Algebra - I

Prof. S. Viswanath & Prof. Amritanshu Prasad
Department of Mathematics
Indian Institute of Technology, Madras

Last time we looked at permutations and some of their properties under composition and mentioned that those properties abstractly give the Axioms for a group.

A group consists of 2 pieces of data: the first is the set G and the second is a binary operation. These data need to satisfy the axioms of *closure, associativity, identity* and *inverse*.

Example 1.
Let Z denote the set of integers (positive, negative and zero) under addition.
You know that integer addition has the **associativity** property.
What is the **identity** in the integers? It is the element 0.
The **inverse** of an integer x is -x.
So, the integers under addition form a group that will give you a slightly more interesting example.

Example 2.
Fix a positive integer N and look at the group of *residue classes* mod N(residue classes are indexed by the set of possible remainders upon dividing by N) under addition.
This is the the group of what is sometimes called 'clock arithmetic'. Everyday For example, if it is 9 o clock right now, then 4 hours later it is going to be 1 o clock, because 9 plus 4 is 13 and when you divide 13 by 12 the remainder that you get is 1. So, this is the arithmetic of remainders modulo n. Given 2 elements x and y in the set , x+y is the remainder when x+y, as an integer, is divided by n.
Associativity is easy because ordinary addition has associativity and then you are taking remainders.
It is easy to see that 0 is the **identity** here.
What is the inverse? The inverse of 0 is clearly 0, the inverse of 1 is N-1, because N-1 + 1 = N and when you divide N by N the remainder is 0 and the inverse of 2 is N-2 and so on. For i in 0,...,N-1, the **inverse** of i is N-i.
So this is a group, which we denote Z/NZ. The operation of modulo addition is denoted a+b mod N.

Example 3.
Let me give you a non-example of group- the integers, but under multiplication. Why is this not a group?
Well it does have an **identity**- which is 1.
What about inverse? What is the inverse of 2 for example? So, 2 into what is equal to 1? Well there is no integer which if you multiply by 2 you will get 1. There is a rational number, but there is no integer which if you multiply by 2 you will get 1. So in general there is **no inverse.**
Similarly you can see that for example Z/4Z under multiplication is not a group since here again there is no inverse.

Now let us look at some simple properties of groups that we can derive just from the axiom. The first property is *cancellation.*

Corollary 1.
Given $x, y, z \in G$ suppose $x \cdot z = y \cdot z$ then $x = y$.
Proof:
Let us prove this just using the group axioms. We know $x \cdot z = y \cdot z$. Now by the inverse axiom we know that there is an element z^{-1} which when multiplied by z gives the identity. We multiply this on both sides of the equality on the right of the existing term:
$x \cdot (z \cdot z^{-1}) = y \cdot (z \cdot z^{-1})$,
and now we use associativity on both sides of the equation as indicated by the brackets. Recall that $(z \cdot z^{-1}) = id$, and that multiplication by id yields the element itself.

Another simple property of groups is the uniqueness of the identity. In the axioms we just said that there exists an element identity of G, which has the property that $x \cdot id = id \cdot x = x$ for all x in G. But what I want to say is that there is exactly one such element.

Corollary 2.
The identity element of a group is unique.
Proof:
So suppose we had 2 identity elements: id, id'. If there is one $x \in G$ such that $x \cdot id = x \cdot id'$, you use cancellation on the x and you get $id = id'$.

Exercise 1.
Prove the uniqueness of inverse.

Now let me tell you how we can think more abstractly of a group. The examples we looked at came from some other branch of mathematics- the theory of permutations, or addition of integers, addition of integers mod N. But more generally a group is just a set and we need to keep track of this function from $G \times G \to G.$.
So, once we specify the elements of G and this function G cross G to G we have specified the group, and so this can be stored in the form of a table.

Example 4.
Let me do this with an example: let us look at the group Z/3Z. So, this has elements 0, 1, 2 and I will write down this in the form of a table with rows and columns both indexed by the elements of the group. So in the (x,y)th cell of the table I will store $x + y \, mod \, 3$.

Z /3Z multiplication table	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Once you write down the multiplication table you have completely specified the group
Suppose we have a group G with 2 elements. What groups have 2 elements? One example you can think of readily is Z/2Z.

Z/2Z multiplication table	0	1
0	0	1
1	1	0

Suppose G is some other group with 2 elements, say {id,a}. Let us write down the multiplication table.

Multiplication table for {id,a}	id	a
id	id	a
a	a	?

There are two possibilities for $a \cdot a$: either it could be a or it could be identity.
If we just put down a here and see if this gives rise to a group. It satisfies the identity axiom; but what is the inverse of a in this group? Observe that there is no inverse of the element a. So, we cannot have $a \cdot a = a.$
So, instead let us put identity.

Exercise 2.
Check that $a \cdot a = id$ in the above table gives rise to a group.

Here I have 2 groups with 2 elements- they look rather similar right? If instead of identity I put 0 and instead of a, I put 1 then it is the same table. This is an example of group isomorphism. So, I have this bijection $f : Z/2Z \to G$ where $f(0) = id, f(1) = a$. Then what we have is $f(x + y \, mod 2) = f(x) \cdot f(y)$. So these two groups are isomorphic.

Suppose I have 2 groups $(G, * : G \times G \to G)$ and $(H, \cdot : H \times H \to H)$ are *isomorphic* if there exists a bijection f from G to H, such that $f(x * y) = f(x) \cdot f(y)$ for all $x, y \in G.$.

What we have showed in the above example is that if you have any group with 2 elements then it has to be isomorphic to Z/2Z. Let us try this with 3 elements.

Example 5.
So, suppose you have a group with 3 elements- {id,a,b}.

Multiplication table for {id,a,b}	id	a	b
id	id	a	b
a	a	?	??
b	b	??	???

Now, can $a \cdot a = a ?$ Now the objection that we had earlier that a must have an inverse is no longer valid because you could have $a \cdot b = id.$ But by the cancellation I get a is equal to identity. So, I cannot have $a \cdot a = a$, I have to have $a \cdot a = b^{?}$, and similarly $b \cdot b = a^{???}$.
Now by inverse axiom which says that a must have an inverse (similarly for b), we have $a \cdot b = id^{??}$. Note that in general a.b is not always equal to b.a.
So if a group has 3 elements, then it is multiplication table has to have this form and this is exactly the same as the multiplication table of Z/3Z you calculated earlier. The bijection
$f(0) = id, f(1) = a, f(2) = b,$
is an isomorphism between Z/3Z and the abstract group {id,a,b}.

So, in this lecture we have seen:

- A group is a tuple (G, *) comprising a set G and a binary operation *, following the axions of closure, associativity, possessing an identity element and for each element of G possessing an inverse for that element.
- The uniqueness of the identity element, and for each element the uniqueness of its inverse are corollaries of the group axioms. Another corollary is cancellation.
- Some examples of groups: Integers under addition, Integers mod N under addition mod N.
- A group is completely defined by its multiplication table.
- Two groups (G,*) and (H,.)are said to be isomorphic if there is a bijection between the two such that $f(x * y) = f(x) \cdot f(y)$ for all $x, y \in G.$