# Week 3

## 3.1 Dihedral groups

Consider the subset $\mathcal{T}$ of transformations of $\mathbb{R}^2$, consisting of all rotations by fixed angles about the origin, and all reflections over lines through the origin.

Consider a regular polygon $P_n$ with $n$ sides in $\mathbb{R}^2$, centered at the origin. Identify the polygon with its $n$ vertices, which form a subset $P_n = \{x_1, x_2, \ldots, x_n\}$ of $\mathbb{R}^2$. If $\tau(P_n) = P_n$ for some $\tau \in \mathcal{T}$, we say that $P_n$ is **symmetric** with respect to $\tau$.

Intuitively, it is clear that $P_n$ is symmetric with respect to $n$ rotations

$$\{r_0, r_1, \ldots, r_{n-1}\},$$

and $n$ reflections

$$\{s_1, s_2, \ldots, s_n\}$$

in $\mathcal{T}$. In particular $|D_n| = 2n$.

**Proposition 3.1.1.** *The set $D_n := \{r_0, r_1, \ldots, r_{n-1}, s_1, s_2, \ldots, s_n\}$ is a group, with respect to the group operation defined by composition of transformations: $\tau * \gamma = \tau \circ \gamma$.*

**Terminology:** $D_n$ is called the **$n$-th dihedral group**.

Let $r = r_1 \in D_n$ be the rotation by the angle $2\pi/n$ in the anticlockwise direction (and similarly $r_k$ denotes the rotation by the angle $2k\pi/n$ in the anticlockwise direction). Then the set of rotations in $D_n$ is given by

$$\langle r \rangle = \{\text{id}, r, r^2, \ldots, r^{n-1}\}.$$

Furthermore, the composition of two reflections is a rotation (which can be seen, e.g. by flipping a Hong Kong 2-dollar coin). So if we let $s = s_1 \in D_n$ be one of the reflections, then the set of reflections in $D_n$ is given by

$$\{s, rs, r^2s, \ldots, r^{n-1}s\}.$$

So we can enumerate the elements of $D_n$ as

$$D_n = \{\text{id}, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}.$$

## 3.2 Subgroups

**Definition.** Let $G$ be a group. A subset $H$ of $G$ is a **subgroup** of $G$ (denoted as $H < G$) if it is a group under the induced operation from $G$.

More precisely, a subset $H \subset G$ is a subgroup of $G$ if

- $H$ is *closed* under the operation on $G$, i.e.

$$a * b \in H \text{ for any } a, b \in H,$$

  so that the restriction of the binary operation $G \times G \to G$ to the subset $H \times H \subset G \times G$ gives a well-defined binary operation $H \times H \to H$, called the *induced operation* on $H$, and

- $H$ is a group under this induced operation.

**Example 3.2.1.**

- For any group $G$, we have the **trivial subgroup** $\{e\} < G$ and also $G < G$. We call a subgroup $H < G$ **nontrivial** if $\{e\} \subsetneqq H$ and **proper** if $H \subsetneqq G$.

- We have $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$ under addition, and $\mathbb{Q}^\times < \mathbb{R}^\times < \mathbb{C}^\times$ under multiplication.

- For any $n \in \mathbb{Z}$, $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$.

- $\mathrm{SL}(n, \mathbb{R})$ is a subgroup of $\mathrm{GL}(n, \mathbb{R})$.

- The set of all rotations (including the trivial rotation) in a dihedral group $D_n$ is a subgroup of $D_n$.

- By viewing $D_n$ as permutations of the vertices of a regular $n$-gon $P_n$, we can regard $D_n$ as a subgroup of $S_n$.

- Consider the symmetric group $S_n$ where $n \in \mathbb{Z}_{>0}$.

  *Proposition* 3.2.2. *Each element of $S_n$ is a product of (not necessarily disjoint) transpositions.*

*Sketch of proof.* Show that each permutation not equal to the identity is a product of cycles, and that each cycle is a product of transpositions:

$$(i_1 i_2 \cdots i_k) = (i_1 i_k)(i_1 i_{k-1}) \cdots (i_1 i_3)(i_1 i_2)$$

□

**Example 3.2.3.**

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix} = (15)(246) = (15)(26)(24) = (15)(46)(26)$$

Note that a given element $\sigma$ of $S_n$ may be expressed as a product of transpositions in different ways, but:

*Proposition* 3.2.4. *In every factorization of $\sigma$ as a product of transpositions, the number of factors is either always even or always odd.*

*Proof.* **Exercise.** One approach: There is a unique $n \times n$ matrix, with either $0$ or $1$ as its coefficients, which sends any vector $(x_1, x_2, \ldots, x_n)$ to $(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$. Use the fact that the determinant of the matrix corresponding to a transposition is $-1$, and that the determinant function of matrices is multiplicative. □

We say that $\sigma \in S_n$ is an **even** (resp. **odd**) **permutation** if it is a product of an even (resp. odd) number of transpositions. The subset $A_n$ of $S_n$ consisting of even permutations is a subgroup of $S_n$. $A_n$ is called the $n$-th **alternating group**.

**Proposition 3.2.5.** *A nonempty subset $H$ of a group $G$ is a subgroup of $G$ if and only if, for all $a, b \in H$, we have $ab^{-1} \in H$.*

*Proof.* Suppose $H \subseteq G$ is a subgroup. For any $a, b \in H$, existence of inverse implies that $b^{-1} \in H$, and then closedness implies that $ab^{-1} \in H$.

Conversely, suppose $H$ is a nonempty subset of $G$ such that $xy^{-1} \in H$ for all $x, y \in H$.

- (Identity:) Let $e$ be the identity element of $G$. Since $H$ is nonempty, it contains at least one element $h$. Since $e = h \cdot h^{-1}$, and by hypothesis $h \cdot h^{-1} \in H$, the set $H$ contains $e$.
- (Inverses:) Since $e \in H$, for all $a \in H$ we have $a^{-1} = e \cdot a^{-1} \in H$.
- (Closure:) For all $a, b \in H$, we know that $b^{-1} \in H$. Hence, $ab = a \cdot (b^{-1})^{-1} \in H$.

- (Associativity:) This follows from that in $G$.

Hence, $H$ is a subgroup of $G$. □

One can use this criterion to check that all the previous examples are indeed subgroups.

## 3.3 Cyclic subgroups

Recall that for any group $G$ and any element $g \in G$, we have the subset

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}.$$

**Proposition 3.3.1.** *Let $G$ be a group. Then for any element $g \in G$, the subset $\langle g \rangle$ is the smallest subgroup of $G$ containing $g$, which we call the* **cyclic subgroup** *generated by $g$.*

*Proof.* Let $g^k, g^l$ be two arbitrary elements in $\langle g \rangle$. Then $g^k(g^l)^{-1} = g^{k-l} \in \langle g \rangle$. So $\langle g \rangle$ is a subgroup of $G$ by Proposition 3.2.5.

Now let $H < G$ be any subgroup containing $g$. Then $g^k \in H$ for any $k \in \mathbb{Z}$ since $H$ is a subgroup. Hence $\langle g \rangle \subset H$. □

**Proposition 3.3.2.** *The intersection of any collection of subgroups of a group $G$ is also a subgroup of $G$.*

*Proof.* **Exercise.** □

**Corollary 3.3.3.** *Let $G$ be a group. Then for any $g \in G$, we have*

$$\langle g \rangle = \bigcap_{\{H : g \in H < G\}} H.$$