MATH 433

Applied Algebra

Lecture 12:
Sign of a permutation (continued).
Abstract groups.

Permutations

Let X be a finite set. A **permutation** of X is a bijection from X to itself. The set of all permutations of $\{1, 2, \ldots, n\}$ is called the **symmetric group** on n symbols and denoted $S(n)$.

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

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 $\pi \in S(n)$ 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.

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 $\tau_1, \tau_2, \dots, \tau_k$ be adjacent transpositions. Then **(i)** for any $\pi \in S(n)$ the numbers k and $N(\tau_1\tau_2 \dots \tau_k\pi) - N(\pi)$ are of the same parity,
(ii) the numbers k and $N(\tau_1\tau_2 \dots \tau_k)$ 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 $N(\pi)$.

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

$$\det A = \sum_{\pi \in S(n)} \operatorname{sgn}(\pi)\, a_{1,\pi(1)}\, a_{2,\pi(2)} \dots a_{n,\pi(n)},$$

where π runs over all permutations of $\{1, 2, \dots, n\}$.

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 $A(n)$.

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. It follows that 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 $(1\ 2\ 3\ 4\ 5)$.

Abstract groups

Definition. A **group** is a set G, together with a binary operation $*$, that satisfies the following axioms:

(G1: closure)
for all elements g and h of G, $g * h$ is an element of G;

(G2: associativity)
$(g * h) * k = g * (h * k)$ for all $g, h, k \in G$;

(G3: existence of identity)
there exists an element $e \in G$, called the **identity** (or **unit**) of G, such that $e * g = g * e = g$ for all $g \in G$;

(G4: existence of inverse)
for every $g \in G$ there exists an element $h \in G$, called the **inverse** of g, such that $g * h = h * g = e$.

The group $(G, *)$ is said to be **commutative** (or **Abelian**) if it satisfies an additional axiom:

(G5: commutativity) $g * h = h * g$ for all $g, h \in G$.

Basic examples. • Real numbers $\mathbb{R}$ with addition.

(G1) $x, y \in \mathbb{R} \implies x + y \in \mathbb{R}$

(G2) $(x + y) + z = x + (y + z)$

(G3) the identity element is 0 as $x + 0 = 0 + x = x$

(G4) the inverse of x is $-x$ as $x + (-x) = (-x) + x = 0$

(G5) $x + y = y + x$

• Nonzero real numbers $\mathbb{R} \setminus \{0\}$ with multiplication.

(G1) $x \neq 0$ and $y \neq 0 \implies xy \neq 0$

(G2) $(xy)z = x(yz)$

(G3) the identity element is 1 as $x1 = 1x = x$

(G4) the inverse of x is x^{-1} as $xx^{-1} = x^{-1}x = 1$

(G5) $xy = yx$

The two basic examples give rise to two kinds of notation for a general group $(G, *)$.

Multiplicative notation: We think of the group operation $*$ as some kind of multiplication, namely,

- $a * b$ is denoted ab,
- the identity element is denoted 1,
- the inverse of g is denoted g^{-1}.

Additive notation: We think of the group operation $*$ as some kind of addition, namely,

- $a * b$ is denoted $a + b$,
- the identity element is denoted 0,
- the inverse of g is denoted $-g$.

Remark. The additive notation is used **only** for commutative groups.

More examples

- Integers $\mathbb{Z}$ with addition.
- $\mathbb{Z}_n$, i.e., congruence classes modulo n, with addition.
- G_n, i.e., invertible congruence classes modulo n, with multiplication.
- Permutations $S(n)$ with composition ($=$ multiplication).
- Even permutations $A(n)$ with multiplication.
- Any vector space V with addition.
- Invertible $n \times n$ matrices with multiplication.