Lecture 09: Sign function

Thursday, October 25, 2018 8:38 AM

Recall. \( \Delta(x_1, \ldots, x_n) := \prod_{i < j} (x_i - x_j) \) and

\[
\Delta_\sigma(x_1, \ldots, x_n) := \Delta(x_{\sigma(i)_1}, \ldots, x_{\sigma(i)_n}) = \prod_{i < j} (x_{\sigma(i)_1} - x_{\sigma(i)_j})
\]

We showed \( \prod_{i \neq j} (x_i - x_j) = (-1)^{\frac{n(n-1)}{2}} \Delta^2 \), and so

\[
\Delta_\sigma = \prod_{i \neq j} (x_{\sigma(i)_1} - x_{\sigma(i)_j}) = \prod_{i \neq j} (x_i - x_j) = (-1)^{\frac{n(n-1)}{2}} \Delta^2.
\]

Therefore, \( \exists \epsilon : S_n \rightarrow \{ \pm 1 \}, \Delta_\sigma \epsilon = \epsilon(\sigma) \Delta \).

**Lemma.** \( \epsilon \) is a group homomorphism.

**Proof.** \( \Delta_\sigma^\tau(x_1, \ldots, x_n) = \Delta(x_{\sigma^\tau(i)_1}, \ldots, x_{\sigma^\tau(i)_n}) \)

\[
\Delta^\tau(x_{\sigma(i)_1}, \ldots, x_{\sigma(i)_n})
\]

\( y_i = x_{\sigma(i)_1} \Rightarrow \Delta^\tau(y_1, \ldots, y_n) = (y_{\sigma(i)_1}, \ldots, y_{\sigma(i)_n}) \)

and \( y_{\sigma^\tau(i)_j} = x_{\sigma^\tau(i)_j} \).

\[
\epsilon(\tau) \Delta(x_{\sigma(i)_1}, \ldots, x_{\sigma(i)_n})
\]

\( \Rightarrow \epsilon(\sigma^\tau) \Delta = \epsilon(\tau) \epsilon(\sigma^\tau) \Delta \Rightarrow \epsilon(\sigma^\tau) = \epsilon(\sigma) \epsilon(\tau). \)

**Def.** \( \epsilon \) is called the sign function.
Sometimes \( e \) is denoted by \( \text{sgn} \).

Notice that \( \Delta_\sigma = \prod_{1 \leq i < j \leq n} (\sigma_\circ(i) - \sigma_\circ(j)) \)

\[ = (-1)^{\eta_\sigma} \Delta \quad \text{where} \]

\[ \eta_\sigma := \frac{q(i,j)}{2} \mid i < j \text{ and } \sigma(i) > \sigma(j) \gtrless \text{, so } \eta_\sigma \text{ is the # of crossings in} \]

\[
\begin{array}{cccccc}
1 & 2 & \ldots & i & j & \ldots & n \\
i & 2 & \ldots & \sigma(c) & 0 & \ldots & \sigma(c) \\
\end{array}
\]

In the theory of root systems it is proved that \( \eta_\sigma = l(\sigma) \)

where \( l(\sigma) \) is the word metric of \( \sigma \) w.r.t. the generating set \( \frac{q}{2}(1 2), (2 3), \ldots, (n-1 \ n) \gtrless \).

One can use "box of signs" to understand \( \eta_\sigma \) as well:

permute rows & columns according to \( \sigma \)

\[ \eta_\sigma \text{ is # of - that go to the upper half.} \]

Lemma \( n(a\ b) = 2(b-a) - 1 \).

If in class we used "box of signs" to study this, here I use crossing #:

\[ 2(b-a-1) + 1 \]

\[
\begin{array}{cccccccccccc}
1 & a-1 & a & a+1 & b-1 & b & b+1 & \ldots & n \\
a-1 & a & a+1 & \ldots & b-1 & b & b+1 & \ldots & n \\
\end{array}
\]
Theorem. (a) Suppose \( \tau_1, \ldots, \tau_m \) and \( \sigma_1, \ldots, \sigma_n \) are transpositions and 
\[ \tau_1 \cdots \tau_m = \sigma_1 \cdots \sigma_n ; \] then \( m \equiv n \pmod{2} \).

(b) \( \ker \varepsilon = \{ \sigma \in S_n \mid \sigma \text{ can be written as a product of even } \# \text{ of transpositions.} \}

Proof. (a) \( \tau_1 \cdots \tau_m = \sigma_1 \cdots \sigma_n \Rightarrow \varepsilon(\tau_1 \cdots \tau_m) = \varepsilon(\sigma_1 \cdots \sigma_n) \)
\[ \otimes \]
By the previous lemma, \( \varepsilon(a b) = (\varepsilon 1) = -1 \). And so
\[ \otimes \implies (\varepsilon 1)^m = (-1)^n \; \text{ therefore } m \equiv n \pmod{2} \).

(b) \( \sigma \in \ker \varepsilon \) can be written as a product of transpositions 
\( \tau_1, \ldots, \tau_m \). So \( 1 = \varepsilon(\sigma) = \varepsilon(\tau_1 \cdots \tau_m) = (\varepsilon 1)^m \); and so
\( m \) is even. By a similar argument \( LHS \geq RHS \). \( \blacksquare \)

A nice application of parity of permutations is on possible patterns in a 15-puzzle. In a 15-puzzle, there are

15 small squares (numbered) and an empty spot.

\[
\begin{array}{ccc}
1 & 2 & 3 \\
5 & 6 & 7 \\
9 & 10 & 11 \\
13 & 14 & 15 \\
\end{array}
\]

And one can use the empty spot to move around numbers. \( \blacksquare \) Can one reach to the
Following pattern \[
\begin{array}{cccc}
1 & 2 & 3 & 4 \\
5 & 6 & 7 & 8 \\
9 & 10 & 11 & 12 \\
13 & 14 & 15 & 16
\end{array}
\] ? The answer is No! Let's number the empty spot 16; and think about any possible pattern as an element of $S_{16}$. Notice any move $\uparrow, \downarrow, \leftarrow, \rightarrow$ can be viewed as a transposition that involves 16. If we reach to the new pattern, 16 is moved back to its initial position. So $\# \, \uparrow$'s = $\# \, \downarrow$'s and $\# \, \rightarrow$'s = $\# \, \leftarrow$'s. Therefore it should be an even permutation of $S_{16}$; so it cannot be $(14 \ 15)$. □

Def. ker $e$ is called Alternating group; and it is denoted by $A_n$. Elements of $A_n$ are called even and elements of $S_n \setminus A_n$ are called odd.

Observe. $A_n \leq S_n$ and $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$ if $n \geq 2$.

Next we will show that $A_n$ is simple if $n \geq 5$. We start with a few lemmas.
Lemma 1. \( A_n \) is generated by 3-cycles.

\[ \text{Proof.} \] Since any element of \( A_n \) is a product of even number of transpositions, it is enough to write a product of two transpositions as a product of 3-cycles. Now notice:

\[ (a \ b) (a \ b) = I; \quad (a \ b)(b \ c) = (a \ b \ c); \]

\[ (a \ b)(c \ d) = (a \ b)(b \ c)(b \ c)(c \ d) = (a \ b \ c)(b \ c \ d); \]

And \( (a \ b \ c) = (a \ b)(b \ c) \in A_n \). \[ \blacksquare \]

Lemma 2. \( N \triangleleft A_n \), \( n \geq 5 \), and \( N \) contains a 3-cycle. Then \( N = A_n \).

\[ \text{Proof.} \] Suppose \( \tau_1 \) and \( \tau_2 \) are two 3-cycles. So \( \exists \sigma \in S_n \) s.t. \( \sigma \tau_1 \sigma^{-1} = \tau_2 \). Since \( |\text{Supp } \tau_1| = 3 \) and \( n \geq 5 \), \( \exists a, b \) s.t.

\[ a, b \not\in \text{Supp } \tau_1 = \emptyset. \] Hence \( (a \ b) \tau_1 (a \ b) = \tau_1 \), and so \( (\sigma (a \ b)) \tau_1 ((\sigma (a \ b))^{-1} = \tau_2 \). Either \( \sigma \in A_n \) or \( \sigma (a \ b) \in A_n \), which implies \( \tau_2 \) is a conjugate of \( \tau_1 \) in \( A_n \).

Since \( N \triangleleft A_n \) and it contains a 3-cycle \( \tau \), all the
conjugates of \( C \) are in \( N \); and so all 3-cycles are \( A_n \).

And claim follows from Lemm 1.

Lemma 3. \( A_5 \) is simple; that means there is no \( \varphi : N \not
A_5 \).

Proof. Suppose to the contrary that \( \exists \varphi : N \not
A_5 \).

Case 1. \( 3 \mid |N| \).

In this case \( N \) has an element of order 3.

The cycle type of an element of order \( p \) is

\[
p \geq p^2 \geq 2p \geq 12 \cdots 21.
\]

So the only possible cycle type of this element is \( 3 \geq 1 \geq 1 \); this means \( N \) has a 3-cycle. Therefore by Lemm 2 \( N = A_5 \) which is a contradiction.

Case 2. \( 5 \mid |N| \), \( 3 \nmid |N| \).

In this case \( N \) has a subgroup of order 5. Since \( 5 \nmid |A_5| \), \( N \) has a Sylow 5-subgroup of \( A_5 \) as a subgroup. Therefore all the Sylow 5-subgps of \( A_5 \) are subgps of \( N \). Hence all
elements of order 5 are in $N$. The cycle type of an element of order 5 in $S_5$ is 5; that means it is a 5-cycle. Number of 5-cycles is $\frac{5!}{5} = 24$; and so $|N| \geq 25$. As $|N| \mid 60$, we deduce $|N| = 30$; this implies $3 \mid |N|$ which is a contradiction.

Case 3. $3 \nmid |N|, 5 \nmid |N| \implies |N| \mid 4$.

$|N| \mid 60$

$N$ has an element of order 2. Possible cycle types of an element of order 2 are $2 \geq 1 \geq 1 \geq 1$ and $2 \geq 2 \geq 1$.

Since the first type gives us an odd permutation and $N \subseteq A_5$, $\exists$ an element of the form $(a\ b)(c\ d)$ in $N$. After reordering we can assume $(1\ 2)(3\ 4) \in N$; and so

$$\sigma(1\ 2\ 3)^{-1} = (2\ 3)(1\ 4) \in N,$$

$$\sigma(1\ 3\ 2)^{-1} = (3\ 1)(2\ 4) \in N,$$

which is a contradiction.
Theorem. $A_n$ is simple if $n \geq 5$.

Proof. We proceed by induction on $n$. We have already proved the base of induction. Next we will prove the induction step for $n \geq 6$. Let $G_i := \{ \sigma \in A_n \mid \sigma(i) = i \}$. Notice that

$$G_i \rightarrow A_{n-1} \setminus \{i\} \quad \sigma \rightarrow \overline{\sigma} \quad \text{where} \quad \overline{\sigma}(j) = \sigma(j) \text{ for } j \neq i.$$

are group homomorphisms that are inverse of each other.

So $G_i \cong A_{n-1}$ for any $1 \leq i \leq n$. So by the induction hypothesis $G_i$'s are simple. Suppose $I \neq N \neq A_n$. Then $N G_i < G_i$ for any $i$. Since $G_i$ is simple, either $G_i \cap N = G_i$ or $G_i \cap N = \{I\}$. If $G_i \cap N = G_i$, then $N$ contains a 3-cycle.

Lemma 2 implies $N = A_n$ which is a contradiction. So for any $i$, $G_i \cap N = I$; that means $\forall \overline{\sigma} \in N, \forall i, \overline{\sigma}(i) \neq i$. Hence

$$\forall \sigma \neq I \in N, \forall i, \overline{\sigma}(i) \neq \overline{\sigma}(i).$$

Next we will find two elements of $N$ that violate $(\star)$. 


Lecture 09: $A_n$ is simple

Friday, October 26, 2018 1:16 PM

Suppose $\sigma \in \mathbb{N} \setminus I$ and $p_1 \geq p_2 \geq \ldots$ is its cycle type.

Case 1. $p_1 \geq 3$.

So $\sigma = (a \ b \ c \ \ldots)(\ldots) \ldots \in \mathbb{N}$. Since $n \geq 6$, $\exists e, f, \frac{e}{p_1} \wedge \frac{f}{p_2} \wedge \frac{a}{b} \wedge \frac{c}{d} = \emptyset$. And so

$$(c \ e \ f) \sigma = (c \ e \ f)^{-1} = (a \ b \ e \ \ldots)(\ldots) \ldots \in \mathbb{N}$$

$\sigma''$

and $\sigma'(a) = \sigma''(a) = b$, which contradicts $\sigma$. $\sigma' \neq \sigma''$ as $\sigma(b) \neq \sigma''(b)$

Case 2. $p_1 = 2$

Since $\sigma \in A_n$, $p_2 = 2$; and so $\sigma = (a \ b)(c \ d)(\ldots) \ldots$

Since $n \geq 6$, $\exists e, f$, $\exists e \wedge \exists f \wedge \exists a, b, c, d = \emptyset$; and so

$$(d \ e \ f) \sigma = (d \ e \ f)^{-1} = (a \ b)(c \ e)(\ldots) \in \mathbb{N}$$

$\sigma''$

and $\sigma'(a) = \sigma''(a) = b$ and $\sigma' \neq \sigma''$ as $\sigma(c) \neq \sigma''(c)$, which contradicts $(\star)$. ■