

Degree Topics in Mathematics

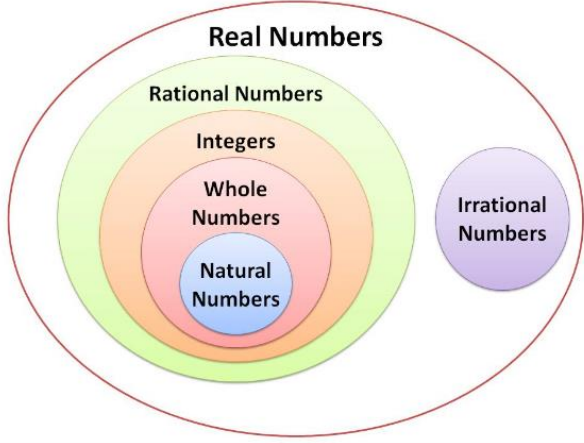
Groups

A **group** is a mathematical structure that satisfies certain rules, which are known as axioms. Before we look at the axioms, we will consider some terminology.

Elements – these are the individual members of a set. They form a collection of objects which have something in common,

e.g. The set of natural numbers $\mathbb{N} = \{1, 2, 3, 4, \dots\}$

The set of integers $\mathbb{Z} = \{\dots -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$



This diagram shows sets of numbers, some of which are subsets of others.

Find out what letter symbols are used to represent each of these sets e.g. \mathbb{N} for natural numbers.

What would the large set which encloses all of the others be called?

<http://www.bing.com/images/search?q=sets+of+numbers+diagram&go=Submit+Query&qs=bs&form=QBIR#view=detail&id=ED0A16069BF53CC1DCA7CE6247001096C37ED29C&selectedIndex=12>

Binary operation – this is a function which is applied to two elements of a set.

The binary operation $+$ on elements of \mathbb{N} produces other elements of \mathbb{N} , for example

$3 + 5 = 8$ and 8 is an element of \mathbb{N} .

The binary operation $*$ on \mathbb{Z} could be defined as $a*b = \min(a, b)$ where \min indicates the minimum of the two integers. For example, $3*5 = \min(3,5) = 3$ and $-3 * 6 = -3$. Notice that once again the answer is also an element of the set \mathbb{Z} .

When the answer to a binary operation on two elements of a set is also in the set, we say that the set is **closed** under that binary operation.

By contrast, the binary operation $-$ on the set \mathbb{N} can produce answers that are not elements of the original set, for example $2 - 6 = -4$, therefore we say that ' \mathbb{N} is not closed under subtraction'.

Associativity – When carrying out a binary operation on more than two elements, the operation should be applied in pairs. For example, $a*b*c$ could be done as $(a*b)*c$ or $a*(b*c)$. If the answers to both of these give the same answer, we say the binary operation is associative.

Task 1

Determine which of the following are associative.

1. The set \mathbb{N} under the binary operation $+$
2. The set \mathbb{N} under the binary operation $-$
3. The set \mathbb{Z} under the binary operation $a*b = a + 2b$

Commutativity – For some binary operations, the order in which the pairs occur is important. In a simple case, \mathbb{N} is commutative under the binary operation $+$ but not under $-$ as $3 + 5 = 5 + 3$ is true, but $3 - 5 = 5 - 3$ is not true.

Task 2

If you have studied matrices, investigate whether matrix addition on 2×2 matrices is commutative.

Is matrix multiplication commutative?

Identity – An identity element is usually denoted by the letter e . When combined with another element of a set under a binary operation, the element is unchanged.

For example, $5 + 0 = 5$ so 0 is the identity element for addition on the set \mathbb{Z} .

For multiplication on this set however, the identity would be 1 as, for example, $5 \times 1 = 5$.

Task 3

Explain why the following sets do not have an identity element:

1. The set \mathbb{N} under addition $+$
2. The set of even numbers under multiplication \times

Inverses – For an element of a set g an inverse g^{-1} is an element for which $g * g^{-1} = e$ and $g^{-1} * g = e$.

For example, for the set \mathbb{N} under addition, the identity is 0 and so the inverse of say 3, is (-3) as $3 + (-3) = (-3) + 3 = 0$.

However, \mathbb{Z} does not have inverses under multiplication. The identity is 1 and so the inverse of 3 would be $\frac{1}{3}$ as $3 \times \frac{1}{3} = 1$. However, $\frac{1}{3}$ is not an integer and so is not an element of the set.

Group Axioms

A set of numbers S forms a group under a binary operation $*$ if the following axioms hold:

1. S is closed under $*$
2. $*$ is associative
3. There is an identity element e which is a member of S
4. Every element of S has an inverse

Task 4

By checking the axioms above, determine whether the following sets are groups under the binary operations given.

1. The positive rational numbers \mathbb{Q} under multiplication \times .
(Note: Rational numbers are those which can be expressed as fractions)
2. The integers \mathbb{Z} under the binary operation $a * b = a + b - 1$
3. The positive integers \mathbb{Z}^+ under multiplication

Why have groups?

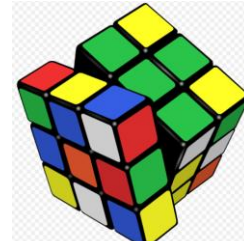
Groups allow diverse collections of objects to be compared and similarities in the structure to be identified. They are an important way in which mathematicians organise and compare ideas.

They can also be used in a variety of ways outside mathematics, for example in solving the Rubic Cube puzzle. The possible moves that

could be made are elements of a group and these

can be combined and studied as part of a

symmetric group (see Symmetry Group activity for more details) or visit



http://en.wikipedia.org/wiki/Rubik%27s_Cube_group#Group_structure

How many groups are there?

As recently as 1981, it was thought that it had finally been proved that the classification of finite simple groups (ones with a fixed number of elements and satisfies some additional mathematical rules) that had been previously identified was in fact a complete list. It was a huge piece of pure mathematics spanning over 10,000 pages in journals, and written by around 100 authors. Even now, gaps within the proof have been identified and remedied.

Find out more:

Nrich - Groups – an interesting collection of articles including the history of the development of groups.

Schools' Wikipedia - Group Theory - an introduction to the topic.

Solutions

Task 1

These examples are not formal proofs but they give an indication of associativity.

- The set \mathbb{N} under the binary operation +
 $3 + (5 + 2) = (3 + 5) + 2$ shows associativity in this case as $3 + 7 = 8 + 2$.
- The set \mathbb{N} under the binary operation –
 $3 - (5 - 2) = (3 - 5) - 2$ shows non-associativity in this case as $3 - 3 \neq -2 - 2$
- The set \mathbb{Z} under the binary operation $a*b = a + 2b$
 $5*(7*2) = (5*7)*2$ shows non-associativity in this case.
 On the left hand side $7*2 = 7 + 4 = 11$ and then $5*11 = 5 + 22 = 27$.
 On the right hand side $5*7 = 5 + 14 = 19$ and then $19*2 = 19 + 4 = 23$.

Task 2

Choosing any 2×2 matrices allows us to see that matrix addition is commutative but matrix multiplication is not.

e.g. $\begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} + \begin{pmatrix} 5 & -2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 7 & 1 \\ 1 & 5 \end{pmatrix} = \begin{pmatrix} 5 & -2 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}$ so commutative

$\begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 5 & -2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 10 & -1 \\ 5 & 2 \end{pmatrix}$ but $\begin{pmatrix} 5 & -2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 8 & 7 \\ 1 & 4 \end{pmatrix}$ so not commutative

Task 3

- The set \mathbb{N} under addition +
 Under addition, the identity element would have to be 0; however 0 is not a member of the set of natural numbers. Hence there is no identity element in this set.
- The set of even numbers under multiplication \times
 Under multiplication of number, the identity would be 1; however 1 is not even. Hence there is no identity element in this set.

Task 4

- The positive rational numbers \mathbb{Q} under multiplication \times .

Closure: Multiplying together two fractions would produce a fraction and so the set \mathbb{Q} is closed under multiplication.

Associativity: $\left(\frac{a}{b} \times \frac{c}{d}\right) \times \frac{e}{f} = \frac{ac}{bd} \times \frac{e}{f} = \frac{ace}{bdf}$

$\frac{a}{b} \times \left(\frac{c}{d} \times \frac{e}{f}\right) = \frac{a}{b} \times \frac{ce}{df} = \frac{ace}{bdf}$

These expressions are equal so this confirms associativity.

Identity: Multiplying any fraction by 1 would leave the fraction unchanged. 1 is a rational number and therefore there is an identity element.

Inverse: For any fraction $\frac{a}{b}$ we know that multiplying by the fraction $\frac{b}{a}$ would give an answer of 1. Hence every element of \mathbb{Q} has an inverse under multiplication.

Therefore \mathbb{Q} does form a group under multiplication.

$$2. a * b = a + b - 1$$

Closure: adding two integers gives an integer, so adding 1 would also give an integer. Hence the set is closed.

Associativity: $(a * b) * c = (a + b - 1) * c = (a + b - 1) + c - 1 = a + b + c - 2$

$$a * (b * c) = a * (b + c - 1) = a + (b + c - 1) - 1 = a + b + c - 2$$

These expressions are equal, hence $*$ is associative.

Identity: We need an element e such that $a * e = a$, which means that $a + e - 1 = a$.

Hence $e = 1$ and this is an integer.

Inverse: Suppose the inverse of element a is b , then $a * b = e$. This means that $a * b = 1$.

So $a + b - 1 = 1$ and therefore $b = 2 - a$ (which is an integer) and so the inverse of a is $2 - a$.

Therefore the integers \mathbb{Z} under the binary operation $a * b = a + b - 1$

3. The positive integers \mathbb{Z}^+ under multiplication

Closure: Multiplying together two positive integers gives a positive integer, so this axiom holds.

Associativity: Multiplication of integers is associative i.e. $(a \times b) \times c = (ab)c = abc$ and $a \times (b \times c) = a \times (bc) = abc$. These expressions are equal.

Identity:

Identity: We need an element e such that $a * e = a$, which means that $e = 1$ and this is a positive integer.

Inverse: Suppose b is the inverse of an element a , then $a \times b = 1$. Hence $b = \frac{1}{a}$

This is not an element of \mathbb{Z}^+ unless $a = 1$. Hence it is not possible to find an inverse for most elements and so \mathbb{Z}^+ does not form a group under multiplication.