Groups

A group G is a set of elements $G = \{I, a, b, c, ...\}$ and an operation (denoted $\circ$) between the elements in the group.

A group has the following properties (Note that w, x, and y in what follow could be any element from the set G):

- closure: The result of one element operating on another is itself an element of the group.
- identity element: There is a special element, called I, in the group such that the result of an operation involving I and another element from the group is the same element, $I \circ w = w$.
- inverses: For any element of the group, there is another element of the group x such that $w \circ x = I$. The element x is called the inverse of w, denoted $w^{-1} = x$.
- associativity: The result of several consecutive operations is the same regardless of the grouping, provided the consecutive order of operations is maintained. $w \circ x \circ y = w \circ (x \circ y) = (w \circ x) \circ y$.

Groups, studied in the field of abstract algebra, apply to many things in mathematics, from common arithmetic, to the theory underlying quantum mechanics.

To prove you have a group, you have to verify that all the above conditions hold for every possible combination of w, x, and y.

Symmetry groups have elements (the a, b, c, etc.) which are the rigid motions which preserve a pattern, and are called the symmetry group of the pattern. If you change the pattern, you change the group. The operation $\circ$ for the symmetry group is carried out by applying one rigid motion and then the next (sometimes called the "followed by" operator).

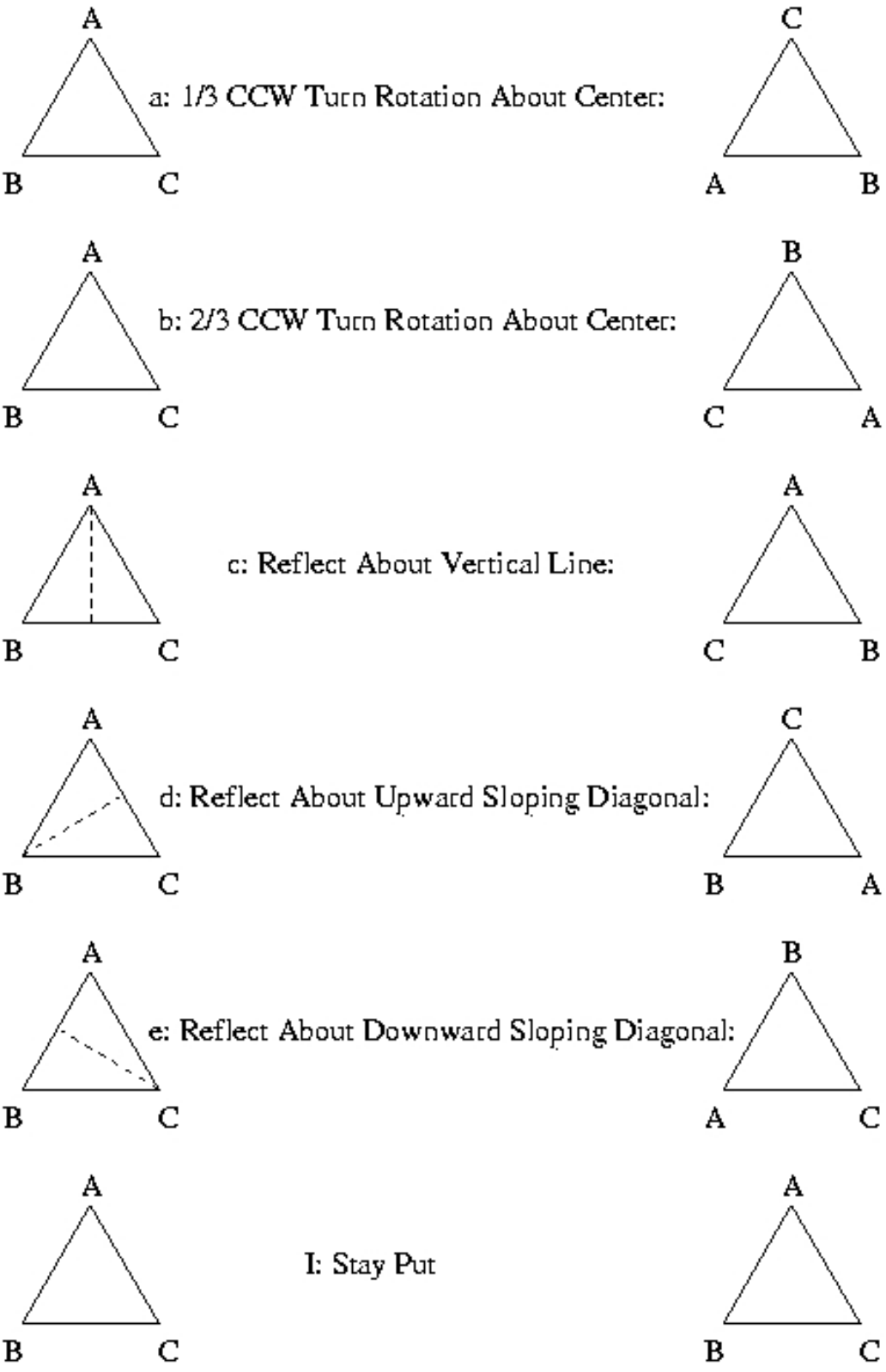
The operator is read from right to left, so we read $a \circ c$ and c followed by a.

The Symmetry Group of an Equilateral Triangle

An equilateral triangle has all sides equal length. Rigid motions can be applied to the triangle and the triangle will end up with its original appearance (this would be a symmetry). However, the corners of the original triangle have actually moved.

I will label the vertices of the triangle, so we can follow the effects of any rigid motions we apply to the triangle.

The rigid motions that leave the triangle unchanged are the following:



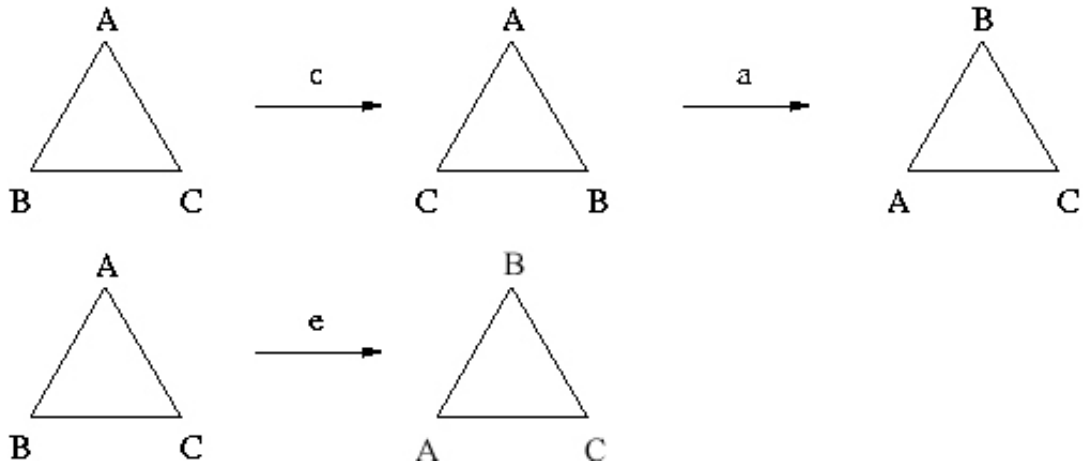
These six rigid motions form the symmetry group of the equilateral triangle, which we can denote as $G = \{I, a, b, c, d, e\}$. These are the rigid motions which leave the pattern (equilateral triangle) unchanged. Any rigid motion not in the symmetry group would change the pattern. Notice that we could have described a as a clockwise rotation of 240 degrees (or 2/3 turn).

Let's check some of the group properties. To verify this is a group mathematically we would have to check *every possible combination*, but we won't do that here!

- closure

  $a \circ c$ means we reflect across a vertical line, and then rotate 120 degrees counter-clockwise around the center of the triangle. Notice we do the rigid motion on the right first, then the rigid motion on the left.

  Here is the effect of performing these two rotations in succession:



  Notice that $a \circ c = e$.

  To prove that closure exists for our set, we would have to fill in all the entries of the following table, and show that the entries of the table were all elements of the group. The first motion performed comes from left hand column, and the second motion comes from the top row.

  So we have shown $a \circ c = e$:

$\circ$	I	a	b	c	d	e
I						
a						
b						
c		e				
d						
e						

  Exercise: Show $c \circ e = b$.

$\circ$	I	a	b	c	d	e
I						
a						
b						
c		e				
d						
e				b		

- identity element

  This is just I, the stay put element.

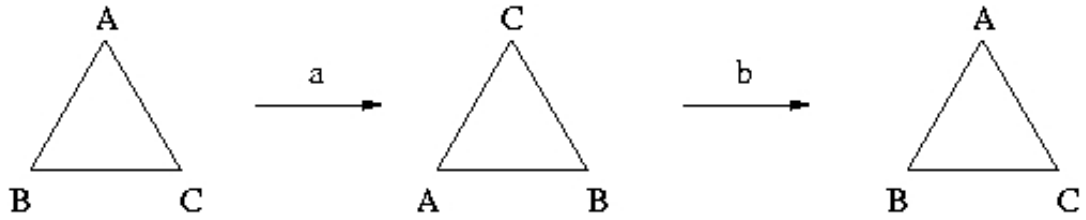
  So we can fill in more of our table, using things like $I \circ a = a$, etc.:

$\circ$	I	a	b	c	d	e
I	I	a	b	c	d	e
a	a					
b	b					
c	c	e				
d	d					
e	e			b		

- inverses

  Exercise: Show the reflection all have themselves as inverses, ie. $c \circ c = I$, $d \circ d = I$, and $e \circ e = I$.

  Exercise: Let's find the inverse of a.



  Notice that we have shown $a^{-1} = b$, since $a \circ b = I$. We could have read this off the table if we had filled it in completely earlier, but since we didn't we have another entry in the table:

$\circ$	I	a	b	c	d	e
I	I	a	b	c	d	e
a	a					
b	b	I				
c	c	e		I		
d	d				I	
e	e			b		I

  At this point we see the benefit of filling in the table, so let's do that. I am not showing the detail here, but you should be able to see from our earlier work that this is all about working out things like $a \circ a = b$.

$\circ$	I	a	b	c	d	e
I	I	a	b	c	d	e
a	a	b	I	d	e	c
b	b	I	a	e	c	d
c	c	e	d	I	b	a
d	d	c	e	a	I	b
e	e	d	c	b	a	I

- associativity

  If you have filled in all the elements of the table above, you can check associativity using the results of the multiplication table.

  Let's verify it for one case, $a \circ c \circ e$:

$$\begin{aligned} (a \circ c) \circ e &= e \circ e = I \\ a \circ (c \circ e) &= a \circ b = I \end{aligned}$$

  We have verified associativity for this particular case.

Cayley Table for a Group

The table we have constructed is called a multiplication table or more generally a Cayley Table. You can have Cayley tables for sets and operations which do not form groups. If the set G and operation $\circ$ form a group, the Cayley table will have the following properties:

- each column contains all the elements of G, with no repeats.
- the same is true for rows,
- the identity element I leaves the top row unchanged, and the identity element will leave the left hand column unchanged (you can use this to figure out what the identity is for a given Cayley table).

Other Cayley Tables

Rotations Only

If you consider just the rotations of the triangle (so only a and b) and the identity element, then you also get a group.

$\circ$	I	a	b
I	I	a	b
a	a	b	I
b	b	I	a

Modulo Addition

The expression $a \mod n$ means the remainder when a is divided by n, where a and n are positive integers.

Examples:

$32 \mod 5 = 2$ since $\frac{32}{5} = 6 + \frac{2}{5}$ or $32 = 5 \times 6 + 2.$

$14 \mod 8 = 6$ since $\frac{14}{8} = 1 + \frac{6}{8}$ or $14 = 1 \times 8 + 6.$

$15 \mod 3 = 0$ since $\frac{15}{3} = 5$ or $15 = 5 \times 3 + 0.$

Now, if we use the set of integers $\{0, 1, 2\}$ we can work out the Cayley table for $a \circ b = (a + b) \mod 3$. We will take a from the first column and b from the first row (this doesn't matter too much, as long as you are consistent when you create your table).

$(a+b) \mod 3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

From this table, we can see the identity element is 0.

Compare this to the Cayley table for rotations of the triangle. The Cayley tables for each have exactly the same structure. Addition modulo 3 on the set $\{0, 1, 2\}$ and the symmetric rotations of an equilateral triangle are exactly the same mathematical concepts!

Multiplication of integers

What we have just seen with Cayley tables is conceptually the same as the multiplication tables you have seen in the past. The only thing that changes is the set and the the operator. For example, in arithmetic multiplication, with the set all the integers and the operation arithmetic product, we have $G = \{\ldots -2, -1, 0, 1, 2, 3, 4, 5, \ldots\}$, and $\circ = \times$. Here is a portion of the infinite Cayley table:

$\times$	-2	-1	0	1	2	3
-2	4	2	0	-2	-4	-6
-1	1	1	0	-1	-2	-3
0	0	0	0	0	0	0
1	-2	-1	0	1	2	3
2	-4	-2	0	2	4	6
3	-6	-3	0	3	6	9

- This satisfies the closure requirement.
- The identity operator is 1.
- However, since some inverse elements are missing, this does not form a group. For example, there is no way to multiply 3 by an integer and get 1
- Associativity is also satisfied.

Addition of integers

However, the integers under addition does from a group. Here is a portion of the infinite Cayley table:

$+$	-2	-1	0	1	2	3
-2	-4	-3	-2	-1	0	1
-1	-3	-2	-1	0	1	2
0	-2	-1	0	1	2	3
1	-1	0	1	2	3	4
2	0	1	2	3	4	5
3	1	2	3	4	5	6

- This satisfies the closure requirement.
- The identity operator is 0.
- Each element has an inverse. For example, the inverse of 2 is -2, since $2 + (-2) = 0$.
- Associativity is also satisfied. For example, $(-2 + 5) + 7 = -2 + (5 + 7)$.
- So the integers under addition do form a group.

What this tells us is that there is something fundamentally different between the underlying structure of integers under multiplication and addition (one forms a group, one does not).