MATH 415

Modern Algebra I

Lecture 7:
Order and sign of a permutation.

Order of a permutation

The **order** of a permutation $\pi \in S_n$, denoted $o(\pi)$, is defined as the smallest positive integer m such that $\pi^m = \mathrm{id}$, the identity map. In other words, this is the order of π as an element of the symmetric group S_n.

(Recall that every element of a finite group has finite order.)

Theorem Let π be a permutation of order m. Then $\pi^r = \pi^s$ if and only if $r \equiv s \bmod m$. In particular, $\pi^r = \mathrm{id}$ if and only if the order m divides r.

Remark. Notation $r \equiv s \bmod m$ (r is congruent to s modulo m) means that r and s leave the same remainder under division by m.

Theorem Let π be a cyclic permutation. Then the order $o(\pi)$ is the length of the cycle π.

Examples. • $\pi = (1\ 2\ 3\ 4\ 5)$.
$\pi^2 = (1\ 3\ 5\ 2\ 4)$, $\pi^3 = (1\ 4\ 2\ 5\ 3)$,
$\pi^4 = (1\ 5\ 4\ 3\ 2)$, $\pi^5 = \mathrm{id}$.
$\implies o(\pi) = 5$.

• $\sigma = (1\ 2\ 3\ 4\ 5\ 6)$.
$\sigma^2 = (1\ 3\ 5)(2\ 4\ 6)$, $\sigma^3 = (1\ 4)(2\ 5)(3\ 6)$,
$\sigma^4 = (1\ 5\ 3)(2\ 6\ 4)$, $\sigma^5 = (1\ 6\ 5\ 4\ 3\ 2)$, $\sigma^6 = \mathrm{id}$.
$\implies o(\sigma) = 6$.

• $\tau = (1\ 2\ 3)(4\ 5)$.
$\tau^2 = (1\ 3\ 2)$, $\tau^3 = (4\ 5)$, $\tau^4 = (1\ 2\ 3)$,
$\tau^5 = (1\ 3\ 2)(4\ 5)$, $\tau^6 = \mathrm{id}$.
$\implies o(\tau) = 6$.

Lemma 1 Let π and σ be two commuting permutations: $\pi\sigma = \sigma\pi$. Then
(i) the powers π^r and σ^s commute for all $r, s \in \mathbb{Z}$,
(ii) $(\pi\sigma)^r = \pi^r\sigma^r$ for all $r \in \mathbb{Z}$.

Lemma 2 Let π and σ be disjoint permutations in S_n. Then
(i) the powers π^r and σ^s are also disjoint,
(ii) $\pi^r\sigma^s = \mathrm{id}$ implies $\pi^r = \sigma^s = \mathrm{id}$.

Lemma 3 Let π and σ be disjoint permutations in S_n. Then
(i) they commute: $\pi\sigma = \sigma\pi$,
(ii) $(\pi\sigma)^r = \mathrm{id}$ if and only if $\pi^r = \sigma^r = \mathrm{id}$,
(iii) $o(\pi\sigma) = lcm\big(o(\pi), o(\sigma)\big)$.

Theorem Let $\pi \in S_n$ and suppose that $\pi = \sigma_1\sigma_2\ldots\sigma_k$ is a decomposition of π as a product of disjoint cycles. Then the order of π is the least common multiple of the lengths of cycles $\sigma_1, \ldots, \sigma_k$.

Sign of a permutation

Theorem 1 (i) Any permutation is a product of transpositions.
(ii) If $\pi = \tau_1\tau_2\ldots\tau_n = \tau'_1\tau'_2\ldots\tau'_m$, where τ_i, τ'_j are transpositions, then the numbers n and m are of the same parity (that is, both even or both odd).

A permutation π is called **even** if it is a product of an even number of transpositions, and **odd** if it is a product of an odd number of transpositions.

The **sign** $\operatorname{sgn}(\pi)$ of the permutation π is defined to be $+1$ if π is even, and -1 if π is odd.

Theorem 2 (i) $\operatorname{sgn}(\pi\sigma) = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma)$ for any $\pi, \sigma \in S_n$.
(ii) $\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi)$ for any $\pi \in S_n$.
(iii) $\operatorname{sgn}(\mathrm{id}) = 1$.
(iv) $\operatorname{sgn}(\tau) = -1$ for any transposition τ.
(v) $\operatorname{sgn}(\sigma) = (-1)^{r-1}$ for any cycle σ of length r.

Let $\pi \in S_n$ and i, j be integers, $1 \leq i < j \leq n$. We say that the permutation π preserves order of the pair (i, j) if $\pi(i) < \pi(j)$. Otherwise π makes an **inversion**. Denote by $N(\pi)$ the number of inversions made by the permutation π.

Lemma 1 Let $\tau, \pi \in S_n$ and suppose that τ is an adjacent transposition, $\tau = (k\ k{+}1)$. Then $|N(\tau\pi) - N(\pi)| = 1$.

Proof: For every pair (i, j), $1 \leq i < j \leq n$, let us compare the order of pairs $\pi(i), \pi(j)$ and $\tau\pi(i), \tau\pi(j)$. We observe that the order differs exactly for one pair, when $\{\pi(i), \pi(j)\} = \{k, k{+}1\}$. The lemma follows.

Lemma 2 Let $\pi \in S_n$ and $\tau_1, \tau_2, \ldots, \tau_k$ be adjacent transpositions. Then **(i)** for any $\pi \in S_n$ the numbers k and $N(\tau_1\tau_2 \ldots \tau_k\pi) - N(\pi)$ are of the same parity,
(ii) the numbers k and $N(\tau_1\tau_2 \ldots \tau_k)$ are of the same parity.

Sketch of the proof: **(i)** follows from Lemma 1 by induction on k. **(ii)** is a particular case of part (i), when $\pi = \mathrm{id}$.

Lemma 3 (i) Any cycle of length r is a product of $r-1$ transpositions. **(ii)** Any transposition is a product of an odd number of adjacent transpositions.

Proof: **(i)** $(x_1\ x_2\ \dots\ x_r) = (x_1\ x_2)(x_2\ x_3)(x_3\ x_4)\dots(x_{r-1}\ x_r)$.
(ii) $(k\ k{+}r) = \sigma^{-1}(k\ k{+}1)\sigma$, where $\sigma = (k{+}1\ k{+}2\ \dots\ k{+}r)$.
By the above, $\sigma = (k{+}1\ k{+}2)(k{+}2\ k{+}3)\dots(k{+}r{-}1\ \ k{+}r)$ and $\sigma^{-1} = (k{+}r\ \ k{+}r{-}1)\dots(k{+}3\ k{+}2)(k{+}2\ k{+}1)$.

Theorem (i) Any permutation is a product of transpositions. **(ii)** If $\pi = \tau_1\tau_2\dots\tau_k$, where τ_i are transpositions, then the numbers k and $N(\pi)$ are of the same parity.

Proof: **(i)** Any permutation is a product of disjoint cycles. By Lemma 3, any cycle is a product of transpositions.

(ii) By Lemma 3, each of $\tau_1, \tau_2, \dots, \tau_k$ is a product of an odd number of adjacent transpositions. Hence $\pi = \tau_1'\tau_2'\dots\tau_m'$, where τ_i' are adjacent transpositions and number m is of the same parity as k. By Lemma 2, m has the same parity as $N(\pi)$.

Examples

- $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 4 & 7 & 9 & 1 & 12 & 5 & 11 & 3 & 10 & 6 & 8 \end{pmatrix}$.

First we decompose π into a product of disjoint cycles:

$$\pi = (1\ 2\ 4\ 9\ 3\ 7\ 5)(6\ 12\ 8\ 11).$$

The cycle $\sigma_1 = (1\ 2\ 4\ 9\ 3\ 7\ 5)$ has length 7, hence it is an even permutation. The cycle $\sigma_2 = (6\ 12\ 8\ 11)$ has length 4, hence it is an odd permutation. Then

$$\operatorname{sgn}(\pi) = \operatorname{sgn}(\sigma_1\sigma_2) = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2) = 1 \cdot (-1) = -1.$$

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

π is represented as a product of cycles. The transposition has sign -1 while the cycles of length 3 have sign $+1$. Even though the cycles are not disjoint, $\operatorname{sgn}(\pi) = 1 \cdot (-1) \cdot 1 = -1$.

Theorem The symmetric group S_n is generated by two permutations: $\tau = (1\ 2)$ and $\pi = (1\ 2\ 3\ \dots\ n)$.

Proof: Let $H = \langle \tau, \pi \rangle$. We have to show that $H = S_n$.

First we obtain that $\alpha = \tau\pi = (2\ 3\ \dots\ n)$. Then we observe that $\sigma(1\ 2)\sigma^{-1} = (\sigma(1)\ \sigma(2))$ for any permutation σ.
In particular, $(1\ k) = \alpha^{k-2}(1\ 2)(\alpha^{k-2})^{-1}$ for $k = 2, 3 \dots, n$.
It follows that the subgroup H contains all transpositions of the form $(1\ k)$.

Further, for any integers $2 \le k < m \le n$ we have $(k\ m) = (1\ k)(1\ m)(1\ k)$. Therefore the subgroup H contains all transpositions. Finally, every permutation in S_n is a product of transpositions, therefore it is contained in H.
Thus $H = S_n$.

Remark. Although the group S_n is generated by two elements, its subgroups need not be generated by two elements.

Alternating groups

Given an integer $n \geq 2$, the **alternating group** on n symbols, denoted A_n or $A(n)$, is the set of all even permutations in the symmetric group S_n.

Theorem The alternating group A_n is a subgroup of the symmetric group S_n.

In other words, the product of even permutations is even, the identity function is an even permutation, and the inverse of an even permutation is even.

Theorem The alternating group A_n has $n!/2$ elements.

Proof: Consider the function $F : A_n \to S_n \setminus A_n$ given by $F(\pi) = (1\ 2)\pi$. One can observe that F is bijective. Hence the sets A_n and $S_n \setminus A_n$ have the same number of elements.

Examples. • The alternating group A_3 has 3 elements: the identity function and two cycles of length 3, $(1\ 2\ 3)$ and $(1\ 3\ 2)$.

• The alternating group A_4 has 12 elements of the following **cycle shapes**: id, $(1\ 2\ 3)$, and $(1\ 2)(3\ 4)$.

• The alternating group A_5 has 60 elements of the following cycle shapes: id, $(1\ 2\ 3)$, $(1\ 2)(3\ 4)$, and $(1\ 2\ 3\ 4\ 5)$.