Lecture 11: Order and sign of a permutation.
Permutations

Let $X$ be a finite set. A permutation of $X$ is a bijection from $X$ to itself.

Two-row notation. $\pi = \left( \begin{array}{ccc} a & b & c & \ldots \\ \pi(a) & \pi(b) & \pi(c) & \ldots \end{array} \right)$, where $a, b, c, \ldots$ is a list of all elements in the domain of $\pi$.

The set of all permutations of a finite set $X$ is called the symmetric group on $X$. Notation: $S_X$, $\Sigma_X$, $\text{Sym}(X)$.

The set of all permutations of $\{1, 2, \ldots, n\}$ is called the symmetric group on $n$ symbols and denoted $S(n)$ or $S_n$.

Given two permutations $\pi$ and $\sigma$, the composition $\pi \sigma$ is called the product of these permutations. In general, $\pi \sigma \neq \sigma \pi$, i.e., multiplication of permutations is not commutative.
Cycles

A permutation $\pi$ of a set $X$ is called a **cycle** (or **cyclic**) of length $r$ if there exist $r$ distinct elements $x_1, x_2, \ldots, x_r \in X$ such that

$$
\pi(x_1) = x_2, \ \pi(x_2) = x_3, \ldots, \ \pi(x_{r-1}) = x_r, \ \pi(x_r) = x_1,
$$

and $\pi(x) = x$ for any other $x \in X$.

**Notation.**  $\pi = (x_1 \ x_2 \ \ldots \ x_n)$.

The identity function is (the only) cycle of length 1. Any cycle of length 2 is called a **transposition**. An **adjacent transposition** is a transposition of the form $(k \ k+1)$.

The inverse of a cycle is also a cycle of the same length. Indeed, if $\pi = (x_1 \ x_2 \ \ldots \ x_n)$, then $\pi^{-1} = (x_n \ x_{n-1} \ \ldots \ x_2 \ x_1)$. 
Cycle decomposition

Let $\pi$ be a permutation of $X$. We say that $\pi$ moves an element $x \in X$ if $\pi(x) \neq x$. Otherwise $\pi$ fixes $x$.

Two permutations $\pi$ and $\sigma$ are called disjoint if the set of elements moved by $\pi$ is disjoint from the set of elements moved by $\sigma$.

**Theorem** Any permutation can be expressed as a product of disjoint cycles. This cycle decomposition is unique up to rearrangement of the cycles involved.

**Examples.**
- $(1 \ 2)(2 \ 3)(3 \ 4)(4 \ 5)(5 \ 6) = (1 \ 2 \ 3 \ 4 \ 5 \ 6)$.
- $(1 \ 2)(1 \ 3)(1 \ 4)(1 \ 5) = (1 \ 5 \ 4 \ 3 \ 2)$.
- $(2 \ 4 \ 3)(1 \ 2)(2 \ 3 \ 4) = (1 \ 4)$. 
Powers of a permutation

Let \( \pi \) be a permutation. The positive powers of \( \pi \) are defined inductively:

\[
\pi^1 = \pi \quad \text{and} \quad \pi^{k+1} = \pi \cdot \pi^k \quad \text{for every integer} \quad k \geq 1.
\]

The negative powers of \( \pi \) are defined as the positive powers of its inverse: \( \pi^{-k} = (\pi^{-1})^k \) for every positive integer \( k \).

Finally, we set \( \pi^0 = \text{id} \).

**Theorem** Let \( \pi \) be a permutation and \( r, s \in \mathbb{Z} \). Then

(i) \( \pi^r \pi^s = \pi^{r+s} \),
(ii) \( (\pi^r)^s = \pi^{rs} \),
(iii) \( (\pi^r)^{-1} = \pi^{-r} \).

**Idea of the proof:** First one proves the theorem for positive \( r, s \) by induction (induction on \( r \) for (i) and (iii), induction on \( s \) for (ii)). Then the general case is reduced to the case of positive \( r, s \).
**Theorem**  Let $\pi$ be a permutation. Then there is a positive integer $m$ such that $\pi^m = \text{id}$.

**Proof:**  Consider the list of powers: $\pi, \pi^2, \pi^3, \ldots$. Since there are only finitely many permutations of any finite set, there must be repetitions within the list. Assume that $\pi^r = \pi^s$ for some $0 < r < s$. Then $\pi^{s-r} = \pi^s \pi^{-r} = \pi^s (\pi^r)^{-1} = \text{id}$.

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

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

**Theorem**  Let $\pi$ be a cyclic permutation. Then the order $o(\pi)$ is the length of the cycle $\pi$. 
Examples. \( \bullet \pi = (1 \ 2 \ 3 \ 4 \ 5) \).

\( \pi^2 = (1 \ 3 \ 5 \ 2 \ 4) \), \( \pi^3 = (1 \ 4 \ 2 \ 5 \ 3) \),
\( \pi^4 = (1 \ 5 \ 4 \ 3 \ 2) \), \( \pi^5 = \text{id} \).

\[ \implies o(\pi) = 5. \]

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

\( \sigma^2 = (1 \ 3 \ 5)(2 \ 4 \ 6) \), \( \sigma^3 = (1 \ 4)(2 \ 5)(3 \ 6) \),
\( \sigma^4 = (1 \ 5 \ 3)(2 \ 6 \ 4) \), \( \sigma^5 = (1 \ 6 \ 5 \ 4 \ 3 \ 2) \), \( \sigma^6 = \text{id} \).

\[ \implies o(\sigma) = 6. \]

\( \bullet \tau = (1 \ 2 \ 3)(4 \ 5) \).

\( \tau^2 = (1 \ 3 \ 2) \), \( \tau^3 = (4 \ 5) \), \( \tau^4 = (1 \ 2 \ 3) \),
\( \tau^5 = (1 \ 3 \ 2)(4 \ 5) \), \( \tau^6 = \text{id} \).

\[ \implies o(\tau) = 6. \]
Lemma 1 Let $\pi$ and $\sigma$ be two commuting permutations: $\pi\sigma = \sigma\pi$. Then

(i) the powers $\pi^r$ and $\sigma^s$ 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 $\pi$ and $\sigma$ be disjoint permutations in $S(n)$. Then (i) they commute: $\pi\sigma = \sigma\pi$,
(ii) $(\pi\sigma)^r = \text{id}$ if and only if $\pi^r = \sigma^r = \text{id}$,
(iii) $o(\pi\sigma) = \text{lcm}(o(\pi), o(\sigma))$.

Idea of the proof: The set $\{1, 2, \ldots, n\}$ splits into 3 subsets: elements moved by $\pi$, elements moved by $\sigma$, and elements fixed by both $\pi$ and $\sigma$. All three sets are invariant under $\pi$ and $\sigma$.

Theorem Let $\pi \in S(n)$ and suppose that $\pi = \sigma_1\sigma_2\ldots\sigma_k$ is a decomposition of $\pi$ as a product of disjoint cycles. Then the order of $\pi$ is the least common multiple of the lengths of cycles $\sigma_1, \ldots, \sigma_k$. 
Sign of a permutation

**Theorem 1**  Given an integer $n \geq 1$, there exists a unique function $\text{sgn} : S(n) \to \{-1, 1\}$ such that

- $\text{sgn}(\pi \sigma) = \text{sgn}(\pi) \text{sgn}(\sigma)$ for all $\pi, \sigma \in S(n)$,
- $\text{sgn}(\tau) = -1$ for any transposition $\tau \in S(n)$.

The value of the function $\text{sgn}$ on a particular permutation $\pi \in S(n)$ is called the **sign** of $\pi$.

If $\text{sgn}(\pi) = 1$, then $\pi$ is said to be an **even** permutation.
If $\text{sgn}(\pi) = -1$, then $\pi$ is an **odd** permutation.

**Theorem 2 (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 $\tau_i, \tau_j'$ are transpositions, then the numbers $n$ and $m$ are of the same parity.

*Remark.* Theorem 1 follows from Theorem 2. Indeed, we let $\text{sgn}(\pi) = 1$ if $\pi$ is a product of an even number of transpositions and $\text{sgn}(\pi) = -1$ if $\pi$ is a product of an odd number of transpositions.
Definition of determinant

**Definition.** \( \det (a) = a, \)

\[
\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc,
\]

\[
\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - \\
- a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}.
\]

If \( A = (a_{ij}) \) is an \( n \times n \) matrix then

\[
\det A = \sum_{\pi \in S(n)} \text{sgn}(\pi) \ a_{1,\pi(1)} \ a_{2,\pi(2)} \cdots \ a_{n,\pi(n)},
\]

where \( \pi \) runs over all permutations of \( \{1, 2, \ldots, n\} \).