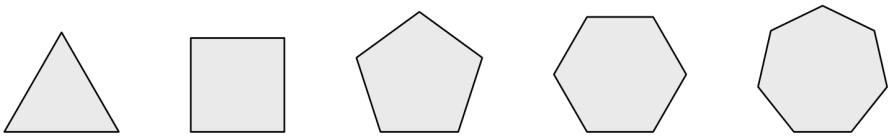
1. The dihedral group

Objects have bilateral symmetry if they look the same when flipped over (usually in a specific direction, say vertically). The easiest geometric examples of objects with both rotational and bilateral symmetry are regular polygons.

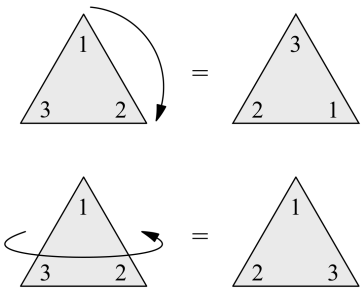


Observe that is not necessary to track the movement of all the points that make up a polygon in order to describe a rigid motion. Instead, we can simply keep track of their vertices. This motivates an important example of groups.

Some definitions first. A permutation of a set X is a bijection from X onto X. A regular polygon with n sides is called an n-gon. A symmetry of the n-gon is any rigid motion of of the n-gon. To be precise, a symmetry of the n-gon is just a permutation of $\{1, \ldots, n\}$. From now and on, we will denote $[n] = \{1, \ldots, n\}$.

It turns out, we can associate a group to the n-gon to study its rigid motions, that is, its symmetries. It is called the dihedral group of order $2n$ and denoted D_{2n}. Dihedral groups describe objects that have both rotational and bilateral symmetry. Before defining precisely D_{2n}, let us see an example.

Example 1. Both rotations and horizontal flips respect the shape of an equilateral triangle.



The first symmetry is described by the permutation $\sigma\colon [3] \to [3]$ defined by

$$\sigma(1) = 2, \quad \sigma(2) = 3, \quad \sigma(3) = 1.$$

The second one is described by $\tau\colon [3] \to [3]$ where

$$\tau(1) = 1, \quad \tau(2) = 3, \quad \tau(3) = 2.$$

Suppose we have a regular n-gon centered at the origin in the plane and label the vertices consecutively from 1 to 1, clockwise.

(i) Let r be the rotation clockwise about the origin through $2\pi/n$ radians.

(ii) Let s be the reflection about the line of symmetry through vertex 1 and the origin.

The dihedral group D_{2n} is the set of rotations and reflections of the n-gon endowed with the following operation.

(iii) If $a, b \in D_{2n}$, then ab is the symmetry obtained by first applying b and then a to the n-gon.

Remark 1.0.1.
- We choose the notation D_{2n} because there are $2n$ symmetries associated to a n-gon. Namely, n rotations and n reflections.
- The identity of D_{2n} is the identity symmetry, that is the effect of doing nothing to the n-gon.
- Think of the operation as function composition: we apply one function after another, writing the last application consecutively to the left.

Theorem 1.1.

(i) $\{1, r, r^2, \ldots, r^{n-1}\}$ *are all distinct,* $r^n = 1$ *and* $|r| = n$.

(ii) $|s| = 2$

(iii) $s \neq r^i$ *for all* $i \in [n]_0$.

(iv) $sr^i = sr^j$ *for all* $i, j \in [n-1]$ *distinct.*

(v) $rs = sr^{-1}$, *so* D_{2n} *is nonabelian*

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

Proof. Classwork. □

Remark 1.1.1. Facts (i), (ii) and (v) are so important that they together serve to give an alternative definition of the dihedral group of order $2n$, namely

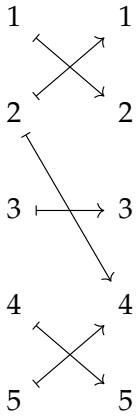
$$D_{2n} = \left\langle r, s \,\middle|\, r^n = s^2 = 1, rs = sr^{-1} \right\rangle.$$

Exercise 1. Prove or disprove $(sr^9)(sr^6) = r^9$.

2. Permutations and the symmetric group

Recall a permutation of a set X is a bijective function $\alpha \colon X \to X$. The set of all permutations of X is denoted S_X. If X is a finite set with n elements, then we choose the notation S_n instead and regard S_n as the set of bijections from $[n]$ to $[n]$. The set S_X is a group under the operation of composition of functions (why?). We call $(S_X, \circ)$ the symmetric group on X.

There is a convenient way to denote the elements of S_n. Keep in mind that an element σ of S_n is an injective function onto $[n]$ that is entirely determined by its values $\sigma(1), \ldots, \sigma(n)$. Let $\sigma \in S_n$ be the permutation defined by



We come up with a useful notation: write $(1\,2)(3)(4\,5)$ to represent σ. This notation entirely captures what σ does to the set $[5]$. For instance, $(1\,2)$ means $\sigma\colon 1 \mapsto 2$ and $\sigma\colon 2 \mapsto 1$. Since (3) means $\sigma\colon 3 \mapsto 3$, that is, σ leaves 3 fixed, we can omit it from our notation and just write $(1\,2)(4\,5)$.

Let us formalize what we have seen.

A cycle is a string of integers which represents the element of S_n which cyclically permutes these integers (and fixes all other integers). The cycle $(a_1\, a_2\, \cdots\, a_m)$ is the permutation which sends a_i to a_{i+1}, for all $1 \leq i \leq m-1$ and sends a_m to a_1 (so the cycle is closed).

There is not a single way to write a cycle. For instance, both

$$(1\,5\,3\,4\,2) \quad \text{and} \quad (3\,4\,2\,1\,5)$$

denote the same permutation.

Remark 2.0.1. It is also possible to use the notation

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

where the elements of $[n]$ are listed in the first row and their image under σ below it in the second row. In this case, the order of the elements in the first row does not matter.

Lemma 2.1. *S_X is a nonabelian group.*

Proof. In S_3, take $\sigma = (1\,2\,3)$ and $\tau = (1\,2)$. We have

$$\sigma \circ \tau = (1\,3) \quad \text{and} \quad \tau \circ \sigma = (2\,3),$$

which are not equal. □

Definition 2.2. Let $i_1, i_2, \ldots, i_r$ be distinct integers in $[n]$. If $\alpha \in S_n$ fixes the other integers (if any) and if

$$\alpha(i_1) = i_2, \quad \alpha(i_2) = i_3, \quad \ldots, \quad \alpha(i_{r-1}) = i_r, \quad \alpha(i_r) = i_1,$$

then α is called an r-cycle.

Given $\sigma \in S_X$, we say σ fixes $x \in X$ if $\sigma(x) = x$, otherwise σ moves x.

A 2-cycle is called a transposition. A transposition interchanges two integers and fixes everything else. Note that any 1-cycle is the identity.

Algorithm to factor a permutation into the product of cycles

- To start a new cycle, pick the smallest element of $\{1, 2, \ldots, n\}$ that has not yet appeared in a previous cycle. Call it a. If you are just starting, set $a = 1$. Begin the new cycle: $(a$
- Read off $\sigma(a)$ from the given description of σ. Call it b. If $b = a$, close the cycle with a right parenthesis (without writing b down). This completes a cycle; return to step 1. If $b \neq a$, write b next to a in this cycle: $(a\, b$
- Read off $\sigma(b)$ from the given description of σ. Call it c. If $c = a$, close the cycle with a right parenthesis to complete the cycle and return to step 1. If $c \neq a$, write c next to b in this cycle: $(a\, b\, c$. Repeat this step using the number c as the new value for b until the cycle closes.
- Final Step: Remove all cycles of length 1

Remark 2.2.1. (i) Not all permutations are cycles. Indeed, the permutation

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

is equivalently written as $(1\,2)(3\,4\,5)$.

(ii) Every permutation has a cycle decomposition.

(iii) The cycle decomposition of σ^{-1} is is obtained by writing the numbers in each cycle of the cycle decomposition of in reverse order. For instance, if

$$\sigma = (1\,12\,8\,10\,4)(2\,13)(5\,11\,7)(6\,9)$$

then

$$\sigma^{-1} = (4\,10\,8\,12\,1)(13\,2)(7\,11\,5)(9\,6).$$

Definition 2.3. Two permutations σ and τ are said to be **disjoint** if the set of moved elements of σ is contained in the set of fixed elements of τ, or conversely.

In other words, σ and τ are disjoint if every element that one of them fixes is moved by the other.

Remark 2.3.1. If α and β are disjoint, there are three possibilities for $i \in [n]$:

(i) i is moved by α and fixed by β.

(ii) i is moved by β and fixed by α.

(iii) i is fixed by both α and β.

Lemma 2.4. *Disjoint permutations commute.*

Proof. Classwork. □

Lemma 2.5. *Every permutation of $[n]$ is either a cycle or a product of disjoint cycles.*

Proof. Classwork. □

2.1. Computing products in S_n

Example 2. Let

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

We have

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

Moreover, their cycle decomposition are

$$\alpha = (1\,2\,3), \quad \text{and} \quad \beta = (1\,2)(3\,4).$$

3. An additional example of groups: Matrix Groups

In order to present this example, let us first begin with a preliminary definition.

Definition 3.1. A **field** is a set F together with two binary operations $+$ and $\cdot$ on F such that

(i) $(F, +)$ is an abelian group.

(ii) $(F \setminus \{0\}, \cdot)$ is an abelian group.

(iii) The operations $+$ and $\cdot$ are compatible by the distributive law:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

for all $a, b, c \in F$.

Roughly speaking, a field is the *smallest* mathematical structure in which we can perform all the basic arithmetic operations: $+, -, \times, \div$ (on non-zero elements).

Example 3. (i) $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a (finite) field for every prime p.

(ii) $\mathbb{Q}$, and $\mathbb{R}$ are infinite fields

Matrix Groups

Let F be a field and for a fixed $n \in \mathbb{Z}^+$ define

$$GL_n(F) = \{A \mid A \text{ is an } n \times n \text{ matrix with entries from } F \text{ and } \det(A) \neq 0\}$$

For $A, B \in GL_n(F)$, the operation $A \cdot B = (C_{ij})$ defined by

$$C_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

gives $GL_n(F)$ a group structure.

Remark 3.1.1. In this group:

- Since
$$\det(A \cdot B) = \det(A) \cdot \det(B)$$
it follows that the product is defined, so that $GL_n(F)$ is closed under $\cdot$.
- A^{-1} exists for any $A \in GL_n(F)$ nonzero.
- The identity of the group is the identity matrix $I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$.