Lecture 11

Def: A group G is called

(1) a **torsion group** if every element of G is of finite order.

(2) a **torsion-free group** if every nonidentity element of G is of infinite order.

(3) If G is abelian, define $\mathrm{Tor}(G) := \{a \in G \mid a \text{ has finite order}\}$.

We call $\mathrm{Tor}(G)$ the **torsion subgroup of G**.

Remark: $\mathrm{Tor}(G)$ is a group under the operation in G. (prove this!)

Lemma 6: Let G be a group. Let $a, b \in G$ be commuting elements, i.e. $ab = ba$. If $\gcd(|a|, |b|) = 1$, then $|ab| = |a||b|$.

Proof: Let $m := |a|$, $n := |b|$, and $r := |ab|$.

Observe that $(ab)^{mn} = a^{mn} b^{mn} = (a^n)^m (b^m)^n = 1$, then $r \mid mn$ by Thm 5(1). ①

($=$: hypothesis + Q5(c), PS5)

By Thm 5(3), $|a^n| = \frac{m}{\gcd(n,m)} = m$ and $|b^m| = n$.

Also, $1 = (ab)^r = a^r b^r$. This implies, $(a^n)^r = (a^n)^r (b^n)^r = ((ab)^r)^n = 1$ and $(b^m)^r = 1$. Therefore, $m \mid r$ and $n \mid r$. Since $\gcd(m,n) = 1$, $mn \mid r$. ②

From ① and ②, $r = mn$.

Corollary 7: Let G be an abelian torsion group. If $c \in G$ is an element of largest order in G (i.e. $|a| \leq |c| \ \forall a \in G$), then the order of every element of G divides $|c|$.

Proof: By contradiction. Suppose $\exists\, a \in G$ s.t. $|a| \nmid |c|$.

Think of the prime factorization of $|a|$ and $|c|$.

$\exists\, p$ prime s.t. p is in the factorization of $|a|$ raised to a higher power than it does in the factorization of $|c|$

Write $|a| = p^r m$ and $|c| = p^s n$, $r > s \geq 0$ and $m, n \in \mathbb{Z}^+$ with $\gcd(p, m) = 1 = \gcd(p, n)$ by the Fundamental Theorem of Arithmetic (FTOA).

By Thm 5 (3), $|a^m| = \frac{|a|}{\gcd(|a|, m)} = \frac{p^r m}{\gcd(p^r m, m)} = \frac{p^r m}{m} = p^r$. Similarly, $|c^{p^s}| = n$.

From Lemma 6, $|a^m c^{p^s}| = |a^m||c^{p^s}| = p^r n$. Hence $|a^m c^{p^r}| = p^r n > p^s n = |c|$.

Contradiction!!!

The Dihedral Group of Order 2n

Def: Let X be a set. A permutation of X is a bijective function

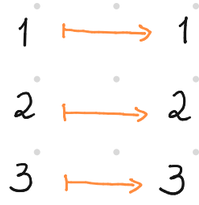
$$\sigma : X \longrightarrow X.$$

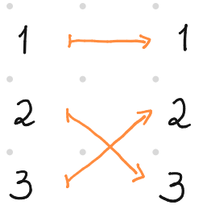
Informally, a permutation of $X_n = \{1, 2, \ldots, n\}$ is an ordering of its elements.

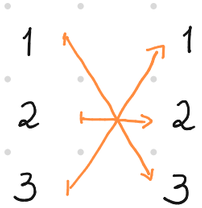
Ex: $X_3 = \{1, 2, 3\}$ has 6 different orderings:

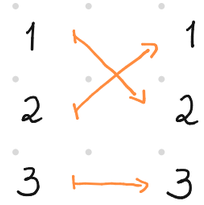
1, 2, 3 | 1, 3, 2 | 3, 2, 1 | 2, 1, 3 | 2, 3, 1 | 3, 1, 2

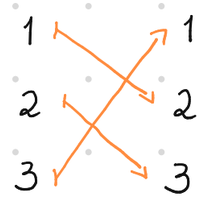
Each ordering determines a bijective function $X_3 \longrightarrow X_3$:

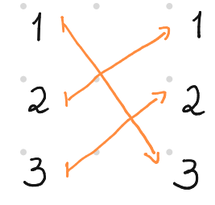










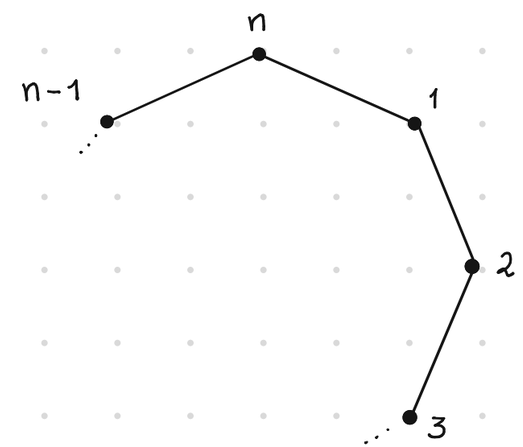


This means that X_3 has 6 permutations.

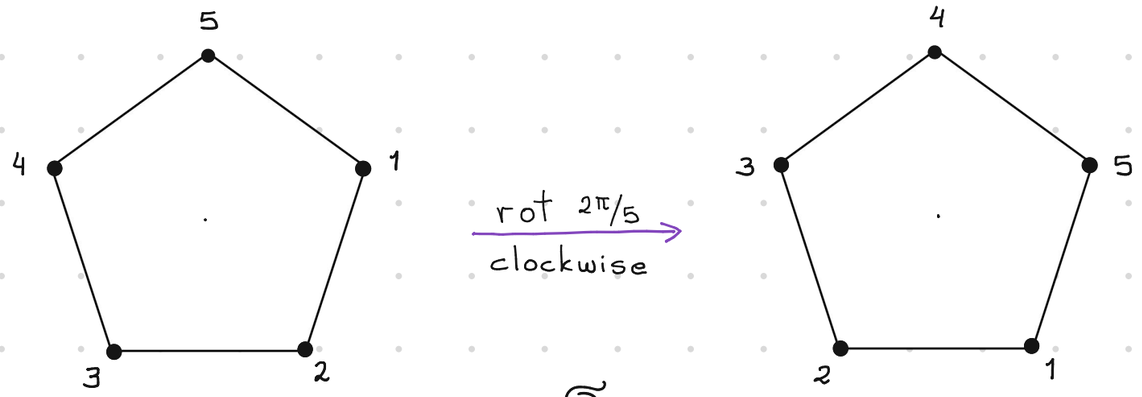
Let $n \in \mathbb{N}$, $n \geq 3$.

Consider the regular polygon of n vertices, or n-gon.

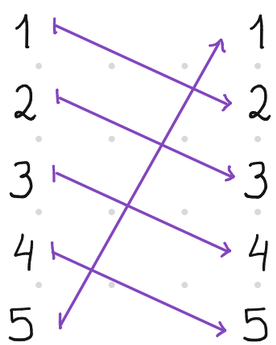
Let D_{2n} be the set of all the symmetries (rigid motions in 3D, i.e. rotations and reflections) of the n-gon with vertices labeled as in the figure on the RHS.



A symmetry of the n-gon is a function from the n-gon to itself that preserves distances. Each symmetry can be described uniquely by a permutation of Xn. vertices

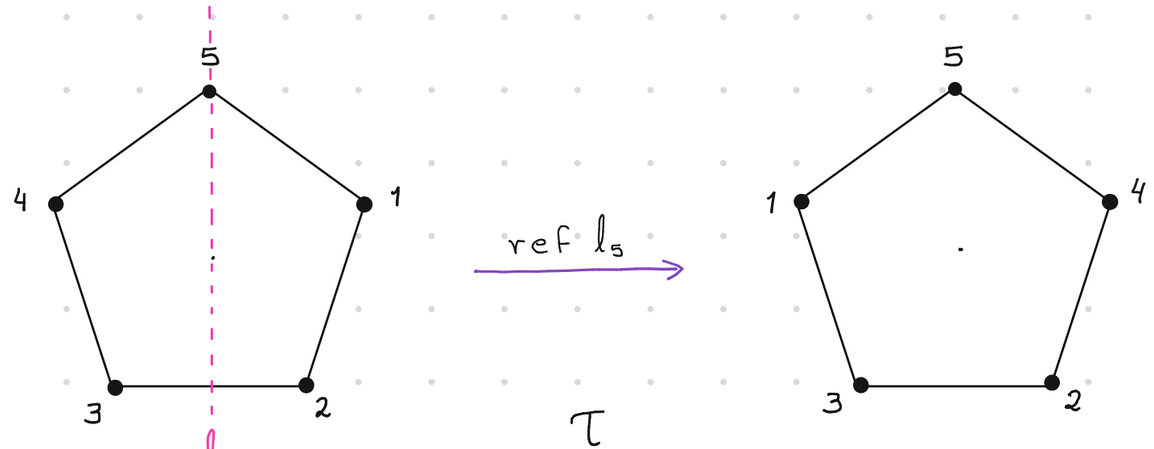


σ

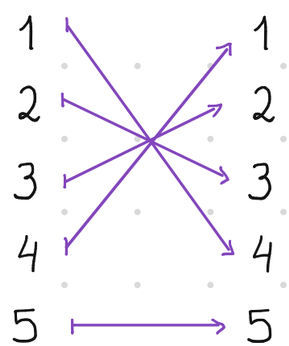


$\sigma(i) = i+1$ if $1 \leq i < 5$

$\sigma(5) = 1$



τ



$\tau(1) = 4$ $\tau(2) = 3$ $\tau(5) = 5$

$\tau(3) = 2$ $\tau(4) = 1$

Proposition 8: Let $n \in \mathbb{N}$, $n \geq 3$. Then $(D_{2n}, \cdot)$ is a group.

Proof: We make D_{2n} into a group by using function composition.

- Let $f, g \in D_{2n}$ and let fg denote the composite $f \circ g$. Observe that fg is a symmetry of the n-gon obtained by applying g and then f.
- If σ_f and σ_g are the permutations corresponding to f and g, respectively, then $\sigma_{fg} = \sigma_f \circ \sigma_g$.
- Composition of functions is associative.
- The identity, 1, of D_{2n} is the identity symmetry, i.e. the one that does not change the n-gon ($\sigma_1 = id_{X_n}$ where $id_{X_n}(i) = i$ for $i = 1, 2, \ldots, n$).

- If $f \in D_{2n}$, then f^{-1} is the symmetry that reverses all rigid motions of the n-gon $\left(\sigma_{f^{-1}} = (\sigma_f)^{-1} \right)$.

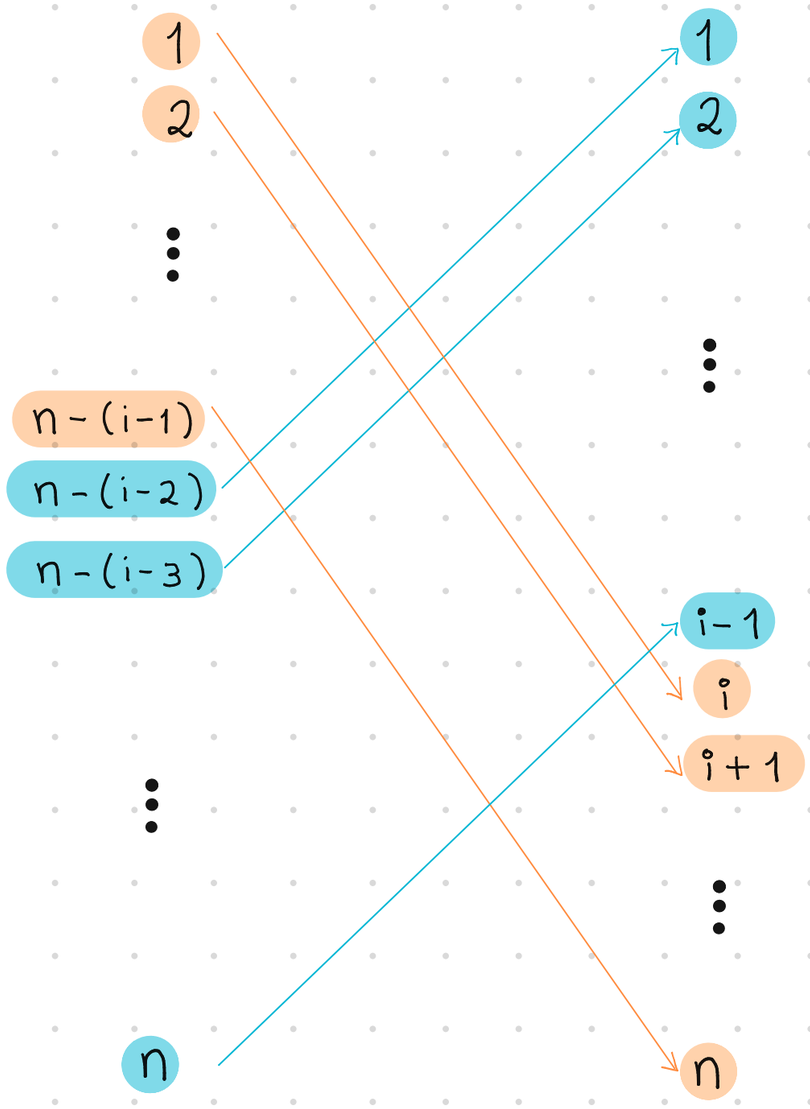
Proposition 9: The group $(D_{2n}, \cdot)$ has order $2n$.

Proof: Let $i = 1, 2, \ldots, n$ and let r_i denote the symmetry that rotates the n-gon $\frac{2\pi(i-1)}{n}$ radians clockwise about its center. Observe that r_i corresponds to the permutation $\sigma_i : X_n \longrightarrow X_n$ given by $\sigma_i(k) = i + (k-1) \pmod n$ where for all $k = 1, 2, \ldots, n$, and $\pmod n$ means $j + n \equiv j \pmod n$ for $j = 1, 2, \ldots, n$.

What is σ_i explicitly?

- $\sigma_i(1) = i$
- $\sigma_i(k) = i + (k-1)$ for $k = 2, 3, \ldots, n - (i-1)$
- $\sigma_i(k) = j$ for $k = n - (i-1-j)$ and $j = 1, 2, \ldots, i-1$

$X_n \xrightarrow{\sigma_i} X_n$



Let us see how few σ_i are defined:

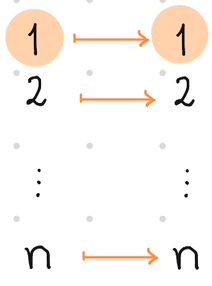
If $k = 1, 2, \dots, n$, then

$$\sigma_1(k) = 1 + (k-1) \pmod n \quad \Rightarrow \quad \sigma_1 = id_{X_n}$$
$$= k \pmod n$$

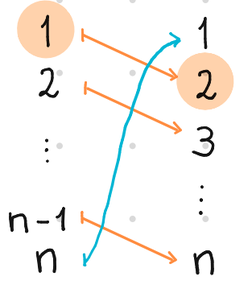
$$\sigma_2(k) = 2 + (k-1) \pmod n \quad \Rightarrow \quad \sigma_2(k) = \begin{cases} 2, & k = 1 \\ k+1, & 2 \le k \le n-1 \\ 1, & k = n \end{cases}$$
$$= k + 1 \pmod n$$

$$\sigma_n(k) = n + (k-1) \pmod n \quad \Rightarrow \quad \sigma_2(k) = \begin{cases} n, & k = 1 \\ k-1, & 2 \le k \le n \end{cases}$$

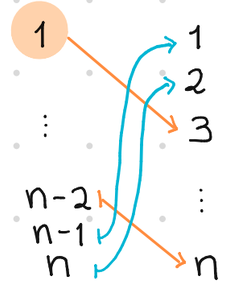
id_{X_n}



σ_2

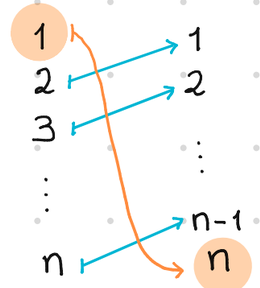


σ_3



...

σ_n



It can be shown that σ_i is bijective. Prove it!

By definition, $\sigma_i \neq \sigma_j$ if $i \neq j$. Thus, there are n different rotations in D_{2n}.

We can show that there are n different reflections in D_{2n}. Prove it!