# Groups

A ***system*** consists of a ***set*** and a ***binary operation.*** The system consisting of the set $S$ and the operation $\circ$ can be written as $[S, \circ]$

A set is a collection of discrete things. Examples are the set {1, 2, 3}, the set of integers, or the set of people in a classroom.

A binary operation is a rule for taking any two elements of the set (input) and producing a single thing (the output). An example is addition, where we might have 4 and 3 as inputs and 7 as the output . Another example is the operation $\sqrt{a^2 + b^2}$, where $a$ and $b$ are the inputs and $\sqrt{a^2 + b^2}$ is the output.

An unspecified operation can be written $a \circ b$, pronounced 'a o b'.

A system is a ***group*** if it has four properties:

1. It is closed;
2. The operation is associative;
3. There is an identity;
4. Every element had an inverse.

Given a system, you need to be able to tell which of these properties it has.

## Closure

A system is closed if, when the operation is performed on elements of the set, the output is always an element of the set.

To show that a system is closed, common sense is generally enough: if you add two integers, you will always get an integer. To show that a system is not closed, you just need to fine one counter-example: the whole numbers are not closed under subtraction because $2 - 5$ does not produce a whole number.

## Associativity

This is the property that for any three elements in the set, $a \circ (b \circ c) = (a \circ b) \circ c$.

We can assume that normal addition and multiplication are associative, subtraction and division aren't. For operations like $a \circ b = a+b+1$, we can show it algebraically:

$a \circ (b \circ c) = a+(b+c+1)+1 = a+b+c+2$

$(a \circ b) \circ c = (a+b+1)+c+1 = a+b+c+2$

To show that a system isn't associative, we need just one counter-example. E.g. to show that subtraction on the integers isn't commutative we can use:

$1-(0-1) = 2$

$(1-0)-1 = 0$

## Identity

The set, $S$, must include an identity. An identity, $u$, is an element such that

$\forall a \in S,\ a \circ u = u \circ a = a$

To determine if there is an identity and what it is, we use the following procedure.

Suppose the system is the set of real numbers and the operation defined by $a \circ b = a+b+1$.
Let the identity be u.

$a \circ u = a+u+1 = a$

$a+u+1 = a$

$u+1 = 0$

$u = -1$ So the right identity is –1

$u \circ a = u+a+1 = a$

$u+a+1 = a$

$u+1 = 0$

$u = -1$ So the left identity is –1. So the identity is –1.

Note that to be an identity, the element must be a right identity and a left identity.

If it turns out that the left and right identities are different or that $u$ is an expression containing $a$, then $u$ is not an identity. For example
Suppose the system is the set of real numbers and the operation defined by $a \circ b = a-b$.

$a \circ u = a-u = a$

$-u = 0$

$u = 0$

$u \circ a = u-a = a$

$u = 2a$

Here the left and right identities are different and the left identity will be different for different values of $a$. The identity must be the same value for all $a$.

## Inverse

Every element of the set must have an inverse. We call the inverse of $a$ $a^{-1}$. This does not mean $1/a$.
In other words $\forall a \in S, \exists\ a^{-1}: a \circ a^{-1} = a^{-1} \circ a = u$, where $u$ is the identity.
Inverses can only exist if there is an identity.

To determine if every element has an inverse and what it is, we use the following procedure.
Suppose the system is the set of real numbers and the operation defined by $a \circ b = a+b+1$. We have found that the identity is –1.
Let the inverse of $a$ be $a^{-1}$
So $a \circ a^{-1} = a+a^{-1}+1 = -1$

$\therefore\ a^{-1} = -2-a$

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

$\therefore\ a^{-1} = -2-a$

So every element $a$ has an inverse $-2-a$

If the left and right inverses are different or not defined for all $a$, then not every element has an inverse.

To show that a system is a group, you have to show that all four properties hold. Showing that any one doesn't hold shows that the system is not a group.

A system with a finite set can be represented as a ***Cayley table***. This shows the output of the operation for all pairs of input elements. For example, the system [{0, 1, 2},–] looks like this.

| – | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | –1 | –2 |
| 1 | 1 | 0 | –1 |
| 2 | 2 | 1 | 0 |

Note the order of operation. For instance the output –2 comes from 0 – 2, not 2 – 0.

Some group properties can be determined from a Cayley table as follows.

*Closure*: all elements in the body of the table are in the header row and column.

*Identity*: If a column is the same as the header column, then the element at the head of the column is a right identity. If a row is the same as the header row, then the element at the head of that row is a left identity. If a column is the same as the header column and the corresponding row is the same as the header row, then the header element is the identity.

*Inverse*: If every column contains the identity element, then every element has a right inverse. If every row contains the identity element, then every element has a left inverse. If every row and every column contains the identity element, then every element has an inverse.

*Associativity*: There is no simple test for associativity.

*Closure, identity and inverse*: If every element occurs in every row and in every column, then the system is closed, and has an identity and every element has an inverse. Thus, if we also know the system is associative, then it is a group.

A group in which the operation is commutative is called an Abelian group. The Cayley table for an Abelian group is symmetrical about the leading diagonal, like this:

| × | 1 | $i$ | –1 | $-i$ |
|---|---|---|---|---|
| 1 | 1 | $i$ | –1 | $-i$ |
| $i$ | $i$ | –1 | $-i$ | 1 |
| –1 | –1 | $-i$ | 1 | $i$ |
| $-i$ | $-i$ | 1 | $i$ | –1 |