**Notes on Group Theory**

We'll throw some light on the title question of this page by asking another question. What is the solution of the equation

(1) 4x = 3

The answer depends on what "things" we allow *x* to be. If we are doing all our arithmetic using the integers then there is no solution--there is no integer that gives 3 upon being multiplied by 4. On the other hand if we are doing our arithmetic in **Z**/5 ("Integers mod 5" as it's sometimes called) then *x* = 2 is a solution. If we are using the more usual rational number system **Q**, then the solution is *x* = 3/4.

We can gain insight into all such questions by considering the equation

(2) a • x = b

and then bringing up the question of solutions. Well, what objects are *a* and *b*? To what class of objects is *x* allowed to belong? What is the operation symbolized by the dot (•)?

Group theory is concerned with systems in which (2) always has a unique solution. The theory does not concern itself with what *a* and *b* actually are nor with what the operation symbolized by • actually is. By taking this abstract approach group theory deals with many mathematical systems at once. Group theory requires only that a mathematical system obey a few simple rules. The theory then seeks to find out properties common to all systems that obey these few rules.

The axioms (basic rules) for a **group** are:

1. **CLOSURE**: If **a** and **b** are in the group then **a • b** is also in the group.
2. **ASSOCIATIVITY**: If **a, b** and **c** are in the group then **(a • b) • c = a • (b • c)**.
3. **IDENTITY**: There is an element **e** of the group such that for any element **a** of the group **a • e = e • a = a.**
4. **INVERSES**: For any element **a** of the group there is an element **a**-1 such that
   * **a • a**-1 **= e**  and
   * **a**-1 **• a = e**

That's it. Any mathematical system that obeys those four rules is a group. The study of systems that obey these four rules is the basis of **GROUP THEORY**

**A Look at the Axioms**

**Closure**

**CLOSURE**: If **a** and **b** are in the group then **a • b** is also in the group.

The first axiom of group theory is the **CLOSURE** axiom. For a system to be a group the binary operation (symbolized here by "**•**") must be valid for any pair of elements in the group and the result of the operation must be an element of the group. The set of negative integers, for example, is not closed under multiplication because the product of two negative integers is not a negative integer. The set of vectors of unit magnitude is not closed under vector addition because the vector sum of two unit vectors is not necessarily a unit vector. More interestingly, the set of three-dimensional vectors is not closed under scalar (sometimes called "dot") product since the scalar product of two vectors is not a vector. On the other hand the counting numbers are closed under addition and multiplication. They are not closed under either subtraction or division. The set of three dimensional vectors is closed under vector (or "cross") product since the result of the operation is a three-dimensional vector.

**Associativity**

**ASSOCIATIVITY**: If **a, b** and **c** are in the group then **(a • b) • c = a • (b • c)**.

The group operation must be **ASSOCIATIVE**. Addition and multiplication of real numbers is associative. As the following examples show, subtraction and division of real numbers is not associative.

**(5 - 3) - 2 = 2 - 2 = 0**

but

**5 - (3 - 2) = 5 - 1 = 4**

Thus **(5 - 3) - 2** does not equal **5 - (3 - 2).** Similarly with division we can see that

**5/(3/2) = 5/(1.5) = 3 1/3**

but

**(5/3)/2 = (1 2/3)/2 = 5/6**

Another example of a binary operation that is not associative is the binary operation of averaging, which I will represent as *av*. It gives the average of the pair of numbers that it acts upon. For instance 4 *av* 6 = 5 and 9 *av*2 = 5 1/2. When trying to find the usual average of three numbers we cannot simply apply the binary *av* operation twice:

**2 *av* (3 *av* 7) = 2 *av* 5 = 3 1/2**

but

**(2 *av* 3) *av* 7 = (2 1/2) *av* 7 = 4 3/4**

**Identity**

**IDENTITY**: There is an element **e** of the group such that for any element **a** of the group

**a • e = e • a = a.**

A group must have an **IDENTITY** element. This is an element with a neutral action. When the identity element is combined with any element of the group in the group operation the result is always to give back the same member of the group. For multiplication of real numbers the identity element is 1; for addition of real numbers it is 0. For 2 × 2 matrix multiplication the identity is

**| 1 0 |**

**| 0 1 |**

The binary operation of *av*, given above, is an example of an operation without an identity element. There is no number which when averaged with any chosen number gives that chosen number back again. True, for any chosen number there is a number that may be averaged with it to give the original chosen number back again, namely itself. However, there is no one number that works this way for any chosen number. (Saying, "everybody has a mother" is very different from saying, "someone is the mother of everybody.")

Cross product of three dimensional vectors is another example of a binary operation that does not have an identity element. Since the cross product of vector **A** with any other vector is either the zero vector or a vector perpendicular to **A** there can be no vector **E** with **A**×**E** = **A**. (otherwise **A** would be perpendicular to itself!)

**Inverses**

**INVERSES**: For any element **a** of the group there is an element **a**-1 such that

* **a • a**-1 **= e**  and
* **a**-1 **• a = e**

In order for an operation to satisfy the axiom for **INVERSES** the operation must have an identity element. Thus we know without further investigation that the *av* operation and the cross product operation do not have inverses since they do not have identity elements. An inverse element is a way to *undo* an operation. For example suppose I add 7 to a number and get the result 12. If I want to undo the addition of 7 and return to my original number that I added 7 to I simply add the inverse of 7 which is -7. This shows that my original number that I added to 7 was 5. I *undid* the addition. Similarly I can undo multiplication by 2 by multiplying by the inverse of 2 which is 1/2. Many of the extensions of the number systems of arithmetic were made to create inverses. The integers are an extension of the natural numbers in which addition has an inverse. The rational numbers are an extension of the integers in which each non-zero number has an inverse under multiplication. A 2 × 2 matrix may or may not have an inverse under matrix multiplication. Those matrices which do not have multiplicative inverses are called *singular.*

**Back to Equation (2)**

Now let's go back to our original question: what is the solution of

**a • x = b**

In "solving" this equation we will assume that **a** and **b** are elements of a group with the group operation symbolized by **•**. We are looking for the member of the group that **x** could be replaced by to satisfy the equation. We'll use the group axioms to "solve" the equation in any group.

Using the **closure** axiom and the axiom for **inverses** we operate on both sides of the equation by the inverse of **a**. The inverse axiom says that **a**-1, the inverse of **a** exists and the closure axiom says that the product of **a**-1 and any other group element exists and is still in the group.

**a**-1 **• (a • x) = a**-1 **• b**

Now applying the **associative** axiom,

**(a**-1 **• a) • x = a**-1 **• b**

The axiom of **inverses** gives

**e • x = a**-1 **• b**

Finally using the axiom of **identity** we get,

**x = a**-1 **• b**

So we "solved" equation (2) without answering the questions about **a, b** or **x** actually were or even what the operation indicated by **•** was. This is the power of abstraction. Group theory is a clear example of abstraction in modern mathematics. The emphasis is not on the particular group we might be interested in for some given application. The emphasis is on the basic quality of *groupness* that all groups have in common. Once a result is demonstrated to be valid for all groups then it is clearly valid for any specific group we may choose.

http://dogschool.tripod.com/groups.html