MATH 415

Modern Algebra I

Lecture 8:
Sign of a permutation (continued).
Classical definition of the determinant.
Cosets. Langrange's theorem.

Sign of a permutation

Theorem 1 (i) Any permutation of $n \geq 2$ elements is a product of transpositions. **(ii)** If $\pi = \tau_1 \tau_2 \dots \tau_k = \tau_1' \tau_2' \dots \tau_m'$, 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 $\pi, \sigma \in S_n$.
(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 $N(\pi)$.

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

Classical definition of the determinant

Definition. $\det(a) = a, \quad \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc,$

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

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 $\{1, 2, \dots, n\}$.

Theorem $\det A^T = \det A$.

Proof: Let $A = (a_{ij})_{1\le i,j\le n}$. Then $A^T = (b_{ij})_{1\le i,j\le n}$, where $b_{ij} = a_{ji}$. We have

$$\begin{aligned}
\det A^T &= \sum_{\pi\in S_n} \operatorname{sgn}(\pi)\, b_{1,\pi(1)}\, b_{2,\pi(2)} \dots b_{n,\pi(n)} \\
&= \sum_{\pi\in S_n} \operatorname{sgn}(\pi)\, a_{\pi(1),1}\, a_{\pi(2),2} \dots a_{\pi(n),n} \\
&= \sum_{\pi\in S_n} \operatorname{sgn}(\pi)\, a_{1,\pi^{-1}(1)}\, a_{2,\pi^{-1}(2)} \dots a_{n,\pi^{-1}(n)}.
\end{aligned}$$

When π runs over all permutations of $\{1, 2, \dots, n\}$, so does $\sigma = \pi^{-1}$. It follows that

$$\begin{aligned}
\det A^T &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma^{-1})\, a_{1,\sigma(1)}\, a_{2,\sigma(2)} \dots a_{n,\sigma(n)} \\
&= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)\, a_{1,\sigma(1)}\, a_{2,\sigma(2)} \dots a_{n,\sigma(n)} = \det A.
\end{aligned}$$

Theorem 1 Suppose A is a square matrix and B is obtained from A by exchanging two rows. Then $\det B = -\det A$.

Theorem 2 Suppose A is a square matrix and B is obtained from A by permuting its rows. Then $\det B = \det A$ if the permutation is even and $\det B = -\det A$ if the permutation is odd.

Proof: Let $A = (a_{ij})_{1 \le i,j \le n}$ be an $n \times n$ matrix. Suppose that a matrix B is obtained from A by permuting its rows according to a permutation $\sigma \in S_n$. Then $B = (b_{ij})_{1 \le i,j \le n}$, where $b_{\sigma(i),j} = a_{ij}$. Equivalently, $b_{ij} = a_{\sigma^{-1}(i),j}$. We have

$$\det B = \sum_{\pi \in S_n} \operatorname{sgn}(\pi)\, b_{1,\pi(1)}\, b_{2,\pi(2)} \dots b_{n,\pi(n)}$$

$$= \sum_{\pi \in S_n} \operatorname{sgn}(\pi)\, a_{\sigma^{-1}(1),\pi(1)}\, a_{\sigma^{-1}(2),\pi(2)} \dots a_{\sigma^{-1}(n),\pi(n)}$$

$$= \sum_{\pi \in S_n} \operatorname{sgn}(\pi)\, a_{1,\pi\sigma(1)}\, a_{2,\pi\sigma(2)} \dots a_{n,\pi\sigma(n)}.$$

When π runs over all permutations of $\{1, 2, \dots, n\}$, so does $\tau = \pi\sigma$. It follows that

$$\det B = \sum_{\tau \in S_n} \operatorname{sgn}(\tau\sigma^{-1})\, a_{1,\tau(1)}\, a_{2,\tau(2)} \dots a_{n,\tau(n)}$$

$$= \operatorname{sgn}(\sigma^{-1}) \sum_{\tau \in S_n} \operatorname{sgn}(\tau)\, a_{1,\tau(1)}\, a_{2,\tau(2)} \dots a_{n,\tau(n)} = \operatorname{sgn}(\sigma) \det A.$$

The Vandermonde determinant

Definition. The **Vandermonde determinant** is the determinant of the following matrix

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \cdots & x_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix},$$

where $x_1, x_2, \dots, x_n \in \mathbb{R}$. Equivalently, $V = (a_{ij})_{1 \le i,j \le n}$, where $a_{ij} = x_i^{j-1}$.

Theorem

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \cdots & x_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Corollary Consider a polynomial

$$p(x_1, x_2, \dots, x_n) = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Then

$$p(x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(n)}) = \operatorname{sgn}(\pi)\, p(x_1, x_2, \dots, x_n)$$

for any permutation $\pi \in S_n$.

Cosets

Definition. Let H be a subgroup of a group G. A **coset** (or **left coset**) of the subgroup H in G is a set of the form $aH = \{ah \mid h \in H\}$, where $a \in G$. Similarly, a **right coset** of H in G is a set of the form $Ha = \{ha \mid h \in H\}$, where $a \in G$.

Theorem Let H be a subgroup of G and define a relation R on G by $aRb \iff a \in bH$. Then R is an equivalence relation.

Proof: We have aRb if and only if $b^{-1}a \in H$.
Reflexivity: aRa since $a^{-1}a = e \in H$.
Symmetry: $aRb \implies b^{-1}a \in H \implies a^{-1}b = (b^{-1}a)^{-1} \in H \implies bRa$. **Transitivity**: aRb and $bRc \implies b^{-1}a, c^{-1}b \in H \implies c^{-1}a = (c^{-1}b)(b^{-1}a) \in H \implies aRc$.

Corollary The cosets of the subgroup H in G form a partition of the set G.

Proof: Since R is an equivalence relation, its equivalence classes partition the set G. Clearly, the equivalence class of g is gH.

Examples of cosets

- $G = \mathbb{Z}$, $H = n\mathbb{Z}$.

The coset of $a \in \mathbb{Z}$ is $a + n\mathbb{Z}$, the congruence class of a modulo n (all integers b such that $b \equiv a \bmod n$).

- $G = \mathbb{R}^3$, H is the plane $x + 2y - z = 0$.

H is a subgroup of G since it is a subspace. The coset of $(x_0, y_0, z_0) \in \mathbb{R}^3$ is the plane $x + 2y - z = x_0 + 2y_0 - z_0$ parallel to H.

- $G = S_n$, $H = A_n$.

There are only 2 cosets, the set of even permutations A_n and the set of odd permutations $S_n \setminus A_n$.

- G is any group, $H = G$.

There is only one coset, G.

- G is any group, $H = \{e\}$.

Each element of G forms a separate coset.

Lagrange's Theorem

The number of elements in a group G is called the **order** of G and denoted $|G|$. Given a subgroup H of G, the number of cosets of H in G is called the **index** of H in G and denoted $(G : H)$.

Theorem (Lagrange) If H is a subgroup of a finite group G, then $|G| = (G : H) \cdot |H|$. In particular, the order of H divides the order of G.

Proof: For any $a \in G$ define a function $f : H \to aH$ by $f(h) = ah$. By definition of aH, this function is surjective. Also, it is injective due to the left cancellation property:
$f(h_1) = f(h_2) \implies ah_1 = ah_2 \implies h_1 = h_2$.
Therefore f is bijective. It follows that the number of elements in the coset aH is the same as the order of the subgroup H. Since the cosets of H in G partition the set G, the theorem follows.

Corollaries of Lagrange's Theorem

Corollary 1 If G is a finite group, then the order $o(g)$ of any element $g \in G$ divides the order of G.

Proof: The order of $g \in G$ is the same as the order of the cyclic group $\langle g \rangle$, which is a subgroup of G.

Corollary 2 If G is a finite group, then $g^{|G|} = e$ for all $g \in G$.

Proof: We have $g^n = e$ whenever n is a multiple of $o(g)$. By Corollary 1, $|G|$ is a multiple of $o(g)$ for all $g \in G$.

Corollary 3 Any group G of prime order p is cyclic.

Proof: Take any element $g \in G$ different from e. Then $o(g) \neq 1$, hence $o(g) = p$, and this is also the order of the cyclic subgroup $\langle g \rangle$. It follows that $\langle g \rangle = G$.

Corollary 4 Any group G of prime order has only two subgroups: the trivial subgroup and G itself.

Proof: If H is a subgroup of G then $|H|$ divides $|G|$.
Since $|G|$ is prime, we have $|H| = 1$ or $|H| = |G|$.
In the former case, H is trivial. In the latter case, $H = G$.

Corollary 5 The alternating group A_n, $n \geq 2$, consists of $n!/2$ elements.

Proof: Indeed, A_n is a subgroup of index 2 in the symmetric group S_n. The latter consists of $n!$ elements.

Theorem Let G be a cyclic group of finite order n. Then for any divisor d of n there exists a unique subgroup of G of order d, which is also cyclic.

Proof: Let g be the generator of the cyclic group G. Take any divisor d of n. Since the order of g is n, it follows that the element $g^{n/d}$ has order d. Therefore a cyclic group $H = \langle g^{n/d} \rangle$ has order d.

Now assume H' is another subgroup of G of order d. The group H' is cyclic since G is cyclic. Hence $H' = \langle g^k \rangle$ for some $k \in \mathbb{Z}$. Since the order of the element g^k is d while the order of g is n, it follows that $\gcd(n, k) = n/d$. We know that $\gcd(n, k) = an + bk$ for some $a, b \in \mathbb{Z}$. Then $g^{n/d} = g^{an+bk} = g^{na} g^{kb} = (g^n)^a (g^k)^b = (g^k)^b \in \langle g^k \rangle = H'$. Consequently, $H = \langle g^{n/d} \rangle \subset H'$. However H and H' both consist of d elements. Thus $H' = H$.