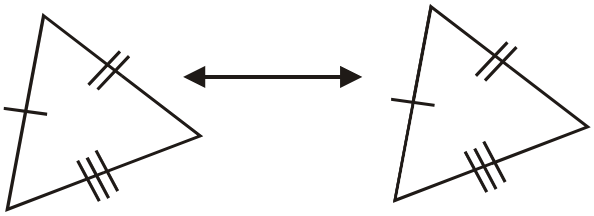
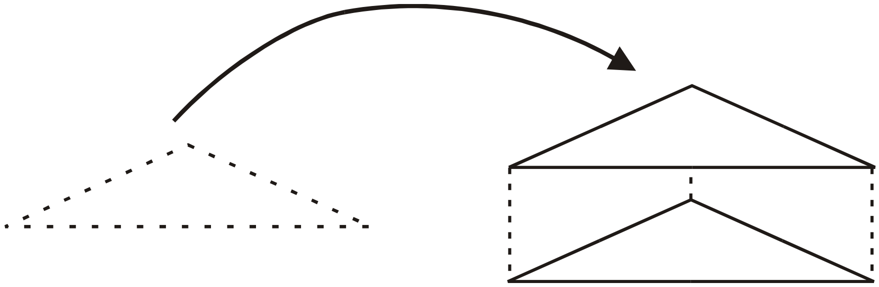
Group structure

Mathematical structure is the idea that different mathematical objects can share common features. A simple example of mathematical structure is the idea of congruency.



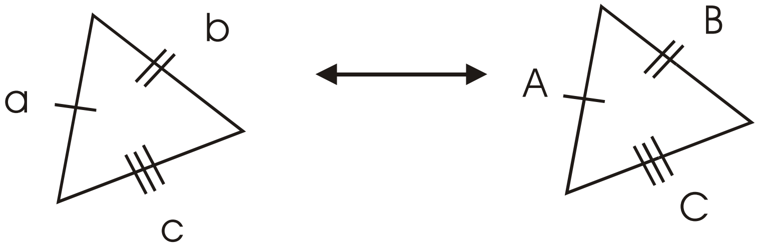
Two triangles are congruent if it is possible to take one triangle, pick it up, and fit it exactly over the other.



What this diagram illustrates is that the study of structure – which is the study of what is similar between different objects – requires

1. A description of the different objects
2. A description of the process by which one object is compared to another

In order to describe the two congruent triangles we could label their sides; congruency establishes a correspondence between these sides.



The correspondence is a mapping

© blacksacademy.net

$$\begin{tikzcd}
a \arrow[r, leftrightarrow] & A \\
b \arrow[r, leftrightarrow] & B \\
c \arrow[r, leftrightarrow] & C
\end{tikzcd}$$

There are an enormous number of different structures studied in mathematics. The idea of congruency is concerned with the similarities that exist between spatial structures.

Algebra is generally concerned with the similarity of structures of objects that can be placed into sets. Sets are collections of objects. Numbers, for example can be collected into sets. However numbers are not the only mathematical objects that can be collected into sets. There are an extraordinary number of objects that may be collected. Geometrical processes, such as rotating and reflecting objects, can be collected into sets. Sets can also be finite or infinite in size.

Set theory is the study of the similarity of structures that exist between objects merely because they are sets

Further mathematical structure arises when two elements of a set are combined in some way. Addition and multiplication of numbers are examples of operations on elements of a set . Because they take tow elements and combine them to form a third they are called binary operations.

For example:-

$2 + 3 = 5$

is the binary operation

$(2, 3) \to 5$

Similarly , $2 \times 3 = 6$

is the binary operation

$(2, 3) \to 6$

In general, a binary operation is a function (mapping) from two elements to a third element.

Thus new structures arise when we specify

(1) A set if elements
(2) A binary operation defined no all elements of that set.

However it will emerge that these requirement are not sufficient to define a structure meaningfully. Other conditions will need to be added. But firstly let us illustrate the idea of similarity of structure with the simplest structure of them all.

Multiplication of positive and negative numbers.

Set = The set made of the set of all positive numbers and the set of all negative numbers

Operation = multiplication

×	+	-
+	+	-
-	-	+

Multiplication of +1 and –1

Set = $\{+1,-1\}$
Operation = multiplication

×	+1	- 1
+1	+1	- 1
- 1	- 1	+1

Consider a sheet of paper and two processes of (1) touching a sheet of paper –doing nothing to it; (2) turning the sheet over. We will label these two processes TOUCH and FLIP. The binary operation, O, will be the operation of doing one of these processes followed by the other. There are four possible combinations.

TOUCH and TOUCH	=	TOUCH
TOUCH and FLIP	=	FLIP
FLIP and TOUCH	=	FLIP
FLIP and FLIP	=	TOUCH

The structure is represented by a table thus:

Set = $\{$touch, flip$\}$
Operation = Do one after the other

$\circ$	touch	flip
touch	touch	flip
flip	flip	touch

Intuitively, all the structures are identical as structures and differ only in the application of that structure to different sets.

If we could discover what was common to a structure we would be then be able to use the results in any situation which possessed that structure. Mathematicians study structure because if they can solve a problem for a structure in general then the result will hold for all applications of that structure.

Whilst our three structures:

$\times$	+	-
+	+	-
-	-	+

$\Leftrightarrow$

$\times$	+1	- 1
+1	+1	- 1
- 1	- 1	+1

$\Leftrightarrow$

$\circ$	touch	flip
touch	touch	flip
flip	flip	touch

Are intuitively different applications of the same structure, we have not proven this yet. But before we discuss what is required to prove the equivalence of such structures we must continue our discussion of the structures themselves.

Recall that our study of structure begins with the specification for a given structure of

(1) A set of elements, G
(2) A binary operation defined on elements of that set, O

The symbol (G,O) will specify such a structure. G stands for the set - Other symbols such as H,J,K could be used. O stands for the operation – Other symbols such as □ , ×, + could be used.

(1) Identity

In order for the structure (G,O) to be a group the set G must possess an element e that is the identity under operation O.

Consider, for example, multiplication of –1 and +1. The identity is the +1 since

$$+1\times+1=+1$$
$$-1\times+1=-1$$

Operating with the identity leaves the element unchanged. Formally,

Let G be a set and $\circ$ an operation on elements of that set. Then *e* is the identity element for that set under $\circ$ for all elements *a* in G. Thus,

$$e\circ a=a$$
$$a\circ e=a$$

Note that for the set of all natural numbers under the operation of multiplcationthe identity is the number 1. For the set of all natural numbers under the operation of addition , the identity is the number 0 (zero). This illustrates that the identity element of a group depends upon the operation defined upon it. The same set can have different identities when different operations are defined upon it.

(2) Inverses

In order for the structure (G,O) to be a group for every element a in G there must be another element a^{-1} inG that is the inverse of a.

If a^{-1} is the inverse of a, then a is the inverse of a^{-1} .Inverses go in pairs.

Two elements are inverses of eachother if, when combined together, the result is the identity element,

$$a\circ a^{-1}=e$$
$$a^{-1}\circ a=e$$

or just

$$aa^{-1} = e$$
$$a^{-1}a = e$$

Where *e* is the identity element.

The identity element is always its own inverse. For the multiplication of +!, -1 the inverse of –1 is also itself, since

-1 × -1 = +1

For the set of all integers , ℤ, under addition the inverse of any number a is the integer –a , since

$$a + (-a) = 0$$

and O is the identity for the set of all integers under addition. For example the inverse of 2 is –2.

Note that the set of natural numbers, ℕ does not contain its own inverses. The set ℕ comprises all positive integers.

ℕ = {0, 1, 2, 3,-----}

so, for example, -2 is not in ℕ. Thus ℕ is not in a group. In order to make ℕ into a group under addition we must extend it to the set ℤ- the set of all positive and negative integers.

But whilst ℤ is a group under addition, (as shall be fully shown), ℤ is not a group under multiplication. This is because, for example, the inverse of 2 under multiplication is $^1/_2$, since

$$2 \times {}^1\!/_2 = 1$$

and 1 is the identity under multiplication, and $^1/_2$ is not an element of ℤ.

Hence in order to make ℤ into a group under multiplication we must extend it to the set Q = the set of all rational numbers. Then Q is a group under multiplication, as shall be shown.

This illustrates that the same set, ℤ, can be a group under one operation (addition) but not a group, under another (multiplication).

(3) Closure

In order for a structure $(G,\circ)$ to be a group, then for every pair of elements, *a,b* in *G*, the object that arises from the binary combination of these elements, $a \circ b$, must also be an element of *G.* In other words, the binary operation does not lead us out of the set on which it is defined.

The set G = {0,1} under addition is not closed since 1+1 = 2 and 2 is not in G.

The set G = {1, -1} under multiplication is closed.

To define a closed set under addition there are two approaches: (1) define an infinite set that does contain every result of adding two other elements of the set.(2) modify the operation of addition in some way so that finite sets of numbers are included.

The first approach leads us once again to the structure (ℤ, +)- that is the set of all (positive and negative) numbers under the operation of addition.

The second approach leads us to modular arithmetic.

Students of mathematics should have already met the idea of modular arithmetic through the addition of angles. Since it is not possible to have an angle bigger than 360° (2π rad) whenever addition of two angles leads to an angle bigger than 360° (2π rad) we subtract 360° (2π rad) and start again.

For example, $270^\circ + 180^\circ \equiv 450^\circ \equiv 90^\circ \ (\text{mod } 360^\circ)$

The bracket indicates (mod 360°) indicates that the angle 0° is treated as equivalent to 360° and we are starting all over again.

Modular arithmetic can be defined for any integer. The symbol $\mathbb{Z}_n$ stands for the group defined by addition module n.

For example

$$\mathbb{Z}_2 = (\{0,1\}, +(\text{mod } 2))$$

Thus

$0+0=0$

$0+1=1$

$1+0=1$

$1+1=2\equiv 0(\operatorname{mod} 2)$

So the group table (the combination square) is :

$+(\operatorname{mod} 2)$	0	1
0	0	1
1	1	0

Note that this is the same structure as $\left(\left\{+1.-1\right\},\times\right)$ illustrated earlier.
For a second example

$$\mathbb{Z}_5=\left(\left\{0,1,2,3,4\right\}+\left(\operatorname{mod} 5\right)\right)$$

With combination square:

$+(\operatorname{mod} 5)$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

These modular addition groups are also called cyclic groups. This is because in each case there is an element of the group that is combined with itself repeatedly (using the group operation (will generate every element in the group. For example in the case of $\mathbb{Z}_5$ the group generator is the number 1

$1=1$

$1+1=2$

$1+1+1=3$

$1+1+1+1=4$

$1+1+1+1+1=0$

We denote the cyclic group generated by an element a of a group by $\langle a \rangle$. Thus

$\mathbb{Z}_5$ is an equivalent to the cyclic group $\langle 1 \rangle$ under addition modulo 5

(4) Associativity

In order for a structure $(G, \circ)$ to be a group, the operation, $\circ$, must be associative.

An operation $\circ$ is associative if, for any three elements *a,b,c* in *G*:

$$(a \circ b) \circ c = a \circ (b \circ c)$$

Thus we ar enot obliged to bracket the elements when performing the group operation them and we can write unambiguously:

$$a \circ b \circ c$$

Addition of integers is associative. For example.

$$2+3+(-6)=-1$$

whatever way we add the numbers:

$$\begin{aligned} 2+3+(-6) &= (2+3)+(-6) \\ &= 5+(-6) \\ &= -1 \end{aligned}$$

or

$$\begin{aligned} 2+3+(-6) &= 2+(3+(-6)) \\ &= 2+(-3) \\ &= -1 \end{aligned}$$

Thus the introduction of the additional bracket is not required and merely complicates the working.

At this level failure of associativity is actually quite rare, and we are usually told to assume it. You can assume that addition and multiplication of numbers are associative.

However one example of a structure which would be a group but for the failure of associativity is $\left(\{0,1,2,3,4\},*\right)$ where $*$ is defined by

*	0	1	2	3	4
0	0	1	2	3	4
1	1	0	3	4	2
2	2	4	0	1	3
3	3	2	4	0	1
4	4	3	1	2	0

The group is closed; the identity is 0 and each element is its own inverse. But

$$(1*2)*4 = 3*4 = 1$$
$$1*(2*4) = 1*3 = 4$$

so associativity fails for this structure.

Summary

A group is an abstract mathematical structure comprising a set G and a binary operation o that satisfies the following properties (axioms).

(1) Identity

There is an element $e \in G$ such that for any element $a \in G$

$$e \circ a = a$$
$$a \circ e = a$$

(2) Inverses

For every element $a \in G$ there is another element $a^{-1} \in G$ such that

$$a \circ a^{-1} = e$$
$$a^{-1} \circ a = e$$

(3) Closure

For every pair of elements $a,b, \in G$ there is a third element $a \circ b \in G$

(4) Associativity

For all elements $a,b,c \in G$

$$(a \circ b) \circ c = a \circ (b \circ c)$$

Questions

Questions on the definition of group structure ask you:

(1) To construct a combination table for a given set and binary operation

(2) To prove that a given structure is a group by verifying the axioms (i.e. identity, inverses, closure and associativity)

(3) To prove that given structure is not a group by showing that one of the axioms fails by providing a counter example