Group theory is basically speaking the study of symmetry in sets. Group theory has real world applications in telecommunications, cryptography, and puzzle theory.

It contains some quite challenging concepts so for this section, we’ll take it slow, I’ve split it into two chapters, in this first chapter we’ll cover the basics of group theory so you can familiarize yourself with the notation necessary.

A set is just a collection of objects, these objects are known as the elements of the set. Notated by curly braces {} , { 3, 5, 2, 65, 1 } would be the set containing the numbers 3, 5, 2, 65 and 1. There is also a lot of predefined notation for common sets, e.g. every integer has the shorthand , or every natural number , every positive number, instead of being described as { 1, 2, 3, 4, … } has the shorthand .

If S is the set and x is an element in the set then we say x ∈ S, “x belongs to S”

e.g.

4 ∈ { 2, 7, 4, 9 } but 4 ∉ { 1, 8, 3, 0 } “4 does not belong to the set { 1, 8, 3, 0 }”

elephant ∈ { pig, elephant, lion } but fox ∉ { pig, elephant, lion } (sets don’t have to just contain numbers).

Sets can also be defined in a more complex way to get a large amount of elements without having to write out each element e.g. {x, x ∈ x mod2 =0 } would be the set of all positive even integers. (x mod 2 just returns the remainder when x is divided by 2).

A basic group consists of a set of elements, linked with a *‘binary operator’* which is just a fancy term for , ‘a function of those two elements’ . E.g. multiplication, addition, subtraction, division are all examples of binary operations, however it could also be something more abstract like, the last digit of the product of two numbers.

The binary operator is symbolized by the \* symbol, so if a,b ∈ G then a\*b would be the binary operation of a and b, don’t worry if you don’t understand it’ll soon all make sense.

e.g. if the binary operation was addition then a\*b would mean a+b , if the binary operation was then 2\*4= .

For a set and binary operation to become a group they must follow four axioms.

1. Closure – the result of a\*b , a,b ∈ S is also in the set S
2. Associativity – (a\*b)\*c = a\*(b\*c)
3. Identity – if there exists an element e such that a\*e=a for all a where a,e ∈ S then e is said to be the identity element
4. Inverse – if there exists an element b such that a\*b=e , where a,b,e ∈ S, then b is the inverse of a

E.g. Prove the set { 1, -1, i, -i } where i = and the binary operation is multiplication is also a group. We can construct a table to show the possible results of each operation.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| X | 1 | -1 | i | -i |
| 1 | 1 | -1 | i | -i |
| -1 | -1 | 1 | -i | i |
| i | i | -i | -1 | 1 |
| -i | -i | i | 1 | -1 |

1. Closure – As you can see the operation is closed as every result is also contained in the set
2. Associativity – It is known that multiplication is associative in the same way 3x2=2x3
3. Identity – The element 1 is the identity as a\*1=1\*a=a for each element in the set
4. Inverse – The inverse of 1, -1, i, -i are 1, -1, -i, i respectively , as they follow the rule a\*b= 1 , as 1 is the inverse.

As the set follows the 4 axioms it must also be a group.