What is a group?

One concept that underpins group theory is that of a set. For us, a set is nothing more complicated than a collection of objects. For instance, this is a set containing three words:

$$\{\text{apple}, \text{banana}, \text{cherry}\}\,.$$

There are infinite sets (like the set of all whole numbers) and finite sets (like the set of symmetries of a mattress).

A second concept that we need is that of a binary operation. This is a way of combining two objects to get a third. Addition and multiplication are both examples of binary operations (note that the third object you get from combining does not always have to be a new one, for example $2 + 0 = 2$). Combining symmetries of a shape by doing one symmetry after the other is also a binary operation: you put two symmetries in and get a third one out.

You're now ready for the formal definition of a group: a group is a set, along with a binary operation that can be applied to any pair of elements in the set (including any element and itself). When we work in the abstract, so that we have no particular name or symbol to give to the operation, we simply call it "multiplication" and use the symbol $\times$. The elements do not have to be numbers or symmetries, so the binary operation does not have to be addition or doing one symmetry after another. However, we are not allowed to make up the way in which the operation works in any way we like, it has to obey four rules called axioms:

Axiom 1: The product of any two elements from the set is another element of the set. That is, if a and b are elements of a group G, then $a \times b$ is an element of G too.

Axiom 2: There is a special element called the identity in the set. We often write e for the identity. It is the analogue of the number zero in addition or the number one in multiplication: if a is any element of a group G, then $e \times a = a \times e = a$. In our square example, the identity symmetry is simply doing nothing and leaving the square exactly as it is.

Axiom 3: The binary operation must be what is called associative. This means that it doesn't matter how we put brackets when we multiply:

$$((a \times b) \times c) \;=\; (a \times (b \times c)).$$

Addition and multiplication of numbers are both associative, but subtraction is not:

$$((1-2)-3) \;=\; -1-3 \;=\; -4,$$

but

$$(1-(2-3)) \;=\; 1-(-1) \;=\; 1+1 \;=\; 2.$$

Thus we can't use subtraction as our binary operation to define a group.

Axiom 4: Our final rule requires that if a is any element of the group, then there exists a unique group element called the inverse of a, often written a^{-1}, with the property that

$$a \times a^{-1} \;=\; a^{-1} \times a \;=\; e,$$

where e is the identity element from axiom 2.

1. Check that the set of all integers $\{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$ with the addition operation form a group. (Hint: re-express axioms 1–4 in terms of addition. What plays the role of 0? What are inverses?) Explain why this fails if you leave out the negative integers.

2. Convince yourself that if you take all the symmetries of an object (e.g. a the four symmetries of a mattress we looked at last week....), then you get a group. What is the binary operation here?

3. Last week we met the Klein-4 group which has four elements (we referred to them as four *symmetries*), which today we'll call e, f, g and h. We found that its multiplication table is:

	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	h	e	f
h	h	g	f	e

   By consulting this multiplication table, check axioms 1, 2, 4 for the Klein-4 group. Could you, in principle, check axiom 3 also?

   (Many of you noticed last time that the Klein 4-group has a special extra property, 'commutativity' that says that $a \times b = b \times a$ for any elements a and b of the group.)

Acknowledgement. This worksheet is based on a +plus magazine blog posts by Colva Roney-Dougal.