Algebra-01

Yifan Wei

May 11, 2018

1 Introduction

Our course begins from this definition:

Definition 1.1 (Binary operation)**.** A binary operation on a set S, is a function from $S \times S$ to S.

When we confine our self to only one binary operation, we can freely assign a name to it such as "apple", "hahaha", "f", "addition", "multiplication"...

It's plain and uninteresting if we don't assume further properties on this binary operation, let's just call it multiplication, such as *associativity*:

Definition 1.2 (Associativity)**.** A multiplication is said to be associative iff $\forall a, b, c \in S$, $a(bc) = (ab)c$.

Later we'll see almost always associativity comes along with non-associativity, which makes things more interesting, or, mixed up...

2 Groups

Definition 2.1 (Group)**.** A group is a set G with an associative binary operation (usually wrote like multiplication), and this operation has two (simple but profound) properties:

1. There exists an identity element $e \in G$, such that $\forall a \in G$, $ae = a$.

2. For every element, say $a \in G$, there exists an inverse element $b \in G$, such that $ab = e$(identity element).

I think we will only focus on groups this time, because it's so weird and interesting! Though the definition looks pretty plain at the first glance, but you will see the order of operation really matters.

Remark. If $ab = e$, then $ba = e$.

Proof. $b \to \exists c \to bc = e \to ec = abc = ae = a \to e = bc = bec = ba$ □

This means the distribution of identity elements has certain symmetry. Such symmetry can be visualized once we draw a *multiplication table*.

Remark. If $ae = a$ then $ea = a$.

Proof. $ea = (ab)a = a(ba) = ae = a$ □

Remark. There is only one identity element.

Proof. $e_1 = e_1e_2 = e_2$ □

Remark. And only one inverse for each element.

Proof. $b = b(ac) = (ba)c = c$ □

This means there is only one identity element that occurs only once at each column and row on the multiplication table. From now on we will denote the inverse element of a by a^{-1}. Can you see things are getting a little tricky?

I think most people will find an obvious property now. But I will show the converse of your guess is true and make it a theorem!

Theorem 2.1. *In a group these two equations a solvable and each has only one solution in that group: $ax = b$, $ya = b$. The solution to the first one is $a^{-1}b$, to the second one is ba^{-1}. Conversely, if G is a set with an associative multiplication which makes both equations has a solution in G, then G is a group.*

Proof. The first part is trivial. To the second part, notice that $ax = a$ has a solution, then solve $ya = b$ for all bs in G, multiply y to the left on both sides of $ax = a$ then we come to that x is an identity element, then solve $ay = x$ for all as in G we finally return to the definition of group. □

3 Exercise

1. Find a set with a binary operation such that:

   (a) There exists an identity element $e \in G$, such that $\forall a \in G$, $ae = a$.

   (b) For every element, say $a \in G$, there exists an inverse element $b \in G$, such that $ab = e$.

   that is not a group!

   (**Hint:** use multiplication table)

2. Define the multiplication of functions to be the composition of functions, i.e. if $f : A \to B$, $g : B \to C$, $gf := \{(x, z) | \exists y \in B, (x, y) \in f, (y, z) \in g\}$(you can also write this as $(gf)(x) := g(f(x))$)

   Prove if S is non-empty, then $\{f | f : S \to S\}$ forms a group under the multiplication above.