Lecture 12

Theorem 10: $D_{2n} = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$ where

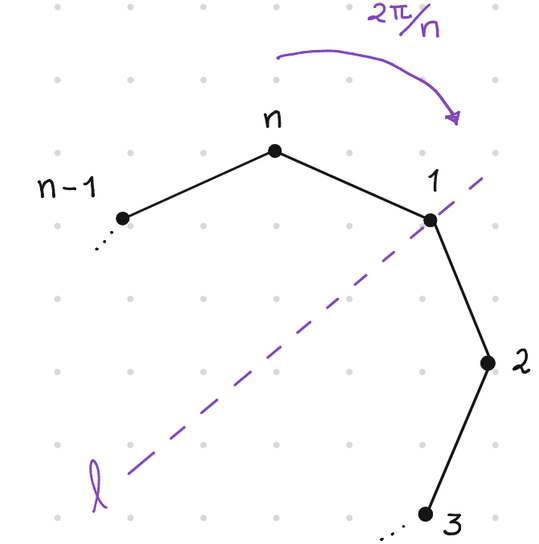
r is the rotation clockwise about the center through $\frac{2\pi}{n}$ radians, and

s is the reflection about the line passing through vertex 1.

Proof: Let A denote the group above. Observe that $A \subseteq D_{2n}$.

WTS that $|A| = 2n$.

Part 1: $1, r, r^2, \dots, r^{n-1}$ are all distinct and $r^n = 1$.



The permutation corresponding to r is σ_2 (in Prop 9). Write σ for σ_2.

Let us prove that $\sigma^i = \sigma_{i+1}$ for $i = 1, 2, \dots, n$ and $\sigma_{n+1} := \sigma_1$. ($\sigma^i := \sigma \circ \sigma \circ \cdots \circ \sigma$ i-times)

By induction on i: If $i=1$, clearly $\sigma^1 = \sigma_2$.

Suppose $\sigma^{i-1}(k) = \sigma_i(k) = i + (k-1) \pmod n$ for all $k = 1, 2, \dots, n$.

Let $k = 1, 2, \dots, n$, then $\sigma^i(k) = \sigma^{i-1}(\sigma(k))$

$= \sigma^{i-1}(k+1 \pmod n)$ def of σ

$= i + (k+1-1) \pmod n$ induction hypothesis

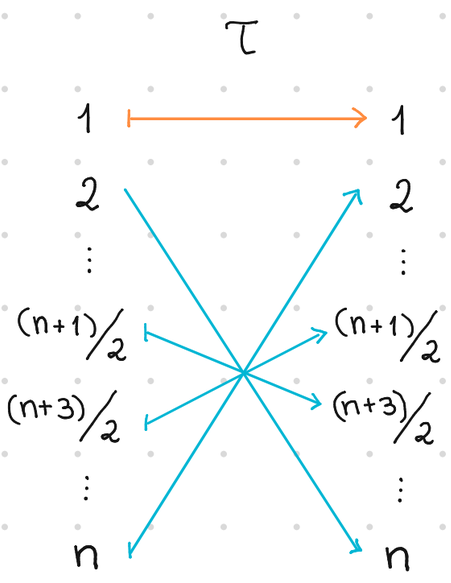
$= i + k \pmod n$

From this we have that $\sigma, \sigma^2, \dots, \sigma^{n-1}$ are different. Furthermore, $\sigma^n = \sigma_1 = id_{X_n}$.

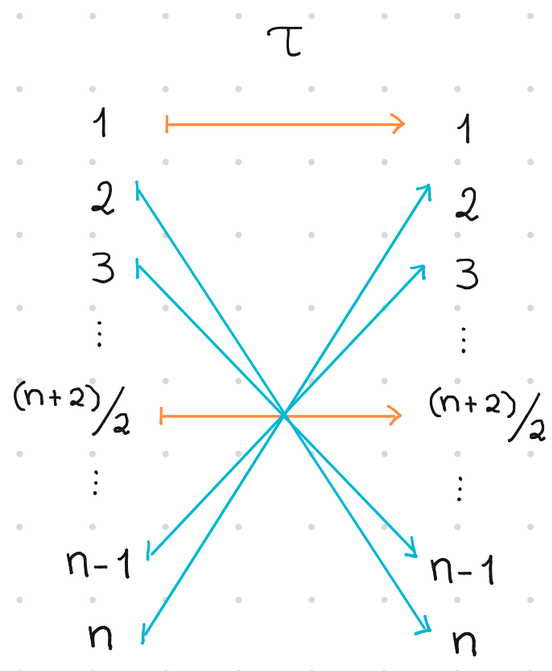
Part 2: $S^2 = id_{X_n}$.

The permutation corresponding to S is τ defined as follows:

if n is odd



if n is even



In both cases, $\tau^2 = id_{X_n}$. Prove it!

Part 3: $sr^i \neq sr^j$ for all $0 \leq i,j \leq n-1$ with $i \neq j$. See Q1(a), PS6.

Part 4: $s \neq r^i$ for all $0 \leq i \leq n-1$. Exercise

■

Proposition 11: In D_{2n} we have that

(1) $rs = sr^{-1}$.

(2) $r^i s = sr^{-i}$ for all $0 \leq i \leq n$.

Proof: See Q1(b,c), PS6.

Def: For $n \geq 3$, the nonabelian group D_{2n} is called the dihedral group of order $2n$.

The Symmetric Group on a Set

Def: Let $\Omega \neq \phi$ be a set. Let S_Ω be the set of permutations of Ω

The group $(S_\Omega, \circ)$ is called the symmetric group on Ω.

- $\circ$ is associative
- $e = id_\Omega$, $id_\Omega(a) = a$ for all $a \in \Omega$
- For every permutation, we have an inverse permutation.

Def: Let $n \geq 1$. If $\Omega = X_n$, then S_Ω is called the symmetric group of degree n, and it is denoted S_n.

Ex:

- $(S_{\mathbb{R}}, \circ)$ All linear functions $f(x) = mx + b$ belong to $S_{\mathbb{R}}$.

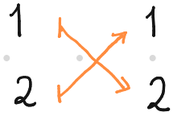
  Constant functions and some polynomials don't belong to $S_{\mathbb{R}}$.

- $(S_2, \circ)$ id_{X_2}

  $1 \longmapsto 1$

  $2 \longmapsto 2$

  α

  $\alpha \circ \alpha = 1 \Rightarrow \alpha^{-1} = \alpha$

Let 1 denote id_{X_2}, then $S_2 = \{1, \alpha\}$.

- $(S_5, \circ)$ id_{X_5}

  $1 \longmapsto 1$

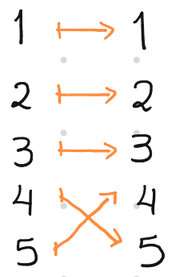
  $2 \longmapsto 2$

  $3 \longmapsto 3$

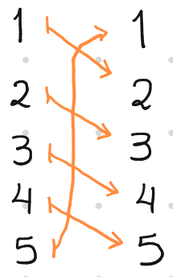
  $4 \longmapsto 4$

  $5 \longmapsto 5$

  α

  β

  ...

  $|S_5| = 5!$

Array notation: Let α be a permutation on X_n, this means we have a set of coordinates: $(1, \alpha(1)), (2, \alpha(2)), (3, \alpha(3)), \ldots, (n, \alpha(n))$.

$$\begin{array}{cc} X_n & \xrightarrow{\alpha} X_n \\ 1 & \alpha(1) \\ 2 & \alpha(2) \\ 3 & \alpha(3) \\ \vdots & \vdots \\ n & \alpha(n) \end{array}$$

It will be convenient to write α in array form as

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \cdots & \alpha(n) \end{pmatrix}$$

Ex:

- $(S_2, \circ)$ $\quad 1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ and $\alpha = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$
- $(S_5, \circ)$ $\quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$

Composition in array notation: It is carried out from right to left by going from top to bottom, then again from top to bottom.

Ex: $(S_5, \circ)$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} \quad \text{and} \quad \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\gamma\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}$$

$$\gamma\sigma \neq \sigma\gamma$$

$$\sigma\gamma \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}$$

Theorem 12: (1) $(S_\Omega, \circ)$ is a group for any $\Omega \neq \phi$.

(2) $|S_n| = n!$

(3) If $n \geq 3$, then $(S_n, \circ)$ is nonabelian.

Proof: (1) and (2) in PS5.

(3) Consider $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 3 & 2 & 1 & 4 & \cdots & n \end{pmatrix}$.

Then

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 3 & 1 & 4 & \cdots & n \end{pmatrix} \quad \text{and} \quad \beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 3 & 1 & 2 & 4 & \cdots & n \end{pmatrix}$$

Observe that $\alpha\beta \neq \beta\alpha$ because $\alpha\beta(1) = 2 \neq 3 = \beta\alpha(1)$.