = 3, \sigma(3) = 6, \sigma(4) = 7, \sigma(5) = 1, \sigma(6) = 2, \sigma(7) = 4,$$

and

$$\tau(1) = 1, \tau(2) = 2, \tau(3) = 3, \tau(4) = 6, \tau(5) = 7, \tau(6) = 5, \tau(7) = 4.$$

- **Array notation:**

$$\begin{aligned} \sigma &= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 6 & 7 & 1 & 2 & 4 \end{bmatrix} \\ \tau &= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 6 & 7 & 5 & 4 \end{bmatrix} \\ \tau \circ \sigma &= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ & & & & & & \end{bmatrix} \end{aligned}$$

[1] These notes are copied mostly verbatim from the lecture notes from the Fall 2010 offering, authored by Prof. Salil Vadhan. I will attempt to update them, but apologies if some references to old dates and contents remain.

2 Cycle Notation

- **Def:** An *m-cycle* is a permutation α for which there exist distinct $i_1, \ldots, i_m$ such that $\alpha(i_1) = i_2, \alpha(i_2) = i_3, \ldots, \alpha(i_{m-1}) = i_m, \alpha(i_m) = i_1$, and $\alpha(j) = j$ for all $j \notin \{i_1, \ldots, i_m\}$.
- **Cycle notation:** $\alpha = (i_1 i_2 \cdots i_m) = (i_2 i_3 \cdots i_m i_1) = \cdots$
- **Examples:**
- **Q:** What is the order of an m-cycle?
- **Thm 5.1+:** Every permutation in S_n can be written as a product of one or more *disjoint* cycles, whose union includes all elements of $[n]$. This representation is unique up to the order of the cycles (and cyclic shifts when writing the cycles).
  - We usually don't write the 1-cycles!
- **Proof by example:** $\sigma =$
- **Graphical view:** View a permutation as a directed graph in which every vertex has indegree and outdegree 1 (possibly with self-loops). Such a graph consists of disjoint cycles.
- **Q (Thm 5.3):** How can we calculate the order of a permutation in terms of its cycles?
- **Example:** $\text{order}(\sigma) =$
- **Proof in general:**

3 Transpositions

- **Def:** A *transposition* is a 2-cycle.
- **Thm 5.4:** Every permutation can be written as a product of transpositions.
  - Not uniquely!
- **Proof:**

- **Thm 5.5+:**

  1. (Even permutations) If a permutation σ has an even number of even-length cycles in disjoint cycle notation, then σ can only be written as product of an even number of transpositions. In such a case, σ is called an *even permutation*.
  2. (Odd permutations) If a permutation σ has an odd number of even-length cycles in disjoint cycle notation, then σ can only be written as product of an odd number of transpositions. In such a case, σ is called an *odd permutation*.

- **Proof:** (different from book) Show by induction on n that if $\sigma = \alpha_1 \cdots \alpha_n$ for transpositions α_i, then the parity of the number of even-length cycles in σ equals the parity of n.

  - Base case ($n = 0$): σ consists of zero even-length cycles.
  - Induction step: Consider what happens when we multiply a permutation $\sigma = \alpha_1 \cdots \alpha_n$ by an additional transposition α_{n+1}. Let's do a case analysis depending on how $\alpha_{n+1} = (ij)$ intersects the disjoint cycles of σ.
    * Case 1: i and j are both within the same cycle.
    * Case 2: i and j are within different cycles.

- **Cor:** The set of even permutations in S_n is a subgroup, called the *alternating group A_n*.

- **Q:** What is $|A_n|$?