What is a group?

See the heart symbol in Fig. 1. It is symmetric. What does it exactly mean that it is symmetric? See Fig. 2. If you reflect the heart symbol with respect to the dotted line, the shape remains the same. In other words, the heart symbol is symmetric because it remains the same under an action.

Figure 1: a heart symbol [1]

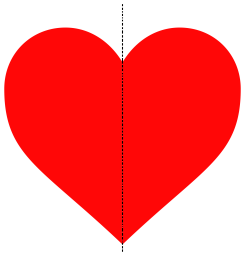

Figure 2: A heart symbol is symmetric, because it doesn't change under reflection of dotted line. [1]

Let's see another example of a symbol that is symmetric. See Fig. 3 for a square. You see that it has more symmetries than the heart symbol. See Fig. 4 for four blue lines. The square remains the same upon the reflection of each blue line. There are four possible reflections: s_0, s_1, s_2, s_3.

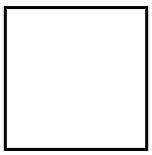

Figure 3: a square

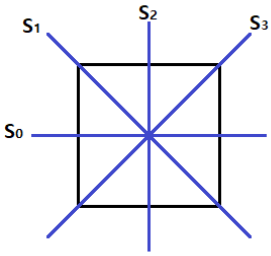

Figure 4: A square is symmetric, because it doesn't change under reflections

However, reflections are not the only symmetries a square has. See Fig. 5. If you rotate the square with O as its axis of rotation by 0°, 90°, 180°, 270° in a counter-

clockwise direction the square remains the same. (You may wonder why I included the rotation by 0° here, which seems redundant, but we will see why it is convenient to include it soon.)

Figure 5: A square is symmetric, because it doesn't change under rotations

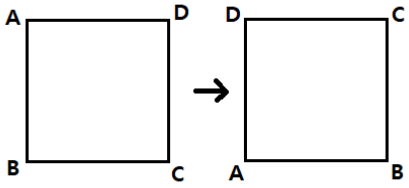

Figure 6: 90° counter clockwise rotation

So, we have a total of 8 actions that do not change the square. 4 reflections and 4 rotations. At this point, you may wonder why I didn't include the rotation in clockwise direction, but its net effect is the same as in counter-clockwise direction. Let's see why by examining how 90° clockwise rotation acts on the square as an example. See Fig. 6. Under such an action, A goes to D, B goes to A, C goes to B and so on. We can write it as:

$$A \to D \tag{1}$$

$$B \to A \tag{2}$$

$$C \to B \tag{3}$$

$$D \to C \tag{4}$$

The same can be said about 270° counter-clockwise rotation.

Actually, one can even make a table on how each of the 8 actions act on a square. Let's denote 0° counter-clockwise rotation by r_0, 90° counter-clockwise rotation by r_1, 180° counter-clockwise rotation by r_2, 270° counter-clockwise rotation by r_3. Then, we can write (4) as $r_1(D) = C$. In the table below, look for the row that begins with D (i.e., the last row) and see the r_1 column. There you find C.

	r_0	r_1	r_2	r_3	s_0	s_1	s_2	s_3
A	A	D	C	B	B	A	D	C
B	B	A	D	C	A	D	C	B
C	C	B	A	D	D	C	B	A
D	D	C	B	A	C	B	A	D

Given this, we will present four properties these 8 actions satisfy.

The first property is called "closure." If you perform one of the 8 actions, then perform one of the 8 actions again (the same one or a different one), the square will remain the same, as each of these two consecutive actions preserves the square. Thus, we can think of two consecutive actions as one action, which also preserves the square. For example, rotating 90° (r_1), then rotating 180° (r_2) is the same action as rotating 270° (r_3). In other words,

$$r_2(r_1(A)) = r_2(D) = B = r_3(A) \tag{5}$$

$$r_2(r_1(B)) = r_2(A) = C = r_3(B) \tag{6}$$

$$r_2(r_1(C)) = r_2(B) = D = r_3(C) \tag{7}$$

$$r_2(r_1(D)) = r_2(C) = A = r_3(D) \tag{8}$$

We can express it as $r_2 \bullet r_1 = r_3$.

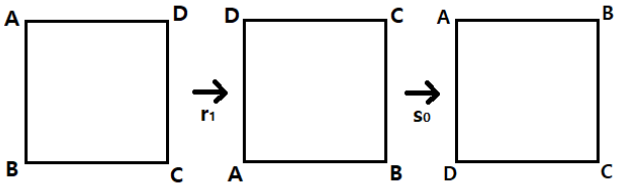

Figure 7: $s_0 \bullet r_1 = s_1$

Let's see another example. See Fig. 7. We see that rotating 90° counter clockwise (r_0), then reflecting through s_0 is the same action as reflecting through s_1. Compared to the first figure, the third figure shows that A and C, which are on the dotted line s_1 remain untouched, while B and D are swapped. In other words,

$$s_0(r_1(A)) = s_1(A) \tag{9}$$

$$s_0(r_1(B)) = s_1(B) \tag{10}$$

$$s_0(r_1(C)) = s_1(C) \tag{11}$$

$$s_0(r_1(D)) = s_1(D) \tag{12}$$

Thus, we have

$$s_0 \bullet r_1 = s_1 \tag{13}$$

Problem 1. Check that $r_1 \bullet s_0 = s_3$.

Let's express what we just explained in somewhat mathematical notations. If we denote the two actions by f and g, it means that there is another action h that satisfies

$h = f \bullet g$. Notice that this action h is one among the 8 actions, just like f and g are. It never happens that such an action h does not exist among the 8 actions.

The second property is called "associativity." If f, g, and h are in the 8 actions, then, we have

$$f \bullet (g \bullet h) = (f \bullet g) \bullet h \tag{14}$$

This can be understood as follows. Both the expressions on the left-hand side and the right-hand side mean that you act h, then g, then f. The left-hand side combines the first step and the second step (i.e, $g \bullet h$) then perform the third step (i.e., f), while the right-hand side combines the second step and the third step (i.e., $f \bullet g$), which you act after the first step (i.e., f). They should be the same.

Problem 2. Even though this property is obvious, let's just check (14) for one example. Show

$$s_1 \bullet (s_0 \bullet r_1) = (s_1 \bullet s_0) \bullet r_1 \tag{15}$$

by explicit calculation.

The third property is the existence of "identity element." There is a single special action among these 8 actions. Unlike all the other actions, r_0 does nothing on A, B, C, D. Such an action is called "identity" and often denoted as "e." In our case, we can write $e = r_0$. Now, notice that performing an action, say, f and doing nothing is the same thing as just performing the original action f. This can be written as $e \bullet f = f$. Similarly, doing nothing and performing an action, say, f is the same thing as just performing the original action f. In other words, $f \bullet e = f$. Notice that the identity element is unique. There is no two actions that satisfy $e \bullet f = f$.

The final property is the existence of "inverse element." For each action on the square, there is another action (either the same one or a different one) that can be performed to undo the original action. For example, if you rotate the square by 90° in a counter clockwise direction (i.e., r_1), it can be undone by 90° rotation in a clockwise direction (i.e., 270° rotation in a counter clockwise direction, r_3). In other words, first acting r_1 and then acting r_3 is the same thing as doing nothing, namely, e. In other words,

$$r_3 \bullet r_1 = e \tag{16}$$

We call r_3, the "inverse" of r_1. In a mathematical language, we express this statement as

$$r_3 = r_1^{-1} \tag{17}$$

More generally, for any f among the 8 actions, we always have a unique f^{-1} that satisfies

$$f^{-1} \bullet f = e \tag{18}$$

Problem 3. What is the inverse of r_3?

Problem 4. What is the inverse of s_2? (Hint[1])

Now, consider the expression $(f \bullet f^{-1}) \bullet f$. From the associativity, we have

$$(f \bullet f^{-1}) \bullet f = f \bullet (f^{-1} \bullet f) \tag{19}$$

from (18), we have

$$(f \bullet f^{-1}) \bullet f = f \bullet e = f \tag{20}$$

from $e \bullet f = f$, we see that the expression in the parenthesis must be

$$f \bullet f^{-1} = e \tag{21}$$

Thus, the action that satisfies (18) for f also satisfies (21).

So far, we found that the set of 8 actions on a square $(e, r_1, r_2, r_3, s_0, s_1, s_2, s_3)$ satisfy these four properties, but there are many other sets of actions that satisfy these four properties. So, such sets deserve a special name. They are called "group."

Let me put it this way. Mathematicians call any set of such actions that satisfy these four properties "group." In other words, this is the *definition* of group. Now, let me formerly introduce our friend "group."

A group G is a set with an operation $\bullet$ that combines any two elements f and g to form another element, (often called "multiplication") denoted $f \bullet g$ or fg. To qualify as a group, the set and operation, (G, $\bullet$), must satisfy following four requirements known as the group axiom.

(Closure) If f and g are in G then $h = f \bullet g$ is always in G.
(Associativity) If f, g and h are in G then $f \bullet (g \bullet h) = (f \bullet g) \bullet h$ is always satisfied.
(Identity element) There exists an element e in G such that for every element f in G, $e \bullet f = f \bullet e = f$ is satisfied.
(Inverse element) For every element f in G, there exists an inverse f^{-1} such that $f \bullet f^{-1} = f^{-1} \bullet f = e$

The 8 actions in our example of the symmetry of square is called "D_4." More generally, the Dihedral group D_n is a group of actions that preserve the n-polygon.

Of course, the Diheral groups are not the only examples of groups. Another good example of a group is integer with the operation (or "group multiplication") being addition. It satisfies the group axiom as follows.

[1]Reflecting with respect to s_2 can be undone by reflecting with respect to s_2. In other words, if you reflect with respect to s_2 twice, you get e.

(Closure) If a and b are integers then $a+b$ is always integer.
(Associativity) If a, b and c are integers, then $a+(b+c)=(a+b)+c$ is always satisfied.
(Identity element) For any integer a, $0+a=a+0=a$ is satisfied. Therefore 0 is the identity element.
(Inverse element) For any integer a, there exists an inverse $-a$ such that $a+(-a)=(-a)+a=0$

Problem 5. Do even integers with the group multiplication as addition form a group? How about odd integers?

Now, let's come back to the general properties of group. In a group G, is the identity element unique? After all, the identity element axiom only says that there is at least one identity element. It doesn't say that there *couldn't* be two or three elements that can serve as the identity element. However, it is easy to show that there is only one identity element, if G satisfies the four group axioms. Assume there are two identity elements, say, e_1 and e_2. Then, we have

$$f \bullet e_1 = f \bullet e_2 = f \tag{22}$$

Then, by the inverse element axiom, there is an inverse element to f. That is f^{-1}. Let's apply this inverse element f^{-1} to both sides. We have,

$$f^{-1} \bullet (f \bullet e_1) = f^{-1} \bullet (f \bullet e_2) \tag{23}$$

However, by the associativity axiom, we have

$$\begin{aligned} (f^{-1} \bullet f) \bullet e_1 &= (f^{-1} \bullet f) \bullet e_2 && (24) \\ e \bullet e_1 &= e \bullet e_2 && (25) \\ e_1 &= e_2 && (26) \end{aligned}$$

Therefore, the two identity elements we chosse are actually the same. There is only one identity element.

Problem 6. Show that for an arbitrary element f of G, there is only one inverse element. In other words, show that $g_1 = g_2$ is satisfied, if both g_1 and g_2 satsisfy

$$f \bullet g_1 = f \bullet g_2 = e \tag{27}$$

Problem 7. Show that the set of real number with multiplication as group multiplication is not a group. Which of the four axiom is violated? (Hint: the third axiom is not violated if you set the identity element to be 1.) On the other hand, show that the set of real number without 0 and with multiplication as group multiplication is a group.

A group is an abelian group if it satisfies the following additional axiom.

(Commutativity) If f, g are in G then $f \bullet g = g \bullet f$ is always satisfied.

For example, integer with the operation being addition is an abelain group, because

$$a + b = b + a \tag{28}$$

is always satisfied for any two integers a and b.

A group is called a non-abelian group, if it is not an abelian group.

Problem 8. Is D_4 an abelian group or a non-abelian group? (Hint[2])

Now, we introduce a new concept. If H, a subset of a group G satisfies the group axiom, we say H is a "subgroup" of G. For example, it is easy to check that the group of rotation of a square, i.e., $\{e, r_1, r_2, r_3\}$ is a subgroup of D_4. Another subgroup of D_4 is $\{e, s_0\}$. You can check the closure axiom, and the associativity axiom as follows. The identity element is obviously satisfied, because e is there, and the inverse element is easy to check as $e^{-1} = e$ and $s_0^{-1} = s_0$ which are both elements of $\{e, s_0\}$.

To make sure that you understand, let me give you an example of a subset which is *not* a subgroup of D_4. $\{e, r_1, r_2\}$ is not a subgroup, because the inverse of r_1, which is r_3 is not in the subset.

Note also that every group G has e and G as its subgroups.

Problem 9. Let H be a subgroup of G. If H is a non-abelian group, is G necessarily also a non-abelian group? If H is an abelian group, is G necessarily also an abelian group? Answer and explain your reasoning.

Probelm 10. (Challenging!) D_4 has 8 subgroups. Among these, we have seen four: $\{e\}, D_4, \{e, r_1, r_2, r_3\}, \{e, s_0\}$. Can you find the other four? (Hint[3])

Summary

- A group G is a set with an operation $\bullet$ that combines any two elements f and g to form another element, denoted $f \bullet g$. A group needs to satisfy the group axiom.
- Closure, associativity, the existence of the identity element, the existence of inverse element form the group axiom.

References

[1] `https://en.wikipedia.org/wiki/Heart_symbol`

[2] See (13) and Problem 1.

[3] Each of them has two elements.