Recap

Now is probably a good time for a quick recap of our exploration into symmetry so far. Philosophically, our broad goal is to give a mathematically precise definition of symmetry and see where this definition can take us. When we began, I tried to convince you that the notion of symmetry in geometry is somehow tied to the notion of distance. In particular, this observation motivated us to define isometries, functions which take points in the plane to points in the plane and which preserve distances. Mathematicians are always trying to classify things, so it made sense to try to classify all of the possible isometries. We discovered that there were essentially four types — namely, translations, rotations, reflections and glide reflections. The definition of an isometry allowed us to mathematically define a symmetry of a subset of the Euclidean plane as an isometry which leaves the subset exactly where it is. We observed that the symmetries of a given shape can be composed with each other and are collectively known as the symmetry group of the shape. Then we found that the structure of a symmetry group is encapsulated in its "multiplication table", which is more accurately known as its Cayley table.

At this point, we turned to more abstract matters, using four very simple properties of symmetry groups to define the notion of a group. 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) 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 $(g \cdot h) \cdot k = g \cdot (h \cdot k)$.

So, from the seeds of our intuition about symmetry, we have developed the abstract notion of a group. And now we're in a position to delve a little deeper into the mysterious world of group theory.

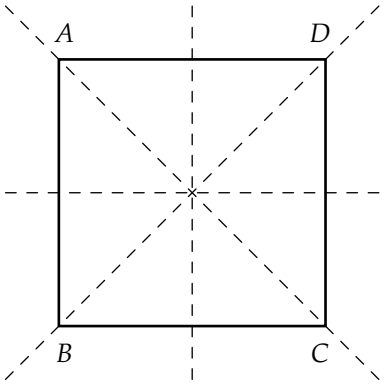
When are Two Groups the Same?

Quite a while ago, we noted that the letters **H** and **X** have the same symmetry group structure — the identity, a rotation by 180°, a reflection in a horizontal mirror, and a reflection in a vertical mirror. We also decided that the letters **A** and **B** have the same symmetry group structure, even though they superficially seem to be different. The crucial point is that, in both cases, there is the identity as well as one reflection, and that reflection composed with itself gives back the identity. This all sounded like mumbo jumbo back then and it probably sounds like mumbo jumbo now — but it's time now to make all this mumbo jumbo mathematically precise.

Remember that we looked at the symmetry group of the square and named its elements

$$I, R_1, R_2, R_3, M_h, M_v, M_{AC}, M_{BD}.$$

In fact, we actually wrote out the whole Cayley table for this group, which is an example of a dihedral group — the dihedral group D_4, to be precise.



If you don't actually remember, then that's fine because here's the Cayley table once again.

$\circ$	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

Now suppose that, due to failing the course, you were forced to take it again next summer.[1] And suppose that I was the lecturer once again and decided to write out the Cayley table for the symmetry group of the square. If I had instead named the elements

$$i, r_1, r_2, r_3, m_h, m_v, m_{AC}, m_{BD},$$

would you think that I had made some sort of mistake? Would you think that this new Cayley table is different from its capitalised version? No, of course you wouldn't, and rightly so. And that's because the two Cayley tables have essentially the same structure, even though we are using different symbols for each element of the group. In fact, by this reasoning, I could even have changed the names of the symmetries of the square to

$$A, B, C, D, E, F, G, H,$$

and you'd still have to agree that the resulting Cayley table and the resulting symmetry group have essentially the same structure. It would certainly be silly to treat two groups differently just because you've written their Cayley tables using different symbols. This idea is most aptly described by Shakespeare himself, in his play Romeo and Juliet.

> *What's in a name? That which we call a rose*
> *By any other name would smell as sweet.*

Translating this couplet from the world of Shakespearean tragedy to its group theoretic equivalent, we have the following.

> *Taking a Cayley table and renaming the elements*
> *Gives a group with the same structure.*

So we consider two groups to be the same if the entries in the Cayley table of one can be renamed to give the Cayley table of the other. If this is the case, then we say that the two groups are *isomorphic*, which in ancient Greek means "same structure". An even more mathematically precise way to express this is as follows. Two groups G and H are *isomorphic* if there exists a bijection — that is, a one-to-one dictionary correspondence — $f : G \to H$ such that

$$f(g_1 \cdot g_2) = f(g_1) \cdot f(g_2).$$

[1] Hopefully none of you will fail the course, so this story is purely hypothetical.

Here, the function f is called an *isomorphism* and simply describes the relabelling of the elements of G into elements of H. The equation above simply encapsulates the idea that the elements of G should be relabelled into elements of H in such a way that respects the structure of the two Cayley tables.[2] If two groups G and H are isomorphic, then we usually write this using the shorthand notation $G \cong H$.

Examples of Isomorphisms

The notion of isomorphism is a very powerful one indeed in mathematics, appearing in all sorts of areas apart from group theory. The definition is truly very simple, but it will be useful to see some small examples of isomorphisms.

Example. We've actually already considered an isomorphism between two groups a long time ago, when we discussed direct and opposite isometries. Back then, we observed that the following two tables seem to have a very similar structure.

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

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

More formally, you can verify that they both correspond to Cayley tables of groups and that the two groups are isomorphic. In fact, it's easy to describe the isomorphism between them as

$$f(\text{dir}) = \text{pos} \quad \text{and} \quad f(\text{opp}) = \text{neg}.$$

To verify that this is indeed an isomorphism, all you need to do is check that the following statements are true, which is quite easy to do.

$$\begin{aligned} f(\text{dir} \circ \text{dir}) &= f(\text{dir}) \times f(\text{dir}) \\ f(\text{dir} \circ \text{opp}) &= f(\text{dir}) \times f(\text{opp}) \\ f(\text{opp} \circ \text{dir}) &= f(\text{opp}) \times f(\text{dir}) \\ f(\text{opp} \circ \text{opp}) &= f(\text{opp}) \times f(\text{opp}) \end{aligned}$$

Example. Now consider the group — let's call it G — whose Cayley table looks like the table below left.

$\cdot$	a	b	c
a	c	a	b
b	a	b	c
c	b	c	a

$\circ$	I	R_1	R_2
I	I	R_1	R_2
R_1	R_1	R_2	I
R_2	R_2	I	R_1

We know about a group with three elements already — namely, the cyclic group C_3. Recall that this consists of the rotational symmetries of an equilateral triangle or, if you prefer, the symmetries of a decorated equilateral triangle. Above right is the Cayley table of C_3, where we denote the identity isometry by I, the rotation

[2] Note that the $\cdot$ on the left hand side of the equation corresponds to composition using the Cayley table of G while the $\cdot$ on the right hand side corresponds to composition using the Cayley table of H, even though I've used the same symbol for both.

by 120° about the centre of the equilateral triangle by R_1 and the rotation by 240° about the centre of the equilateral triangle by R_2. With this notation, an isomorphism $f : G \to C_3$ is given by

$$f(a) = R_2 \quad f(b) = I \quad f(c) = R_1.$$

I was careful to say "an isomorphism" because it's not a priori clear that there will only be one of them. And, in fact, there happen to be two possible isomorphisms in this case and the other one is given by

$$f(a) = R_1 \quad f(b) = I \quad f(c) = R_2.$$

Example. At one stage, we wrote out the Cayley table for the symmetric group S_3, which consists of the permutations of the numbers 1, 2, 3. Another group with six elements is the group D_3, which consists of the symmetries of an equilateral triangle ABC. The Cayley tables for these two groups are listed below, where I is the identity isometry, R_1 is a rotation by 120° about the centre of ABC, R_2 is a rotation by 120° about the centre of ABC, M_A is a reflection through a mirror passing through A, M_B is a reflection through a mirror passing through B, and M_C is a reflection through a mirror passing through C.

∘	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

∘	I	R_1	R_2	M_A	M_B	M_C
I	I	R_1	R_2	M_A	M_B	M_C
R_1	R_1	R_2	I	M_C	M_A	M_B
R_2	R_2	I	R_1	M_B	M_C	M_A
M_A	M_A	M_B	M_C	I	R_1	R_2
M_B	M_B	M_C	M_A	R_2	I	R_1
M_C	M_C	M_A	M_B	R_1	R_2	I

It turns out that these two groups are isomorphic, but an isomorphism is a little tricky to find. And once you've found it, there would still be thirty-six things to check to make sure that it's an isomorphism, at least if you try to do it the naive way.

We can actually describe the isomorphism quite easily in such a way that it should be reasonably clear that it's an isomorphism, without having to check all thirty-six entries of the Cayley table. Simply label the vertices of the equilateral triangle 1, 2, 3 rather than A, B, C. Then any symmetry of the equilateral triangle permutes the vertices and hence, corresponds to a permutation of the numbers 1, 2, 3 — in other words, an element of the group S_3. Since composition of symmetries will behave in the same way as composition of permutations, this is an isomorphism between D_3 and S_3. If you really want to, you can write out the isomorphism explicitly, and this is what you'd get.

$$f(I) = 123 \quad f(R_1) = 231 \quad f(R_2) = 312 \quad f(M_A) = 132 \quad f(M_B) = 321 \quad f(M_C) = 213$$

When are Two Groups Different?

If you know what it means for two groups to be the same, then you must also know what it means for two groups to be different. To prove that two groups are the same — remember the technical term is isomorphic — you can just go ahead and find the isomorphism and check that it is indeed an isomorphism. On the other hand, how do you prove that two groups are different – in other words, that there exists no possible isomorphism? Well, there are various tricks, but here are two very simple ones.

Example. Two groups of different sizes cannot be isomorphic. This is simply because if two groups have different numbers of elements, then there cannot possibly exist a bijection — in other words, a one-to-one dictionary correspondence — between them. Therefore, we can say things like C_3 and C_4 are not isomorphic.

Example. Two groups cannot be isomorphic if one is abelian while the other is not. We say that a group G is *abelian* if for all g and h in G, it is true that $g \cdot h = h \cdot g$. So in an abelian group, it doesn't matter in which order you compose elements. In terms of the Cayley table, an abelian group is one where the entries are symmetric when you flip over the main diagonal.[3] Therefore, we can say things like D_4 and C_8 are not isomorphic, even though they have the same number of elements. This is because we know that D_4 is not abelian since the two Cayley table entries $M_h \circ M_{BD}$ and $M_{BD} \circ M_h$ aren't equal. On the other hand, you can see from the Cayley table for C_8 — which I've written below — that it's abelian.

$\circ$	I	R_1	R_2	R_3	R_4	R_5	R_6	R_7
I	I	R_1	R_2	R_3	R_4	R_5	R_6	R_7
R_1	R_1	R_2	R_3	R_4	R_5	R_6	R_7	I
R_2	R_2	R_3	R_4	R_5	R_6	R_7	I	R_1
R_3	R_3	R_4	R_5	R_6	R_7	I	R_1	R_2
R_4	R_4	R_5	R_6	R_7	I	R_1	R_2	R_3
R_5	R_5	R_6	R_7	I	R_1	R_2	R_3	R_4
R_6	R_6	R_7	I	R_1	R_2	R_3	R_4	R_5
R_7	R_7	I	R_1	R_2	R_3	R_4	R_5	R_6

Actually, it's useful to know that the cyclic group C_n is abelian for all $n \geq 1$. This is essentially because it consists of n rotations all with the same centre, and it doesn't matter in which order you compose such rotations. It's also useful to know that the dihedral group D_n is not abelian for $n \geq 3$, a fact that you can and should try to prove on your own.

Properties of Cayley Tables

From a group, we obtain a Cayley table and from a Cayley table, we obtain a group. So any property that applies to all Cayley tables is really a property that applies to all groups. Here are two important facts that apply to all Cayley tables and which we'll prove right now.

- *Sudoku property : In any row or column of a Cayley table, no element of the group appears twice.*
  If this were not true, then there might be a row labelled r in which there are two equal entries. So let's suppose that these two equal entries happen to be in the column labelled c_1 and the column labelled c_2. Of course, part of this setup is the assumption that the columns c_1 and c_2 are distinct. Now the fact that these two entries are equal implies the equation $r \circ c_1 = r \circ c_2$. We'll use the group axioms to deduce a contradiction from this equation in the following way.

$$\begin{aligned} r^{-1} \circ (r \circ c_1) &= r^{-1} \circ (r \circ c_2) \\ (r^{-1} \circ r) \circ c_1 &= (r^{-1} \circ r) \circ c_2 \\ e \circ c_1 &= e \circ c_2 \\ c_1 &= c_2 \end{aligned}$$

[3] The main diagonal is the one which runs from top left to bottom right.

To obtain the first line, we've used the inverse property to multiply both sides of the equation by the inverse of r on the left.[4] To get from the first line to the second, we've used the associative property. To get from the second line to the third, we've used the inverse property. And to get from the third line to the fourth, we've used the identity property. So we have proved that $c_1 = c_2$, which is in clear violation of the assumption that the columns c_1 and c_2 are distinct. This contradiction means that it's not possible for two entries of the same row to be equal in a Cayley table. And by an analogous argument, we also know that it's not possible for two entries of the same column to be equal in a Cayley table.

There are two important consequences of our proof. The first is that if G is a finite group, then every row and every column of the Cayley table of G must contain every element of G exactly once. The second is that you can always "cancel group elements from an equation".

- *Symmetric identity property : The entries of the Cayley table in which the identity appears are symmetric when you flip over the main diagonal.*
  Another way to say this is that if the identity e appears in row r and column c, then it also appears in row c and column r. So our goal is to show that the equation $r \circ c = e$ implies that $c \circ r = e$.

$$\begin{aligned} r^{-1} \circ (r \circ c) &= r^{-1} \circ e \\ (r^{-1} \circ r) \circ c &= r^{-1} \\ e \circ c &= r^{-1} \\ c &= r^{-1} \\ c \circ r &= r^{-1} \circ r \\ c \circ r &= e \end{aligned}$$

  To obtain the first line, we've used the inverse property to multiply both sides of the equation by the inverse of r on the left. To get the from the first line to the second, we've used the associative property. To get from the second line to the third, we've used the inverse property. To get from the third line to the fourth, we've used the identity property. To get from the fourth line to the fifth, we've multiplied both sides of the equation by r on the right. And to get from the fifth line to the sixth, we've used the inverse property. And this completes the proof of the symmetric identity property.

I've been really meticulous here and broken down these proofs into very basic steps, each one involving at most one of the group axioms. It's good for you to see all of the gory details of the proof now since these are our first real proofs in group theory. However, once you get the hang of working with groups, you can take a lot of shortcuts and not go into quite so much detail.

Finite Symmetry Groups

A while ago, we managed to define the symmetery group of a subset of the Euclidean plane. We used certain properties which these symmetry groups obey to broaden our definition of symmetry. The resulting object is a group, an abstract algebraic object which was constructed to behave a lot like a symmetry group. This just begs the question... which groups arise as symmetry groups of subsets of the Euclidean plane?

One phenomenon which occurs in group theory — the area of mathematics dealing with groups — is the fact that finite groups have certain qualitative differences to infinite groups. Of course, for infinite groups,

[4] It is very important here to say "on the left" because you would get a different answer if you multiplied both sides of the equation on the right. And you are definitely not allowed to multiply one side of the equation on the left and the other side of the equation on the right — you must do the same thing to both sides.

you'll find it pretty hard to write down the Cayley table, but there are various other fundamental differences between the two. So let's start with the following simpler question… which finite groups arise as symmetry groups of subsets of the Euclidean plane? This question was raised way back in the fifteenth century by Leonardo da Vinci who was interested in the notion of symmetry in art, particularly in architecture.

We already know that the cyclic group C_n and the dihedral group D_n are finite groups which arise as the symmetry group of a subset of the Euclidean plane. In fact, we know it because that's precisely how they were defined. The following result states that these are actually the only finite groups which arise as the symmetry group of a subset of the Euclidean plane.

Theorem (Leonardo's Theorem)**.** *If a subset of the Euclidean plane has finitely many symmetries, then its symmetry group must be the cyclic group C_n or the dihedral group D_n for some positive integer n.*

At this point, we should point out that our previous definition of cyclic and dihedral groups only really worked for $n \geq 3$. However, it's easy enough to define the cyclic and dihedral groups for $n = 1$ and $n = 2$ by writing down their Cayley tables. The Cayley tables of C_1 and C_2 are as follows. Note that C_1 is the symmetry group for the letter **R** while C_2 is the symmetry group for the letter **N**.

$\circ$	I
I	I

$\circ$	I	R
I	I	R
R	R	I

The Cayley tables of D_1 and D_2 are as follows. Note that D_1 is the symmetry group for the letter **M** while D_2 is the symmetry group for the letter **O**.

$\circ$	I	M
I	I	M
M	M	I

$\circ$	I	R_1	M_v	M_h
I	I	R_1	M_h	M_v
R_1	R_1	I	M_v	M_h
M_1	M_h	M_v	I	R_1
M_2	M_v	M_h	R_1	I

You can hopefully see from the Cayley tables for C_2 and D_1 that they're isomorphic. However, the groups C_{2n} and D_n — despite having the same number of elements — are certainly not isomorphic for any $n \geq 2$. For $n = 2$, you can prove this by nothing that every element of D_2 composed with itself gives the identity, a fact which doesn't hold for C_4. For $n \geq 3$, you can prove this using our earlier observation that C_{2n} is abelian while D_n is not.

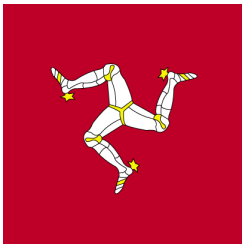
Dihedral and Cyclic Symmetry

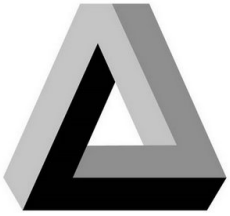
Since Leonardo's theorem claims that every subset of the Euclidean plane has either cyclic or dihedral symmetry, we should be able to find lots of examples of each and recognise the difference between the two types. Just keep in mind that the main difference between dihedral and cyclic symmetry is that the former includes reflective and rotational symmetries while the latter only includes rotational symmetries.

Example. As examples of dihedral symmetry, we have an apple, the logo for Mercedes–Benz and The Pentagon.[5]



Example. As examples of cyclic symmetry, we have the blades of a windmill, the Isle of Man flag, the periwinkle flower, the Penrose triangle and the logo for Sun Microsystems.[6]

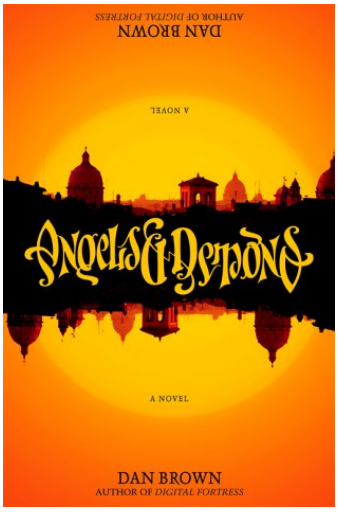


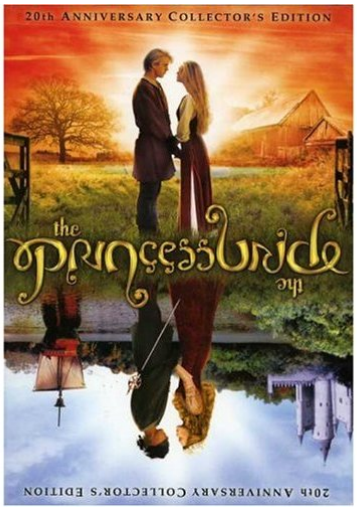

Example (Examples of ambigrams)**.** An ambigram is a design or artform that may be read as one or more words not only in its form as presented, but also from another viewpoint, direction or orientation. The following shows some interesting examples of ambigrams — you should easily be able to determine which ones have dihedral symmetry and which ones have cyclic symmetry.

[5] As with any real object, the symmetry is not quite exact — no apple is going to be perfectly circular and have five equally spaced seeds and The Pentagon doesn't have exactly the same rooms and furniture on all five sides. Also, if you look carefully, you'll see that the drawn logo for Mercedes–Benz does not really have dihedral symmetry — it's the three-dimensional object which the drawing represents which has dihedral symmetry.

[6] The Penrose triangle is an "impossible object" named after the well-known mathematical physicist Sir Roger Penrose. The logo for Sun Microsystems is one of my favourites.

Ambigrams have been recently popularised through Dan Brown's book Angels and Demons. They also appear on the front cover of the twentieth anniversary collector's edition of The Princess Bride.[7]





Facts about Finite Symmetry Groups

So how does one go about proving Leonardo's theorem? Well, you need a couple of useful little lemmas under your belt before you can start. In the following, when we say finite symmetry group, we are referring to the symmetry group of a subset of the Euclidean plane.

Lemma. *A finite symmetry group cannot contain a translation or a glide reflection.*

Proof. Of course, when we say translation here, we mean a translation which is not the identity. And when we say glide reflection, we mean a glide reflection which is not itself a reflection. That's because we already know that every group of isometries necessarily contains the identity and we've already seen examples of symmetry groups which contain reflections.

If a symmetry group contains the translation T, then the group must also contain $T \circ T$, $T \circ T \circ T$, $T \circ T \circ T \circ T$, and so on. These isometries cannot possibly be the same, because they are translations by different distances. Since these infinitely many isometries can't possibly fit into a finite group, a finite symmetry group cannot contain a translation.

If a symmetry group contains the glide reflection G, then the group must also contain the translation $T = G \circ G$. However, we've already deduced that translations cannot occur in a finite symmetry group, so nor can glide reflections. □

Lemma. *In any finite symmetry group, either every isometry is direct or there is an equal number of direct and opposite isometries.*

Proof. Let's call the direct isometries $R_1, R_2, \ldots, R_m$. If there is at least one opposite isometry, then let's call the opposite isometries $M_1, M_2, \ldots, M_n$. So our finite symmetry group has m direct isometries and n opposite isometries, and our goal is to prove that $m = n$.

[7] I've never read anything by Dan Brown, so I can't comment on this book, but I can say that The Princess Bride is an excellent film, at least in my opinion.

Suppose that M is any one of the opposite isometries. Then $M \circ R_1, M \circ R_2, \ldots, M \circ R_m$ are all opposite isometries since they are compositions of direct and opposite isometries. Furthermore, they must all be distinct by the sudoku property of groups. Therefore, $\{M \circ R_1, M \circ R_2, \ldots, M \circ R_m\}$ is a subset of $\{M_1, M_2, \ldots, M_n\}$ and this implies that $m \leq n$.

Again suppose that M is any one of the opposite isometries. Then $M \circ M_1, M \circ M_2, \ldots, M \circ M_m$ are all direct isometries since they are compositions of two opposite isometries. Furthermore, they must all be distinct because by the sudoku property of groups. Therefore, $\{M \circ M_1, M \circ M_2, \ldots, M \circ M_n\}$ is a subset of $\{R_1, R_2, \ldots, R_m\}$ and this implies that $n \leq m$.

The two inequalities $m \leq n$ and $n \leq m$ obviously lead to $m = n$, and we're done. □

Problems

Problem. *Show that any group with three elements must be isomorphic to C_3.*

Proof. Let's call the elements of the group e, a, b, where e is the identity element. Given that e is the identity, we can fill in most of the Cayley table, as shown below left. In fact, if we use the sudoku property, there is only one way in which we can complete the table, as shown below right.

$\cdot$	e	a	b
e	e	a	b
a	a	$*$	$*$
b	b	$*$	$*$

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

We can see that this group is isomorphic to C_3 via the isomorphism

$$f(e) = I \qquad f(a) = R_1 \qquad f(b) = R_2,$$

where I is the identity isometry, R_1 is rotation by 120° and R_2 is rotation by 240°. □

Problem. *The following is a* groupoku *puzzle — a Cayley table for the group G, where some of the entries are missing. Use the properties which you know about Cayley tables to fill in all of the missing entries. Give full reasoning only for the first entry of the table that you manage to fill in.*

$\cdot$	a	b	c	d	e	f
a	e	d	f	$*$	$*$	$*$
b	d	f	e	$*$	$*$	$*$
c	$*$	$*$	$*$	$*$	$*$	b
d	b	$*$	$*$	$*$	$*$	$*$
e	$*$	$*$	$*$	$*$	e	$*$
f	c	a	b	$*$	$*$	$*$

In the lectures, we have seen two groups with six elements — the cyclic group C_6 and the dihedral group D_3. Prove that G is isomorphic to one of these groups by writing down an explicit isomorphism. Prove that the cyclic group C_6 and the dihedral group D_3 are not isomorphic to each other.

Proof.

The first thing to notice from the Cayley table is that a cannot be the identity since $a \cdot a \neq a$. Similarly, b, c, d and f cannot be the identity since $b \cdot a \neq a$, $c \cdot f \neq f$, $d \cdot a \neq a$ and $f \cdot a \neq a$. But every group has to have an identity so in this case, it must be e. This allows us to fill in all of the entries of the Cayley table in the row and column labelled by e.

$\cdot$	a	b	c	d	e	f
a	e	d	f	$*$	a	$*$
b	d	f	e	$*$	b	$*$
c	$*$	$*$	$*$	$*$	c	b
d	b	$*$	$*$	$*$	d	$*$
e	a	b	c	d	e	f
f	c	a	b	$*$	f	$*$

Now we use the sudoku property to fill out the rest of the table. As an example, consider the $c \cdot b$ entry. Since it's in the same row as entries equal to b and c and in the same column as entries equal to a, b, d and f, the only possibility left is that $c \cdot b = e$. Using this strategy, we can fill in all of the missing entries to give the complete table.

$\cdot$	a	b	c	d	e	f
a	e	d	f	b	a	c
b	d	f	e	c	b	a
c	f	e	d	a	c	b
d	b	c	a	f	d	e
e	a	b	c	d	e	f
f	c	a	b	e	f	d

The group G is isomorphic to C_6, which is the symmetry group formed by the rotational isometries of a regular hexagon. If we write the elements of C_6 as follows, then its Cayley table will look like the one below.

- I : the identity isometry
- R_1 : rotation by 60° counterclockwise
- R_2 : rotation by 120° counterclockwise
- R_3 : rotation by 180° counterclockwise
- R_4 : rotation by 240° counterclockwise
- R_5 : rotation by 300° counterclockwise

$\cdot$	I	R_1	R_2	R_3	R_4	R_5
I	I	R_1	R_2	R_3	R_4	R_5
R_1	R_1	R_2	R_3	R_4	R_5	I
R_2	R_2	R_3	R_4	R_5	I	R_1
R_3	R_3	R_4	R_5	I	R_1	R_2
R_4	R_4	R_5	I	R_1	R_2	R_3
R_5	R_5	I	R_1	R_2	R_3	R_4

An explicit isomorphism $F : G \to C_6$ is given by the equations

$$F(a) = R_3 \qquad F(b) = R_1 \qquad F(c) = R_5 \qquad F(d) = R_4 \qquad F(e) = I \qquad F(f) = R_2.$$

This is certainly not the only isomorphism possible. To find one, you can use the fact that the identity in G must map to the identity in D_2. After this, the problem can be finished with a little trial and error.

Note that C_6 is an abelian group and, in fact, so are all cyclic groups. On the other hand, D_3 is not abelian, so C_6 cannot be isomorphic to D_3. □

Problem. *Prove that a group G can only have one identity. In other words, prove that there is only one $e \in G$ such that $e \circ g = g \circ e = g$ for all $g \in G$.*

Proof. This proof is so short that it can be hard to find. The idea is to argue by contradiction — so suppose that there is a group with two elements which could be the identity and call them e and f. What we'll do now is show that they must actually be the same element. Since e is an identity, it follows that $e \circ f = f$ and since f is an identity, it follows that $e \circ f = e$. And there's the proof, since this means that $e = f$. □

Cayley

Arthur Cayley, between his birth in 1821 and his death in 1895, was a British mathematician who also worked as a lawyer. As a child, Cayley enjoyed solving math problems for amusement and when he entered Trinity College, Cambridge, he excelled in Greek, French, German, and Italian, as well as mathematics.

Cayley only became a lawyer because he had a pretty limited fellowship, but this didn't seem to slow his mathematics down. Another well-known British mathematician by the name of James Joseph Sylvester, was in a similar position to Cayley and became an actuary in London. The two would walk together around the courts, discussing mathematics. It was during this fourteen-year span of his life that Cayley produced over two hundred mathematical papers. At the age of 42, Cayley was offered a prestigious professorship at Cambridge. He never regretted giving up his lucrative practice for a modest salary because it enabled him to end the divided allegiance between law and mathematics, and to devote his energies to the pursuit which he liked best.

If you've studied some linear algebra, then you may already have come across a result of Cayley's known as the Cayley–Hamilton theorem. He was very interested in symmetries, which is why the multiplication tables for groups are usually known as *Cayley tables*.