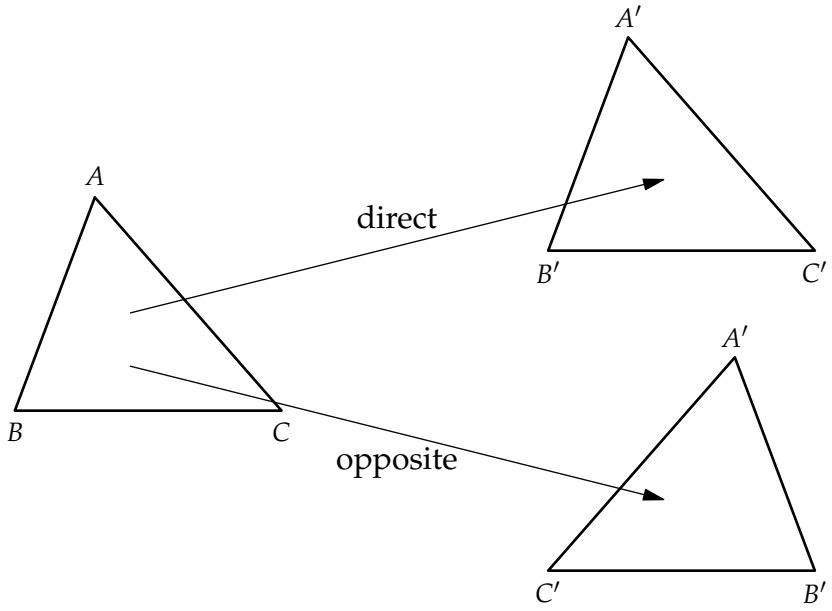
Direct and Opposite Isometries

Consider a triangle ABC in the plane such that the vertices A, B, C occur counterclockwise around the boundary of the triangle. If you apply an isometry to the triangle, then the result will be a triangle where the vertices A, B, C can occur clockwise or anticlockwise. If the orientation stays the same, then we say that the isometry is *direct* but if the orientation changes, then we say that the isometry is *opposite*.



Remember that we classified the isometries into four types — translations, rotations, reflections and glide reflections. It's easy to see which of these are direct and which are opposite.

- Every single translation is a direct isometry.
- Every single rotation is a direct isometry.
- Every single reflection is an opposite isometry.
- Every single glide reflection is an opposite isometry.

One of the nice things about composition of direct and opposite isometries is that they behave very much like multiplication of positive and negative numbers. This should be obvious when you compare the following two "multiplication tables" which have the same underlying structure. We're going to be looking at many "multiplication tables" like this and examining their underlying structure, so keep this example in mind.

$\circ$	dir	opp
dir	dir	opp
opp	opp	dir

$\times$	pos	neg
pos	pos	neg
neg	neg	pos

Fixed Points of Isometries

A *fixed point* of an isometry f is a point P such that $f(P) = P$ — in other words, a point which does not get moved by the isometry. Remember that we classified the isometries into four types — translations, rotations, reflections and glide reflections. It's easy to see which of these have fixed points and which of these don't.

- Every single translation which is not the identity has no fixed points.
- Every single rotation has one fixed point — namely, the centre of rotation.
- Every single reflection has infinitely many fixed points — namely, the points on the mirror.
- Every single glide reflection which is not a reflection has no fixed points.

Putting this information together with our knowledge of direct and opposite isometries, we have the following table. As long as the isometry we're interested in is not the identity, this table allows us to deduce the type of an isometry just by knowing whether it's direct or opposite and whether or not it has fixed points.

isometry	direct or opposite	fixed points
translation	direct	no
rotation	direct	yes
reflection	opposite	yes
glide reflection	opposite	no

Symmetry in the Plane

So we now know something about isometries — but what does this all have to do with symmetry? Well, we're now in a position where we can define what we mean by a symmetry, at least in the realm of Euclidean geometry. Informally, a symmetry of a geometric shape will be something we can do to the Euclidean plane while someone's back is turned so that when they turn around again, the shape will look exactly the same. More precisely, given a set X of points in the plane — it could be finite or infinite — a *symmetry of* X is an isometry which leaves the set X unchanged. You should think of X as a black and white picture, where the points in the plane coloured black are those that belong to X while the points in the plane coloured white are those that don't belong to X.

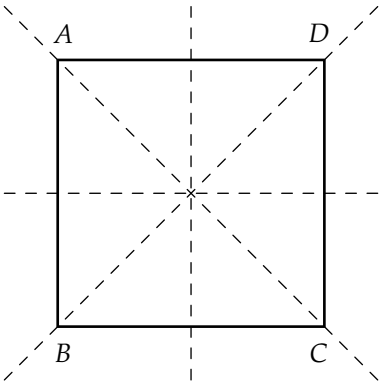
Note that the isometry doesn't have to leave every point of X exactly where it is — that would be way too restrictive — but only has to leave X as a whole exactly where it is. By this precise mathematical definition, every single subset of the Euclidean plane, no matter how crazy it looks, has at least one symmetry — namely, the identity isometry. Our intuitive notion of a shape being symmetric corresponds to the mathematically precise fact that it has a symmetry which is not the identity.

Example. The following diagram lists the letters of the alphabet and below it, the number of symmetries that it has. You should check to see that all the numbers are correct and, for each letter, determine what the isometries are which leave the letter exactly where it is.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
2	2	2	2	2	1	1	4	4	1	1	1	2

N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
2	4	1	1	1	2	2	2	2	2	4	2	2

Example. As another example, consider the symmetries of the square $ABCD$. We can prove that there are at most eight symmetries, since any symmetry must take the triangle ABC to one of the triangles ABC, BCD, CDA or DAB. Each of these triangles is isosceles, so there are two ways to map the triangle ABC to each of them. Tally all these up and, as promised, you see that there can be at most eight symmetries of the square.



To see that there are, in fact, exactly eight symmetries of the square, we simply need to write them all down. Below, we give each symmetry a symbol, describe the isometry geometrically, and describe what the isometry does to the vertices of the square.

- I : the identity isometry
  $A \to A, B \to B, C \to C, D \to D$
- R_1 : rotation by 90° anticlockwise about the centre of the square
  $A \to B, B \to C, C \to D, D \to A$
- R_2 : rotation by 180° anticlockwise about the centre of the square
  $A \to C, B \to D, C \to A, D \to B$
- R_3 : rotation by 270° anticlockwise about the centre of the square
  $A \to D, B \to A, C \to B, D \to C$
- M_h : reflection across the horizontal line passing through the centre of the square
  $A \to B, B \to A, C \to D, D \to C$
- M_v : reflection across the vertical line passing through the centre of the square
  $A \to D, B \to C, C \to B, D \to A$
- M_{AC} : reflection across the line AC
  $A \to A, B \to D, C \to C, D \to A$
- M_{BD} : reflection across the line BD
  $A \to C, B \to B, C \to A, D \to D$

Qualifying Symmetry in the Plane

So we're now in a position where we can quantify — in other words, count — the symmetries of a shape. However, it will be much more interesting to qualify — in other words, examine the structure of — the symmetries of a shape.[1]

Earlier, we stated that the letters **H** and **X** each have four symmetries. Not only do they have the same number, but their symmetries also seem to have a similar structure — there is the identity, rotation by 180°, reflection in a horizontal axis, and reflection in a vertical axis. So in some sense, the letters **H** and **X** not only have the same quantity of symmetries, but also the same quality of symmetries, whatever that might mean.

[1] People who don't know what mathematics is about seem to think that it is about quantifying — in other words, counting — things, when it is really about qualifying — in other words, examining the structure of — things.

A slightly more interesting example is to compare the symmetries of the letters **A** and **B**, both of which have two symmetries. This time, however, the symmetries of the letter **A** are the identity and reflection in a vertical axis, while the symmetries of the letter **B** are the identity and reflection in a horizontal axis. So it seems that the letters **A** and **B** have the same quantity of symmetries, but not the same quality — or do they? On further thought, if we consider the letter **B** to be simply made up of a set of points in the plane, who cares which way is up, down, left or right? As a mathematical object, it is essentially the same thing as **ꓭ**, which like the letter **A**, has the identity and reflection in a vertical axis as its symmetries.

One crucial observation about the symmetries of an object is that if you compose two of them, then the result is always a symmetry. This means that if you find some symmetries of an object, then you can try to find other ones by composing the ones you already have. The composition of symmetries captures their structure in a way that can be represented by a sort of "multiplication table".

Example. Let's continue with our example from earlier, which involved the symmetries of a square. We were able to verify that there are eight symmetries, each of which we gave a name. We may now use these to fill out a table which describes precisely how these symmetries compose with each other. Note that if you want to work out the entry corresponding to the row labelled A and the column labelled B, then the entry should be $A \circ B$. Remember that this is the composition B followed by A, because we always apply the isometry on the right before the one on the left. You should carefully check the following table to make sure that you understand exactly how to construct it on your own.

$\circ$	I	R_1	R_2	R_3	M_h	M_v	M_{AC}	M_{BD}
I	I	R_1	R_2	R_3	M_h	M_v	M_{AC}	M_{BD}
R_1	R_1	R_2	R_3	I	M_{BD}	M_{AC}	M_h	M_v
R_2	R_2	R_3	I	R_1	M_v	M_h	M_{BD}	M_{AC}
R_3	R_3	I	R_1	R_2	M_{AC}	M_{BD}	M_v	M_h
M_h	M_h	M_{AC}	M_v	M_{BD}	I	R_2	R_1	R_3
M_v	M_v	M_{BD}	M_h	M_{AC}	R_2	I	R_3	R_1
M_{AC}	M_{AC}	M_v	M_{BD}	M_h	R_3	R_1	I	R_2
M_{BD}	M_{BD}	M_h	M_{AC}	M_v	R_1	R_3	R_2	I

The set of symmetries of a subset X of the plane is called the *symmetry group* of X. The "multiplication table" describing how the symmetries of X compose with each other is called the *Cayley table* of the symmetry group. We should note the following things about the Cayley table we have just written down.

- It is not true that $A \circ B = B \circ A$ for all choices of A and B. In particular, you can see in the table that $M_{BD} \circ M_v = R_3$ while $M_v \circ M_{BD} = R_1$. This means that Cayley tables are not all that similar to multiplication tables — the entries are not symmetric when you flip along the diagonal, a property which multiplication tables obey.
- Every row and column contains every element of the symmetry group exactly once. We will restate and prove this property — which I will refer to as the *sudoku* property — later on.
- As we mentioned earlier, the whole table of entries is not symmetric when you flip along the diagonal. However, the location of the entries which are I is symmetric when you flip along the diagonal. Another way to say this is that if $A \circ B = I$, then $B \circ A = I$ as well.

Properties of Symmetry Groups

Symmetry is a very far-reaching idea in mathematics and extends way beyond the notion of symmetry which we have defined. Indeed, we have only defined symmetries for subsets of the Euclidean plane, while the notion of symmetry applies to many, many other things. As a simple example, consider the expressions $x + 2y$ and $x + y$. To many a mathematician, the first expression does not seem symmetric, because swapping x and y changes it. On the other hand, the second expression does seem symmetric, because swapping x and y results in $y + x$ which, although it may look different, is exactly the same expression. This example is so far removed from geometry that, to widen our definition of symmetry to incorporate it, we have to do something rather drastic.

The idea we will use is a relatively modern one in mathematics. Take the set of objects that you are studying — in our case, the symmetries of a geometric shape — write down the most important properties that they obey, and then consider anything at all which obeys those properties. In some cases, this will give a very useful and interesting set of objects which is far more general than the set of objects that you started with. This probably makes no sense to you whatsoever, so the best thing to do is probably just to forge ahead. The following are four very important properties which all symmetry groups obey.

- (Closure) If A and B are symmetries, then the composition $A \circ B$ is also a symmetry.
- (Identity) There always exists the identity symmetry I such that, for each symmetry A, the composition $I \circ A$ and the composition $A \circ I$ are both equal to A.
- (Inverse) For each symmetry A, there exists a symmetry B such that the composition $A \circ B$ and the composition $B \circ A$ are both equal to I.
- (Associative) For all symmetries A, B, C, the symmetry obtained by composing them as $(A \circ B) \circ C$ is the same as the symmetry obtained by composing them as $A \circ (B \circ C)$.

The first property states that composition of symmetries is a symmetry, the second that doing nothing is always a symmetry, and the third that doing the reverse of a symmetry is again a symmetry. Hopefully these are all obvious statements which you believe are true. The fourth statement is a little different, possibly too obvious to seem important. It merely says that when you are calculating the composition of three or more symmetries, you never need to use brackets. So an example like $(A \circ (B \circ C)) \circ ((D \circ E) \circ F)$ is just the same thing as $A \circ B \circ C \circ D \circ E \circ F$. Anyway, if you think that this just seems silly, then you may be right, but it certainly is important mathematically.

The Definition of a Group

So the idea now is to take these four properties and use them as rules to define an object as follows. Whatever object we obtain is going to behave very similarly to a symmetry group but will capture a notion of symmetry that is much broader than the geometric symmetries that we've been discussing.

A *group* is a set G with a "multiplication table" such that the following four properties hold.

- (Closure) For all g and h in G, the expression $g \cdot h$ is also in G.
- (Identity[2]) There is a special element e in G such that if g is in G, we have $e \cdot g = g \cdot e = g$.
- (Inverses) For every g in G, there is an element h in G such that $g \cdot h = h \cdot g = e$.
- (Associative) For all g, h, k in G, we have $(g \cdot h) \cdot k = g \cdot (h \cdot k)$.

[2]For some reason, when you deal with groups, it's common to call the identity element e — hopefully, this won't be too confusing.

Because we are simply assuming that these are the rules of the game and we can never prove them, the four properties above are often called the *group axioms*. Hopefully you can see that the definition mimics the four properties of symmetry groups which we discussed earlier. So, in some sense, you can think of the elements of G as the symmetries of some object, although that object may or may not be geometric and may be something you can't even imagine.

Some Examples of Groups

It's a good habit, whenever anyone throws a mathematical definition at you, to think of as many examples as you can. So here are some simple examples of groups. You should take each one and verify in your own mind why it obeys the group axioms listed above.

- The set of symmetries of any subset of the plane, where $\cdot$ represents composition, is a group. We know that this has to be true, because we constructed the definition of a group so that the set of symmetries of any subset of the plane would be an example.
- The set of all isometries, where $\cdot$ represents composition, is a group. Actually, this is just a particular case of the example above, where the subset of the plane that we take is the empty set consisting of no points.
- The real numbers, where $\cdot$ represents addition, is a group. In this case, the identity is the number 0 and the inverse of x is the number $-x$. The fact that addition of numbers is associative is just something we always take for granted.
- The set of integers, where $\cdot$ represents addition, is a group. If we call this group $\mathbb{Z}$ and the group in the previous example $\mathbb{R}$, note that $\mathbb{Z}$ is a group which lives inside of $\mathbb{R}$, so we say that $\mathbb{Z}$ is a *subgroup* of $\mathbb{R}$.
- The positive real numbers, where $\cdot$ represents multiplication, is a group. In this case, the identity is the number 1 and the inverse of x is the number $\frac{1}{x}$. If $\cdot$ represents multiplication, then you know that the number 0 cannot be a part of the group, because it has no inverse. In fact, you can just remove the number 0 from the real numbers to obtain another example of a group where $\cdot$ represents multiplication.
- The set of all $m \times n$ matrices, where $\cdot$ represents addition, is a group. In this case, the identity is the zero matrix and the inverse of a matrix M is the matrix $-M$. The fact that addition of matrices is associative follows directly from the fact that addition of numbers is associative.
- The set of all $n \times n$ matrices with determinant 1, where $\cdot$ represents multiplication, is a group. You need the condition that the determinant is 1 — or at least, something similar to it — to get rid of examples like the zero matrix which have no inverse. In this case, the fact that multiplication of matrices is associative is something you may have taken for granted but is definitely not immediately obvious. Try to prove it — even just for 2×2 matrices — and you'll see what I mean.
- The set of two numbers $\{1, -1\}$, where $\cdot$ represents multiplication, is a group. In this case, the identity is the number 1 and the inverse of each element is itself. Note that the Cayley table for this group looks remarkably similar to the two tables we wrote down when talking about direct and opposite isometries, just with some of the names changed.

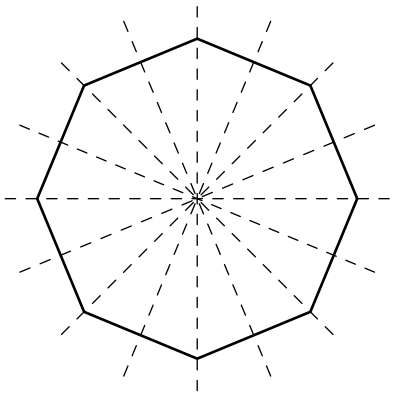
In fact, it's a good habit, whenever anyone throw a mathematical definition at you, to also think of counterexamples. Obviously, examples of things which aren't groups are easy to come up with — a banana, a hippopotamus, your index finger, and so on. However, can you think of something which obeys the group axioms except for the identity property, something which obeys the group axioms except for the inverse property, and something which obeys the group axioms except for the associative property?

Three Special Types of Group

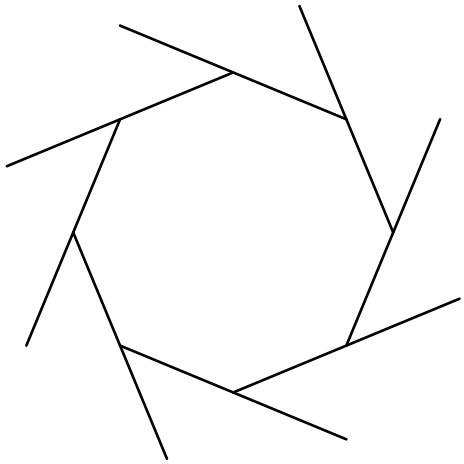
The examples of groups that we have seen, as special as they are, will not feature very much in this course. But there are three types of groups which will, and they are known as dihedral groups, cyclic groups and symmetric groups.

- *Dihedral Groups D_n*
  We can describe the dihedral group D_n as the symmetries of the regular polygon with n sides.[3] The case $n = 4$ amounts to studying the symmetries of a square, which we considered earlier. We noted then that there are four rotations (including the identity) and four reflections which are symmetries of the square. In the general case, there are n rotations (including the identity) and n reflections which are symmetries of the regular polygon with n sides. Therefore, the group D_n contains $2n$ elements.

  The diagram below shows a regular polygon with eight sides and the mirrors corresponding to the eight reflective symmetries.



- *Cyclic Groups C_n*
  We can describe the cyclic group C_n as the symmetries of the "decorated" regular polygon with n sides. The diagram below shows a decorated regular polygon with eight sides and hopefully you'll be able to draw a decorated regular polygon with any number of sides. The extra decoration removes all of the reflections as symmetries, but keeps all of the rotations. Another way to describe the cyclic group C_n is as the set of direct symmetries of a regular polygon with n sides. Either description you decide to use, you see that the group C_n contains n elements.



[3] A regular polygon is just a polygon whose side lengths are all equal and whose angles are all equal.

- *Symmetric Groups S_n*

  The elements of the group S_n are simply the permutations of the numbers from 1 up to n. For example, the group S_3 contains the following six elements — these are the ways to write the numbers 1, 2, 3 in some order.

  $$123 \quad 132 \quad 213 \quad 231 \quad 312 \quad 321$$

  You should think of the element abc as the function which takes a number from the set $\{1,2,3\}$ and spits out a number from the set $\{1,2,3\}$ in the following way.

  $$1 \to a \qquad 2 \to b \qquad 3 \to c$$

  In this group, the $\cdot$ stands for composition of these permutations — maybe an example is the best way to illustrate this. Suppose that we want to determine which permutation corresponds to the product $132 \cdot 231$. The permutation 231 takes

  $$1 \to 2 \qquad 2 \to 3 \qquad 3 \to 1$$

  while the permutation 132 takes

  $$1 \to 1 \qquad 2 \to 3 \qquad 3 \to 2.$$

  Let's see where the permutation $132 \cdot 231$ takes the number 1. We always start from the rightmost permutation which, in this case, is 231. This takes 1 to 2 and this 2 is then fed into the next permutation along which, in this case, is 132. This takes 2 to 3, so the composition $132 \cdot 231$ takes 1 to 3.

  Now let's see where the permutation $132 \cdot 231$ takes the number 2. We always start from the rightmost permutation which, in this case, is 231. This takes 2 to 3 and this 3 is then fed into the next permutation along which, in this case, is 132. This takes 3 to 2, so the composition $132 \cdot 231$ takes 2 to 2.

  Finally, let's see where the permutation $132 \cdot 231$ takes the number 3. We always start from the rightmost permutation which, in this case, is 231. This takes 3 to 1 and this 1 is then fed into the next permutation along which, in this case, is 132. This takes 1 to 1, so the composition $132 \cdot 231$ takes 3 to 1.

  Putting all of these facts together, we see that the composition $132 \cdot 231$ is a permutation which takes 1 to 3, 2 to 2 and 3 to 1 and this resulting permutation we have called 321. Therefore, we can write the composition as

  $$132 \cdot 231 = 321.$$

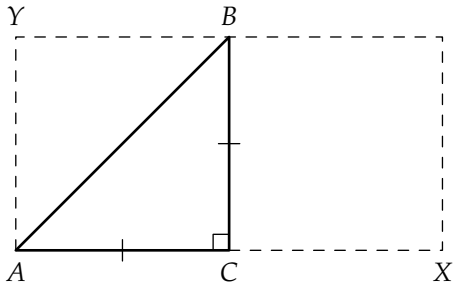
  Hopefully, you can see that when you compose permutations in this way, the identity of S_3 will be the element we've described as 123. That's because this permutation does nothing — it takes 1 to 1, 2 to 2 and 3 to 3.

Problems

Problem. *Let ABC be a triangle with the vertices labelled clockwise such that $AC = BC$ and $\angle ACB = 90^\circ$. Let M_{AB} be the reflection in the line AB, M_{AC} be the reflection in the line AC, and R be the rotation by 90° counterclockwise around B. Identify the composition $R \circ M_{AB} \circ M_{AC}$.*

If X denotes the composition $R \circ M_{AB} \circ M_{AC}$, let n be the minimum number of reflections whose composition is equal to X. Determine the value of n and carefully describe n reflections whose composition is equal to X.

Proof. We solved this problem in the previous lecture, but today we'll give a slightly different solution. The diagram below shows triangle ABC drawn on a grid of two squares. The composition $R \circ M_{AB} \circ M_{AC}$ must be direct because it's the composition of two opposite isometries and one direct isometry. It's easy to check that $M_{AC}(C) = C$, $M_{AB}(C) = Y$ and $R(Y) = C$ — in other words, $R \circ M_{AB} \circ M_{AC}(C) = C$ and C is a fixed point of the composition. Since the composition $R \circ M_{AB} \circ M_{AC}$ is a direct isometry with C as a fixed point, it must be the identity or a rotation about C.



To determine which of these cases applies, we consider the location of $R \circ M_{AB} \circ M_{AC}(A)$. It should be clear that $M_{AC}(A) = A$, $M_{AB}(A) = A$ and $R(A) = X$ — in other words, $R \circ M_{AB} \circ M_{AC}(A) = X$ and A is not a fixed point of the composition. Hence, the composition $R \circ M_{AB} \circ M_{AC}$ must be a rotation by $\angle ACX = 180°$ about C. □

As we've already learnt with these sorts of problems, it's useful to draw the diagram on a grid of squares. We've also learnt that it's useful to keep in mind the table which characterises isometries by whether they are direct or opposite and whether they have fixed points or not.

Problem. *Write down the Cayley table for the group S_3.*

Proof. We've already seen an example of how the composition of permutations works, but it's probably a good idea to see another example. Makes sure you understand very carefully how the notation and the process works. Suppose that we want to determine which permutation corresponds to the product $213 \cdot 321$. The permutation 213 takes

$$1 \to 2 \qquad 2 \to 1 \qquad 3 \to 3$$

while the permutation 132 takes

$$1 \to 3 \qquad 2 \to 2 \qquad 3 \to 1.$$

Let's see where the permutation $213 \cdot 321$ takes the number 1. We always start from the rightmost permutation which, in this case, is 321. This takes 1 to 3 and this 3 is then fed into the next permutation along which, in this case, is 213. This takes 3 to 3, so the composition $132 \cdot 231$ takes 1 to 3.

Now let's see where the permutation $213 \cdot 321$ takes the number 2. We always start from the rightmost permutation which, in this case, is 321. This takes 2 to 2 and this 2 is then fed into the next permutation along which, in this case, is 213. This takes 2 to 1, so the composition $132 \cdot 231$ takes 2 to 1.

Finally, let's see where the permutation $213 \cdot 321$ takes the number 3. We always start from the rightmost permutation which, in this case, is 321. This takes 3 to 1 and this 1 is then fed into the next permutation along which, in this case, is 213. This takes 1 to 2, so the composition $132 \cdot 231$ takes 3 to 2.

Putting all of these facts together, we see that the composition $132 \cdot 231$ is a permutation which takes 1 to 3, 2 to 1 and 3 to 2 and this resulting permutation we have called 312. Therefore, we can write the composition as

$$213 \cdot 321 = 312.$$

This means that we can fill in the entry in the Cayley table whose row is labelled by 213 and whose column is labelled by 321 with the permutation 312. After a while, you can get pretty quick are doing these computations, and I'm sure it won't take you long to check that the resulting Cayley table looks like the following. □

$\circ$	123	132	213	231	312	321
123	123	132	213	231	312	321
132	132	123	312	321	213	231
213	213	231	123	132	321	312
231	231	213	321	312	123	132
312	312	321	132	123	231	213
321	321	312	231	213	132	123

Galois

I'm going to tell you about one of my favourite mathematicians ever, the French mathematician Évariste Galois. It seems that Galois was a very passionate man, particularly when it came to mathematics, politics and women — the first made him famous, the second got him locked up in prison and the third caused his death. In fact, after being born in 1811, Galois didn't even make it to his 21st birthday before dying, all because of a woman.

Apparently, Galois wasn't particularly fond of school — you can't blame him — and his teachers didn't recognise his talents at all. In fact, the story goes that it wasn't until Galois was a teenager and confined to bed with illness that he really discovered mathematics. Once hooked, it seems that Galois devoted much of his time to mathematics in the few remaining years of his life.

After school, Galois attempted the entrance exam to the École Polytechnique in Paris, but failed due to his lack of explanation in the oral exam. This was due to Galois' unusual upbringing in mathematics, learning everything on his own from advanced textbooks. So instead, he went to the École Préparatoire, a far inferior institution where he found some professors who were sympathetic to him. The following year, Galois tried, for his second and last time, the entrance exam to the École Polytechnique and, for reasons we aren't too sure about, failed again despite being more than qualified. Some say that he thought the exercise given to him was boring and rather than solve it, decided to throw the blackboard cleaner at the examiner's head. Another possible reason is that Galois' logical leaps were far too advanced for the incompetent examiner, which angered Galois. Yet another explanation could be Galois' emotional state, since his father had committed suicide two days earlier.

There were other ways to get ahead in the mathematical world in those days. So Galois decided to write up his thoughts and send them to the very prestigious Academy of Sciences. For very mysterious reasons, the famous mathematician Augustin Louis Cauchy read these papers but refused to publish them. When he tried the following year to submit them, but this time to another famous mathematician by the name of Joseph Fourier, it turns out that Fourier suddenly died and the paper was lost. Later on, Galois tried once again, this time turning to the famous mathematician Simeon Poisson. However, Poisson declared that Galois' work was incomprehensible, saying that his "argument is neither sufficiently clear nor sufficiently developed to allow us to judge its rigour".

Meanwhile, Galois was also involved in the political turmoil going on in France. He was expelled from his university for a particularly heated letter concerning the political situation and then joined the staunchly Republican artillery unit of the National Guard. At a large and rather riotous banquet, Galois made a toast to King Louis–Philippe with a dagger above his cup, which was interpreted as a threat against the king's life. Although he was arrested, he was later acquitted. But on the following Bastille Day, Galois headed a protest, while wearing the uniform of the National Guard, carrying pistols, a rifle and a dagger. For this he was arrested and sentenced to six months in prison — but this quiet time allowed him to return to mathematics and further develop his ideas.

Only one month after Galois' release from prison, it appears that he was involved in a duel. Although the reasons behind the duel are not particularly clear, we know that it was the result of a love affair. Some conspiracy theorists believe that the whole situation was orchestrated by the government in order to get rid of the troublemaking Galois, but this doesn't seem to be too likely. Whatever the reasons behind the duel, Galois was so convinced of his impending death that he stayed up all night writing letters and composing what would become his mathematical testament, a famous letter to Auguste Chevalier outlining his ideas. Hermann Weyl, one of the greatest mathematicians of the twentieth century, said that "this letter, if judged by the novelty and profundity of ideas it contains, is perhaps the most substantial piece of writing in the whole literature of mankind." Weyl's statement is undoubtedly an exaggeration, but you get the point.

Unfortunately for the world of mathematics, in the very early morning on 30 May 1832, Galois was shot in the abdomen and died the following day with his brother at his side, at the tender age of twenty. I always wonder whether Galois would have done better in the duel had he not stayed up all night writing down his mathematical ideas.

Galois laid the foundations for a whole new area of mathematics which we now call Galois theory. One of the main applications was the problem of solving the quintic equation. So we all know that a quadratic equation is something which looks like $ax^2 + bx + c = 0$ and that its solution is given by the quadratic formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

It's much less commonly known that there is a formula for the solutions of the cubic equation $ax^3 + bx^2 + cx + d = 0$ which was discovered in the seventeenth century. This formula would probably take me about a third of this page to write down, but it pales in comparison to the formula for for the solutions of the quartic equation $ax^4 + bx^3 + cx^2 + dx + e = 0$. This beast of a formula would probably take me pages, but it was discovered not long after its cubic cousin. Then, there was a dry spell, when mathematicians tried to look for a formula for the solutions to the quintic equation $ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$. They tried and tried but to no avail.

The reason why they weren't successful is because there is no formula, and we know that because Galois proved it.[4] To understand the significance of this, you have to realise that to find a formula is easy because you just have to write it down and demonstrate that it works. But how do you prove that there is no formula for the quintic equation? Galois' did it by finding some "hidden symmetry" among the solutions of polynomials, which led to him using the concept of groups in his work. In fact, we have Galois to thank for the word *group* in mathematics.

[4] Actually, the Norwegian mathematician Niels Henrik Abel proved the same thing at around the same time, although the ideas in his proof are not as far-reaching. Unfortunately, Abel also reached an untimely end, dying at the tender age of twenty-six.