

GROUP THEORY 101

GIRLS TALK MATH

CONTENTS

1. Symmetry	2
2. First examples from geometry	2
2.1. Illustrations:	3
3. Counting symmetries	4
3.1. Symmetries of a triangle	4
3.2. A formal definition of group	6
3.3. Some basic properties of groups	8
4. More examples of groups	11
4.1. The dihedral groups	11
4.2. The Symmetric group on n letters	16
4.3. From abstract group back to concrete symmetry	21
5. Subgroups and generators	24
5.1. An illuminating example	24
5.2. Generalization to abstract groups	25
6. Finite subgroup of rigid motions: a geometric recipe	27
6.1. The case of dimension 2	27
6.2. The case of dimension 3	28
7. Suggested reading and visuals for further exploration	33

1. SYMMETRY

Groups arise in nature whenever we can find symmetry. There is a rigorous way of understanding symmetry using rigid motions in geometric objects, which is the leitmotif in our discussion throughout. For example, the human body has a lateral symmetry: if you imagine reversing left and right, most people would look more-or-less the same. (In fact, we see an example of this every time we look in a mirror.)

Another example is in the formation of crystals. In a crystal, the atomic structure arranges itself into a very symmetrical pattern, which you can see even with the unaided eye. The symmetry of the atomic structure means the atoms are packed very regularly, which leads to the nice shapes we see. In the late 1800's, mathematicians used group theory to classify all of the shapes of crystals that could ever exist in the world.

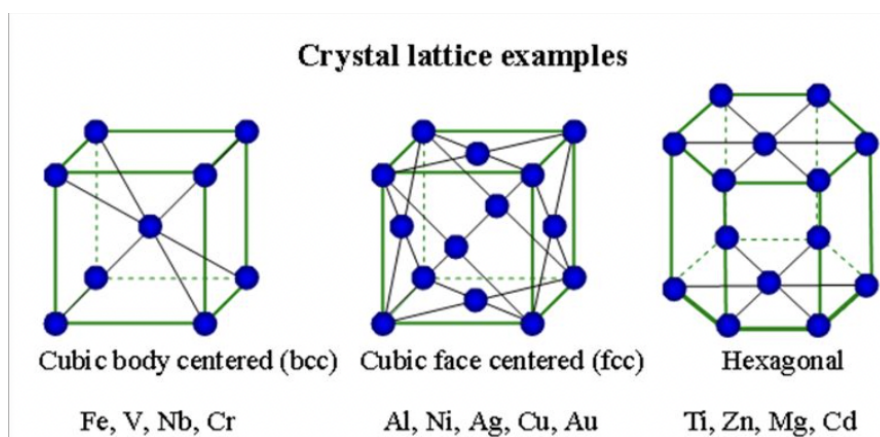


FIGURE 1. A crystal structure is a solid with a unique arrangement of atoms that results in a pattern.

2. FIRST EXAMPLES FROM GEOMETRY

Symmetry abounds in mathematics, and it pervades physical systems in innumerable ways too. Our first experience with symmetry might be an encounter with a butterfly, or perhaps with the face of our mother or father. Group theory is the mathematical study of symmetry. Informally, a symmetry of an object is a way of moving the object back onto itself without changing it. In this section we shall see how a group arises ‘in nature’ by considering some examples from Euclidean geometry. We will start by considering *rigid motions*, or *isometries*¹ of the two dimensional plane. A rigid motion is a distance preserving transformation of the plane. Let us parse that last sentence into a more tangible form.

Definition 2.1. *A rigid motion is a way of moving all the points in the plane such that*

- (1) *the relative distance between points stays the same, and*
- (2) *the relative position of the points stays the same.*

*There are mainly three types of rigid motions that we will consider: translation, rotation and reflection.*²

¹The word stems from Greek components: *isos*, meaning “equal, identical” and *metron*, meaning “measure”.

²In fact, we can mathematically show that any rigid motion comes from application of these three types, although this is beyond the scope of our discussion here.

Translation: In a translation, everything is moved by the same amount and in the same direction. Every translation has a direction and a distance (see Figure 2(a) for an example).

Rotation: A rotation fixes one point (the rotocenter) and everything rotates by the same amount around that point. Every rotation has a rotocenter and an angle (see Figure 2(b) for an example).

Reflection: A reflection fixes a mirror-line in the plane and exchanges points from one side of the line with points on the other side of the mirror-line at the same distance from the mirror-line. Every reflection has a mirror-line(see Figure 2(c) for an example).

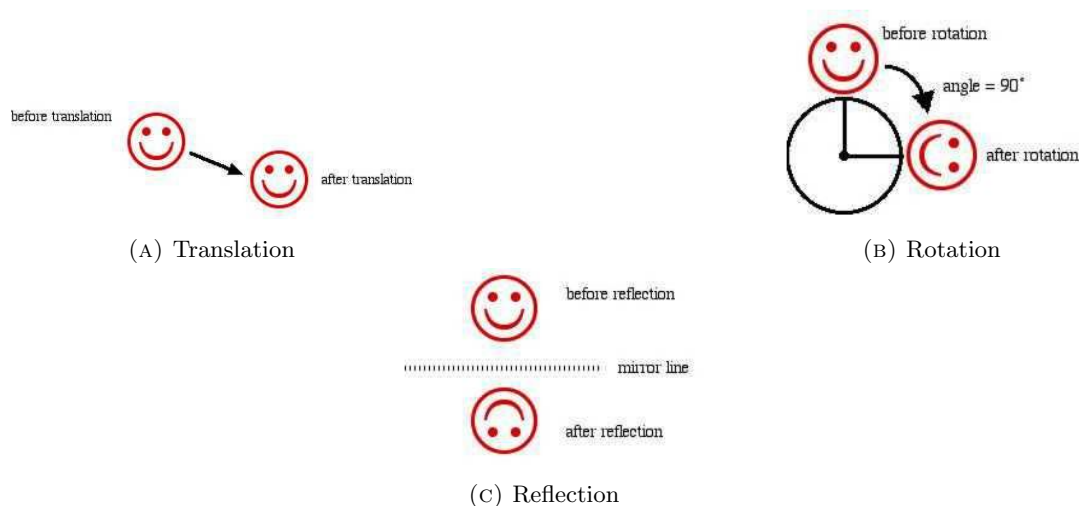


FIGURE 2. An example of rigid motions i.e, translation, rotation and reflection.

The idea of rigid motion is closely related to the notion of congruent triangles that you learned in high school geometry! If you are given any two congruent triangles, you can always find a rigid motion such that when you apply it to the first triangle, you get the second one. Said another way, we can loosely identify all the congruent triangles as one single triangle, upto the notion of applying an isometry.

2.1. Illustrations: Following videos can help you understand rigid motions in two dimensions for various 2D objects. The second video can help you with the vocabulary we used in this section. Please have a look at it to have a visual understanding of the concepts described above.

- (1) <https://www.youtube.com/watch?v=XiAoUDfrar0>
- (2) <https://www.youtube.com/watch?v=m73VMHLzt-4>

3. COUNTING SYMMETRIES

Now that we learned what symmetries are, how can we use mathematics to study symmetry? Well, the first thing we learn about in mathematics is counting, so perhaps we should try to count symmetries!

3.1. Symmetries of a triangle. Let us do a small activity to find all the symmetries of a triangle.

- (1) Suppose that you draw an equilateral triangle on the floor, and cut out a triangle of exactly the same size and shape from paper and also label each corner of your paper triangle with letters a, b, c as shown in the Figure below.
- (2) You line up the paper with the picture on the floor so that it looks exactly like the first triangle in Figure below.
- (3) Now the goal is to pick up the paper and put it back down on the floor however you want: the only rule is that it has to line up with the picture on the floor.
- (4) The question is, what different motions can you apply here? In somewhat abstract terms, what we are asking for are *the rigid motions of the plane that fixes a given equilateral triangle Δ , i.e. places the triangle back on top of itself.*

We will call such possible arrangements to be *symmetries* of the triangle. You can keep track of the various symmetries by labelling the corners of the triangle, and seeing where they end up after applying one of the symmetries. (See the Figure below for all symmetries). Let us label the following triangle in the Figure 3 using (1)-(6).

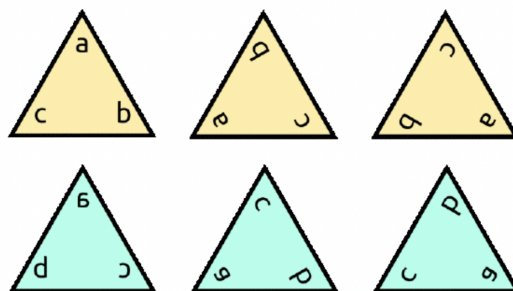


FIGURE 3. Effect of the six symmetries of an equilateral triangle

An equilateral triangle has six symmetries:

- (1) Three rotations (including the rotation by 0 degrees). Rotating the triangle about the center point by 120 degrees counter-clockwise is a symmetry; let's call this rigid motion R_{120} . There are two other rotational symmetries: one which rotates by 0 degrees and one by 240 degrees counter-clockwise about that same point (call these R_0 and R_{240} for consistency).



FIGURE 4. The figures (1), (2), (3) above are formed after applying rotational symmetries R_0, R_{120} and R_{240} respectively.

- (2) Three reflections (see figure 5). For instance, reflecting (or flipping) the triangle across the line labeled ℓ_1 is such a rigid motion; let's call this rigid motion F_1 . Similarly, let F_2 and F_3 stand for the reflections across lines ℓ_2 and ℓ_3 . The effect of these symmetries on the configurations listed in figure (4) can be found in figure (6). For instance, as we see the example above, F_1 on (1) leads to (6) and F_2 leads to (4). More examples can be found in Exercise 3.3.

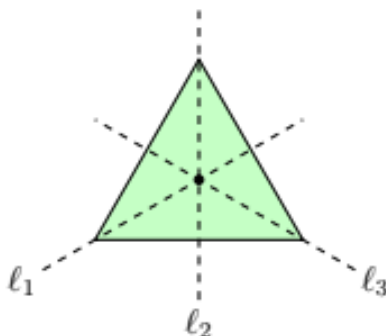


FIGURE 5. Reflection symmetries of equilateral triangle



FIGURE 6. The figures (4), (5), (6) are formed by composition earlier of rotational symmetries followed by reflection symmetries

The crucial observation is this: two symmetries of Δ can be “put together” in a meaningful way. If, say, one flips the triangle over ℓ_1 and then rotates it counter-clockwise by 120 degrees, what is the resulting rigid motion? We record the effect on labels of corners of Δ as shown in the figures above: The end result is that the triangle has been flipped across ℓ_1 (notice how the corners labelled a and b switched places, but the corner labelled c stayed put). The two rigid motions F_1 and R_{120} were applied in that order, or “composed”, to yield a different rigid motion: F_2 . Let's write this as $F_1 * R_{120} = F_2$.

All the following exercises assumed to have initial configuration at (1).

Exercise 3.1. Explain why $R_{60} * R_{120}$ results in (1).

Exercise 3.2. Explain why $R_{60} * R_{180}$ results in (2). (Note that R_{60}, R_{300} are not symmetries of Δ .)

Exercise 3.3. Summarise the resulting symmetry of some of the compositions using rotations and reflections of an equilateral triangle. Fill in each entry with the resulting symmetries (1)-(6) when the motion on the left column is performed first, followed by the motion on the top row. You may split up the work among your group members.

*	R_0	R_{120}	R_{240}	F_1	F_2	F_3
R_0						
R_{120}			(1)			
R_{240}	(2)					
F_1	(6)	(4)			(2)	
F_2	(4)					
F_3	(5)					

Exercise 3.4. Explain why $R_{60} * R_{120} = R_{180}$.

Exercise 3.5. Explain why $R_{60} * R_{300} = R_0$. (Note that R_{60}, R_{300} are not symmetries of Δ .)

Exercise 3.6. What is $F_1 * F_2$? Is it same as $F_2 * F_1$?

Exercise 3.7. Summarise compositions of the six symmetries we found above. Fill in each entry with the resulting motion when the motion on the left is performed first, followed by the motion on the top. You may split up the work among your group members.

*	R_0	R_{120}	R_{240}	F_1	F_2	F_3
R_0						
R_{120}			R_0			
R_{240}	R_{240}					
F_1		F_2				
F_2						R_{240}
F_3						

So we now have many examples of symmetry, but what, exactly is a group?

3.2. A formal definition of group. In last subsection, we considered an object X (i.e. the triangle) with a collection S of symmetries (which consists of three rotations and three reflections). We've seen that we can compose any of the symmetries in S and obtain another symmetry of X . We've also seen that these symmetries obey certain rules. We can now state a definition that captures these properties.

Definition 3.1. We say that a set G is a **group** if it obeys the following rules:

- (1) If a, b are two elements of G , then we can 'multiply' them to get a third element c lying in the group G ; this is expressed as $a * b = c$, where the function $*$: $G \times G \rightarrow G$ is called the "operation" of the group.

- (2) If a, b, c are three elements of G , then $a * (b * c) = (a * b) * c$; this is expressed by saying that group operation $*$ is “associative”.
- (3) There is a special element of G called the “identity”, usually denoted by e . It has the unique property that $a * e = e * a = a$ for any element a of G .
- (4) For every element a of G , there is a corresponding element b called the “inverse” of a , such that $a * b = b * a = e$. Sometimes we denote this inverse element as a^{-1} .

This already looks quite a tedious list of things, but let us notice that all the properties listed above do hold true for our earlier collection of symmetries of a triangle. The operation in this context is composition of two symmetries.

Exercise 3.8. What is the identity element of the group of triangle symmetries and composition operation?

Let’s now dive into the inverse of each symmetry. Observe that if you apply any symmetry to the triangle, you can undo its effect by applying another symmetry. For instance, if you rotate the triangle by 120° , you can further rotate it back by 240° to get back to the original configuration, so this says $R_{120} * R_{240} = R_0$, similarly we see $R_{240} * R_{120} = R_0$, therefore $R_{120}^{-1} = R_{240}$.

Exercise 3.9. What is the inverse of R_{240} ?

Exercise 3.10. What is the inverse of F_1 ? How about R_0 ?

Let us note a super important feature of our definition at this point. It does not need to be true in general that $a * b = b * a$! It might happen for *some* pair of elements a, b , in which case we say that a and b *commutes*. By property 3 of the definition above, every element in the group commutes with the identity. If this happens for all possible pairs of elements of G , then we say that G is a **commutative** or **abelian group**.

Exercise 3.11. Use your answer from exercise 4.7 to come up with two elements a, b of D_3 such that $a * b \neq b * a$, that is to say a and b do not commute.

Let us now list a few examples of groups that you are already familiar with.

- (a) The integers, commonly denoted by \mathbb{Z} , is the group $\{\dots, -2, -1, 0, 1, 2, 3, \dots\}$, where the operation is usual addition of numbers. Therefore, instead of $*$ we use the $+$ symbol here; e.g., $5 + 8 = 13$. The identity element is 0 since $z + 0 = z = 0 + z$ for any integer z . The inverse of 17 is -17 , etc. Note that if a and b are any integers then $a + b = b + a$, therefore $(\mathbb{Z}, +)$ is an abelian group. With the same operation, the rational numbers (denoted \mathbb{Q}), the real numbers (denoted \mathbb{R}), and the complex numbers (denoted \mathbb{C}) are also abelian groups. Note that all of these sets are infinite, so they are examples of infinite groups.
- (b) The set of rational numbers barring 0, denoted by $\mathbb{Q} \setminus \{0\}$, forms a group whose operation is regular multiplication. That is, $\frac{a}{b} * \frac{c}{d} = \frac{ac}{bd}$, for any non-zero integers a, b, c, d . The identity of this group is 1, and the inverse of $\frac{a}{b}$ is $\frac{b}{a}$. This group is also abelian.
- (c) Of course, the set of symmetries of an equilateral triangle form a group whose operation is what we referred to above as composition. This group has a standard name: D_3 . It is the simplest example of a group which is not abelian.

Let us play with the group properties a little bit more in form of the following exercise.

Exercise 3.12. For each following set with a given operation $(G, *)$, determine whether or not it is a group and find the identity element and inverses if it is a group. For those that are not groups, identify which of the properties fail(s).

- (1) $G = \mathbb{R}$, with respect to usual multiplication.
- (2) $G = \mathbb{Q} \setminus \{0\}$, with respect to the operation $a * b = \frac{ab}{3}$.
- (3) $G = \mathbb{Z}$, with respect to usual subtraction.
- (4) $G = \mathbb{Z}_{\geq 0}$, the set of non-negative integers with respect to usual addition.
- (5) (*Harder*) $G = \mathbb{R} \setminus \{1\}$, with respect to the operation $a * b = a + b - ab$.
- (6) (*Harder*) $G = \{1, 2, 3, 4, 6, 12\}$ i.e. the divisors of 12, with respect to the operation $a * b = \gcd(a, b)$.

A word of caution: hopefully by now you have become comfortable at grappling with the concept of group operation: it is an abstract way of putting together two elements that sometimes coincides with usual operations we are familiar with, but not always! So we must exercise caution in applying our intuition from the world of numbers.

A word on notation: As writing $*$ multiple times in a long expression might result in a cumbersome notation, we sometimes drop it - this should not cause any confusion when the group operation is understood from the context; e.g. we might write $R_{120}F_2R_{240}F_1F_3$ instead of $R_{120} * F_2 * R_{240} * F_1 * F_3$.

3.3. Some basic properties of groups. The solution of the exercise 3.7 is below for your reference. Let us spend some time to intuitively understand what the group properties mean. We start by looking at the table below - a group of symmetries of a triangle.

*	R_0	R_{120}	R_{240}	F_1	F_2	F_3
R_0	R_0	R_{120}	R_{240}	F_1	F_2	F_3
R_{120}	R_{120}	R_{240}	R_0	F_2	F_3	F_1
R_{240}	R_{240}	R_0	R_{120}	F_3	F_1	F_2
F_1	F_1	F_2	F_3	R_0	R_{120}	R_{240}
F_2	F_2	F_3	F_1	R_{240}	R_0	R_{120}
F_3	F_3	F_1	F_2	R_{120}	R_{240}	R_0

Notice how orderly this table looks! This is no accident.

Closure property: Perhaps the most important feature of this table is that it has been completely filled in without introducing any new motions. Of course, this is because, as we have already pointed out, any sequence of rigid motions for the equilateral triangle turns out to be the same as one of these six. Algebraically, this says that if a and b are in D_3 , then so is ab . This is the closure property (1) in the list appearing in definition 3.1.

Existence of identity: Next, notice that if a is any element of D_3 , then $aR_0 = R_0a = a$. Thus, combining any element a on either side with R_0 yields a back again. An element R_0 with this property is the identity, and every group must have one.

Existence of inverse: We see that for each element a in D_3 , there is exactly one element b in D_3 such that $ab = ba = R_0$. In this case, b is said to be the inverse of a and vice versa - if a and b are inverses of each other, then b “undoes” whatever a “does,” in the sense that a and b taken together in either order produce R_0 , representing no change.

The remaining condition required for a group is associativity; that is, $(ab)c = a(bc)$ for all a, b, c in the set. This is not so obvious to assert just by skimming through the table. To be sure that D_3 is indeed a group, we should in principle check this equation for each of the $6^3 = 216$ possible choices of a, b and c in D_3 . In practice, however, this is rarely done! Here, for example, we simply observe that the six motions are functions and the operation is function composition. Then, since function composition is associative, we do not have to check the equations.

We already noted that D_3 is not an abelian group, in other words there are elements in D_3 that do not commute with one another. Notice that this fact can be discovered just by looking into the multiplication table above. You can quickly spot that $F_1F_2 \neq F_2F_1$.

Exercise 3.13. *Suppose that the multiplication table of some group G looks symmetric about the diagonal joining upper left and lower right corner. From this information alone, can you tell whether the group is abelian or nonabelian?*

3.3.1. Laws of cancellation. Another striking feature of the table is that every element of D_3 appears exactly once in each row and column. If you think about it, the row version of this statement says that if $ab = ac$ for some a , then $b = c$. Let us use group properties to see why this holds. First, by property (4) we have an inverse for a , called a^{-1} . Multiplying this, we get $a^{-1}(ab) = a^{-1}(ac)$. Now, we use property (2) to rewrite this as $(a^{-1}a)b = (a^{-1}a)c$, but then the property of inverse tells us that $a^{-1}a = e$, the identity. Therefore we get $eb = ec$. Finally we use property (3) to conclude $b = c$ by appealing to definition of e .

Exercise 3.14. *Mimic the argument above to show that in a group if $ba = bc$ for three elements a, b, c , then $b = c$.*

Effectively, this means that we have right and left cancellation in a group. Beware though, we can only cancel elements from the same side in general. Whenever a group is not abelian, our usual intuition from the world of numbers might be misleading. For example, if $ab = ca$, it doesn't necessarily tell us that $b = c$! Can you find an instance of this phenomenon in the table from exercise 4.7? Note that if G is abelian then $ca = ac$, therefore having $ab = ca$ would imply $ab = ac$ - thereby giving us $b = c$ by left cancellation.

3.3.2. Laws of exponent. We already saw that our standard notation for inverse of an element a is a^{-1} . This notation is suggested by that used for ordinary nonzero real numbers under multiplication. Similarly, when n is a positive integer, the associative law allows us to use a^n to denote unambiguously the product $aa \cdots a$ (a being repeated n times). We define $a^0 = e$. When n is negative, we define $a^n = (a^{-1})^{-n}$; since $-n$ is positive in this case, this is a $-n$ -fold product of a^{-1} with itself. For example, if $n = -3$, we would write a^{-3} to denote $(a^{-1})^3$, which is the result of a^{-1} multiplied with itself 3 times. Unlike for real numbers, in an abstract group we do not permit non-integer exponents such as $a^{\frac{1}{2}}$.

With this notation, the familiar laws of exponents hold for groups; that is, for all integers m and n and any group element a , we have $a^m a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$. Although the way one manipulates the group expressions $a^m a^n$ and $(a^m)^n$ coincides with the laws of exponents for real numbers, the laws of exponents fail to hold for expressions involving *two group elements*. Thus, for groups in general, $(ab)^n \neq a^n b^n$. Even for $n = 2$, you can see this happening in D_3 by taking $a =$ and $b =$.

Exercise 3.15. (Optional) Show that if G is abelian, $(ab)^n = a^n b^n$ for any two elements a, b of G and any integer n . (Hint: try showing this for $n = 2$ first.)

3.3.3. Socks and shoes property. You might be interested in knowing how the group operation interacts with taking inverses. Well, although groups do not have the property that $(ab)^n = a^n b^n$, there is a simple relationship between $(ab)^{-1}$ and a^{-1} and b^{-1} . We claim that

$$(ab)^{-1} = b^{-1}a^{-1}.$$

There is a fairly intuitive way to see this. If you imagine of a as putting on socks and b as putting on shoes, then the intuition for inverses suggest a^{-1} as taking off socks, and b^{-1} as taking off shoes. In context of this thought experiment, the equation above demonstrates the order in which one must perform these actions. ab would represent putting on socks followed by shoes. In order to take them off, they must be removed in reverse order, that is, you first have to remove your shoes and then take off your socks. In group theory lingo, this amounts to $b^{-1}a^{-1}$!

Let us back up this argument with a more formal proof. We start by computing the expression $(ab)(b^{-1}a^{-1})$. Luckily, we can use associativity to simplify this mess! We get $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$. Similarly, you should compute that $(b^{-1}a^{-1})(ab) = e$. Taken together, all these says that ab and $b^{-1}a^{-1}$ multiplied in either order produces e - but that is exactly the definition of inverse at work!

Exercise 3.16. Guess in a similar way as above what the inverse of $(abc)^{-1}$ is in terms of a^{-1}, b^{-1}, c^{-1} , and then prove it. Can you see a general pattern for the inverse of $(a_1 a_2 \cdots a_n)^{-1}$ for any n elements a_1, \dots, a_n of the group?

3.3.4. Order of an element. Let us conclude this section by noting one important feature shared by all finite groups. Suppose that G is finite and a is an element of G that is not an identity. Consider the collection of all the powers of a , i.e. a, a^2, a^3 etc. Since G is a group, any product of its elements lie inside G , hence all of these elements are inside G . If all of these elements were different, we would end up getting an infinite collection of elements in G arising this way. But G is finite by our initial assumption - so we must get repetition in our list above. In other words, there must be two different powers of a that are equal, i.e. there are two *distinct* positive integers i, j such that $a^i = a^j$. One of these integer is bigger than the other, let us say $i > j$. Then multiply both side with a^{-j} (recall this is a^{-1} multiplied with itself j times) and get $a^{-j}a^i = a^{-j}a^j$, hence $a^{i-j} = e$. So we see that a positive power of a is equal to identity. Let n be the smallest exponent which makes $a^n = e$. Then we can see that $a, a^2, a^3, \dots, a^{n-1}, a^n = e$ are all distinct and any higher power of a is just going to be one of these! For example, $a^{n+1} = a^n a = ea = a$, similarly, $a^{n+2} = a^n a^2 = ea^2 = a^2$ and so on. The smallest positive integer n for which $a^n = e$ is called the order of a . What we just discussed above shows that in a finite group every element has finite order and the sequence of powers of a looks like $\{a^0 = e, a, a^2, \dots, a^{n-1}, a^n = e, a, a^2, \dots\}$. So, to find the order of a group element a , you need only compute the sequence of products a, a^2, a^3, \dots , until you reach the identity for the first time. If the identity never appears in the sequence, then a has infinite order. We can find instances of such elements inside infinite groups.

Exercise 3.17. What is the order of R_{120} in D_3 ?

Exercise 3.18. What is the order of 1 in \mathbb{Z} ? How about 5? Make a general observation about order of elements of \mathbb{Z} .

4. MORE EXAMPLES OF GROUPS

4.1. The dihedral groups.

4.1.1. *Motivation.* The analysis carried out above for an equilateral triangle can similarly be done for a square or regular pentagon or, indeed, any regular n -gon ($n \geq 3$). The corresponding group is denoted by D_n and is called the *dihedral group of order $2n$* .

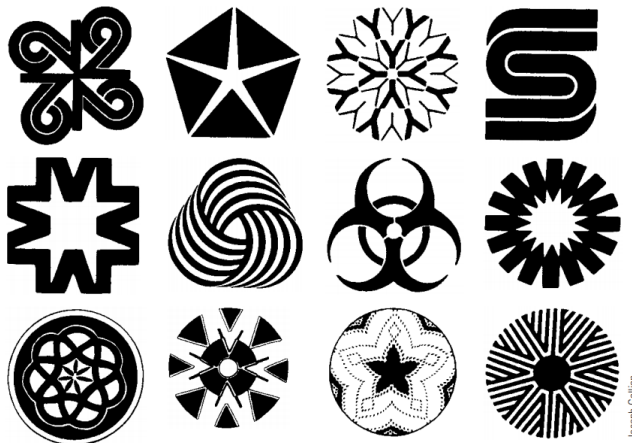


FIGURE 7. Designer logos exhibiting dihedral symmetry

The dihedral groups arise frequently in art and nature. Many of the decorative designs used on floor coverings, pottery, and buildings have one of the dihedral groups as a group of symmetry. Corporation logos are rich sources of dihedral symmetry. Chrysler's logo has D_5 as a symmetry group, and that of Mercedes-Benz has D_3 . The ubiquitous five-pointed star also has symmetry group D_5 . Commonly occurring symmetry patterns are D_4 and D_6 ³.

4.1.2. *Counting symmetries of regular n -gon.* Let us now delve into analysing symmetries of regular n -gons in style of section 3.1. These polygons for $n = 3, 4, 5$, and 6 are pictured below.

The dotted lines are lines of reflection: reflecting the polygon across each line brings the polygon back to itself, so these reflections are in D_3, D_4, D_5 , and D_6 .

Exercise 4.1. Draw a regular n -gon and its reflection symmetries for $n = 3, 4, 5, 6$.

You have to get something similar to Figure 8 as your solution. You can use this figure as a reference to get more insights into the symmetries of the regular n -gon.

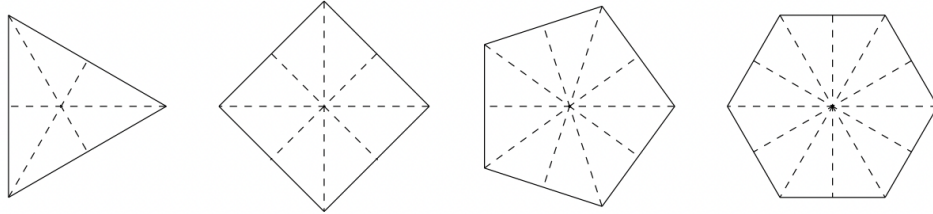
Observation 4.1. From the exercise above, we observe that $n = 3, 5$ there are lines of reflection connecting each vertex to the midpoint of the opposite side, and if $n = 4, 6$ there are lines of reflection connecting opposite vertices and lines of reflection connecting midpoints of opposite sides.

These descriptions of reflections work in general, depending on whether n is even or odd:

- For odd n , there is a reflection across the line connecting each vertex to the midpoint of the opposite side. This is a total of n reflections (one per vertex). They are different because each one fixes a different vertex.

³Interestingly, it is mathematically impossible for a crystal to possess a D_n symmetry pattern with $n = 5$ or $n > 6$.

- For even n , there is a reflection across the line connecting each pair of opposite vertices ($\frac{n}{2}$ reflections) and across the line connecting midpoints of opposite sides (another $\frac{n}{2}$ reflections). The number of these reflections is $\frac{n}{2} + \frac{n}{2} = n$. They are different because they have different types of fixed points on the polygon: different pairs of opposite vertices or different pairs of midpoints of opposite sides.

FIGURE 8. Regular n -gons for $n = 3, 4, 5, 6$

Exercise 4.2. What are the rotation symmetries of D_4 ? Use the notation used for D_3 in Section 3.

Do you see a pattern in the rotation symmetries of D_3 and D_4 ? Now we use this observation to give the rotation symmetries of a n -gon.

Observation 4.2. Rotation symmetries of a n -gon are $0^\circ, \frac{360^\circ}{n}, \frac{2 \times 360^\circ}{n}, \dots, \frac{(n-1) \times 360^\circ}{n}$. This gives us n rotations.

Notice that if a rotation is to carry a regular n -gon back to itself, then it has to be a multiple of $\frac{360^\circ}{n}$: this follows from observing that such rotation must bring back the vertices to themselves and any two successive vertices are $\frac{360^\circ}{n}$ apart. Indeed when $n = 3$, we saw rotations by angles $0^\circ, \frac{360^\circ}{3} = 120^\circ, \frac{2 \times 360^\circ}{3} = 240^\circ$ belonging to D_3 , the group of symmetries of equilateral triangle.

Exercise 4.3. Why don't we get any more rotations other than these n listed above?

Thus, for a regular n -gon we get $2n$ rigid motions that fix it; therefore the symmetry group D_n of such an n -gon has at least $2n$ elements. We now show that there are no more!

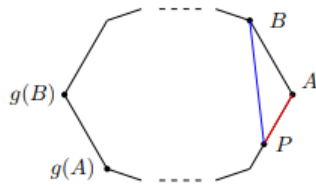


FIGURE 9. Effect of a rigid motion on two adjacent vertices

Pick two adjacent vertices of a regular n -gon, and call them A and B as in the figure below. An element g of D_n is a rigid motion taking the n -gon back to itself, therefore it must carry vertices to vertices and g must preserve adjacency of vertices, so $g(A)$ and $g(B)$ are adjacent vertices of the polygon. Now, a moment's thought should convince you that point on a regular polygon is determined, among all points on the polygon, by its distances from two adjacent

vertices of the polygon. For each point P on the polygon, the location of $g(P)$ (which is another point on the polygon) is determined by $g(A)$ and $g(B)$, because the distances of $g(P)$ from the adjacent vertices $g(A)$ and $g(B)$ equal the distances of P from A and B (remember rigid motions preserve distance), and therefore $g(P)$ is determined on the polygon. To find the number of rigid motions of the polygon, it thus suffices to find the number of possibilities for $g(A)$ and $g(B)$. Since $g(A)$ and $g(B)$ are a pair of adjacent vertices, $g(A)$ has at most n possibilities (there are n vertices), and for each choice of that $g(B)$ has at most 2 possibilities (one of the two vertices adjacent to $g(A)$). That gives us at most $n \times 2 = 2n$ possibilities, so there are at most $2n$ rigid motions of a regular n -gon. Altogether, we have thus shown there are exactly $2n$ of these!

4.1.3. Deeper analysis of symmetry. Now that we know the members of D_n , let us tabulate them in a coherent way that works for all n . What we mean is that we want to list the symmetries of a regular n -gon in an economical way that brings out which of them are rotations and which are reflections, and this scheme should work for any n -gon.

Keeping things in the style of section 3.1., we might write the rotations as

$$R_0, R_{\frac{360}{n}}, R_{\frac{720}{n}}, \dots, R_{\frac{(n-1) \times 360}{n}}$$

Similarly we can perhaps write down the reflections as

$$F_1, F_2, \dots, F_n$$

once we make a choice of numbering for dotted axes of reflections (as per Figure 6 above). In fact, we can do much better than this!

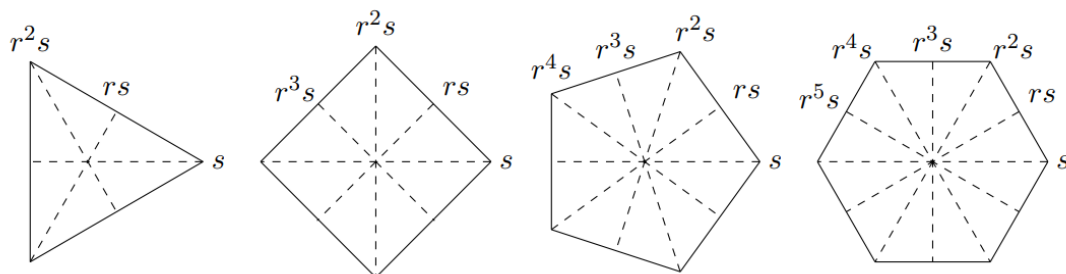


FIGURE 10. Reflections for regular n -gons

As a first clue, let us observe that instead of rotating the triangle by 240° , we could have performed rotation by 120° in the same direction (say anti-clockwise) twice: the end result would be same. In group theory term, we are therefore asserting $R_{240} = R_{120}R_{120}$, or more succinctly $R_{240} = R_{120}^2$. Similarly, $R_0 = R_{120}^3$, as rotating by 120° thrice has the same effect as rotating by 360° , which bring things back to exactly the beginning configuration. The upshot is that we can express all the rotations as powers of the rotation by smallest angle. Let us therefore extrapolate this observation to general n -gon in the following way. Write r for the counter-clockwise rotation by $\frac{360^\circ}{n}$. This rotation depends on n , so the r in D_3 means something different from the r in D_4 . However, as long as we are dealing with one value of n , there should be no confusion. Thus we conclude:

$$\text{The } n \text{ rotations in } D_n \text{ are } \{e, r, r^2, \dots, r^{n-1}\}.$$

Now, to the reflections: let s be a reflection across a line through one of the vertices. See examples in the polygons below. Since a reflection applied twice in succession yields the original configuration, we have $s^2 = e$, so $s^{-1}s^2 = s^{-1}e$ and therefore $s = s^{-1}$. We now get a handle on the reflections:

The n reflections in D_n are $\{s, rs, r^2s, \dots, r^{n-1}s\}$.

Here's why. The rigid motions $s, rs, r^2s, \dots, r^{n-1}s$ are all different since $e, r, r^2, \dots, r^{n-1}$ are different and we just multiply them all on the right by s , so the resulting motions must be all distinct (otherwise right cancellation of s would lead to repetition among the rotations).

Exercise 4.4. *Explain why each $r^i s$ is a reflection for every $i = 0, 1, 2, \dots, n-1$.*

Suppose $r^i s$ is a rotation; then $r^i s = r^j$ implying $s = r^{j-i}$; the right hand side is a rotation, but s is not a rotation. Since D_n has n rotations and n reflections, and no $r^i s$ is a rotation, they are all reflections.

Since each element of D_n is a rotation or reflection, there is no “mixed rotation-reflection”: the product of a rotation r^i and a reflection $r^j s$ (in either order) is a reflection. The geometric interpretation of the reflections s, rs, r^2s and so on is this: drawing all lines of reflection for a regular n -gon and moving clockwise around the polygon starting from a vertex fixed by s , we meet successively the lines fixed by $rs, r^2s, \dots, r^{n-1}s$. See the polygons above.

Exercise 4.5. *Explain the following claim, as seen in Figure 9 above: if s is the reflection across the line through the rightmost vertex then rs is the next line of reflection counterclockwise.*

Let us now summarize what we have found in this section.

Theorem 4.1. *The group D_n has $2n$ elements, and they can be listed as*

$$D_n = \{e, r, r^2, \dots, r^{n-1}, s, rs, r^2s, \dots, r^{n-1}s\}.$$

4.1.4. Nonabelian nature of symmetry group. We now observe another important feature of the dihedral groups D_n : they are not abelian, just like we saw in the case of equilateral triangle with $n = 3$. To see this, we just need to produce 2 elements of the group such that their product in different order yields different outcome. How about we try the obvious candidates, i.e. r and s ?

Exercise 4.6. *Prove that $rs = sr^{-1}$. Hint: remember that every rigid motion of a regular n -gon is determined by its effect on two adjacent vertices. Therefore you only need to show that the two rigid motions above has the same effect on two adjacent vertices.*

Once we do the above exercise, we can get a complete picture of how to multiply any two elements in an abstract way, i.e. using group properties and not having to refer back to geometry of n -gons. For example, we can now see that $r^2s = sr^{-2}$:

$$r^2s = (rr)s = r(rs) = r(sr^{-1}) = (rs)r^{-1} = (sr^{-1})r^{-1} = s(r^{-1}r^{-1}) = sr^{-2}.$$

Can you see how we combined the exercise with associativity of group operation above? In fact, similar calculation tells us that $r^i s = sr^{-i}$ for any i .

Exercise 4.7. *Use the above observations to multiply r^2sr^6s in D_7 . Your answer should be in the form as listed in theorem 4.1 (that is, powers of r followed by powers of s).*

Let us conclude this section with two optional fun exercises.

Exercise 4.8. *For each design in figure 7, determine its symmetry group. Ignore imperfections in drawing.*

Exercise 4.9. (*Harder*) *Consider an infinitely long strip of equally spaced H's:*

$$\cdots \mathbf{H} \mathbf{H} \mathbf{H} \mathbf{H} \mathbf{H} \cdots$$

Describe the symmetries of the strip. Is this group abelian?

4.2. The Symmetric group on n letters.

4.2.1. *From dihedral symmetries to abstract rearrangements.* In this subsection we introduce a very important class of groups, called the symmetric groups. Historically, they were the first prototype of groups mathematicians recognized to be an important object and in some sense *every finite group sits inside one of the symmetric groups*.

Before moving forward with the symmetric group, let us look back once more to the dihedral groups: this time focusing on symmetries of the square i.e. D_4 . We already saw how to describe elements of any dihedral group in terms of explicit expressions involving a rotation and a reflection. Let us now shift our perspective a bit and observe what these symmetries do to the square itself. As before with the case of the equilateral triangle, we label vertices of the square - this time using numbers 1, 2, 3, 4 instead of letters e.g. a, b, c, d (as we will soon discuss structures too big for the English alphabet to handle).

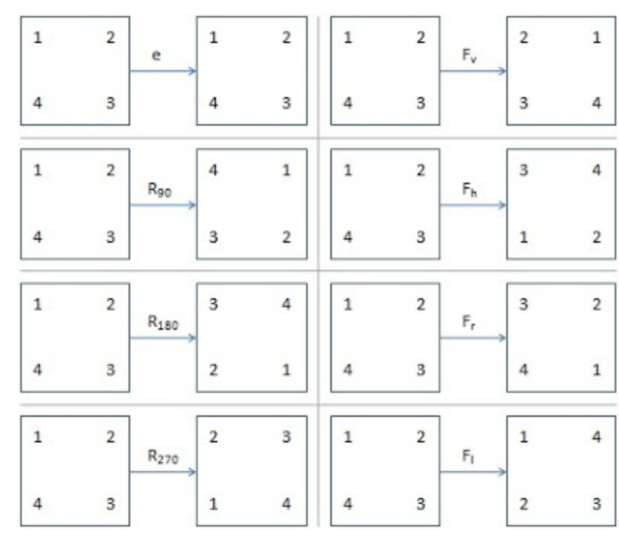


FIGURE 11. Another avatar of D_4 : a mathematical anagram

The effect of D_4 elements on the labeling is demonstrated in Figure 10.

Exercise 4.10. What is the alternate representation of R_{270} in the group D_4 ?

Exercise 4.11. What is the alternate representation of F_v (reflection about the axis passing through the midpoints of the two vertical lines of the square) in the group D_4 ?

We can see that r^3 (or R_{270}) changes the labelling to 2314, whereas horizontal reflection rs (or F_v) changes the labelling to 3412. Based on the representation of the elements shown above for D_4 , solve the following exercise.

Exercise 4.12. Write down the elements of D_4 in terms of an arrangement of numbers $\{1, 2, 3, 4\}$ (as you see in figure 10).

For your convenience, here are some elements of D_4 as recorded by the rearrangement of the numbers on the square, coming from the configurations on the left in figure 10:

$$\{1234, 4123, 3412, 2341\}.$$

Let us go through a quick primer on permutations to understand the symmetric group better!

4.2.2. Permutations. A permutation of a set of objects is the different arrangements of the objects into a sequence. For example, the number of ways in which 3 letters A, B, C can be arranged is $ABC, BCA, ACB, BAC, CAB, CBA$.

Exercise 4.13. Let us say you have 3 letters D, E, F . How many different arrangements of 3 letters are possible?

In the above examples, ABC is called a permutation of $\{A, B, C\}$ and FDE is the permutation of $\{D, E, F\}$. Likewise, [triangle, melon, airplane] is a permutation of three objects as well. From our mathematical point of view, the objects we use don't actually matter; all we care about is the order they are arranged in. So usually we'll just talk about permutations of the numbers 1 through n . You can think of each number as just counting the objects involved: first object, second object, \dots , n -th object.

Any initial ordering of elements can be organized alphabetically, the numbers $\{1, 2, \dots, n\}$ can be organized in order of increasing value. Then every permutation of these elements can be thought of as a mixing-up of this initial order. In this sense, a permutation is a *special* kind of function from the set back to itself⁴. Therefore, we can view the permutation $[b, a, c]$ of $\{a, b, c\}$ as the function f that maps a to b , b to a and fixes c . Alternatively, we can write the permutation as the *ordered list* $[f(a), f(b), f(c)]$ for the function f above; this list is called the one-line notation for permutation specified by f . We denote by S_n the collection of all permutations of a list of n objects, usually taken to be $\{1, 2, \dots, n\}$.

Thus, we can think of symmetries of a square as certain rearrangements, or permutations, of the numbers 1, 2, 3, 4. Not every permutation features in D_4 though: e.g. from exercise 4.12, you can see that 1243 is a valid permutation of 1234 that is not present in the list of elements.

Exercise 4.14. Enumerate all the permutations of $\{1, 2, 3, 4\}$.

Exercise 4.15. Using exercise 4.12 and 4.14, identify the arrangements that are present in the collection of permutations of $\{1, 2, 3, 4\}$ but not in D_4 .

Observation 4.3. In D_4 we only get those permutations that can arise from this imposed geometric condition of 1, 2, 3, 4 sitting at the corners of our square.

This situation somewhat akin to the game of anagram: there you have to rearrange letters of a given word to create other *words* - this is a condition dictated by the English language, not every rearrangement count as a word! While the game of anagram falls apart if we start accepting any combination of letters as a legitimate word, we do get something much more interesting happening mathematically once we start considering all possible permutations of 1, 2, 3, 4: the symmetric group (sometimes called permutation group) on 4 letters, usually denoted S_4 .

On a basic level, suppose you are asked to list your preferences amongst a bunch of presidential candidates. The list you make up, from favorite to least favorite, is a permutation of the candidates. Another example is a deck of playing cards. In a standard deck, each card appears exactly once. When you shuffle the deck, you are just creating a random permutation of the cards. One can use mathematics related to permutations to answer interesting questions about cards, like: "How many times do I need to shuffle the deck before it is truly randomized?"⁵.

⁴The adjective 'special' here means that it's a bijective function, which is to say a one-to-one and onto function.

⁵The answer is 7 and it comes from beautiful application of probability theory with symmetric group, much beyond the scope of our discussion here. In fact, permutations are so ubiquitous in game of chances that Perci Diacones once said "Gambling is just applied representation theory of symmetric group!"

In the spirit of counting symmetries, let us now count how many permutations we get for a list of n objects. Starting with $n = 3$, we can see that $\{a, b, c\}$ has 6 permutations, namely

$$[a, b, c], [a, c, b], [c, a, b], [c, b, a], [b, a, c] \text{ and } [b, c, a].$$

In fact, if you now look back at figure 3 and track down the labelling of all equilateral triangles got by applying its six symmetries, this would immediately convince you that D_3 and S_3 are the same group!

For a general n , suppose we try to build a permutation by successively choosing objects. Given n elements and we want to know different arrangements, then we keep picking up each element one by one. To chose the first element there are n possibilities, once the first element is chosen, we have $n - 1$ elements left. Now, we have $n - 1$ possibilities to chose the second element, $n - 2$ possibilities for the third element and so on. Together we have $n(n - 1)$ choices for the first two elements, which will be multiplied by the number of possible choices for the third element and so on. Therefore, the total number of possibilities is given by multiplying all of them, i.e.,

$$n(n - 1)(n - 2) \cdots 1.$$

This number is called n -factorial, and we write it as $n!$.

Exercise 4.16. Look back at your answer to exercise 4.14. How many permutations of $\{1, 2, 3, 4\}$ did you get?

4.2.3. Group operation for permutations. Now, we promised that we would get a group out of these permutations, so here's how. Two permutations can be put together by composing the functions they are associated to! For example, in S_4 if we take $f = [1, 4, 3, 2]$ and $g = [4, 1, 2, 3]$, then we claim that their composition $f \circ g = [2, 1, 4, 3]$. This can be seen by computing the one line notation for $f \circ g$: from one-line notation $g(1) = 4$ and $f(4) = 2$, therefore $f \circ g(1) = f(4) = 2$ - so the first entry of $f \circ g$ must be 2. The other three entries are computed similarly.

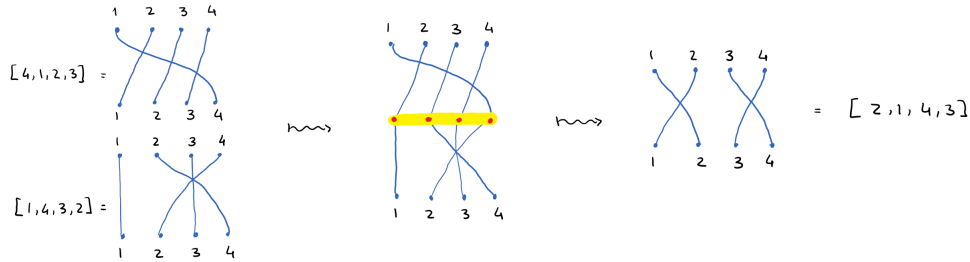


FIGURE 12. Visual composition using braid notation

Visual representation of the composition of permutation functions: A more visual way to keep track of this composition is using the braid notation for a permutation, as shown in figure 11. Briefly, this is how it works.

- (1) A braid is a configuration of two rows consisting of equal number of points, where each point on the top row is attached to exactly one point in the bottom row by a string.
- (2) This visually represents a permutation, where you join any two points as governed by the value of permutation function: i on top row gets attached to j if $f(i) = j$. In this

way, assume that the bottom row is the domain and the top row is a co-domain if you are considering it as a general function notation.

- (3) Composition of functions $f \circ g$ can easily be defined in the braid notation by stacking up the braid configuration corresponding to g on top of the one corresponding to f .
- (4) Finally, merge together the bottom row of g with the top row of f - this will result in the strands for g being ‘glued’ to those of f , giving rise to ‘long’ strands. We then sort of pretend to not see the middle row of points and get rid of it altogether, straighten out the newly joined strands for clearer visual, and voila! We can read off the permutation from the resulting braid notation.

Exercise 4.17. Show that $g \circ f = [4, 3, 2, 1]$, first doing it by composition and then drawing them in braid notation.

In particular, we get two elements f, g in S_4 such that $f \circ g \neq g \circ f$, thereby effectively showing that S_4 is not an abelian group.

Let us finally note that

Claim 4.1. S_n is a group under the operation of “composition” outlined above.

We will use braid notation for visual aid. Let us arrive to the proof of the above claim by solving some simple exercises about S_4 .

Exercise 4.18. Using braid notation show that for any two f, g in S_4 , $f \circ g$ is also in S_4 .

Exercise 4.19. Find the element e of S_4 such that for $g = [2, 4, 1, 3]$, $e \circ g = g$. Hint: we have to find e such that $e(g(i)) = g(i)$ for any $i = 1, 2, 3, 4$. Start by showing that $e(1) = g(3) = 1$ using an appropriate substitution process.

Exercise 4.20. In the spirit of the above exercise, prove that if $e \circ g = g$ for any g in S_4 , then $e = [1, 2, 3, 4]$. Similarly, if $e \circ g = g$ for any g in S_4 , then $e = [1, 2, 3, 4]$.

Exercise 4.21. Find the inverse function of $g = [4, 1, 2, 3]$ i.e. find g^{-1} such that $g^{-1} \circ g = e$ and verify that it is true using the braid notation.

Let us finally sketch an argument that S_n is a group for any positive integer n .

Closure and associativity property: If you compose any two bijective functions in either order, you get back the another bijective function. Alternatively, convince yourself that stacking and merging two braids give rise to another braid. Since the group operation here is composition of functions, it is associative. Can you see this fact from the perspective of braid configurations?

Existence of identity: The identity is $[1, 2, \dots, n]$, i.e. the function $e : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ that sends everything to itself.

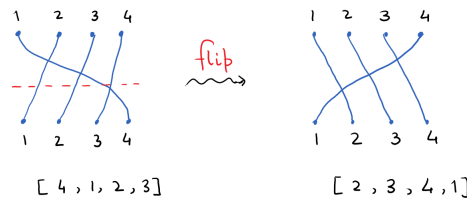


FIGURE 13. Finding inverse using braid

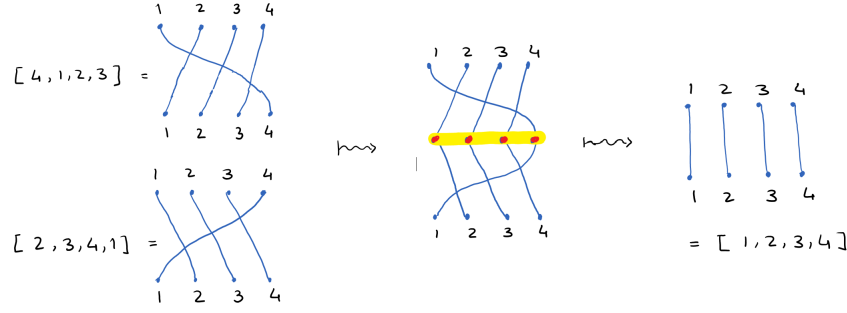


FIGURE 14. Verifying inverse property

Existence of inverse: Lastly, every element in S_n indeed has an inverse, by virtue of bijectivity. A visual verification again emerges from the braid notation. Suppose that we want to find out the inverse of $g = [4, 1, 2, 3]$. Just draw it using the braid notation and flip the diagram along an imagined axis drawn in the middle, as shown in figure 12. The permutation associated to the resulting diagram has to be inverse of the permutation. In this case, we see the inverse is $g^{-1} = [2, 3, 4, 1]$. We first find it in figure 12, and then verify that $g^{-1} \circ g$ is the identity permutation in figure 13. You should check that $g \circ g^{-1}$ also yields the same result. Since this process works for general permutations of n elements, we can see every elements possess inverse.

Therefore, we summarise the discussion from this subsection in form of the following theorem.

Theorem 4.2. *For every positive integer n , S_n is a nonabelian group of size $n!$.*

4.3. From abstract group back to concrete symmetry. So far we have seen how the dihedral group D_4 fit inside the permutation group S_4 i.e, set of permutations on $\{1, 2, 3, 4\}$. But unlike D_4 which arises from symmetries of a well-understood geometric shape, S_4 might seem a rather contrived and esoteric object. We aim to remedy that possible misconception in this subsection. That is, we will illustrate how S_4 can be thought of arising out of *rotational symmetry* of a well known geometric object: a cube!

A cube is a three-dimensional shape made out of 6 faces, 8 vertices and 12 edges. In order to proceed with the symmetries of the cube let us make sure that you agree with the statement that was just made.

Before identifying explicitly the symmetries of a cube, let us count how many there are. We will argue that this number is 24 in two ways.

- Given a cube, pick one corner and call it A (if you have a real cube in hand then mark it as A). You can certainly rotate the cube so that A either stays put or moves to any other chosen corner, of which there are 7. So you have 8 choices for where you want A to be. Once you've done this, the other corners are obviously not free to move as they wish. Let B be some corner adjacent to A , meaning it shares an edge of the cube with A . If A moves to A' , B must move to some corner adjacent to A' - otherwise the edge AB gets distorted - this is reminiscent of our earlier argument of why there can be at most $2n$ elements in D_n . Now, how many corners are adjacent to A ? That's where the 3 comes from. So taken together, these account for 24 choices. Finally you should convince yourself that once A and B have been placed, all other corners are "forced" - their final location is already fixed. *See if you can do that just using the relationships of adjacency, sharing a face and such.*
- Now let us do a similar argument by keeping track of what happens to a face when you rotate. Notice that the knowledge of a single face determines positions of the other faces, thus knowing all possible positions of one fixed face after rotation is tantamount to counting all the rotational symmetries of the cube. As before, pick a face and mark it F . Clearly, the cube can be rotated so as to move this face to any other faces including itself - giving us 6 choices. Once this choice is fixed, we can now rotate the cube with respect to an axis perpendicular to that face - this will give us 4 possibilities of configuration of that face:

$$F, \begin{array}{|c|} \hline \text{F} \\ \hline \end{array}, \begin{array}{|c|} \hline \text{F} \\ \hline \end{array}, \begin{array}{|c|} \hline \text{F} \\ \hline \end{array}.$$

If you think about it, this is exactly the effect of counter clockwise rotations by $0^\circ, 90^\circ, 180^\circ$ and 270° of the face as we have seen before from D_4 . All in all, we have 24 ways to rotate a face, thus we have reached at the same number of rotational symmetries of a cube.

In fact, we can arrive at the same number by focusing on the edges too!

Exercise 4.22. (Optional) Count the number of rotational symmetries of a cube by considering what happens to its 12 edges.

In fact, with some thought we can list out 24 such rotations. Each possible rotation has an axis — think of it as a spindle going through the centre of the cube. There are three possibilities for this spindle. Either it goes through the centres of two opposite faces, or through the centres

of two opposite edges, or through two opposite corners. Therefore, we can categorize these rotations accordingly. Let's do that.

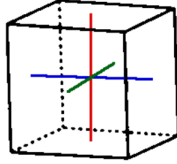


Figure (i)

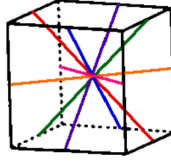


Figure (ii)

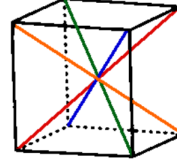


Figure (iii)

FIGURE 15. Rotational symmetries of a cube.

- (1) The first element is, as usual, identity transformation - rotation by 0° . This does not cause any change.
- (2) A cube has six faces, so there are three pairs of opposite faces. Thus we consider the 9 *rotations* of the cube about the 3 axes shown in figure 14(i) above. We can either rotate by 90° , 180° or 270° around either the red, blue or green axis. Each of these rotations will leave two faces fixed and all vertices and edges are not fixed.
- (3) A cube also has twelve edges, so there are six pairs of opposite edges. For a spindle going through the centres of two opposite edges, the only possibility is a rotation of 180° . This gives six rotations, one for each pair of opposite edges. Each of these rotations leave two edges fixed and no faces or vertices fixed. This is depicted in figure 14(ii).
- (4) Finally a cube also has eight corners, so there are four pairs of opposite corners. For each spindle going through two opposite corners, there are two possible rotations: by 120° and 240° as shown in figure 14(iii). This gives 8 *rotations*, each of which leave 2 vertices fixed and no edges or faces fixed.

All together we get $1 + (3 \times 3) + (6 \times 1) + (4 \times 2) = 24$ rotations, so we have counted them all!

Recommended activity: To grapple with such complicated three dimensional configuration, it helps to have a cube in hand. Therefore, you should try to get one - either grab the Rubik's cube lying in your house or better yet, fashion one yourself with instructions from this cool origami video:

<https://www.youtube.com/watch?v=337QxhfpY4w>

Then, the following videos can help you understand and find the rotation symmetries of a cube on your own using a paper cube.

- (1) <https://www.youtube.com/watch?v=X3eOGQGntEs>
- (2) <https://www.youtube.com/watch?v=-PYDcHKPMKk>
- (3) <https://www.youtube.com/watch?v=TggbcOrALMQ>

So we know that the group of rotational symmetries of a cube has 24 elements. We do know from earlier subsection that size of S_4 is indeed 24. If you want to identify two groups as the same, their sizes should match up, so that's a relief! But this alone does not mean that the rotational symmetry group of a cube has to be S_4 - it could be D_{12} for all you know! (recall D_{12} has size 24 too).

Recall that elements of S_4 are permutations of 4 objects. This gives us a subtle hint: to achieve our claim *we need to recognize the symmetries of cube operating on a certain set of 4 objects by permuting them*. If you have been reading this subsection carefully, you will notice at this point that we have seen only one occurrence of the number 4 - in discussion surrounding figure 14(iii). Notice that if two vertices are centrally opposite in initial configuration, no matter what rotation you apply they will remain to be a pair of centrally opposite vertices. This tells us that all rotations take the these 4 diagonals to themselves. So just as a wild guess, you might want to consider taking this set of 4 objects and seeing how the rotations affect them!

Now, you can start performing the aforementioned rotations with your own cube and keep track of where the diagonals go by enumerating them with numbers 1, 2, 3, 4. Just to be clear, we do know at this point that the number of permutations that arises from rotations of the cube cannot be more than 24 - because there are 24 rotations to begin with. What we are trying to assert here is that we do get all 24 permutations of $\{1, 2, 3, 4\}$ (which serves as labels of the diagonals) this way. Said another way, we would like to make sure that no two distinct rotation permutes these diagonals in the same way. Well, you can go through this activity of writing down how each rotation serves as permutation of $\{1, 2, 3, 4\}$ to be sure of this assertion. In case it becomes too exhausting to go through the long list, you can refer to this video:

<https://twitter.com/3blue1brown/status/1295041342486114304?lang=en>

We conclude by pointing out that this result is not that intuitive at all! The diagonals of the cube feel like they must be constrained in some way, whereas we end up showing that they mimic the pattern of 4 objects being rearranged freely, thereby showing that rotations of the cube is same as S_4 .

5. SUBGROUPS AND GENERATORS

5.1. An illuminating example. Let us revert back to the table at the beginning of section 3.3 and focus on the 3-by-3 subtable on the upper left corner. The entries in this sub-table are products of elements from $\{R_0, R_{120}, R_{240}\}$ (or in our more sophisticated notation, $\{e, r, r^2\}$) in either order; let us call this set X . Miraculously enough, the entries themselves are also in X . This means that this subset X of D_3 is closed under the group operation. What's more, the inverses of elements from X also lie in X , as we saw before that $R_{120}^{-1} = R_{240}$ and $R_{240}^{-1} = R_{120}$. Obviously, the identity R_0 of D_3 is in X . Thus we conclude that X is actually a group by itself! Since we get X as a subset of the group D_3 , we say that X is a subgroup of D_3 .

In the same vein, let us now focus on the subset consisting of rotations $\{e, r, r^2, \dots, r^{n-1}\}$ featuring in the dihedral group D_n .

Exercise 5.1. Is the set of rotations $\{e, r, r^2, \dots, r^{n-1}\}$ a subgroup of D_n ?

Let us explore the above question together by checking for the properties of the group.

Closure property: You can check it is closed with respect to group operation of D_n . This holds because geometrically speaking, composition of two rotations is another rotation.

Existence of identity: This subset also has the identity. We will now explore inverses of elements in this set.

Exercise 5.2. If $n \geq 3$, what is the inverse of r^{n-1} ? How about r^2 ?

We can always work out the familiar case of D_3 first and then try to see the general pattern.

Exercise 5.3. What is the inverse of R_{240} i.e. r^2 in D_3 ?

The answer here is R_{120} (or, in sophisticated notation it is r). It is the rotational symmetry that brings the triangle from R_{240} to the original position R_0 , since we know that by rotating 120° or applying a R_{120} we get to R_0 . Mathematically, if $r^2x = e$ then x is the inverse of r^2 . But we know that $r^3 = r^2r = e$, therefore $x = r$ i.e. the inverse of r^2 is r .

We can immediately generalize this to D_n .

Existence of Inverse: Recall that $r^n = e$ in D_n , therefore $r^{n+1} = r^n r = er = r$, similarly $r^{n+2} = r^2$ and so on. So we know that all the positive powers of r are already in the set $\{e, r, r^2, \dots, r^{n-1}\}$. What happens if we start taking negative powers?

Let's first identify r^{-1} . Well, if you rotate the n -gon counter clockwise by $\frac{360^\circ}{n}$, then how much more do you need to rotate in order to go back to the original configuration? To get back to the original configuration we must end up having a full rotation of 360° , so we have $360^\circ - \frac{360^\circ}{n}$ more to go. Since $360^\circ - \frac{360^\circ}{n} = \frac{(n-1) \times 360^\circ}{n}$, we see that rotating by this angle is same as performing r^{n-1} . Hence, to undo the effect of r we must apply r^{n-1} , thereby proving that $r^{-1} = r^{n-1}$. In an exact similar way, you can show that $r^{-2} = r^{n-2}$ by looking for the inverse of r^2 . Note that in both these cases, we find out that a negative power of r is equal to a positive one!

In fact, here is an easier algebraic hack without taking recourse to our previous geometric discussion. Note that $r^n = e$, so multiplying any group element with r^n does not change the element itself. Thus $r^n r^{-2} = r^{-2}$, but the two powers on left hand side can be combined to give r^{n-2} . Therefore we have $r^{-2} = r^{n-2}$. Do you see a pattern emerging here? We see, then,

that the powers of r “cycle back” periodically with period n . Visually, raising r to successive positive powers is the same as moving counterclockwise around the following circle one node at a time, whereas raising r to successive negative powers is the same as moving around the circle clockwise one node at a time. This is illustrated in figure 15, where r is denoted by R .

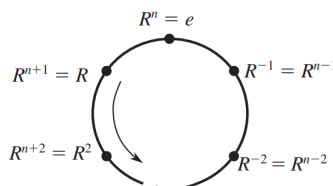


FIGURE 16. Powers of r in D_n

To summarise, we have thus made the following two points.

Observation 5.1. (1) $\{\dots, r^{-3}, r^{-2}, r^{-1}, e, r, r^2, r^3, \dots\} = \{e, r, r^2, \dots, r^{n-1}\}$. That is, the set of all possible powers of r is same as the finite set in the right hand side.
 (2) $\{e, r, r^2, \dots, r^{n-1}\}$ is a subgroup of D_n .

Let us denote this subgroup by C_n , signifying the fact that it is a *cyclic* (to be defined below) group of size n .

5.2. Generalization to abstract groups. We extrapolate an important point from this discussion that applies to any general group. If you read carefully the paragraph before the observation, you will notice that the conclusion does not really use anything specific about the group at all! It only relies on the fact that some finite power of the element r yields identity. In other words, we can carry out the analysis in that paragraph verbatim whenever we are given an element of order n in a group G . This gives us a recipe to cook up some subgroups in a general group. For any element a in a group G , we let $\langle a \rangle$ denote the set $\{a^i : i \text{ is an integer}\} = \{\dots, a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, \dots\}$. What we saw before can be summarized as the following neat statement.

Theorem 5.1. Let G be any group and a be any element in G . Then $\langle a \rangle$ is a subgroup of G . This subgroup is a finite group if a has finite order, otherwise it is an infinite group.

These kinds of subgroups appear so often in group theory that we give them a name for convenience.

Definition 5.1. If a is an element of a group G , then the subgroup $\langle a \rangle$ is called the *cyclic subgroup* of G generated by a . In that case, a is called a *generator* of this subgroup.

Now, if it happens that $G = \langle a \rangle$ for some element a , then we say that G is a cyclic group.

Exercise 5.4. Show that $(\mathbb{Z}, +)$ is a cyclic group by finding an explicit generator. Argue why 2 is not a generator of \mathbb{Z} .

Note that since $a^i a^j = a^{i+j} = a^{j+i} = a^j a^i$, all cyclic groups are abelian. Beware though, a cyclic group may have many generators. The following exercise illustrates that.

Exercise 5.5. In the group $(\mathbb{Z}, +)$, list the elements of the subgroup $\langle -1 \rangle$. In the same group as above, list the elements of $\langle 2 \rangle$, $\langle -2 \rangle$, $\langle 5 \rangle$. Do you see a pattern as to when two different elements of \mathbb{Z} generate the same cyclic subgroup?

Let us do another one to ensure we grasp the concept of generator correctly.

Exercise 5.6. Recall the group $(\mathbb{Q}, +)$ of rational numbers under addition and the group $(\mathbb{Q} \setminus \{0\}, *)$ of nonzero rational numbers under multiplication. In $(\mathbb{Q}, +)$, list the elements of $\langle \frac{1}{2} \rangle$. In $(\mathbb{Q} \setminus \{0\}, *)$, list the elements of $\langle \frac{1}{2} \rangle$.

By way of some easy examples, note that $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, and all of these are groups with the operation of addition, therefore any group in this sequence is a subgroup of all the groups that follow after it. We can have similar assertion about the sequence $\mathbb{Q} \setminus \{0\} \subset \mathbb{R} \setminus \{0\} \subset \mathbb{C} \setminus \{0\}$ with the operation of multiplication. On a more interesting note, we also saw that D_n can be thought of as being a subset of S_n and therefore it becomes a subgroup of S_n . We see in exercise 5.2. that $(\mathbb{Z}, +)$ is a cyclic group. You should try to convince yourself that none of the other groups mentioned above is cyclic, although that is relatively harder to see for S_n .

In fact, we can naturally generalize the concept of cyclic group to what we call a *finitely generated group*. For a subset S of G , we let $\langle S \rangle$ denote the subgroup of all elements of G that can be expressed as the finite product of elements in S and their inverses. Note that inverses are only needed if the group is infinite; in a finite group, the inverse of an element can be expressed as a power of that element. This is consistent with our earlier notation, in the sense that when $S = \{a\}$, we called $\langle a \rangle$ to be generated by the single element a , i.e. a cyclic group. We call $\langle S \rangle$ to be the subgroup generated by S , namely by r and s .

For example, in the group $(\mathbb{R}, +)$ we have $\langle 1, \sqrt{2} \rangle$ consists of numbers of the form $1^a \sqrt{2}^b$ for all integers a, b . Since the group operation is $+$, this means $a \cdot 1 + b \cdot \sqrt{2}$, i.e. $a + b\sqrt{2}$ for integers a, b . You can verify by hand (i.e. checking the four rules) that numbers of this form indeed build a group - which is guaranteed from the construction. It is therefore a subgroup of \mathbb{R} that is generated two elements. You should try to see why it cannot be generated by a single element, i.e. it is not a cyclic subgroup of \mathbb{R} .

Exercise 5.7. Give a generating set for the group D_n . Is it a cyclic group, i.e. generated by a single element?

Note that unlike a cyclic group, a group generated by two (or more) elements does not necessarily have to be abelian. Of course, it will be so if the mother group is abelian as seen with $\langle 1, \sqrt{2} \rangle \subset \mathbb{R}$, but not in general.

6. FINITE SUBGROUP OF RIGID MOTIONS: A GEOMETRIC RECIPE

In the previous section we discussed an abstract way in which we can create subgroups of a given group. We now discuss how they arise naturally in the context of symmetries of geometric objects. We shall try to motivate some interesting results in this direction, but we will not be proving anything in this section as it will take us a bit far from our intended course.

6.1. The case of dimension 2. Let's start with the example of symmetry group of a cube. We saw in section 5.3.2 that this group is same as S_4 , the permutation group on 4 letters. Now suppose that instead of asking for all the symmetries of the cube, we are interested in only those that fixes a chosen face.

Exercise 6.1. *How many rotational symmetries are there for a cube where one of its faces is fixed?*

Let us say that we put the cube on the floor and mark the face facing up as F . Then we want to specify rotations of the whole cube such that after the rotation is performed, F stays put. Let us break the above exercise into further simpler problems for lucid understanding.

Exercise 6.2. *What is the axis of rotation for the cube for the face F to stay put?*

It's not hard to see that the axis of rotation is the line perpendicular to the face F passing through the center of the face. You can check the first video mentioned in section 5.3.2.

Exercise 6.3. *How many rotations are there about the axis perpendicular to the face F and passing through its center, such that the position of F is unchanged?*

Basically, there are four such rotations with respect to the axis perpendicular in space to F by angles $0^\circ, 90^\circ, 180^\circ, 270^\circ$. These are in fact the elements e, r, r^2, r^3 of the group D_4 that consists of symmetries of the square face F .

Observation 6.1. *The cyclic group of size 4 sits inside the group of rotations of a cube, that is we get a subgroup of size 4 of S_4 i.e. $C_4 \subset S_4$.*

The second method of counting in 5.3.2 further tells us the answer: there are only 4 such symmetries.

This points us to a phenomenon that is really fundamental yet quite easy to grasp. Remember that the collection of all rigid motions of plane is a group. From this enormous infinite group we can extract S_4 by singling out only those motions that fix a cube, i.e. the symmetries of the cube. There are 24 of these. If we further want the symmetries to fix a face, we are down to a group of size 4. In other words, the more properties we want our rigid motions to have, the less there are of those! Seems intuitive enough, right? What is important is that *these smaller subsets of symmetries with additional properties often form a group by themselves*, just like we see in the case of $C_4 \subset S_4$ here.

This has an interesting application that we discuss next. We know from section 5.4 that for a geometric shape X in the plane, its symmetries form a group $\text{Sym}(X)$. By our terminology here, it is a subgroup of the group of all rigid motions of the plane.

Question 6.1. *What kind of groups we can get arising in this way, i.e. as $\text{Sym}(X)$ for some geometric configuration X ?*

As you can probably guess, this question might be too hard to answer completely in easy terms. If you solved exercise 4.9, you would probably be convinced that infinite configurations can give rise to pretty complicated groups! However, if we further restrict ourselves to X being a bounded figure in the plane, or equivalently $\text{Sym}(X)$ being a *finite* subgroup of all rigid motions, then we get a surprisingly neat answer.

Theorem 6.1. *Let G be a finite group of the group of all rigid motions of the plane. Then there is a positive integer n such that G is either C_n or D_n .*

The justification of this theorem will require a little bit more than just pure group theory technique, and as such we omit it. You have seen that D_n arises as $\text{Sym}(X)$ where X is a regular n -gon, and C_n is the subgroup consisting of *purely rotations*. At this point, the discerning reader might object to the latter group being phrased as the *full* symmetry group of some object. But we can assure them with an example of X for which C_n is indeed the full symmetry group.

Exercise 6.4. *Can you find an object in the 2 dimensional plane such that the group of rotational symmetries are a full symmetry group of that object.*

To answer the question above, let us consider a regular hexagon with some regularly placed bumps on each side, so that there is no reflection symmetry available. Thus, this bumpy hexagon has six rotational symmetries, but can't be flipped over like the regular hexagon. This works for general n as well.

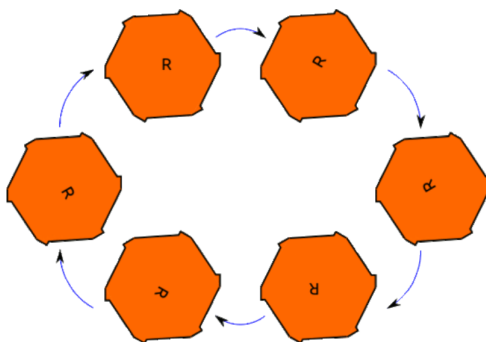


FIGURE 17. Six symmetries of a bumpy hexagon

6.2. The case of dimension 3. Armed with this knowledge, you might be curious as to what the answer looks like, if we instead consider the rigid motions in the three dimensional space that we live in. Here the answer is even more astounding. For the lack of more sophisticated group theory language, we only state a version of it: namely we focus only on rigid motions that are rotation. Note that we can consider the two dimensional plane as being a part of the three dimensional space, and thus we can think of the regular n -gon and bumpy n -gon as being inside the three dimensional space. Therefore, if we ask for finite subgroups of the group of all rotations, we still get D_n and C_n as part of the answer⁶. It turns out that we get only three more new examples.

⁶Interesting observation: reflection of a plane can be achieved by a rotation through the angle 180° in three dimensional space, and in this way the reflective symmetries of a regular polygon can be realized as rotations in three dimensional space.

Theorem 6.2. *Let G be a finite group of the group of all rotations of the three dimensional space. Then there are only five possibilities for G .*

- (1) C_n , the cyclic group of rotations by multiples of $\frac{360^\circ}{n}$ about a line, for some n ;
- (2) D_n , the dihedral group of symmetries of a regular n -gon, for some n ;
- (3) A_4 , or sometimes called the tetrahedral group of 12 rotational symmetries of a tetrahedron;
- (4) S_4 , or sometimes called the octahedral group of 24 rotational symmetries of a cube or an octahedron;
- (5) A_5 , or sometimes called the icosahedral group of 60 rotational symmetries of a dodecahedron or an icosahedron.

Platonic Solids: These three new examples arise out of rotational symmetry of three dimensional solid objects called the Platonic solids. These are three dimensional analogues of regular n -gons we saw before and as such can be built by pasting together certain specific polygons. More precisely, a Platonic solid is a convex body in three dimensional space such that each face is a regular polygon, the faces are identical and the same number of faces meet at each vertex. It is a rather surprising fact that there are only 5 such shapes!

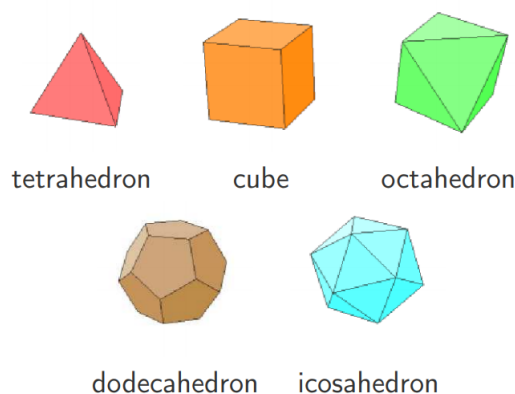


FIGURE 18. Five Platonic Solids

Historical detour: There is a fascinating amount of history in both arts and sciences associated with the Platonic solids. Stones carved into such polyhedral shapes date from about 2000BC in Scotland. These shapes have been known since antiquity, beginning with the ancient Greeks studying them extensively; they are prominent in the work of Plato, their namesake. Plato refers to the solids in the *Timaeus* circa 360BC and follows the Pythagoreans in giving them mystical significance. Four of them represented the four elements: the tetrahedron for fire, the cube for earth, the octahedron for air and the icosahedron for water. This association was justified on the grounds that the icosahedron is the smoothest of the polyhedra while the tetrahedron is the sharpest. The dodecahedron represented the entire universe with the twelve faces showing the twelve signs of the Zodiac. Euclid devoted the 13th and last book of his *Elements* to the discussion of Platonic solids.

In the 16th century, the German astronomer Johannes Kepler attempted to relate the five extraterrestrial planets known at that time to the five Platonic solids. In *Mysterium Cosmographicum*, published in 1596, Kepler proposed a model of the Solar System in which the five

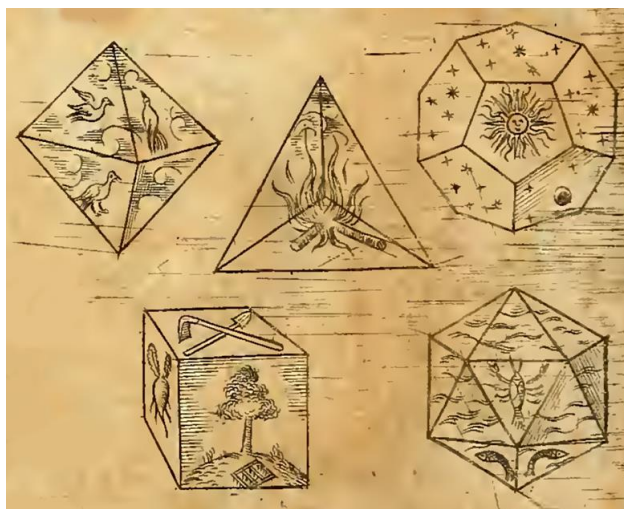


FIGURE 19. Five Platonic Solids in Greek mythology

solids were set inside one another and separated by a series of inscribed and circumscribed spheres. Kepler proposed that the distance relationships between the six planets known at that time could be understood in terms of the five Platonic solids enclosed within a sphere that represented the orbit of Saturn. The six spheres each corresponded to one of the planets (Mercury, Venus, Earth, Mars, Jupiter, and Saturn). The solids were ordered with the innermost being the octahedron, followed by the icosahedron, dodecahedron, tetrahedron, and finally the cube, thereby dictating the structure of the solar system and the distance relationships between the planets by the Platonic solids. In the end, Kepler's original idea had to be abandoned, but out of his research came his three laws of orbital dynamics, the first of which was that the orbits of planets are ellipses rather than circles, changing the course of physics and astronomy.

Coming back to math: Let us now sketch some ideas as to why there are only five Platonic solids. To help us understand them better, here is a table listing the numbers of faces, edges and vertices for these configuration.






Polyhedron		Vertices	Edges	Faces
tetrahedron		4	6	4
cube		8	12	6
octahedron		6	12	8
dodecahedron		20	30	12
icosahedron		12	30	20

FIGURE 20. Number of faces, edges and vertices of five Platonic solids

Now, we can approach this problem by counting the number of ways that one can begin to build one by bringing congruent regular polygons together at a vertex. Let's answer the big question by breaking it into smaller questions. One can assemble three, four, or five equilateral triangles, three squares, or three regular pentagons. (Six triangles, four squares, or three hexagons glue together into flat surfaces.) So there are just five possibilities. This is better explained in the video number 4 listed at the end of the packet, we refer you to that for better clarity at this point. But this analysis omits the interesting question of existence. For example, does an icosahedron exist? Of course, we can build one out of cardboard. But when we do, the triangles never fit together precisely, and we take it on faith that this is due to our imprecision. One way to be sure that the icosahedron exists may be to write down the coordinates of its vertices and check the distances, in other words to use three dimensional coordinate geometry - something we shall not pursue here.

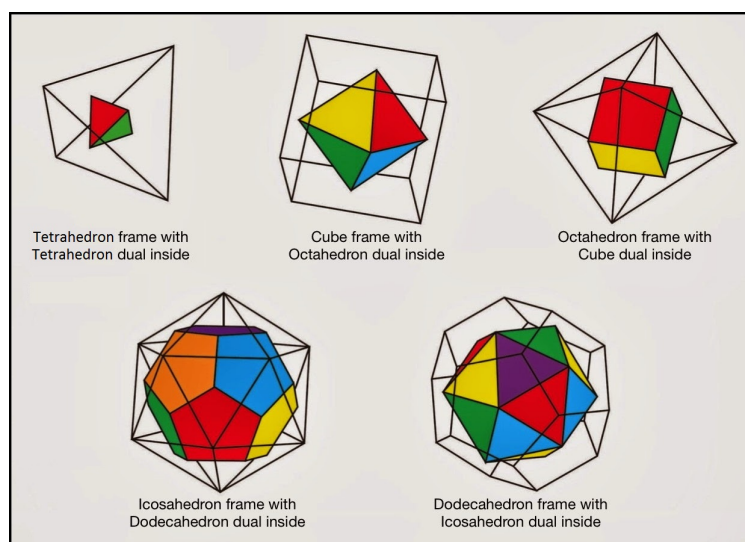


FIGURE 21. Dual Platonic solids

More than just itself being an interesting classification result, theorem 6.2 sheds light upon the importance of the Platonic solids from a group-theoretic perspective. We note that the octahedron and the cube are so called *dual solids*, meaning that one can be constructed by connecting vertices that are placed at the centers of the other. In other words, they are pairs of solids with faces and vertices interchanged. If you think about it, this ensures that rigid motions that preserve a tetrahedron also preserve the cube – therefore they have the same symmetry group, as asserted under item (4) of the theorem. Similarly, the icosahedron and the dodecahedron are dual solids, therefore they have the same symmetry group. The tetrahedron is dual with itself.

We have explored the groups listed under (1), (2) and (4) and studied how they account for symmetries of the mentioned objects. Let us conclude by saying a little bit about the remaining two groups. These groups A_4 and A_5 are in fact certain subgroups of S_4 and S_5 , respectively. In general, the name A_n is used to denote the subgroup of S_n that consists of *even permutations*. It is a subgroup half the size of S_n , just like C_n is a subgroup of D_n with half its size. We are not going to delve into this subgroup, except that we will list out the elements of A_4 visually as

symmetries of a tetrahedron. This is parallel to how we illustrated the rotational symmetries of a cube in section 4.2.4.

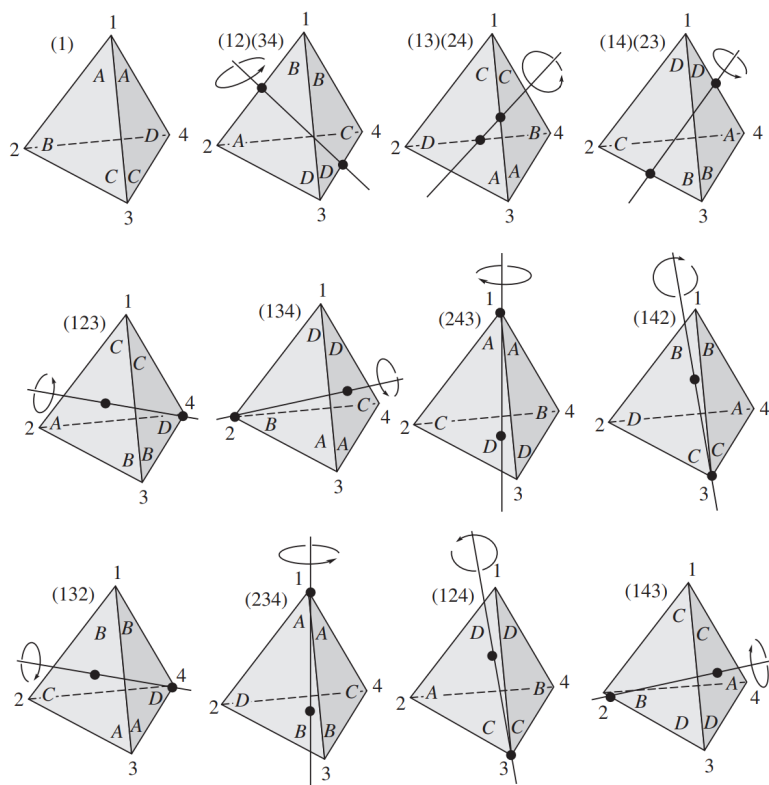


FIGURE 22. A_4 as rotations of a tetrahedron

The top row of figure 20 illustrates the identity and three 180° “edge” rotations about axes joining midpoints of two edges. The second row consists of 120° “face” rotations about axes joining a vertex to the center of the opposite face. The third row consists of 240° “face” rotations. Many molecules with chemical formulas of the form AB_4 , such as methane (CH_4) and carbon tetrachloride (CCl_4), have A_4 as their symmetry group. Therefore understanding this group is a basic and fundamental tool in studying such chemical compounds.

7. SUGGESTED READING AND VISUALS FOR FURTHER EXPLORATION

- (1) <https://www.youtube.com/watch?v=mH0oCDa74tE>: An animated primer to group theory and the leitmotif of abstraction.
- (2) <https://www.quantamagazine.org/mathematicians-chase-moonshine-string-theory-connections-20150312/> and <https://www.quantamagazine.org/moonshine-master-toys-with-string-theory-20160804/>: discusses a deep and mysterious connection between number theory, group theory and string theory, the so called Moonshine conjecture - in a popular science article format.
- (3) <http://www.markronan.com/mathematics/symmetry-corner/> Website for the book “Symmetry and the Monster”, a fast-paced historical narrative ranging across two centuries of mathematical development culminating in classification of finite simple groups.