An Introduction to Algebra

Anthony Voutas

December 16, 2010

This is a introduction to the basics of the topic of Algebra. The prerequisites of this text are basic set theory, set constructor notation and basic propositional logic. An understanding of the counting principle and an understanding of the principles of labelling and variables are assumed, as they are prerequisites of set theory and propositional logic in turn. For some of the examples, a knowledge of basic arithmetic and fractions is assumed, somewhat paradoxically. Rest assured that the examples are independent of the formal definitions, so no circular logic is being applied. The main focus of this text is a definition of the concept of a "group", and a slew of examples for the finite case.

Functions

Functions can be considered as a process being applied to input, to create output. A simple example from basic arithmetic is the squaring function. Call this function "sqaure". An example of the application of this function is:

$$\text{square}(2) = 2 \times 2 = 4$$

Square can be interpreted as a process applied, in this case, to the number 2. The outcome of the process is the number 4. Most mathematical processes can be represented as functions. In some cases, the process requires two or more objects of input to produce its output. These processes can also be represented as functions, and we tend to write them as:

$$\text{function-name}(\text{input 1, input 2,..., input } n) = \text{output}$$

For functions with n inputs, where n is a natural (counting) number such that $n \geq 1$. The remainder of this section will concern single input functions, but everything discussed can easily be extended to many input functions (as will be shown at the end of the section - we need some notation first).

A single input function can be viewed as a specific type of correspondence between the members of two sets. We say that a function maps from set A to set B, if the function's input is a member of the set A and the function's output is a member of the set B. We write this as:

$$f : A \to B$$

Or, equivalently

$$A \xrightarrow{f} B$$

Where, in both cases, f is the name of the function.

Note: The $\rightarrow$ symbol here is the mapping symbol, and has little or nothing to do with implication in logic.

Note: The sets A and B may in fact be equal, but even in this case it is conceptually useful to keep them separate.

Note: A is often called the Domain of f, and B is called the Codomain.

Intuitively speaking, the function f is assigning f-values (which are values in the set B) for the members of the set A. When we have done this, we can talk about define concepts such as surjectivity, injectivity and bijectivity.

The first thing to note about the function f from A to B is that there are f-values for *every* member of A. If the is not an f-value for some member of A, then we say that f is not a function. The second thing to note is that there is only one f-value for every member of A. If there are two, f is not a function. All you need to know is that if a function maps from A to B, then it is defined everywhere in A, and every member of A has only one f-value in B. These are the defining features of a function.

An interesting side note:

The function:

$$f(x) = \frac{1}{x}$$

Is often mislabelled as a function $f : \mathbb{R} \to \mathbb{R}$, where $\mathbb{R}$ is the real numbers. This is actually incorrect, because of course, $\frac{1}{x}$ is undefined when $x = 0$, and $0 \in \mathbb{R}$. The function f is only a function on subsets of the reals without zero. The most general (and honest) labelling of the function would be: $f : \mathbb{R} \backslash \{0\} \to \mathbb{R}$. Note here that it is not important that the function map onto all of the values in the target set, properties like this will be talked about below.

Surjectivity

Surjectivity is a property which certain functions have, and others do not. That said, it is a relative term, as we will see, and we can make any function surjective, if it suits us. We will get to the formal definition of surjectivity in a bit. It will serve our purposes to define another concept in the meantime.

Definition. The "image of an object x" under a function $f : A \to B$ is defined when x is a member of A. It is exactly the f-label that the function f gives to the object x. As such, the image of an object in

A is an object in B. We denote the image of an object x as $f(x)$ (this notation was seen above).

Definition. The "image of a set X" under a function $f : A \to B$ is defined when X is a subset of A. It is denoted $f(X)$. It is defined as follows:

$$f(X) = \{f(x) | x \in X\}$$

That is, it is the set containing the images of all of the objects in the set X.

Finally, we can define surjectivity in very simple terms:

Definition. A function $f : A \to B$ is surjective exactly when $f(A) = B$.

Intuitively speaking, this means if we pick any object from B (call it b), there will be at least one object in A which the function maps to b (that is: For all b in B, there exists at least one a in A such that $f(a) = b$).

Equivalent to saying $f : A \to B$ is surjective is saying that f maps "onto" B, intuitively meaning that f covers all of B.

We can make any function f surjective by restricting its codomain in the following way:

$$f : A \to f(A)$$

The function is still well defined, because we haven't removed any images for the objects of A, and all information about the function is preserved, because the extra stuff in B wasn't having an effect on the function anyway.

Injectivity

Similar to surjectivity, injectivity is a property which certain functions have, and others do not. Also similar to surjectivity, injectivity is a relative term, as we will see, and we can make any function injective, if the mood takes us.

Definition. A function $f : A \to B$ is injective iff for every x and y which are members of A, the condition $f(x) = f(y)$ holds only if $x = y$.

This is a useful concept to define, because knowing that f is injective allows us to say that two different members of A map to different members of B.

Note also that we know that the converse holds. That is, if $f(x) \neq f(y)$ then $x \neq y$, because if $x = y$ then $f(y) = f(x)$ by substitution and $f(x)$ has a single value in the codomain for any x in the domain (notice the proof by logical contraposition).

To make $f : A \to B$ injective, we can restrict the domain to the some subset X, where $f(X) = f(A)$, by picking out all of the elements x and y such that $x \neq y$ and $f(x) = f(y)$, and removing one of the two elements, until we can no longer find such elements.

Bijectivity

Definition. A function $f : A \to B$ is bijective exactly when it is surjective and injective.

Bijective functions are interesting and useful for a number of reasons. I don't have space to write down all of the relevant applications here, but here's some:

- The notion of cardinality of infinite sets is defined in terms of bijections. The non-existence of bijections between sets and their power sets is used in the proof that there are infinitely many infinite cardinals.
- The notions of isomorphism and isometry are notions of bijections with additional structure preserving qualities.
- Bijections can be used to uniquely label every element in one set with that of another. Even when these sets are the same, this can prove useful to manipulate and represent certain mathematical objects.

Multi-input functions

A multi input function can be turned into a single input function by considering the multiple input objects to be a single object.

Definition. A "tuple" (pronounced "tup"-"el") is an ordered finite sequence of objects, often represented in the following ways:

$$\begin{aligned} \text{tuple} &= (\text{object1},\ \text{object2}, ...,\ \text{object}n) \\ \text{tuple} &= \langle \text{object1},\ \text{object2}, ...,\ \text{object}n \rangle \end{aligned}$$

You will notice that there are n objects in the tuple. This is often called an n-tuple.

We often label the objects in the sequence as x_i, where i is the numerical position of x_i in the tuple. We should also say where the objects come from. Thus we often say that $x_i \in X_i$ for all i, where X_i is just a set containing x_i.

In this way, we can define a set $A = X_1 \times ... \times X_n$, (where × here is the cartesian set product which creates a new set of ordered n-tuples with each of their components coming from the relevant X_i). As such we can then define the multi-input function f in the same way we defined the single valued functions: $f : A \to B$.

Operations

Definition. An operation is a function, which typically has two inputs (this is more specifically called a "binary operation"). Further to this, it must map from a set $A \times A$ to a the set A:

$$\text{operation} : A \times A \to A$$

This is often refered to as an operation *on* the set A.

Operations do not have to be surjective or injective. In fact, in the finite case (that is, for finite sets A), these properties are impossible, as $A \times A$ has a strictly larger cardinality than A, unless $A = \emptyset$ or A has only a single element.

After defining the concept of an operation, we tend to place further restrictions on operations to get specific classes of operations. Some of these restrictions may be familiar to you, at least at an intuitive level.

Possible restrictions include: (Let the operation be denoted by $\circ$)

- For all elements a and b in A: $a \circ b \; = \; b \circ a$. This is referred to as the "commutativity" of $\circ$. If this restriction holds for the operation $\circ$, we say that $\circ$ is a "commutative" operation on A. This is a property that you probably know well from arithmetic with multiplication and addition, both of which are commutative. It is also a property of the AND and OR connectives in classical propositional logic. Note that in general, operations do not need to be commutative.

- For all elements a, b and c in A: $a \circ (b \circ c) \; = \; (a \circ b) \circ c$. This is referred to as the "associativity" of $\circ$. If this restriction holds for the operation $\circ$, we say that $\circ$ is an "associative" operation on A. This is an important property for groups (as we will see later).

- For all elements a in A: $a \circ a = a$. This is referred to as the "idempotency" of $\circ$. If this restriction holds for the operation $\circ$, we say that $\circ$ is an "idempotent" operation on A. This property, you may know is one which the logical connectives AND and OR have.

- There exists a distiguished element of A (call it e) such that for all a in A (including e): $e \circ a = a$. This element e is called the "left identity" of $\circ$, as you can apply it to the left of any other object in A without effect. We also say: $\circ$ has a left identity.

- There exists a distiguished element of A (call it e) such that for all a in A (including e): $a \circ e = a$. This element e is called the "right identity" of $\circ$, as you can apply it to the right of any other object in A without effect. We also say: $\circ$ has a right identity.

- There exists a distiguished element of A (call it e) such that for all a in A (including e): $e \circ a = a = a \circ e$. This element e is called the "two-sided identity" of $\circ$, as you can apply it to either side of any other object in A without effect. We also say: $\circ$ has a two-sided identity (or just "an identity", if the meaning is clear from the context).

There are many other possible restrictions on operations, and any combination of these restrictions can be investigated for interesting properties and possible applications to modelling real world scenarios.

Groups

Definition. A group is a set G with an operation $\circ : G \times G \to G$ with the following properties:
1. $\circ$ is *associative*.
2. $\circ$ has a *two-sided identity* (call it e).
3. For every element g in G, there exists an element h, such that $g \circ h = e = h \circ g$. This h is called the *two-sided inverse* of g.

This is a group. We call $\circ$ a *group operation*.

This may seem like a very basic definition, and it is, but it is also very powerful. The study of these objects is called Group Theory, and it forms an essential building block for modern algebra.

Finite Examples

The class of finite groups have been completely characterised by modern Group Theorists. That said, the characterisation is anything but compact, and it is very complicated to achieve. The real point of saying this is that for any finite group you can come up with, somebody else has already thought about an isomorphic group (that is, one which is essentially the same as yours) and they've probably also investigated its properties. As such, every groups has a name, and some have more than one.

That said, let's look at some groups.

Cyclic Groups

Cyclic groups are the simplest groups. For each positive number n, there is only one cyclic group of that size (size of the group corresponds to the cardinality of the set part of the group).

Well, that makes life easy. We can just call a cyclic group C_n, where n is its size.

What do these groups look like though? Why are they called "cyclic"? What are you even on about?

A group is called cyclic if there is an element in the group which "generates" the entire group.G

Before talking about that, let's define some notation:

For all $g \in G$, we define the following notion of natural number powers:

$$\begin{aligned} g^0 &= e \\ g^n &= g \circ g^{n-1} \end{aligned}$$

Note that all elements commute with themselves (if $g = g'$ then $g \circ g' = g' \circ g$), and therefore $g \circ g^{n-1} = g^{n-1} \circ g$, by induction on n.

Now, in any finite group G, for all g in G there is an n such that $g^n = e$. That is, if one continually applies g, starting from e, one will eventually return to e.

(This is a little deep for me to prove at 11pm at night, but it's pretty intuitive, given that the sequence cannot continue forever because G is finite - it has to be proven that it loops back to the start e, and not to some previous g^i, and this can be shown using the existence of the inverse of g and the functional nature of the group operation.)

That means that every g in G can form a cycle in exactly this way.

Definition. If, in the cycle of one of the group elements g, we encounter every element of the group as some g^i, then the group is called cyclic.

Therefore:

$$C_n = \{e, g, g^2, ..., g^n\}$$

Yes, I am aware that it says egg.

These groups are obviously pretty simple, because the simple rule $a \circ b = g^{i_a} \circ g^{i_b} = g^{i_a + i_b}$ defines the group operation for every element of the group. (Here, i_a is used to show that $a = g^i$ for some i, that is i_a)