Snapshots of modern mathematics
from Oberwolfach

№ 3/2018

Computing with symmetries

Colva M. Roney-Dougal

Group theory is the study of symmetry, and has many applications both within and outside mathematics. In this snapshot, we give a brief introduction to symmetries, and how to compute with them.

1 Symmetries and groups

A *symmetry* of a mathematical object is a way of moving that object so that after it has been moved it looks the same as it did before. Technically speaking, we say that an object moved using a symmetry *remains invariant* under this action. For example, as shown in Figure 1, if our object is a square, we can rotate it by a quarter twist clockwise (90°), a half twist (180°) or a quarter twist anti-clockwise (−90°), and the resulting picture will look the same.

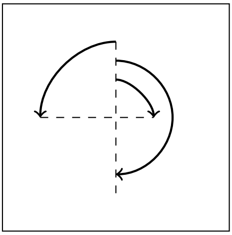

Figure 1: Rotations of a square.

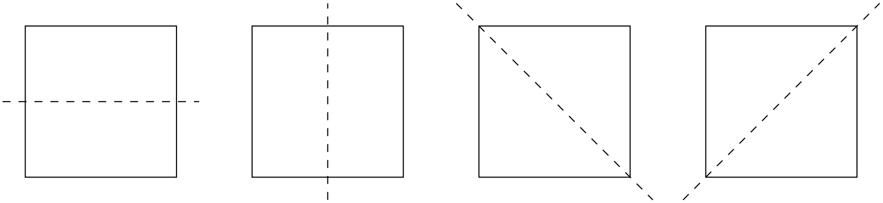

Figure 2: Reflections of a square.

Furthermore, as in Figure 2, we can also reflect the square about a horizontal or vertical line through its middle, or about the diagonal lines through its corners, and it will again still look the same.

There is one symmetry that all objects have, which is to do nothing at all: this is called the *identity*. Thus in total we have found 8 symmetries of the square. We'll see later a way to convince ourselves that this is all of them.

For geometric objects it is quite easy to picture symmetries. However, much more abstract mathematical objects can be thought of as being symmetrical. For instance, as we will see again in the next section, the solutions of polynomial equations can be thought of in terms of symmetry. In physics, a whole system can be symmetric: there is a powerful theorem due to the mathematician Emmy Noether (1882–1935) which states that each symmetry of a physical system corresponds to a particular quantity being conserved. For instance, rotational symmetry corresponds to conservation of angular momentum whereas symmetry in time corresponds to conservation of energy.

Mathematically speaking, it is often more important to see the similarities between apparently different objects and operations than it is to concentrate on their differences. To this end, we introduce the idea of a *group*. In general, a group is a set with an operation defined on it, which we will call *multiplication*, which must satisfy the three properties listed below. (There is one further technical condition, which we'll discuss at the end of this section.)

(G1) The product of any two elements in the group is again a member of the group.

(G2) The set must contain an element which doesn't change anything under multiplication. This element is called the *identity* element.

(G3) Given any element, there is another element that multiplies with it to give the identity. This element is called the *inverse* of the first one.

Now let us consider some examples. One group that you have definitely met already is the set of all nonzero numbers under (ordinary) multiplication: the identity is 1, and the inverse of a number x is $1/x$. Another is the set of all whole numbers (positive, negative and 0) under addition: the identity is 0, and the inverse of a whole number n is $-n$.

It is not too difficult to see that the set of symmetries of an object, with the multiplication operation defined to be applying first one symmetry operation and then another, is a group. We will illustrate the proof using our square example from above. The identity element is the identity symmetry as defined above (the "do nothing" symmetry). The inverse of rotating by 90° clockwise is rotating by 90° anticlockwise. Also, if we do any reflection and then the same one again, we are back where we started. The same holds for rotating by 180° twice, it is equivalent to doing nothing. This shows that conditions (G2) and (G3) are met; it remains to check property (G1). This means we have to check that the composition of any two of our symmetries is again a symmetry, and it will be easier to investigate if we label the corners of the square, as shown in Figure 3.

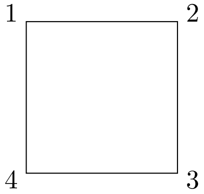

Figure 3: A labelled square.

For example, if we rotate by 180° and then reflect about the vertical line through the centre of the square, we see that this is equivalent to reflecting about the horizontal axis. Similarly, if we first rotate anticlockwise by 90° and then reflect in the diagonal line through the upper left and lower right corners (which will, after the rotation, be labelled 2 and 4, respectively), the outcome is the same as reflecting about the vertical axis. It turns out, and you can check this for yourself, that every such combination of first rotating and then reflecting, or vice versa, is equivalent to another reflection. With the labelled corners we can also easily check that doing two different reflections, one after the other, gives the same result as a rotation. One rotation and then another is equivalent to another rotation. Thus, we have verified also property (G1).

Let us remark here that there is one further technical condition that must be satisfied for a set with multiplication to be a group, called *associativity*, which basically says that it doesn't matter the order in which we do the multiplication. More precisely, we must have that $(a \times b) \times c = a \times (b \times c)$ for every three group elements. Notice that whilst whole numbers with addition, as mentioned above, is a group, the set of whole numbers with subtraction is not, because the associativity condition is not satisfied. For example, $(3-2)-4 \neq 3-(2-4)$. Symmetries, however, always satisfy the associative property.

2 The birth of group theory

The study of group theory goes back to the work of Évariste Galois (1811–1832) in the early 1800s. Galois was interested in the problem of finding the roots of polynomials. At school you may have learnt that you can solve a quadratic equation like

$$ax^2 + bx + c = 0$$

using the *quadratic formula*

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

Galois was interested in finding conditions under which there exist formulae like these to solve more complicated polynomials, such as $x^5 - 8x + 2 = 0$. By "formulae like these", we mean that the solutions must be made by taking the coefficients (the a, b and c in our quadratic equation), and using only addition, subtraction, multiplication, division, and taking roots. A key step is to understand the symmetries of the solutions, for instance, in the quadratic case the two solutions are symmetric about $x = -b/2a$. As Galois thought about these, group theory was born. Galois himself explained the essence of this new idea beautifully, when he said[1]:

> *Go to the roots, of these calculations! Group the operations. Classify them according to their complexities rather than their appearances! This, I believe, is the mission of future mathematicians. This is the road on which I am embarking in this work.*

Galois realised something which we now understand much more precisely, namely, that any finite group can be broken down into groups called *simple groups*, which are themselves indivisible. The simple groups are a little bit like the prime numbers: numbers that are only divisible by 1 and themselves, such as $2, 3, 5, 7, 11, \ldots$, and the breaking of groups down into simple groups works similarly to the way we can factorise any positive whole number into prime numbers, like $12 = 2 \times 2 \times 3$. Galois identified several families of finite simple

[1] According to http://www-history.mcs.st-and.ac.uk/Quotations/Galois.html, this quote is to be found in the preface to his final manuscript.

groups, and hence was able to give a precise condition for when polynomials can be solved in terms of addition, subtraction, multiplication, division and taking roots. Using his techniques one can show that the equation $x^5 - 8x + 2 = 0$ has no such solution.

Tragically, after a turbulent life lived in the aftermath of the French revolution, Galois died in a duel at the age of 20. We can only imagine what further mathematics he might have developed had he lived longer.

3 Finite groups of permutations

When thinking of the symmetries of a finite object, we often don't want to describe them geometrically. Instead, we generally label the object in some suitable way and write the symmetries down as *permutations*: maps from the labels to the labels, such that no two labels get sent to the same one (we are not allowed to collapse our object!). Applying one symmetry and then another is the same thing as first applying one permutation to the labels, and then applying the second to the result.

As an example, we can label the four corners of our square, as in Figure 3. Whereas before we used these labels to clarify the geometric action of combining symmetries, we now want to describe the symmetries just using the numbers $1, 2, 3, 4$. Here are two examples (the symbol $\mapsto$ means "is sent to"):

Symmetry	Map
Rotate clockwise by 90°	$1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 4$, $4 \mapsto 1$
Reflect in horizontal line	$1 \mapsto 4$, $2 \mapsto 3$, $3 \mapsto 2$, $4 \mapsto 1$

Try to work out the permutations for the other six symmetries that we found. We will call the resulting group of eight permutations G.

The English mathematician Arthur Cayley (1821–1895) was the first person to describe groups via the rules (G1), (G2) and (G3), plus associativity, that I gave in Section 1. He also showed in 1854 that every group, no matter how abstractly we have created it, can be written down as a group of permutations. Conversely, any collection of permutations forms a group, provided that it satisfies rules (G1), (G2) and (G3).

4 Computational group theory

The fact that computers might also be useful when working with groups was observed as soon as the concept of a programmable computer was invented: Alan Turing (1912–1954) in 1945 wrote

> *There will positively be no internal alteration [of the computer] to be made even if we wish suddenly to switch from calculating the energy levels of the neon atom to the enumeration of groups of order 720.*

Here, the *order* of a group is the number of elements in it: using modern computational methods it is now straightforward to calculate that there are 840 different groups with 720 elements.

There are many different ways to work with groups on computers, including ways to work with infinite groups. However, in this snapshot we will concentrate on groups of permutations. The main issue that needs to be addressed is that if we are using a computer to do calculations in a group, it's probably because the group is very big: even on my laptop, I have worked with a finite simple group containing 1 255 205 709 190 661 721 292 800 symmetries! To work with these sizes of groups means that we can't possibly store all of the permutations in them, as that would take far too much memory. So, we need to find a way to store a subset of the permutations with which we will calculate that contains enough information to "recover" the entire group.

The American mathematician Charles Sims developed many of the key methods for computing with permutation groups, and in this section we'll see some ideas behind just two of them: how to work out the order of a group, and how to tell if a given permutation belongs to a group.

Some elements of a group are called *generators* for the group if all of the other permutations can be made by multiplying these given elements together. Going back to our group G of symmetries of the square, one pair of generators is:

$$f := 1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 4, 4 \mapsto 1, \text{ and } g := 1 \mapsto 4, 2 \mapsto 3, 3 \mapsto 2, 4 \mapsto 1.$$

The first one of these generators, the one we have called f, corresponds to rotating clockwise by 90° and the second, called g, to reflecting about the horizontal line through the middle of the square. To see that f and g are enough to make all eight elements of G, notice that by repeating f up to four times we get the four rotations (including the identity), and by first repeating f up to four times, and then using g we can make the four reflections.

This means we only need to store two elements of G rather than all eight. Throwing away six permutations obviously saves some memory, but now raises two questions: How do I test if a particular map belongs to our group G? And how do I now tell how big G is?

To answer these questions, we need to introduce another two notions. An *orbit* of a point is the set of all of the points that the group can map it to. For our group G, the orbit of the point 1 is the set $\{1, 2, 3, 4\}$, as we can use f repeatedly to move 1 to each of the other four points. The *stabiliser* of a point is the set of all permutations in the group that fix that point. It turns out that a point stabiliser is also a group in its own right: see if you can see why it satisfies rules (G1), (G2) and (G3). For an example from G, let us see what happens when we stabilise the point 1. If we do this, then we must also fix the opposite corner (point 3) and so the only remaining way that we can move the square is to reflect in the diagonal line through 1 and 3, which means that we are swapping the points 2 and 4. Lets call this map h. So the stabiliser in G of the point 1 contains just two permutations: the map h, and the identity.

Sims invented computational methods to construct generators for the stabiliser of any given point in a group from the original set of generators of the group. He also invented a particularly useful generating set for any group, called a strong generating set, which we will shortly explain. Suppose that a permutation group can send, for instance, the point 1 to every other point, just as our group G can send 1 to the points 2, 3 and 4. Then a strong generating set for the group consists of elements that can be applied to map 1 to each other point, together with generators for the stabiliser of the point 1. In our case, the permutation f on its own will do for the first part, because applying f up to four times sends 1 everywhere. Denoting by G_1 the stabiliser of 1, we have already seen that G_1 consists of only two permutations, namely, h and the identity. So, for our example we can stop there, as the set $\{f, h\}$ forms a strong generating set. Notice that we never need to include the identity in the set of generators, as it is included, as it were, “for free”.

Here our stabiliser G_1 was very small, but in general we may need to repeat this process several times. We would apply the same idea to G_1. That is, we pick some point, say 2, that is moved around by G_1, find elements of G_1 that map 2 to each of its images, and then find generators for the stabiliser $G_{1,2}$ of the point 2 in G_1. We can continue in this way until we reduce our stabiliser to containing only the identity.

Now, to test if a given permutation belongs to a group, the idea is to reduce this original problem to the following “smaller” problem. We construct a new map and ask if it belongs to the stabiliser of the point 1, which as we have seen is a smaller group inside our original group. We do this using the strong generating set that we introduced above. Let us illustrate this using an example. Consider the map p which swaps 1 and 2, and swaps 3 and 4. Since f sends 1 to 2, the inverse permutation of f, which we will denote by f^{-1}, sends 2 to 1 (since, by definition, it undoes f). Hence the map we get by doing first p and then f^{-1} sends 1 to 1, that is, it belongs to the stabiliser of the point 1. Since groups satisfy property (G1), that is, the product of any two elements is again in the group, we have that p is in G if and only if pf^{-1} is in G. We have already seen that if pf^{-1} is in G, it must in fact be in the stabiliser of 1. Our computer can easily calculate that pf^{-1} fixes 1, fixes 3 and swaps 2 and

4, which means that pf^{-1} is the map h that we've seen before. In particular, pf^{-1} belongs to G and so p belongs to G.

Try instead doing this process with the map that swaps 1 and 2, and fixes 3 and 4. Call this permutation q. Since it sends 1 to 2, the first step will be the same: you'll want to fix it again by using the map f^{-1}. But is the product qf^{-1} in the stabiliser G_1?

At the beginning of this snapshot I mentioned that we would see a way of convincing ourselves that we had indeed found all of the symmetries of the square. To do so, we use a beautiful theorem called the orbit-stabiliser theorem[2]. It says that the order of a group is equal to the product of the length of any orbit and the order of the stabiliser of a point in that orbit, where we recall that the order of a group is how many elements it contains. So for our example of a square we get that the total number of symmetries is equal to the length of the orbit of 1 (which is four) times the number of symmetries fixing 1 (there are two). That is, the order of the group is 8, which gives a way of seeing that we have found all of the symmetries of the square. So in general, once we have calculated orbits and stabilisers, we can use this information to also answer our second question.

5 Applications of computational group theory

The biggest proof of all time was a result in group theory proved over the course of the twentieth century: the complete classification of all of the finite simple groups. Like the prime numbers, there are infinitely many of them, but it turns out that they fall into three infinite families, plus twenty-six additional groups that don't belong to these families, called the *sporadic* simple groups. The proof of the classification was the collaborative work of many hundreds of authors, and the proof is more than ten thousand pages long.

The first sporadic groups we discovered by the French mathematician Émile Mathieu in 1860, although of course at this point he didn't know that they would turn out to be sporadic examples. After this, no new sporadic groups were discovered for around a hundred years, until in 1966 the Croatian mathematician Zvonimir Janko discovered a new finite simple group, of order 175 560. In the years after this a flurry of new sporadic groups were discovered, but often there was initially merely a prediction that a certain group should exist: a mathematician would prove that it was possible that there was a new finite simple group of a certain order, and with certain properties, but not know for sure that it exists. For example, Richard Lyons in 1972 [3] established that

[2] To read more about the orbit-stabiliser theorem, see for instance, https://en.wikipedia.org/wiki/Group_action#Orbit-stabilizer_theorem_and_Burnside%27s_lemma.

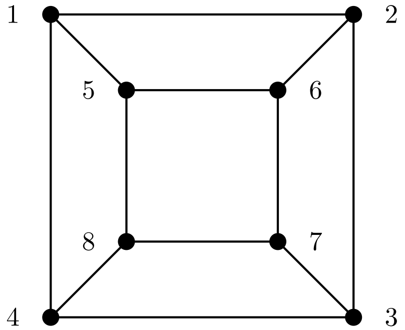

Figure 4: Graph A.

there could exist a new simple group of order 51 765 179 004 000 000, and listed various smaller groups that should be contained in it. However, somebody needed to construct Lyons' group to demonstrate that it did in fact exist, and it was far from clear that it could be done. The mathematician Charles Sims, whom we first encountered in the previous section, managed to construct it as a group of permutations on 8 835 156 points [4], and hence to prove its existence.

Let's finish this snapshot with an application outside of group theory, to an area of mathematics called *graph theory*. A *graph* is a set of vertices (which we draw as dots, sometimes with labels next to them) and a set of pairs of vertices called *edges*. We draw the edges by putting a line between the corresponding vertices.

Figure 4 shows a graph we'll call A. The vertices of A are $1, 2, 3, 4, 5, 6, 7, 8$, and the edges are $\{1, 2\}, \{1, 4\}, \{1, 5\}, \{2, 3\}, \ldots, \{7, 8\}$.

Graphs are used to represent relationships between pairs of objects: for example, we might be interested in how information spreads around a social media network, and to study it we can construct a graph with a vertex for each user of the network, and an edge between two users if they use the network to communicate. In general, graphs are among the most widespread models used to investigate both natural and man-made structures. Besides social science and networks applications, they are useful in various areas of applied mathematics, and in computer science, biology, and physics.

As you can see from the social network example, it really doesn't matter how we have drawn the graph, what is important is which pairs of vertices are connected by edges. The *graph isomorphism problem* asks whether one graph is the same as another graph, just with the names of the vertices changed. For example, we might ask whether it's possible to relabel the vertices of A, and

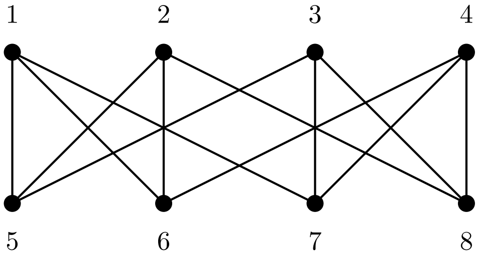

Figure 5: Graph B.

then move around the relabeled vertices (with the edges moving alongside) such that the resulting graph looks like B in Figure 5. To answer this question, we need to find a permutation of the numbers $1, 2, 3, \ldots, 8$ that maps the edges of graph A to the edges of graph B. One way to imagine doing this is to imagine erasing all of the labels of graph A, and seeing if we can relabel it with the numbers $1, 2, \ldots, 8$ so that there are edges between the same numbered vertices as there are in B.

It is natural to think that the symmetries of graphs A and B have a big effect on how we might find a solution, and hence it should be no surprise that group theory comes into play here. Looking at graph A, we can see it has all of the symmetries of the square, and so vertices $1, 2, 3, 4$ are all in the same orbit. Furthermore, there is a symmetry which swaps 1 with 5, 2 with 6, 3 with 7 and 4 with 8 (you can maybe imagine "picking up" the inner square, and moving it outside the outer square – the graph would look the same). So this means that all eight vertices are in the same orbit.

Turning back to the question of whether graphs A and B are the same, the fact that the vertices of graph A are all in the same orbit means that it doesn't matter which vertex of graph A maps to vertex 1 of graph B: so we might as well leave the label 1 of A unchanged. In graph A, vertex 1 had edges to $2, 4$ and 5, whilst in graph B, vertex 1 has edges to $5, 6$ and 7. So we can try replacing label 2 of graph A with a 6. See if you can replace all of the remaining labels of graph A to give the edges of B. This puzzle is not obvious, but it is possible to do!

In the early 1980s, Eugene M. Luks [2] was able to give a fast algorithm (a *polynomial time algorithm*) that quickly solves the graph isomorphism problem for a great many graphs. The only obstruction was a certain (infinite) class of very highly symmetric graphs. In a recent breakthrough, László Babai [1] has given a *quasipolynomial time* algorithm to solve the graph isomorphism problem for all graphs: a quasipolynomial time algorithm is not quite as fast as a polynomial time one, but is still dramatically faster than was known before. Interestingly, both Luks' and Babai's approaches relied on incredibly detailed information about the finite simple groups.

Image credits

All images created by the author.

References

[1] L. Babai, *Graph isomorphism in quasipolynomial time*, arXiv:1512.03547v2, 2016.

[2] E. M. Luks, *Permutation groups and polynomial-time computation*, Groups and Computation, American Mathematical Society, 1993.

[3] R. Lyons, *Evidence for a new finite simple group*, J. Algebra **20** (1972), 540–569.

[4] C. C. Sims, *The existence and uniqueness of Lyons' group*, Finite Groups '72, North Holland, 1973.

Colva Roney-Dougal *is a Reader in pure mathematics at the University of St Andrews.*

Mathematical subjects
Algebra and Number Theory, Discrete Mathematics and Foundations

Connections to other fields
Computer Science

DOI
10.14760/SNAP-2018-003-EN

Snapshots of modern mathematics from Oberwolfach provide exciting insights into current mathematical research. They are written by participants in the scientific program of the Mathematisches Forschungsinstitut Oberwolfach (MFO). The snapshot project is designed to promote the understanding and appreciation of modern mathematics and mathematical research in the interested public worldwide. All snapshots are published in cooperation with the IMAGINARY platform and can be found on www.imaginary.org/snapshots and on www.mfo.de/snapshots.

Junior Editor
Sara Munday
junior-editors@mfo.de

Senior Editor
Carla Cederbaum
senior-editor@mfo.de

Mathematisches Forschungsinstitut
Oberwolfach gGmbH
Schwarzwaldstr. 9 –11
77709 Oberwolfach
Germany

Director
Gerhard Huisken

Mathematisches
Forschungsinstitut
Oberwolfach

Member of
Leibniz
Leibniz
Association

IMAGINARY
open mathematics