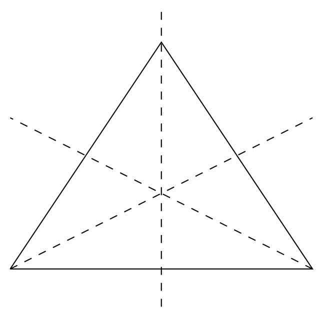
DEFINITION:

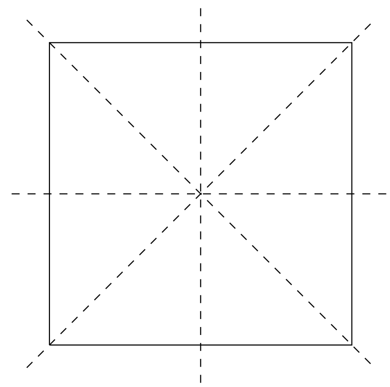
- A **isometry** of $\mathbb{R}^2$ is a bijective function $f : \mathbb{R}^2 \to \mathbb{R}^2$ that preserves distances between pairs of points; examples include rotations around a point, translations, and reflections over a line.
- Let $X \subseteq \mathbb{R}^2$. A **symmetry** of X is an isometry of $\mathbb{R}^2$ such that $f(X) = X$ as a set.
- The **dihedral group** D_n is the group of symmetries of a regular n-gon P_n in the plane, with composition of functions as the group operation.

THEOREM 1: The dihedral group D_n is indeed a group. It has exactly $2n$ elements consisting of:

- The identity map e,
- $n-1$ rotations $r, r^2, \ldots, r^{n-1}$, where r is counterclockwise rotation by $2\pi/n$ (so r^j is counterclockwise rotation by $2\pi j/n$),
- n reflections. More precisely,
  - for n is odd, there are n distinct reflections over lines between a vertex and opposite edge;
  - for n is even, there are $n/2$ distinct reflections over lines between opposite pairs of vertices, and another $n/2$ distinct reflections over lines between opposite pairs of edges.



The reflection lines in D_3



The reflection lines in D_4

(1) Why is the dihedral group a group? I.e., why are the group axioms true for this set and operation?

Let g, h be symmetries of P_n. The composition of isometries is an isometry: if g, h are isometries, for $x, y \in \mathbb{R}^2$, $d(g(h(x)), g(h(y))) = d(h(x), h(y)) = d(x, y)$; and the composition of functions that preserve P_n also preserves P_n: if g, h preserve P_n, then $h(P_n) = P_n$, so $g(h(P_n)) = g(P_n) = P_n$. Thus gh is a symmetry of P_n. The identity is a symmetry of P_n, and the inverse of a symmetry of P_n is also a symmetry of P_n (we should argue along similar lines to the composition argument above, which I'll skip). Finally, composition of functions is associative. This verifies the group axioms

(2) What is the order of the rotation r? What is the order of a reflection in D_n?

The rotation r has order n: rotating n times is the identity, whereas rotating less than n times is not. The order of a reflection is 2.

(3) Proof of Theorem 1:

(a) Show that[1] if f is a symmetry of P_n and c is the center of P_n, then $f(c) = c$.

[1]Hint: After rescaling, we can assume that $d(c, v) = 1$ for any vertex v. Then observe that

(b) Show that[2] if f is a symmetry of P_n and v is a vertex of P_n, then $f(v)$ is a vertex of P_n.
(c) Show that if f is a symmetry of P_n and v, v' are adjacent vertices, then $f(v)$ and $f(v')$ are adjacent vertices of P_n.
(d) Prove[3] the Theorem.

LEMMA: Let $v \in P_n$ be a vertex, and $s \in D_n$ the reflection through the axis containing v. Let $r \in D_n$ be counterclockwise rotation by $2\pi/n$. Then $srs = r^{-1}$.

THEOREM 2: Let $v \in P_n$ be a vertex, and $s \in D_n$ the reflection through the axis containing s. Let $r \in D_n$ be counterclockwise rotation by $2\pi/n$.

(1) Every element of D_n can be written uniquely in the form

$$r^j \quad \text{for } j = 0, \ldots, n-1, \qquad \text{or} \qquad r^j s \quad \text{for } j = 0, \ldots, n-1.$$

(2) D_n is generated by r, s.
(3) D_n has the group presentation $\langle r, s \mid r^n = e, s^2 = e, srs^{-1} = r^{-1} \rangle$.

(4) Show that the elements $r^j s$ for $j = 0, \ldots, n-1$ are n distinct reflections. Deduce Theorem 2(1) from this and Theorem 1.

First, we note that these are distinct, since if $0 \leq i < j \leq n-1$ and $r^i s = r^j s$, then $r^i = r^j$ and $r^{j-i} = e$, a contradiction. Now we note that none of these is a rotation, since each symmetry of the form $r^j s$ reverses the orientation (clockwise vs counterclockwise) of a pair of adjacent vertices. Thus, by Theorem 1, these are reflections, and again by Theorem 1, these are all of the reflections. Part (1) of the Theorem follows.

(5) Use the Theorem 2(1) to prove Theorem 2(2).
(6) Every element can be written as r^j or $r^j s$; in particular, every element is a multiple of powers of r and s, and thus r, s generate.
(7) Prove the Lemma.

(8) Discuss Theorem 2(3).

---

(9) Consider a circle in the plane.
(a) Compute the symmetry group G of the circle; give an answer in a similar form to Theorem 1.
(b) What are all of the possible orders of elements in this group?
(c) Find two elements of order 2 in G whose product has infinite order.
(d) Does G has a finite generating set?

(i) $d(c, x) \leq 1$ for any $x \in P_n$, and
(ii) if $q \in P_n$ is *not* the center, then $d(q, x) > 1$ for some $x \in P_n$.

[2]Hint: Again assume $d(c, v) = 1$ for any vertex v. Observe that v is a vertex of P_n if and only if $d(c, v) = 1$.
[3]You can use the following fact from geometry: if f, f' are two isometries of the plane, $p_1, p_2, p_3 \in \mathbb{R}^2$ are three points not on a line, and $f(p_i) = f'(p_i)$ for $i = 1, 2, 3$, then $f = f'$.