MATH 433

Applied Algebra

Lecture 19:
Order and sign of a permutation.
Alternating group.

Order of a permutation

Theorem Let π be a permutation. Then there is a positive integer m such that $\pi^m = \mathrm{id}$.

The **order** of a permutation π, denoted $o(\pi)$, is defined as the smallest positive integer m such that $\pi^m = \mathrm{id}$.

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 r is divisible by m.

Theorem If a permutation π is a cycle, then the order $o(\pi)$ equals the length of the cycle.

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_X. 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_X. 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) $o(\pi\sigma) = \mathrm{lcm}\big(o(\pi), o(\sigma)\big)$.

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

Examples

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

The cycle decomposition is $\pi = (1\ 2\ 4\ 9\ 3\ 7\ 5)(6\ 12\ 8\ 11)$ or $\pi = (1\ 2\ 4\ 9\ 3\ 7\ 5)(6\ 12\ 8\ 11)(10)$. It follows that $o(\pi) = \mathrm{lcm}(7, 4) = \mathrm{lcm}(7, 4, 1) = 28$.

- $\sigma = (1\ 2)(3\ 4)(5\ 6)$.

This permutation is a product of three disjoint transpositions. Therefore the order of σ equals $\mathrm{lcm}(2, 2, 2) = 2$.

- $\tau = (1\ 2)(1\ 3)(1\ 4)(1\ 5)$.

The permutation is given as a product of transpositions. However, the transpositions are not disjoint and so this representation does not help to find the order of τ. The cycle decomposition is $\tau = (5\ 4\ 3\ 2\ 1)$. Hence τ is a cycle of length 5 so that $o(\tau) = 5$.

Sign of a permutation

Theorem 1 **(i)** Any permutation of $n \geq 2$ elements is a product of transpositions. **(ii)** If $\pi = \tau_1 \tau_2 \ldots \tau_k = \tau'_1 \tau'_2 \ldots \tau'_m$, where τ_i, τ'_j are transpositions, then the numbers k 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 $\pi, \sigma \in S_X$.
(ii) $\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi)$ for any $\pi \in S_X$.
(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.

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

Alternating group

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 (i) For any two permutations $\pi, \sigma \in A(n)$, the product $\pi\sigma$ is also in $A(n)$.
(ii) The identity function id is in $A(n)$.
(iii) For any permutation $\pi \in A(n)$, the inverse π^{-1} is in $A(n)$.

Theorem The alternating group $A(n)$ has $n!/2$ elements.

Proof: Consider a function $F : S(n) \to S(n)$ given by $F(\pi) = (1\ 2)\pi$. Note that F is bijective (indeed, $F^{-1} = F$). Hence $|F(E)| = |E|$ for any set $E \subset S(n)$. We observe that $F\big(A(n)\big) \subset S(n) \setminus A(n)$ and $F\big(S(n) \setminus A(n)\big) \subset A(n)$. Therefore $|A(n)| \leq |S(n) \setminus A(n)|$ and $|S(n) \setminus A(n)| \leq |A(n)|$ so that $|A(n)| = |S(n) \setminus A(n)| = |S(n)|/2 = n!/2$.

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 $(1\ 2\ 3\ 4\ 5)$.