2 Examples

2.1 The cyclic group C_n

The symmetry group of rotations of a regular polygon with n directed sides.

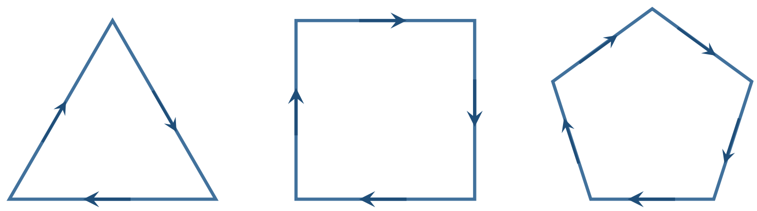

Figure 1: Directed n-gon

The elementary rotation operation that maps a directed n-gon back to itself is rotation through an angle $2\pi/n$. Denote this elementary rotation operation as c. Applying c for r times ($r = 0, 1, ..., n-1$), we can get all the rotation symmetry operations of a directed n-gon. In this sense c is called a 'generator' of the group. We write

$$C_n = gp\{c\}, c^n = e \tag{1}$$

which completely specifies the group.

Applying c for n times is the same as doing nothing and we have

$$c^n = e \tag{2}$$

We say that c is an order n element in the group. In general, the order of an element a in the group is the smallest nonzero positive integer k_a such that composing k_a copies of a together gives e, $a^{k_a} = e$. k_a depends on a.

The set of elements in the group are $\{e, c, c^2, ..., c^{n-1}\}$. The composition rule is

$$c^t c^s = c^{t+s(\text{mod } n)} \tag{3}$$

Obviously this is an abelian group

$$c^s c^t = c^t c^s = c^{s+t(\text{mod } n)} \tag{4}$$

Now consider the set of integers $\{0, 1, ..., n-1\}$ together with the operation of addition modulo n. It forms the group $\mathbb{Z}_n$. In fact, there is a one to one correspondence between the elements of C_n and the elements of $\mathbb{Z}_n$: $c^s \sim s$, $s = 0, 1, ..., n-1$ and their composition rules match exactly. We say that C_n is isomorphic to $\mathbb{Z}_n$, $C_n \cong \mathbb{Z}_n$.

$a\backslash b$	e	c	c^2
e	e	c	c^2
c	c	c^2	e
c^2	c^2	e	c

Another way of specifying the composition rule of a group is to use the multiplication table. That is, to list the composition result for each pair of elements a and $b \in G$ in a square table. For example, for C_3, the multiplication table reads

For abelian groups, the multiplication table is invariant under transpose. Each row and each column corresponds to a permutation of all the group elements.

2.2 The Dihedral Group D_n

The symmetry group of a regular polygon with n undirected sides.

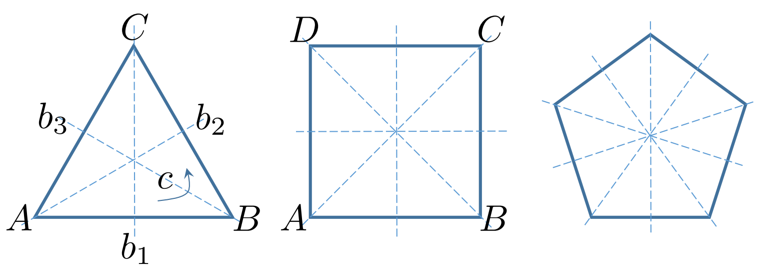

Figure 2: Undirected n-gon

D_n contains all the elements of C_n, c^r, $r = 0, 1, ..., n-1$. The composition of elements in this subset remains in this subset and satisfies the associativity, the existence of identify and the existence of inverse axioms. We say that the subset of elements $\{c^r, r = 0, 1, ..., n-1\}$ form a subgroup of D_n.

Moreover, because now the sides are undirected, the polygon can be mapped back to itself by a reflection with respect to the reflection axes (dotted lines) shown in the figure. For a n polygon, there are n reflection axis. Denote the reflection operations as b_1,..., b_n. Each b_i is an order two element of the group, because doing reflection twice is the same as doing nothing

$$b_i^2 = e \tag{5}$$

Each subset $\{e, b_i\}$ also forms a subgroup of D_n.

The full group contains $2n$ elements $\{c^r(r = 0, 1, ..., n-1), b_i(i = 1, ..., n)\}$. Because of this, the Dihedral groups are also (confusingly) denoted as D_{2n}. In this course, we will use the notation of D_n.

What is the relation between the set of rotation operations c^r and the set of reflection operations b_i?

First note that their composition can be non-commutative.

Consider the case of D_3. The application of b_1 followed by c is different from the application of c followed by b_1, which can be seen by tracking the position of the vertices of the triangle (with respect to the background labeling of A, B and C)

$$\begin{array}{l} cb_1 : A \to B \to C, B \to A \to B, C \to C \to A \\ b_1 c : A \to B \to A, B \to C \to C, C \to A \to B \end{array} \tag{6}$$

From this we see that $cb_1 = b_3$, $b_1 c = b_2$. Therefore, D_3 is nonabelian.

Secondly, all group elements can be generated by c and b_1. We can write $D_3 = gp\{c, b_1\}, c^3 = e, b_1^2 = e$. However, this is not a complete description of D_3. We also need to specify the relation between b_1 and c. We notice that $(b_1 c)^2 = b_2^2 = e$. Adding this condition completes the description of D_3

$$D_3 = gp\{c, b_1\}, c^3 = e, b_1^2 = e, (b_1 c)^2 = e \tag{7}$$

In general, the composition rule of the elements in D_3 is

$$c^t c^s = c^{t+s}, c^s b_i = b_{i-s}, b_i c^s = b_{i+s}, b_i b_j = c^{j-i} \tag{8}$$

where $t, s = 0, 1, 2$; $i, j = 1, 2, 3$; the arithmetic $t + s$, $i - s$ etc. are all defined mod 3 such that the power of c takes value in $0, 1, 2$ and the subscript of b takes value in $1, 2, 3$. If we take $t, s = 0, 1, ..., n - 1$, $i, j = 1, 2, ..., n$, the above equations give the general composition rule for D_n.

Some useful relations in D_3 are

$$cb_1 c^{-1} = b_2, cb_2 c^{-1} = b_3, cb_3 c^{-1} = b_1, c^{-1} b_1 c = b_3, c^{-1} b_2 c = b_1, c^{-1} b_3 c = b_2 \tag{9}$$

That is, if we conjugate a reflection operation by rotation, we get a different reflection operation. This is intuitive to understand: conjugating reflection by rotation corresponds to rotating the reflection axis and through direct observation we can see that the above relations should hold.

Now let's consider the group of D_4. D_4 is similar to D_3 in that it consists of rotations and reflections. The group is of order eight with group elements

$$\{e, c, c^2, c^3, b_1, b_2, b_3, b_4\} \tag{10}$$

Rotations form an order 4 subgroup $\{e, c, c^2, c^3\}$ while each reflection generates an order 2 subgroup $\{e, b_i\}$.

One difference between D_4 and D_3 is that, not all reflection axes can be rotated into each other. In particular

$$cb_1 c^{-1} = b_3, cb_2 c^{-1} = b_4, cb_3 c^{-1} = b_1, cb_4 c^{-1} = b_2 \tag{11}$$

So there are two different types of reflection operations.

The element c^2 is special in D_4 in that it commutes with all the other elements (please check), while no such element exists in D_3. We call the subgroup generated by c^2 – $\{e, c^2\}$ – the center of the group.

In general, a dihedral group D_n is completely specified by

$$D_n = gp\{c, b\}, c^n = e, b^2 = e, (bc)^2 = e \tag{12}$$

2.3 Permutation group S_n

The permutation of n objects.

S_n contains $n!$ elements, which permutes the ordering of objects $(1, ..., n)$ to $(p_1, ..., p_n)$. Composition of group elements is defines as successive application of such permutations. Note that the notation below is different from what I used in the lecture. These are two different ways to label permutations.

- $n = 2$

  The permutation of two objects 1 and 2 involves only one nontrivial operation: the exchange of 1 and 2. Denote this element as $a = (1, 2)$. This notation means that object 1 is moved to position 2 and object 2 to position 1 in this operation. Note the redundancy in this notation because $(1, 2)$ and $(2, 1)$ label the same operation. To remove this redundancy, we put the object with the smallest number in the first position.

  Obviously $a^2 = e$. S_2 is isomorphic to C_2 and $\mathbb{Z}_2$.

- $n = 3$

  The permutation of three objects 1, 2 and 3 involves three exchange operations $(1, 2), (2, 3), (1, 3)$ and two cyclic permutation operations $(1, 2, 3), (1, 3, 2)$. Here (i, j) means that object i is mapped to position j and object j is mapped to position i, the third object is left untouched. (i, j, k) means that object i is mapped to position j, j to k and k to i. The exchange operations are of order 2 while the cyclic permutation operations are of order 3. Note that we have used the same convention to remove redundancy in the notation.

  By comparing to the effect of elements in D_3 on the three vertices of the triangle, it is easy to see that $S_3 \cong D_3$.

- $n = 4$

  S_4 contains $4! = 24$ elements. One is the identity e. Six of them are exchange of two objects (i, j) (i to j and j to i, others untouched) and are of order 2. Three of them are exchanges of two pairs of objects $(i, j)(k, l)$ (i to j and j to i, k to l and l to k), still of order 2. Eight of them are cyclic permutations of three objects (i, j, k) (i to j, j to k, k to i, the other one untouched) and are of order 3. Six of them are cyclic permutations of four objects (i, j, k, l) (i to j to k to l to i) and are of order 4.

  Obviously this is a different group than D_4, but we can identify D_4 as a subgroup of S_4 corresponding to the subset of elements

  $$\{e, (A, C), (B, D), (A, B)(C, D), (A, D)(B, C), (A, C)(B, D), (A, B, C, D), (A, D, C, B)\} \quad (13)$$

  That is, D_4 can be identified as a subgroup of S_4.