MATH 2022  Linear and Abstract Algebra

LECTURE 09  Thursday 12/03/2020
Odd and even permutations

- Permutations of a finite set can be either even or odd, but not both.

- Many surprising applications
Transpositions:

A transposition is a permutation that interchanges two distinct letters $a$ and $b$, leaving all other letters unchanged, described in cycle notation by $(a \ b)$.

Fact: All cycles are products (composites) of transpositions, since

$$(a, a_2 \ldots a_n) = (a, a_2)(a, a_3) \ldots (a, a_n).$$
\[ (1 \ 2 \ 3) = (1 \ 2)(1 \ 3), \]
\[ (1 \ 2 \ 3) = (2 \ 3 \ 1) = (2 \ 3)(2 \ 1), \]
\[ (1 \ 2 \ 3 \ 4) = (1 \ 2)(1 \ 3)(1 \ 4), \]
\[ (5 \ 6 \ 3 \ 1 \ 4 \ 2) = (5 \ 6)(5 \ 3)(5 \ 1)(5 \ 4)(5 \ 2), \]
\[ (6 \ 3 \ 1 \ 4 \ 2 \ 5) = (6 \ 3)(6 \ 1)(6 \ 4)(6 \ 2)(6 \ 5). \]

**Corollary**: Every permutation of a finite set is a product (composite) of transpositions.
\[(1 2 3 4)(5 6 7) = (1 2)(1 3)(1 4)(5 6)(5 7),\]
\[(2 6 4)(3 2 1)(4 7 8 9 2)\]
\[= (2 6)(2 4)(3 2)(3 1)(4 7)(4 8)(4 9)(4 2).\]

Call a permutation **even** or **odd** according to whether it is a product of an even or an odd number of transpositions respectively.

**e.g.** \((1 2 3) = (1 2)(1 3)\) is even,
\((1 2 3 4) = (1 2)(1 3)(1 4)\) is odd,
\(1 = (2 3)(2 3)\) is even.
Call a permutation **even** or **odd** according to whether it is a product of an even or an odd number of transpositions respectively.

**E.g.** \( (1 \ 2 \ 3) = (1 \ 2)(1 \ 3) \) is even, 
\( (1 \ 2 \ 3 \ 4) = (1 \ 2)(1 \ 3)(1 \ 4) \) is odd, 
\( 1 = (2 \ 3)(2 \ 3) \) is even.
The single cycle
\[(a_1, a_2 \ldots a_n)\] is \(\ \star \) even if \(n\) is odd
odd if \(n\) is even.

Note that if
\[\alpha = \tau_1 \tau_2 \ldots \tau_{k-1} \tau_k\]
where \(\tau_1, \tau_2, \ldots, \tau_k\) are transpositions, then
\[\alpha^{-1} = \tau_k^{-1} \tau_{k-1}^{-1} \ldots \tau_2^{-1} \tau_1^{-1} = \tau_k \tau_{k-1} \ldots \tau_2 \tau_1,\]
so the parity of \(\alpha\) and \(\alpha^{-1}\) is the same.

evenness or oddness
Theorem: Every permutation of a finite set is even or odd, but not both.

difficult to prove, see later

Recall \( \text{Sym}(n) = \{ \text{all permutations of } \{1, \ldots, n\}\} \), which is a group under composition, called the symmetric group (on \( n \) letters).
Put
\[ \text{Alt}(n) = \{ \text{all even permutations of } \{1, \ldots, n\} \}, \]
called the alternating group (on \( n \) letters), which is also a group under composition.

- \( \text{Alt}(n) \) is a subgroup of \( \text{Sym}(n) \).

- If \( \alpha, \beta \in \text{Alt}(n) \) then \( \alpha \beta \in \text{Alt}(n) \).
$\text{Alt}(n)$ is a subgroup of $\text{Sym}(n)$.

Closed under composition

- if $\alpha, \beta \in \text{Alt}(n)$ then $\alpha \beta \in \text{Alt}(n)$.

$\alpha = \tau_1 \ldots \tau_k$, $\beta = \sigma_1 \ldots \sigma_l$

where $\tau_1, \ldots, \tau_k, \sigma_1, \ldots, \sigma_l$ are transpositions

and $k, l$ are even

$\Rightarrow \alpha \beta = \tau_1 \ldots \tau_k \sigma_1 \ldots \sigma_l$ product of $k+l$ transpositions, and $k+l$ is also even.
Common to write

$$S_n = \text{Sym}(n), \quad A_n = \text{Alt}(n).$$

E.g.,

$$S_2 = \{1, (12)\},$$

$$A_2 = \{1\},$$

$$S_3 = \{1, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\},$$

$$A_3 = \{1, (1\ 2\ 3), (1\ 3\ 2)\},$$

$$A_4 = \{1, (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (2\ 3\ 4),$$

$$(2\ 4\ 3), (1\ 3\ 4), (1\ 4\ 3), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$
Suppose \( n \geq 2 \).

The single transposition \((12)\) is odd, so \((12) \notin A_n\).

**Claim:** \( S_n = A_n \cup (12)A_n \)

where \( \cup \) denotes *disjoint union* (empty intersection) and

\[(12)A_n = \{ (12) \varphi \mid \varphi \in A_n \} \]

\[= \{ \text{odd permutations of } \{1, \ldots, n\}\} \]

**exercise**
Suppose \( n \geq 2 \). The single transposition \((12)\) is odd, so \((12) \in A_n\).

Claim: \( S_n = A_n \cup (12) A_n \)

- **even permutations**
  - form a **subgroup**

- **odd permutations**
  - form a **coset**, translation of a subgroup
\[ A_3 = \{ 1, (123), (132) \} \]
\[
(12) A_3 = \{ (12) 1, (12)(123), (12)(132) \}
= \{ (12), (13), (23) \}
\]
\[ A_4 = \{ 1, (123), (132), (142), (143), (134), (234), (243), (243), (12)(24), (13)(24), (14)(23) \} \]
\[
(12) A_4 = \{ (12) 1, (12)(123), (12)(152), (12)(124), (12)(142),
(12)(134), (12)(143), (12)(134), (12)(243),
(12)(12)(34), (12)(13)(24), (12)(14)(23) \}
= \{ (12), (13), (23), (14), (24), (1234), (1243), (1342),
(1432), (34), (1423), (1324) \} \]
Suppose $n \geq 2$.

The single transposition $(12)$ is odd, so

$(12) \not\in A_n$.

Claim: \[ S_n = A_n \cup (12) A_n \]

Further

\[ |A_n| = |(12) A_n| \] (exercise)

- i.e. the number of even permutations is the same as the number of odd permutations.
\[ |S_n| = n! \quad \text{and} \quad |A_n| = |(12) A_n|, \]

so

\[ n! = |S_n| = |A_n| + |(12) A_n| = |A_n| + |A_n| = 2 |A_n|, \]

so

\[ |A_n| = \frac{n!}{2}. \]
\[ |A_n| = \frac{n!}{2} \]

\[ |A_3| = \frac{3!}{2} = \frac{6}{2} = 3, \]
\[ |A_4| = \frac{4!}{2} = \frac{24}{2} = 12, \]
\[ |A_5| = \frac{5!}{2} = \frac{120}{2} = 60. \]

As the alternating group on 5 letters, is famous in the history of mathematics.
\[ |A_5| = \frac{5!}{2} = \frac{120}{2} = 60. \]

As \( A_5 \), the alternating group on 5 letters, is famous in the history of mathematics. It is a key example in the proof of the unsolvability of the quintic polynomial equation.

Galois theory (first half of 19th century)
Application to the 8-puzzle:

Theorem: There are precisely \( \frac{8!}{2} = 20,160 \) possible configurations, where the space is in the lower right corner, corresponding to all even permutations of the square labels.
\[\begin{array}{ccc}
2 & 3 & 1 \\
4 & 5 & 6 \\
7 & 8 & \color{orange}\
\end{array}\]

Corresponds to \((132)\), which is even, so possible.

\[\begin{array}{ccc}
3 & 2 & 1 \\
4 & 5 & 6 \\
7 & 8 & \color{orange}\
\end{array}\]

Corresponds to \((13)\), which is odd, so impossible.
e.g.

\[
\begin{array}{ccc}
7 & 8 & 3 \\
1 & 2 & 6 \\
4 & 5 & \text{orange}
\end{array}
\]

corresponds to \((147)(258)\) which is even, so possible \(\checkmark\)

\[
\begin{array}{ccc}
7 & 6 & 1 \\
4 & 3 & 8 \\
5 & 2 & \text{orange}
\end{array}
\]

corresponds to \((1357)(286)\), which is odd, so impossible \(\times\)
What about \[ \begin{array}{ccc} 2 & 6 & 3 \\ 8 & 7 & \text{?} \\ 4 & 1 & 5 \end{array} \] ?

This is possible iff \[ \begin{array}{ccc} 2 & 6 & 3 \\ 8 & 7 & 5 \\ 4 & 1 & \text{?} \end{array} \] is possible,

which corresponds to \((1847562)\), which is even, so the above configuration is possible.