# Group Theory:
A Tutorial

Michael Leyton

Center for Discrete Mathematics & Theoretical Computer Science (DIMACS),
Busch Campus, Rutgers University, New Brunswick, NJ 08904, USA.
mleyton@dimacs.rutgers.edu

## 1 Groups and Symmetry

Symmetry means sameness, or indistinguishability, under some transformation. For example, a human face is indistinguishable from its reflected version, and therefore we say that it is reflectionally symmetric. A circle is indistinguishable from any of its rotated versions (about its center), and therefore we say that it is rotationally symmetric. When one puts together all the transformations that can be applied to an object, that leave it indistinguishable from its original version, one says that one has a *group* of transformations. Standardly, in mathematics, symmetry is characterized by the concept of a group of transformations. Fortunately, the concept of group is one of the simplest to understand in mathematics. One can think of a group simply as a list of the symmetries contained in an object. For example, a cube has a total of 48 symmetries, which are given by its reflectional and rotational axes. The group of a cube is therefore the list of those 48 symmetries. Any object has its own group which is a list of its symmetries. The purpose of this tutorial is to give the reader an introduction to groups and to the way they describe symmetries.

## 2 Symmetry Group $D_3$ of a Triangle

Consider the equilateral triangle in Fig 1. It appears highly symmetrical to us. For example, it is reflectionally symmetric about its vertical axis. Furthermore, it has other axes of symmetry. The group of the equilateral triangle is simply the total collection of symmetries that the figure possesses. By saying that the figure is reflectionally symmetric about the vertical axis, we have identified one of the members of the group. When we have listed all the other symmetries, we will have listed all the other members of the group. Let us therefore enumerate all the symmetries of the figure in order to gain a full specification of the group.

First recall that symmetry means sameness (indistinguishability) under some transformation. Therefore, when we say that the triangle in Fig 1 is reflectionally symmetric about the vertical axis, we are saying that the triangle is the same after applying the reflection about the vertical axis. That is, after applying the *transformation*, reflection, the triangle is brought into complete coincidence with itself.

Thus, to find all the symmetries of the triangle, one simply has to find all the transformations that bring the figure into coincidence with itself.

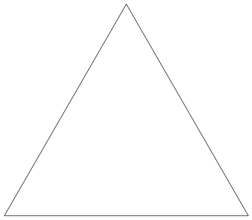

Figure 1: An equilateral triangle.

In order to keep track of the effects of the various transformations, which we try out, we shall label the vertices of the triangle, A, B, C, as shown in Fig 2a. Notice that reflection about the vertical produces Fig 2b. In this transformation, the vertices B and C, at the bottom of the triangle, have exchanged positions, and the top vertex, A, has remained in the same position. We shall label this reflection transformation, $m$, which stands for *mirror*. More precisely, $m$ will mean reflection about the vertical axis. In order to check whether $m$ has happened, we need only check whether the letters have changed in the way shown in Fig 2.

Now let us look at another type of transformation that makes the triangle coincide with itself. This transformation is clockwise rotation by $120^0$, shown in the transition between Fig 3a and 3b. In this transformation, the vertices have simply replaced each other in a simple cycle around the triangle; that is, vertex A has moved to B, vertex B to C, and vertex C to A. We shall label this rotation transformation, $r_{120}$. That is, $r_{120}$ will mean *rotation by* $120^0$ about the center of the triangle. In order to check whether $r_{120}$ has happened, we need only check whether the letters have changed in the way shown in Fig 3b.

Now let us look at the next largest rotation that brings the triangle back into coincidence with itself. This transformation is clockwise rotation by $240^0$, shown in the transition between Fig 4a and Fig 4b. In this transformation, the vertices have replaced each other one further step in a simple cycle around the triangle. We shall label this rotation transformation, $r_{240}$. That is, $r_{240}$ will mean rotation by $240^0$ about the center of the triangle. Again, in order to check whether $r_{240}$ has happened, we need only check whether the letters have changed in the way shown in Fig 4b.

Now let us see what happens when we try to obtain a still larger rotation bringing the triangle into coincidence with itself. This transformation is clockwise rotation by $360^0$. However, rotating the triangle by $360^0$ is equivalent to applying no transformation at all.

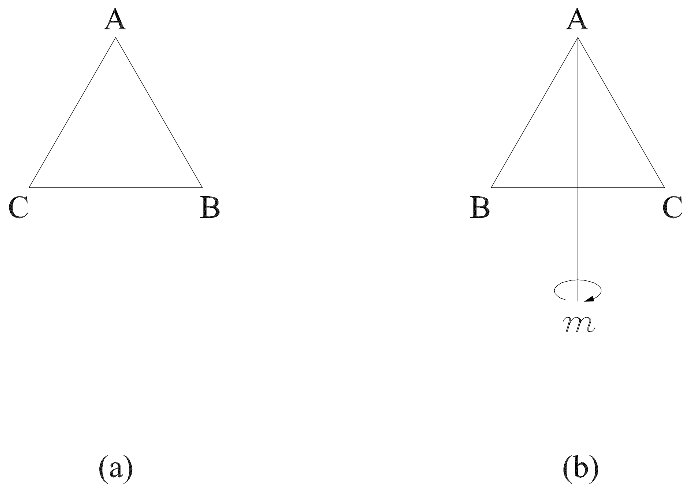

Figure 2: (a) An equilateral triangle. (b) Its vertical reflection.

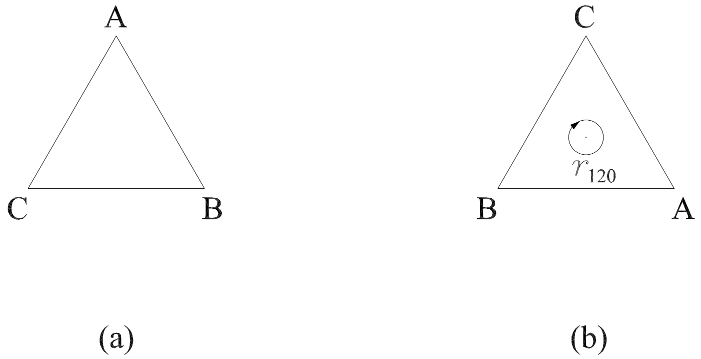

Figure 3: (a) An equilateral triangle. (b) Its rotation by $120^0$.

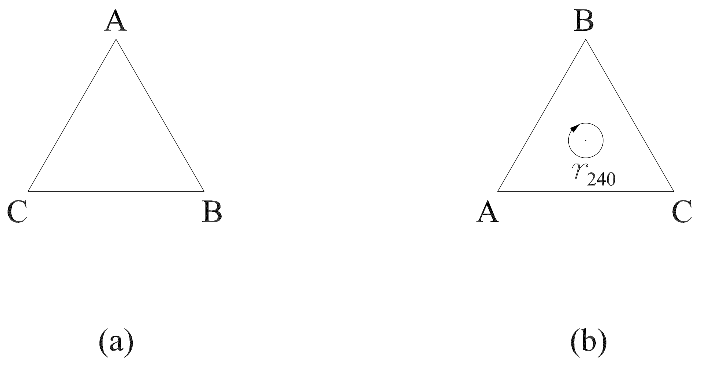

Figure 4: (a) An equilateral triangle. (b) Its rotation by $240^0$.

Thus, we can have a single label, $e$ for any transformation that has no ultimate effect on the vertices. For example, $e$ means rotation by $0^0$; but it also means rotation by $360^0$. The null transformation $e$ will be called the *identity element*.

To summarize so far, we have three rotations that bring the triangle into coincidence with itself:

$e$ the null transformation

$r_{120}$ rotation by $120^0$

$r_{240}$ rotation by $240^0$.

Now let us try to increase the amount of rotation above $360^0$. The next larger rotation, that brings the triangle into coincidence, is rotation by $360^0$ + $120^0$, which is $480^0$. However, observe that the effect of this rotation is exactly the same as rotation by $120^0$. This means that we do not have to include rotation by $480^0$ in our list of symmetries if we already have rotation by $120^0$. Similarly, any higher amount of rotation will simply duplicate the rotations we have already. Thus, the above list of three transformations, $e$, $r_{120}$, and $r_{240}$, exhaust all the distinguishable rotations the triangle can undergo to be brought into coincidence with itself.

Having established all the distinguishable *rotations* that create coincidence, let us return to the possible *reflections*. We have already seen that reflection about the vertical axis brings the triangle into coincidence with itself. This reflection, which is called $m$, is shown in Fig 5a. There are two other reflections that also work. One is shown in Fig 5b, and is the reflection about the axis indicated there. The other is shown in Fig 5c, and is the reflection about the axis shown there.

It is important to observe however that the reflection in Fig 5b can be obtained by combining two of the transformations we already have. This is demonstrated in Fig 6. We start in Fig 6a with the triangle in its initial position. We then apply $r_{120}$ obtaining

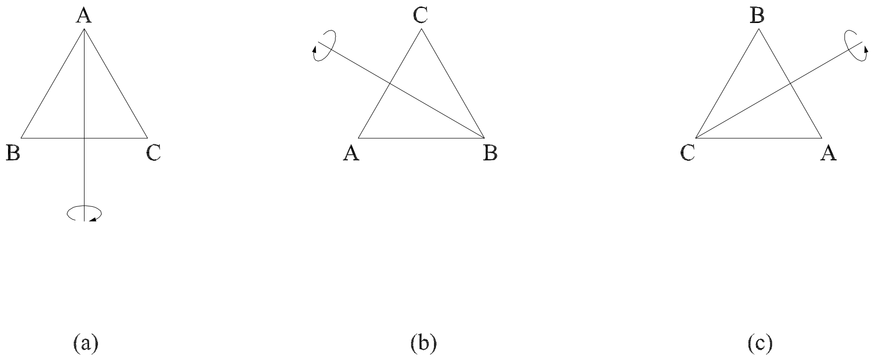

Figure 5: The three possible reflections of an equilateral triangle.

Fig 6b. Then we apply $m$ obtaining Fig 6c. However, the letters around the triangle in Fig 6c are in the same order and position as those in Fig 5b. Therefore the reflection in Fig 5b is equivalent to the application of $r_{120}$ followed by $m$. This combination can be written as $r_{120}m$. Similarly, the reflection in Fig 5c is equivalent to the application of $r_{240}$ followed by $m$, which we shall write as $r_{240}m$.

We have now enumerated all the rotations and all the reflections that bring the equilateral triangle into coincidence with itself. There are three rotations and three reflections, thus:

Rotations: $e,\ r_{120},\ r_{240}$

Reflections: $m,\ r_{120}m,\ r_{240}m.$

These are all the *symmetries* of the equilateral triangle. That is, the equilateral triangle has a total of six symmetries which we list between the parentheses on the next line:

$$D_3 \ = \ \{e,\ r_{120},\ r_{240},\ m,\ r_{120}m,\ r_{240}m\}.$$

The entire list is labelled $D_3$ meaning "Dihedral group of rank three". The first three members of the list (in the parentheses) are the three rotations, and the last three are the three reflections.

$D_3$ is an example of what is called a *group*. Any group is a set of elements that has four very simple properties, as follows:

**(1) Closure.**

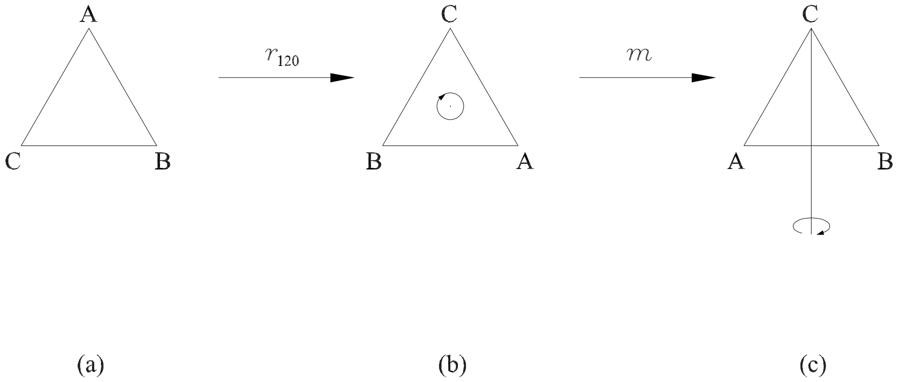

Figure 6: The reflection in Fig 5b can be generated in two successive stages.

Any pair of members of a group can be combined to produce another member of the group. For example, we saw that the rotation $r_{120}$ can be combined with the reflection $m$ to produce the reflection $r_{120}m$. Again, the rotation $r_{120}$ can be combined with the rotation $r_{240}$ to obtain $r_{120}r_{240}$, which turns out to be another member of the group. To see which member this is, observe that $r_{120}r_{240}$ is rotation by $120^0$ followed by rotation by $240^0$. This gives a total rotation of $360^0$ which is the null rotation. Therefore, the combination $r_{120}r_{240}$ is the same as the transformation $e$. As another example, we can combine $r_{120}$ with itself, obtaining $r_{120}r_{120}$, which is a rotation of $120^0$, applied twice. This combination is clearly $r_{240}$, which is also another member of the group.

In summary, therefore, we have illustrated the *closure* property of the group $D_3$. The property is simply this: Combining any pair of members of the group produces another member of that same group.

The closure property assumes the fact that we have a *means* of combining any two members of the group. We will make this means explicit by using the symbol $\circ$ to denote combination. For example, we have

$$r_{120} \circ r_{240}$$

which denotes the combination of $r_{120}$ and $r_{240}$. As we saw above, this combination is the same as the element $e$. That is,

$$r_{120} \circ r_{240} \quad = \quad e \quad .$$

Another example is the combination

$$r_{120} \circ r_{120}$$

which is, of course, $r_{240}$. That is, we have

$$r_{120} \circ r_{120} \quad = \quad r_{240}$$

The symbol $\circ$ will be called the *combination rule*. When the symbol occurs, it can easily be translated into English. For example:

$$r_{120} \circ r_{240}$$

means $r_{120}$ *followed by* $r_{240}$. Thus the combination rule $\circ$ means *followed by*.

We have seen above that the combination rule, $\circ$, in $D_3$ obeys the property called *closure*. That is, if one takes any two members of $D_3$ and combines them, one obtains another member of $D_3$. The combination rule $\circ$ obeys another three simple properties, as follows:

### (2) Associativity.

Note first that the operation $\circ$ combines any *two* elements of a group. Suppose now that we wish to combine *three* elements. For example, suppose we wish to form the combination

$$r_{120} \circ r_{240} \circ r_{240}$$

Then we can do this by a simple trick: we can break the triple into pairs. For example, we can break the triple like this:

$$(r_{120} \circ r_{240}) \circ r_{240}$$

This trick allows us to combine the elements one pair at the time, as follows: First, we combine the two elements in the parentheses to produce one element, which in this case is $e$. Then, we combine $e$ with the third element $r_{240}$ to produce $r_{240}$. At any of these stages, we combined only two elements. The parentheses indicated how to do this.

Observe now that our initial triple,

$$r_{120} \circ r_{240} \circ r_{240}$$

can be broken into pairs, either like this:

$$(r_{120} \circ r_{240}) \circ r_{240}$$

or, like this:

$$r_{120} \circ (r_{240} \circ r_{240})$$

The *Associativity* property of a group guarantees that either method of breaking the triple into pairs yields the same final result. That is,

$$(r_{120} \circ r_{240}) \circ r_{240} \quad = \quad r_{120} \circ (r_{240} \circ r_{240})$$

In other words, we do not have to worry about which way we choose to break a triple into pairs. Both ways will yield the same result. In fact, the reader can check that both sides in the above equation reduce to $r_{240}$.

The Associativity property is this ability to break a string into pairs in any way. It can be simply stated by saying that, for any three elements $x$, $y$, $z$, the following holds:

$$(x \circ y) \circ z \quad = \quad x \circ (y \circ z)$$

**(3) Identity Element.**

The group $D_3$ contains a null element, $e$; that is, an element which has no effect. As we said, this element is called the *identity element*. Any group must contain an identity element, and must contain only one identity element. The way to characterize this element is to specify that it has no effect *when combined* with any other element of the group. For example,

$$r_{120} \circ e$$

gives the result $r_{120}$. Furthermore, the reverse order,

$$e \circ r_{120}$$

also gives $r_{120}$. That is, in general, we characterize the identity element by saying that, given any member $x$ of the group, the following holds:

$$x \circ e \quad = \quad x \quad = \quad e \circ x$$

**(4) Inverses.**

Close examination reveals that any member of $D_3$ has a corresponding member which undoes the effect of that member. For example, consider the element, $r_{120}$, which is *clockwise* rotation by $120^0$. Clearly, the transformation that would undo the effect of $r_{120}$ would be *anti-clockwise* rotation by $120^0$. In fact, there is a member of $D_3$ that has exactly this effect. It is $r_{240}$. Although the element $r_{240}$ is clockwise rotation by $240^0$, its effect is equivalent to anticlockwise rotation by $120^0$. Now because the element $r_{240}$ undoes the effect of $r_{120}$, it is called the *inverse* of $r_{120}$. In fact, the elements $r_{240}$ and $r_{120}$ are mutual inverses. That is, not only does $r_{240}$ undo the effect of $r_{120}$, but $r_{120}$ undoes the effect of $r_{240}$.

Let us consider the reflection $m$. The effect of any reflection is undone by performing the reflection again. For example, consider Fig 7a, the triangle in its initial position. Now apply $m$ and thus obtain Fig 7b. In Fig 7b, the bottom vertices B and C have been reversed. Now apply $m$ again and obtain Fig 7c. Here the bottom vertices, B and C, have been reversed again, which means that they are in the same positions that they had in the initial configuration in Fig 7a. Thus, the second application of $m$ undoes the

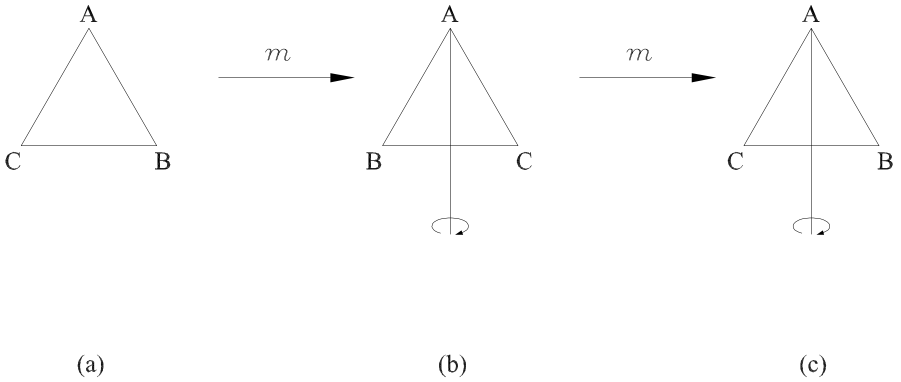

Figure 7: Application of $m$ followed by $m$ returns the figure to its original configuration.

first application of $m$. This means that $m$ must be *its own* inverse. The same argument applies to each of the other reflections $r_{120}m$ and $r_{240}m$. Each is its own inverse.

The inverse of any element $x$ will be denoted by $x^{-1}$. In a group, every element of the group has its own unique inverse. We can characterize this property by saying that, given any member $x$ of the group, there is a unique member $x^{-1}$ in the group, such that $x$ combined with $x^{-1}$ has a total of no effect; that is, the total effect of the combination is equivalent to the identity element, $e$. That is,

$$x \circ x^{-1} \quad = \quad e \quad = \quad x^{-1} \circ x$$

# 3 Four Basic Properties

Let us look back over the discussion in the previous section, in order to extract the general conclusions. We have been considering the symmetries of an equilateral triangle. On systematically elaborating all these symmetries, we found that there are a total of six; that is, three rotations and three reflections. The collection of six symmetries is given the label $D_3$. The collection, $D_3$, is a group for the following reasons. First, quite simply, it is a set of elements – in this case, it is a set of six transformations. Second, there is a rule, $\circ$, for combining any pair of elements. Finally, $D_3$ obeys four basic properties, as follows. (1) *Closure*: When any pair of elements in $D_3$ are combined, the resulting element is also in $D_3$. (2) *Associativity*: The combination of three elements in $D_3$ can be found by breaking the triple into pairs in either possible way. (3) *Identity*

*Element*: There is an element in $D_3$ that has no effect when combined with any other element in $D_3$. (4) *Inverses*: Each element, $x$, in $D_3$ has a corresponding element, $x^{-1}$, that undoes the effect of $x$.

Thus we can state the definition of a group: A group is a set, which has a rule $\circ$ for combining any pair of elements in the set, and which obeys the properties of *Closure*, *Associativity*, *Identity Element*, and *Inverses*.

# 4 Symmetry Group $D_4$ of a Square

The symmetry structure of an equilateral triangle is expressed by the group $D_3$. In exactly the same way, the symmetry structure of a square is captured by the group $D_4$. Because an equilateral triangle has three equal sides, its group $D_3$ consists of three rotations and three reflections. Similarly, because a square has four equal sides, its group $D_4$ consists of four rotations and four reflections. These transformations can be systematically elaborated as follows.

In order to keep track of the effects of the various transformations, which we try out, we shall label the vertices of the square, A, B, C, D, as shown in Fig 8a.

The smallest clockwise rotation that brings the square into coincidence with itself is rotation by $90^0$, shown in the transition between Fig 8a and 8b. In this transformation, the vertices have simply replaced each other in a simple cycle around the square; that is, vertex A has moved to B, vertex B to C, vertex C to D, and vertex D to A. We shall label this transformation, $r_{90}$. In order to check whether $r_{90}$ has happened, we need only check whether the letters have changed in the way shown in Fig 8b.

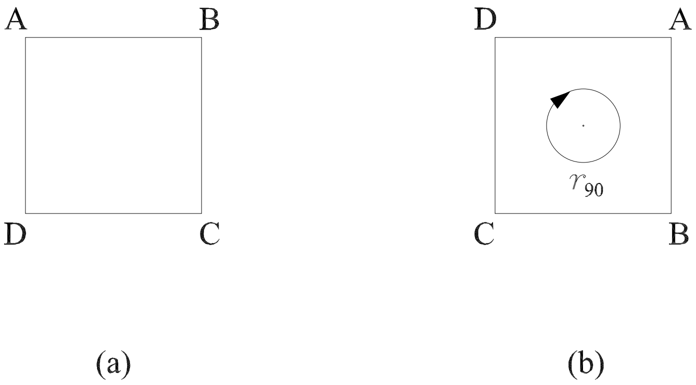

Figure 8: (a) A square. (b) A square after the application of rotation by $90^0$.

Now let us look at the next largest rotation that brings the square back into coincidence with itself. This transformation is clockwise rotation by $180^0$, shown in the transition between Fig 9a and 9b. In this transformation, the vertices have replaced each other one further step in a simple cycle around the square. We shall label this transformation, $r_{180}$. Again, in order to check whether $r_{180}$ has happened, we need only check whether the letters have changed in the way shown in Fig 9b.

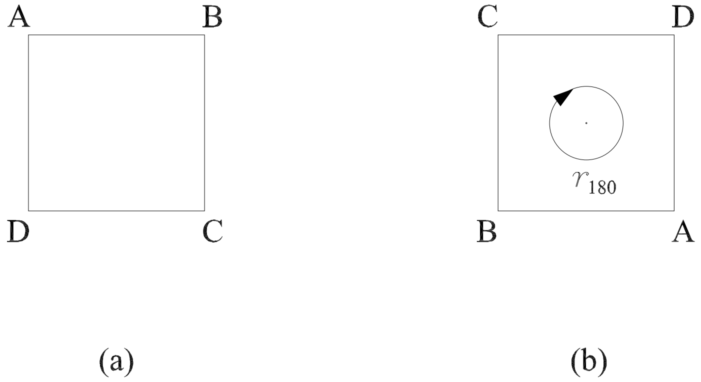

Figure 9: (a) A square. (b) A square after the application of rotation by $180^0$.

Now let us look at the next largest rotation that brings the square back into coincidence with itself. This transformation is clockwise rotation by $270^0$, shown in the transition between Fig 10a and 10b. In this transformation, the vertices have replaced each other one further step in a simple cycle around the square. We shall label this transformation, $r_{270}$. Again, in order to check whether $r_{270}$ has happened, we need only check whether the letters have changed in the way shown in Fig 10b.

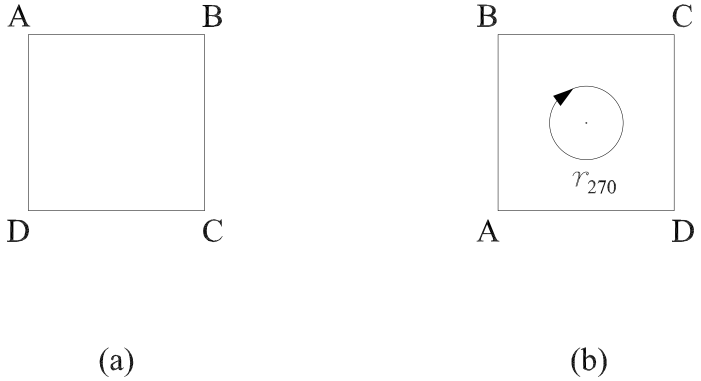

Figure 10: (a) A square. (b) A square after the application of rotation by $270^0$.

Now let us look at the next largest rotation that brings the square into coincidence with itself. This transformation is clockwise rotation by $360^0$. However, rotating the square by $360^0$ is equivalent to applying no transformation at all. Thus, we can have a single label, $e$, for any transformation that has no ultimate effect on the vertices. For example, $e$ means rotation by $0^0$; but it also means rotation by $360^0$. The null transformation $e$ is, of course, the *identity element* of the group $D_4$.

To summarize so far, we have four rotations that bring the square into coincidence with itself:

$e$, the null transformation

$r_{90}$, rotation by $90^0$

$r_{180}$, rotation by $180^0$

$r_{270}$, rotation by $270^0$

Now let us try to increase the amount of rotation above $360^0$. The next possible rotation, above $360^0$, that brings the square into coincidence, is rotation by $360^0$ + $90^0$, which is $450^0$. However, observe that the effect of this rotation is exactly the same as rotation by $90^0$. This means that we do not have to include rotation by $450^0$ in our list of symmetries if we already have rotation by $90^0$. Similarly, any higher amount of rotation will simply duplicate the rotations we have already. Thus, the above list of four transformations, $e$, $r_{90}$, $r_{180}$, and $r_{270}$, exhaust all the distinguishable rotations the square can undergo and be brought into coincidence with itself.

Having established all the distinguishable *rotations*, let us look at the possible *reflections*. Clearly, reflection about the vertical axis brings the square into coincidence with itself. This is the reflection that is shown in the transition from Fig 11a to Fig 11b. Observe that what has happened is that the top pair of vertices have been reversed, and the bottom pair of vertices have been reversed. This reflection will be labelled $m$.

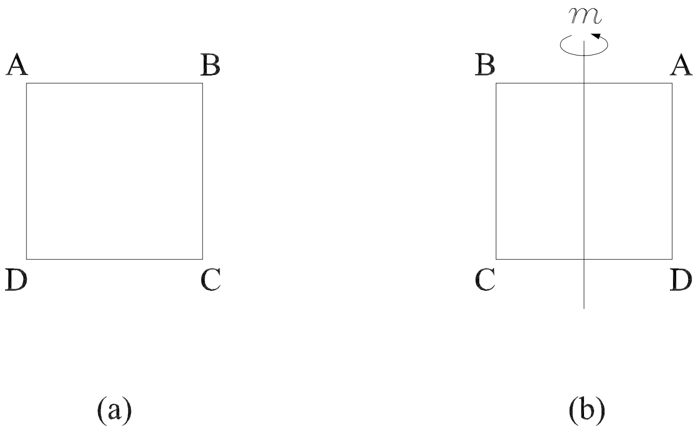

Figure 11: (a) A square. (b) A square after the application of reflection $m$.

There are a total of four distinct reflections that bring a square into coincidence with itself. The effect of reflection about the vertical, which we have just considered, is shown in Fig 12a. The three other reflections are shown in Fig 12b, c, and d, with their respective axes of reflection.

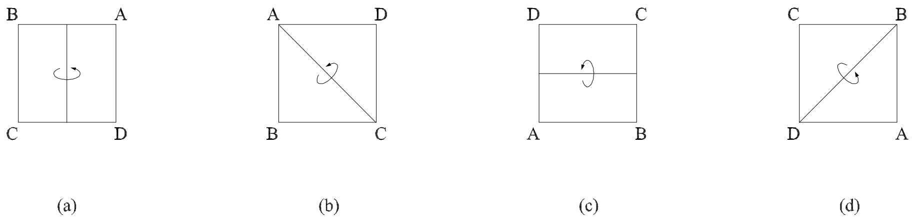

Figure 12: The four possible reflections of a square.

It is important to observe however that the reflection in Fig 12b can be obtained by combining two of the transformations we already have. This is shown in Fig 13. We start in Fig 13a with the square in its initial position. We then apply $r_{90}$ obtaining Fig 13b. Then we apply $m$ obtaining Fig 13c. However, the letters around the square in Fig 13c are in the same order and position as those in Fig 12b. Therefore the reflection in Fig 12b is equivalent to the application of $r_{90}$ followed by $m$. This combination can be written as $r_{90}m$. Similarly, the reflection in Fig 12c is equivalent to the application of $r_{180}$ followed by $m$, which we shall write as $r_{180}m$. Finally, the reflection in Fig 12d is equivalent to the application of $r_{270}$ followed by $m$, which we shall write as $r_{270}m$.

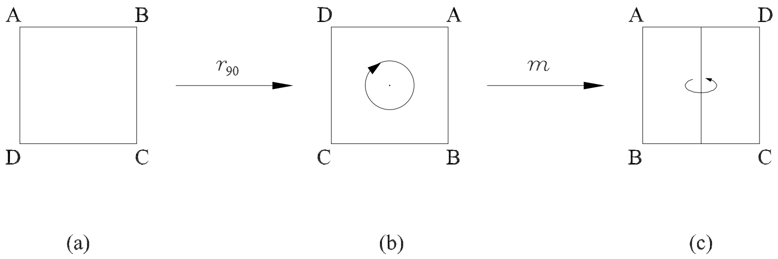

Figure 13: The reflection in Fig 12b can be generated in two stages.

We have now enumerated all the rotations and all the reflections that bring the square into coincidence with itself. There are four rotations and four reflections.

Rotations: $e, \ r_{90}, \ r_{180}, \ r_{270}$

Reflections: $m, \ r_{90}m, \ r_{180}m, \ r_{270}m.$

These are all the *symmetries* of the square. That is, the square has a total of eight symmetries which we list between the parentheses on the next line:

$$D_4 \ = \ \{e, \ r_{90}, \ r_{180}, \ r_{270}, \ m, \ r_{90}m, \ r_{180}m, \ r_{270}m\}$$

As we have said, this entire list is labelled $D_4$ meaning "Dihedral group of rank four". The first four members of the list (within the parentheses) are the four rotations and the last four are the four reflections.

It can easily be shown that $D_4$ is a group. This is done by showing that $D_4$ conforms to the four properties defining a group, as follows:

**(1) Closure.**

Any pair of members of $D_4$ can be combined to produce another member of the group. For example, the rotation $r_{90}$ can be combined with the rotation $r_{180}$ to obtain $r_{90} \circ r_{180}$, which turns out to be another member of the group. To see which member this is, observe that $r_{90} \circ r_{180}$ is rotation by $90^0$ followed by rotation by $180^0$. This gives a total rotation of $270^0$. Therefore, the combination $r_{90} \circ r_{180}$ is the same as $r_{270}$. As another example, we can combine $r_{90}$ with itself, obtaining $r_{90} \circ r_{90}$, which is a rotation of $90^0$, applied twice. This combination is clearly $r_{180}$, which is also another member of the group.

**(2) Associativity.**

As noted earlier, the operation $\circ$ combines any *two* elements of a group. The Associativity property ensures that any *three* elements can be combined with consistent results. For example, suppose we wish to form the combination

$$r_{90} \ \circ \ r_{270} \ \circ \ r_{90}$$

Then the Associativity property assures us that we can break the triple into pairs, in any way. That is, either as

$$(r_{90} \ \circ \ r_{270}) \ \circ \ r_{90}$$

or as

$$r_{90} \ \circ \ (r_{270} \ \circ \ r_{90})$$

In either case, one will obtain the same result, $r_{90}$.

**(3) Identity Element.**

The group $D_4$ contains a null element, $e$; that is, an element that has no effect. As we said, this element is called the *identity element* of the group. When it is combined with any other element of the group, the total effect is the same as the latter element on its own. For example,

$$r_{90} \ \circ \ e$$

is the same as $r_{90}$.

**(4) Inverses.**

Any member of $D_4$ has a corresponding member which undoes the effect of that member. For example, consider the element, $r_{90}$, which is *clockwise* rotation by $90^0$. Clearly, the transformation that would undo the effect of $r_{90}$ would be *anti-clockwise* rotation by $90^0$. In fact, there is a member of $D_4$ that has exactly this effect. It is $r_{270}$. The element $r_{270}$ is clockwise rotation by $270^0$, and this is equivalent to anticlockwise rotation by $90^0$. Because the element $r_{270}$ undoes the effect of $r_{90}$, it is the *inverse* of $r_{90}$.

Now consider the reflections $m$, $r_{90}m$, $r_{180}m$, $r_{270}m$. As noted earlier, the effect of any reflection is undone by performing the reflection again. Therefore, each of these reflections is its own inverse. Therefore, quite trivially, each reflection in $D_4$ has an inverse in $D_4$.

Let us finally look back over the discussion in this section. We have been considering the symmetries of a square. On systematically elaborating these symmetries, we found that there are a total of eight; that is, four rotations and four reflections. This collection of eight symmetries is given the label $D_4$. The collection, $D_4$, is a group for the following reasons. First of all, it is a set of elements – in this case it is a set of eight transformations. Second, there is a rule, $\circ$, for combining any pair of elements. Finally, $D_4$ obeys four basic properties, as follows. (1) *Closure*: When any pair of elements in $D_4$ are combined, the resulting element is also in $D_4$. (2)*Associativity*: The combination of three elements in $D_4$ can be found by breaking the triple into pairs in either possible way. (3) *Identity Element*: There is an element in $D_4$ that has no effect when combined with any other element in $D_4$. (4) *Inverses*: Each element, $x$, in $D_4$ has a corresponding element, $x^{-1}$, that undoes the effect of $x$.

# 5 Symmetry Group $D_n$ of a Regular Planar Polygon

Let us continue looking at polygons in the plane.

The symmetry structure of an equilateral triangle is expressed by the group $D_3$. The symmetry structure of a square is expressed by the group $D_4$. Correspondingly, the symmetry structure of any regular polygon of $n$ sides is given by the group $D_n$. For example, the symmetry group of a pentagon is $D_5$, the symmetry group of a hexagon is $D_6$, and so on.

For each regular polygon of $n$ sides, the associated group $D_n$ has the same general structure. The group consists of $n$ rotations, and $n$ reflections. That is, the group consists of

Rotations: $e, \; r, \; r^2, \; r^3, ........ \; r^{n-1}$

Reflections: $m, \; rm, \; r^2m, \; r^3m, ......., \; r^{n-1}m.$

where $r$ is the smallest rotation that brings the polygon into coincidence with itself. Notice that the rotation list consists of successively increasing multiples of $r$. The highest multiple is $r^{n-1}$ because the next highest multiple, $r^n$, is simply rotation by $360^0$, which is $e$. Notice also that the reflections are exactly the same rotations each multiplied by $m$.

# 6 Cyclic Group $\mathbb{Z}_n$

Consider again the symmetry group $D_3$ of an equilateral triangle. We have seen that $D_3$ splits into two halves.

Rotations: $e, \; r_{120}, \; r_{240}$

Reflections: $m, \; r_{120}m, \; r_{240}m.$

The three rotations, in fact, together form a group. That is, the set

Rotations: $e, \; r_{120}, \; r_{240}$

is a group in its own right. This can easily be checked by showing that this set satisfies the four properties of a group: (1) *Closure*: When any pair of the rotations is combined, the resulting transformation is also one of the rotations. (2) *Associativity*: The combination of three of the rotations (e.g. including possible repetitions) can be found by breaking the triple into pairs in either possible way. (3) *Identity Element*: One of the rotations, $e$, has no effect when combined with any of the other rotations. (4) *Inverses*: To each of the three rotations there is another rotation (amongst the three) that undoes the effect of the rotation.

Thus the three rotations form a group. Now observe the following: $D_3$ is, as we have seen, a group. However, it splits into two halves, its set of rotations and its set of reflections. The set of rotations forms a group in its own right. Generally speaking, if a subset of a group is itself a group, then it is called a *subgroup*. Therefore, the set of rotations is a subgroup of $D_3$.

The set of rotations we have been considering, $e$, $r_{120}$, $r_{240}$, is a particularly simple group. It is a cycle, as follows. Applying $r_{120}$ three successive times moves one successively through the three rotations. That is, applying $r_{120}$ once is simply $r_{120}$ (rotation by $120^0$); applying $r_{120}$ twice yields $r_{240}$ (rotation by $240^0$); applying $r_{120}$

three times is equivalent to no rotation, that is $e$. Now if one continues to apply $r_{120}$, one will again cycle through the three rotations, again and again.

Because the above group of rotations forms a cycle of size three, it is called the *cyclic group of order 3*, and is labelled $\mathbb{Z}_3$. That is we have:

$$\mathbb{Z}_3 \;=\; \{e,\; r_{120},\; r_{240}\}.$$

We have seen therefore that the symmetry group $D_3$ of an equilateral triangle splits into two halves, its set of rotations and its set of reflections. The set of rotations forms a group $\mathbb{Z}_3$.

Consider now the symmetry group, $D_4$, of a square. We have seen, earlier, that $D_4$ also splits into two halves.

Rotations: $e,\; r_{90},\; r_{180},\; r_{270}$

Reflections: $m,\; r_{90}m,\; r_{180}m,\; r_{270}m.$

The four rotations, in fact, together form a group. This can easily be checked by showing that together, they satisfy the four properties of a group: Closure, Associativity, Identity Element, and Inverses.

Therefore, the four rotations $e$, $r_{90}$, $r_{180}$, $r_{270}$, form a *subgroup* of $D_4$. This subgroup is again a *cycle*. That is, applying $r_{90}$ four successive times moves one successively through the four rotations. Therefore, the group formed by the four rotations is called the *cyclic group of order 4*, and will be labelled $\mathbb{Z}_4$. That is we have:

$$\mathbb{Z}_4 \;=\; \{e,\; r_{90},\; r_{180},\; r_{270}\}.$$

Thus, we have seen that the symmetry group $D_4$ of a square splits into two halves, its set of rotations and its set of reflections. The set of rotations forms a group $\mathbb{Z}_4$.

Recall now that, given a regular polygon, of any number of sides $n$, its symmetry group $D_n$ splits into two halves, thus:

Rotations: $e,\; r,\; r^2,\; r^3, \ldots\ldots\ldots\; r^{n-1}$

Reflections: $m,\; rm,\; r^2m,\; r^3m, \ldots\ldots,\; r^{n-1}m.$

The *rotations* together form a group. Furthermore, the group is simply a cycle of size $n$. That is, applying $r$, successively, moves one successively through all the rotations, in a cyclic fashion. This group of rotations will therefore be labelled $\mathbb{Z}_n$. That is,

$$\mathbb{Z}_n \;=\; \{e,\; r,\; r^2,\; r^3, \ldots\ldots\ldots\; r^{n-1}\}.$$

Generally, $\mathbb{Z}_n$ is called the *cyclic group of order* $n$.

# 7 Reflection Group $\mathbb{Z}_2$

As we observed, $D_3$ has three reflections, $m$, $r_{120}m$, and $r_{240}m$. Let us consider $m$. We noted that applying $m$ twice has the same effect as doing nothing; that is, it has the same effect as applying $e$. Now, applying $m$ a third time produces $m$. Furthermore, applying $m$ a fourth time produces $e$. Thus, continuing to apply $m$ simply cycles backwards and forwards between $e$ and $m$. This means that the set consisting purely of $e$ and $m$ forms a group. The group is, of course, $\mathbb{Z}_2$. That is

$$\mathbb{Z}_2 \;=\; \{e,\;m\}$$

The same argument applies to the reflection $r_{120}m$. This means that repetition of $r_{120}m$ produces a cycle of size two. That is, applying $r_{120}m$ once produces $r_{120}m$; applying $r_{120}m$ twice produces $e$; and continuing to apply $r_{120}m$ simply cycles backwards and forwards between $e$ and $r_{120}m$. Thus the set consisting purely of $e$ and $r_{120}m$ forms a group. The group is, again, an example of $\mathbb{Z}_2$.

Exactly, the same argument applies when we take the third reflection $r_{240}m$ in $D_3$. This reflection too forms a group together with $e$. The group is, again, an example of $\mathbb{Z}_2$.

Now consider $D_n$, that is, the symmetry group of the $n$-sided polygon. We saw that, besides its $n$ rotations, it contains $n$ reflections. We can now see that each reflection can be paired with the identity $e$ to form a group of size 2, the group $\mathbb{Z}_2$.

One final point is worth making. Let us return again to $D_3$, the symmetry group of an equilateral triangle. We have often considered $D_3$ split into two halves: the three rotations and the three reflections. We have also observed that the three rotations *together* form a group.

The reader might now ask whether the three reflections also, *together*, form a group; that is, whether the set consisting purely of the reflections, $m,\ \ r_{120}m,\ \ r_{240}m$, is a group. The answer is negative. Nevertheless, we have now seen that each *individual* reflection, paired with the identity element, $e$, forms a group, $\mathbb{Z}_2$.

These considerations are of course general. The symmetry group, $D_n$, of an $n$-sided polygon, contains $n$ rotations and $n$ reflections. However, whereas the $n$ rotations *together* form a group, the $n$ reflections do not. Nevertheless, each *individual* reflection, together with $e$ forms a group of size 2, the group $\mathbb{Z}_2$.

# 8 Continuous Rotation Group $SO(2)$

We have seen that the group $D_n$ of any regular $n$-sided polygon contains a group of rotations given by $\mathbb{Z}_n$. The rotations are $n$ equally spaced rotations. Thus they can be represented by $n$ equally spaced notches around a circular clock. For example, Fig 14 shows the particular notches on a clock which mark each successive quarter of an hour (i.e. the 12, 3, 6, and 9 o' clock positions). There are four such notches, and the hand rotates $90^0$ between each successive notch. Since the hand goes through four such successive rotations to get back to the starting position, the hand goes through the group

$\mathbb{Z}_4$. This is exactly the same group as the rotation group of a square; i.e. the rotation group within $D_4$.

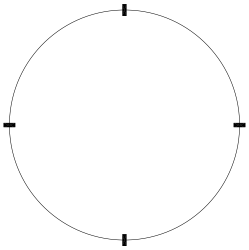

Figure 14: A clock with the quarter hour positions marked.

Again consider those twelve notches that mark the hours on a clock. The hand rotates $30^0$ between each successive notch. Since the hand goes through twelve such successive rotations to get back to the starting position, the hand must go through the group $\mathbb{Z}_{12}$. This group is of course the same group as the group of rotations of a 12-sided polygon. Again, of we increase the number of equally spaced notches to 1000, we will have the group $\mathbb{Z}_{1000}$.

Now let us suppose that we allow *all* the points on the circle to become notches; i.e. the entire continuum of points around the circle. That is, we allow rotations between *any* points on the circle. The entire set of rotations forms a group. For example, consider Fig 15a and 15b. They show rotations to two arbitrary points on the circle. These two rotations can be added as shown in Fig 15c. The combination is of course equivalent to another rotation on the circle.

Observe also that the group forms a cyclic group. This is because rotating past $360^0$ will cause one to "wrap around" and start again.

The main difference between any of the previous cyclic groups, $\mathbb{Z}_n$, and the new cyclic group, is that the former were *discrete*, in this sense: In a previous $\mathbb{Z}_n$ group, the rotations could increase only by discrete steps; e.g. in $\mathbb{Z}_4$, the rotations increased by $90^0$ discrete steps. In the new group, however, the amount of rotation can increase *continuously*, rather than being confined to discrete steps. That is, there is a *continuum* of rotations, one rotation for each point on the circular continuum around the clock.

The continuous group of rotations is standardly labelled $SO(2)$. It is the largest possible group of rotations (around a point in the plane). Any other rotation group is an example of $\mathbb{Z}_n$. Furthermore, any $\mathbb{Z}_n$ is a subgroup of the group $SO(2)$. For example, $\mathbb{Z}_4$, the rotation group of a square, has selected the four $90^0$ rotations from the overall group $SO(2)$. Again, the twelve-hour clock, $\mathbb{Z}_{12}$, has selected the twelve $30^0$ rotations from the overall group $SO(2)$.

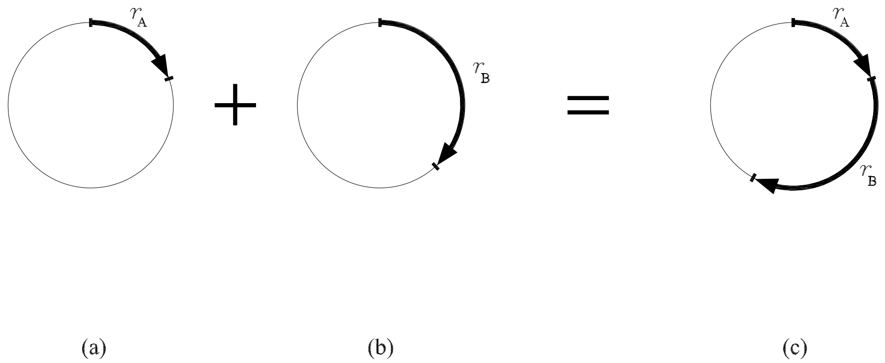

Figure 15: The addition of two rotations produces another rotation.

## 9 Continuous Translation Group $\mathbb{R}$ along a Line

The group $SO(2)$ is a continuous group. That is, rotations can increase continuously around the circle rather than be confined to discrete steps like any $\mathbb{Z}_n$. The group $SO(2)$ has a very simple structure. However, it is not the simplest possible continuous group. There is a continuous group that is even simpler. This is the group of translations along a line.

Imagine an infinite straight line. Now consider translations, or movements, along that line. Notice that any pair of translations can be combined to form another translation. For example, Fig 16a represents a translation by 5 inches and Fig 16b represents a translation by 2 inches. These can be added together, as shown in Fig 16c, to yield a total translation of 7 inches. Consider all possible translations along the line, in both the negative and positive directions. The entire collection forms a group that we will simply call $\mathbb{R}$.

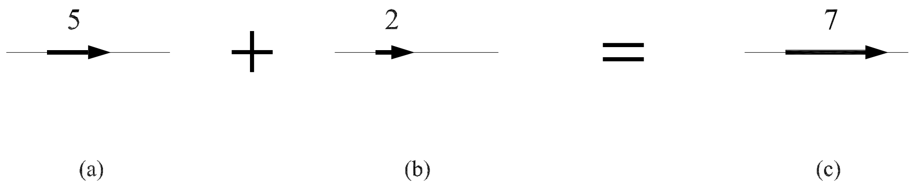

Figure 16: The addition of two translations produces another translation.

One can easily show that $\mathbb{R}$ forms a group, and we will show this, in order to remind the reader of this procedure: First observe that, if we combine any pair of translations, as illustrated in Fig 16, we obtain another translation. This means that the set of translations is *closed* under combination.

Again, observe that a combination of three translations, for example,

$$\text{5 inches} \ + \ \text{2 inches} \ + \ \text{3 inches}$$

can be partitioned into pairs in either way. That is,

$$(\text{5 inches} \ + \ \text{2 inches}) \ + \ \text{3 inches} \quad = \quad \text{5 inches} \ + \ (\text{2 inches} \ + \ \text{3 inches}).$$

Thus translations conform to the *Associativity* property.

Again, observe that there is a translation with no effect: The translation by 0 inches. This acts as an *identity element*. For example,

$$\text{5 inches} \ + \ \text{0 inches} \quad = \quad \text{5 inches}$$

Finally, observe that, for each translation, there is a translation that undoes its effect. The latter is simply the former applied in the opposite direction. For example, the translation, 5 inches, is undone by applying the translation, $-5$ inches. Thus, generally, each translation has an *inverse*.

We conclude therefore that $\mathbb{R}$ is a group, i.e. it conforms to the four requirements for a group: *Closure*, *Associativity*, *Identity Element*, and *Inverses*.

Recall now the relationship between the groups $\mathbb{Z}_n$ (for all sizes $n$) and the group $SO(2)$. The former groups are all discrete; that is, the amount of rotation in a $\mathbb{Z}_n$ can increase through the successive members of $\mathbb{Z}_n$ by only discrete steps (e.g. by intervals of $90^0$ in $\mathbb{Z}_4$). In contrast the amount of rotation in $SO(2)$ can increase by continuous amounts. Each $\mathbb{Z}_n$ is therefore a *discrete subgroup* of the continuous group $SO(2)$.

Now let us return to $\mathbb{R}$. This is a continuous group. That is, one can increase the amount of translation continuously through the group, i.e. along the straight line. However, just as $SO(2)$ has discrete subgroups, $\mathbb{R}$ has discrete subgroups. Each of the discrete subgroups in $\mathbb{R}$ is simply the successive translation by an equal interval. For example, one such subgroup is the group of translations by the following amounts:

$$\{......... - 3, \quad - 2, \quad - 1, \quad 0, \quad 1, \quad 2, \quad 3, .........\}$$

This group is called $\mathbb{Z}$. Thus, whereas the complete group $\mathbb{R}$ allows movement to any point along the line shown in Fig 17a, the subgroup $\mathbb{Z}$ is confined to movements to only the equally-spaced dots in Fig 17b.

# 10 Continuous Translation Group $\mathbb{R} \times \mathbb{R}$ in a Plane

In the previous section, we considered translations along a line. Now let us consider translations in a plane. The plane is depicted in Fig 18a with a horizontal and a vertical axis. Consider any translation in this plane, for example, the translation shown in

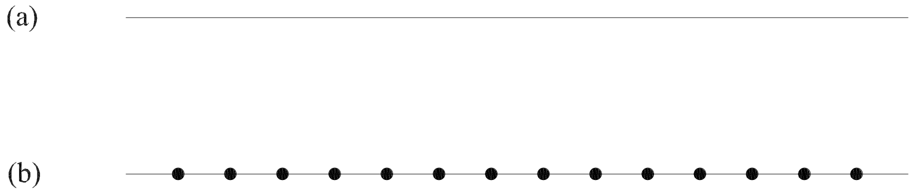

Figure 17: (a) $\mathbb{R}$ allows movements to all points; (b) $\mathbb{Z}$ to equally-spaced points.

Fig 18b from the origin to point $p$. Clearly, this translation can be accomplished by combining a translation in the horizontal direction, and a translation in the vertical direction. However, the set of movements along the horizontal direction is simply a copy of the group $\mathbb{R}$, defined in section 9 (i.e. translations along a line). Similarly, the set of movements along the vertical direction is a copy of the group $\mathbb{R}$ (i.e. translations along a line). This means that the entire set of translations in the plane is produced by a combination of two copies of the group $\mathbb{R}$. This combination will be written simply as

$$\mathbb{R} \times \mathbb{R}$$

The set of translations in the plane, $\mathbb{R} \times \mathbb{R}$, is itself a group. That is, any pair of planar translations can be combined to give another planar translation (i.e. the Closure property holds). A triple of successive planar translations can be broken into pairs in either way (i.e. the Associativity property holds). There is a planar translation that has no effect, i.e. the zero translation, and this serves as the identity element. Finally, any planar translation has its inverse – the translation by the same distance in the opposite direction.

## 11 Euclidean Group $E(2)$

Although we have so far mentioned several examples of groups, the transformations which have made up the groups have been of three types: rotations, reflections, and translations. There exist groups with very different types of transformations, as we shall see. However, rotations, reflections and translations share a common property. *They all preserve size and shape*. For example, consider the letter E on the upper left of Fig 19a. After it has been rotated, as shown in Fig 19a, it has the same size and shape as it had before rotation. Fig 19b shows it undergoing a reflection. Again, although it has changed sidedness, its size and shape are the same. Finally, in Fig 19c, the letter has undergone a translation. Again, its size and shape have been preserved.

A transformation that preserves size and shape is called a *Euclidean transformation*. Any Euclidean transformation is a combination of a rotation, a reflection and

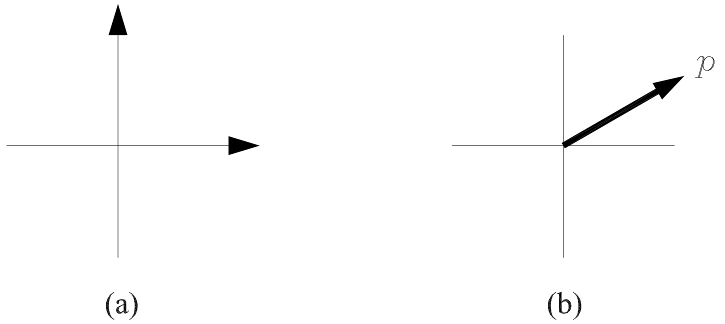

Figure 18: (a) Horizontal and vertical translations. (b) Translation to point $p$.

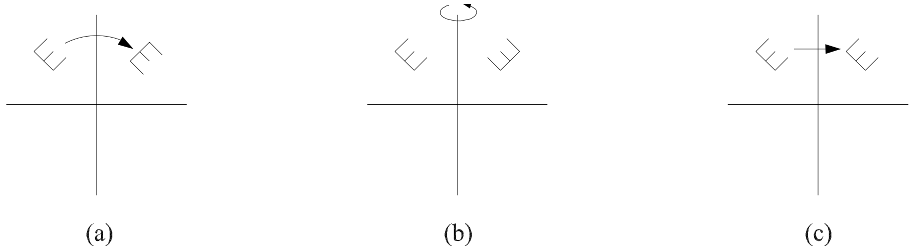

Figure 19: The Euclidean motions of (a) rotation, (b) reflection, and (c) translation.

a translation. For example, Fig 20a shows a letter E that has undergone a Euclidean transformation, i.e. its size and shape have remained the same. Fig 20b shows that this transformation can be reconstructed using a translation followed by a rotation.

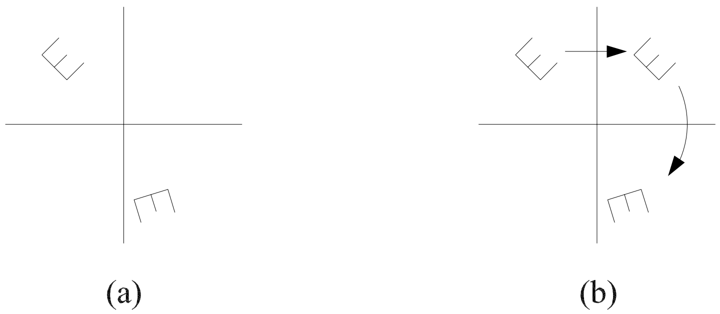

Figure 20: (a) A Euclidean motion, (b) decomposed into a translation followed by a rotation.

The set of all Euclidean transformations, i.e. size-and-shape preserving transformations, forms a group. This is easy to check, as follows: The combination of any pair of size-and-shape preserving transformations is a transformation that also preserves size and shape, and thus is in the same group; i.e. the Closure property is satisfied. A triple of such transformations can be broken into pairs in either possible way; i.e. the Associativity property is satisfied. There is a null transformation that preserves size and shape, i.e. the transformation that does nothing at all; i.e. there exists a unique identity element. And finally, to each transformation that preserves size and shape, there is a transformation that undoes its effect while preserving size and shape; i.e. the existence of inverses.

The group of size-and-shape preserving transformations, called the Euclidean group, will be labelled $E(2)$. The number 2 is the dimension of the space on which it acts, i.e., the plane. This group consists of all the planar rotations, reflections and translations, as well as all their combinations.

All the groups we considered in the previous sections were subgroups of the Euclidean group. For example, the group $D_n$, the symmetry group of the $n$-sided polygon, consists of $n$ rotations and $n$ reflections; i.e. Euclidean transformations. Recall also that the $n$ rotations form a group called $\mathbb{Z}_n$. Observe that both $D_n$ and $\mathbb{Z}_n$ have a finite number of elements. $D_n$ consists of $2n$ elements, and $\mathbb{Z}_n$ consists of $n$ elements. The groups $D_n$ and $\mathbb{Z}_n$ have a special significance in the group $E(2)$: They are the *only* finite subgroups of $E(2)$.

Recall now that three of the groups we examined in the previous sections were

$SO(2)$: the continuous group of rotations.

$\mathbb{Z}_2$: the reflection group of two elements $\{e, m\}$.

$\mathbb{R} \times \mathbb{R}$: the group of translations of the plane.

Each of these groups is a subgroup of the Euclidean group. In fact, the Euclidean group is simply a combination of these three groups. That is, any Euclidean transformation can be written as a combination of transformations from these three groups.

Finally note that the Euclidean group of $n$-dimensional space is labelled $E(n)$.

## 12 General Linear Group $GL(2, \mathbb{R})$

Euclidean transformations preserve shape and size. We shall now consider a slightly more general class of transformations: those that preserve *straightness*; i.e. do not involve bending. Such transformations are called *linear transformations*. In fact, to be more precise, linear transformations preserve straightness *and* the position of the origin.

We can see that any rotation is a linear transformation. For example, consider the rotation shown in going from Fig 21a to Fig 21b. The $x$-axis in Fig 21a is a straight line. After it is rotated, it becomes the axis labelled $X$ in Fig 21b. This is also a straight line. Thus, although the $x$-axis has been moved, its straightness is preserved. The same is true of the $y$-axis.

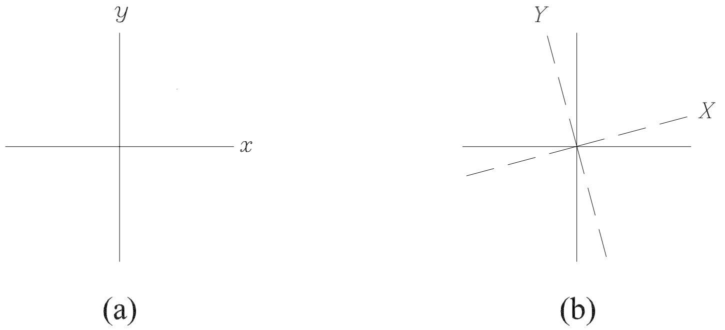

Figure 21: A rotation preserves straightness.

The fact that a rotation preserves straightness is due to the fact that rotation preserves shape; i.e. straightness is a shape-like property. However, there are some transformations that preserve straightness but do not preserve shape. An example is the transformation between a square and a rotated parallelogram as illustrated in Fig 22. Consider, for example, the $x$-axis and $y$-axis in Fig 22a. They are both straight lines. Under the transformation, the axes become the dashed lines shown in Fig 22b. These latter lines are also straight. Thus, as a result of the transformation, the axes in Fig 22a change position and their relation to one another, but nevertheless remain straight. In fact, any of the straight lines in Fig 22a remain straight lines in Fig 22b. Observe also another property of this transformation: the origin has remained in the same position. Nevertheless, the shape has not been preserved.

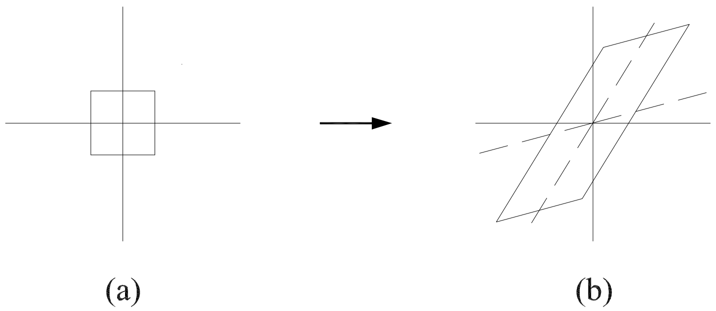

Figure 22: A linear transformation preserves straightness and the origin, but not necessarily shape.

The set of linear transformations forms a *group*. This is not difficult to see. The combination of two transformations which preserve straightness must be another transformation that preserves straightness. Thus, the Closure property holds. Again, a combination of three transformations that preserve straightness can be broken down into pairs, in either way possible. Thus the Associativity property holds. The identity element is simply the transformation that does nothing. Clearly, this transformation preserves straightness. Finally, the inverse of a transformation that preserves straightness must be a transformation that preserves straightness. Thus, the four properties that define a group – Closure, Associativity, Identity Element, and Inverses – are true of the group of linear transformations.

The group of linear transformations of the plane is denoted by $GL(2, \mathbb{R})$, which stands for *General Linear Group on two-dimensional space*. The group of linear transformations of the $n$-dimensional space is denoted by $GL(n, \mathbb{R})$. Because a linear transformation preserves straightness, the result will be that, in a larger dimensional space, a linear transformation preserves not only the straightness of lines, but also the straightness of planes, and any higher dimensional straight slices. For example, a linear transformation of a three-dimensional space preserves the straightness of lines and of planes.

## 13 Affine Group $AGL(2, \mathbb{R})$

The general linear group $GL(2, \mathbb{R})$ consists of all transformations that preserve straightness and the position of the origin of the plane. What about translations? Clearly, translations preserve straightness; i.e. straight lines remain straight under translations. But observe that translations shift the position of the origin. Therefore, they are not members of $GL(2, \mathbb{R})$.

If we wish to have a group that includes all the transformations that preserve straightness, we simply add the translations to the linear transformations. Thus, in two dimensional space, we add the translation group $\mathbb{R} \times \mathbb{R}$ of the plane, to the group, $GL(2, \mathbb{R})$. The resulting, larger, group is called the *affine group*, and is denoted by $AGL(2, \mathbb{R})$. That is:

$$AGL(2, \mathbb{R}) \quad = \quad GL(2, \mathbb{R}) \quad + \quad [\mathbb{R} \times \mathbb{R}]$$

Any transformation in $AGL(2, \mathbb{R})$, i.e. any transformation that preserves straightness, can be decomposed into a transformation from $GL(2, \mathbb{R})$ and a transformation from $\mathbb{R} \times \mathbb{R}$. The corresponding statement holds for the affine group $AGL(n, \mathbb{R})$ acting on $n$-dimensional space.