NPTEL

NPTEL ONLINE COURSE

Introduction to Abstract

Group Theory

MODULE – 01

Lecture – 01 - "Motivational Examples of Groups"

PROF.KRISHNA HANUMANTHU

CHENNAI MATHEMATICAL INSTITUTE

I'm Krishna Hanumanthu from Chennai Mathematical Institute. I'm going to teach a course on abstract group theory over the next 8 weeks. My goal here is to introduce the basic ideas, give some motivation, and do some standard theorems in the subject, and to explain a little bit about why groups are very important in various areas of mathematics and even outside. So today I want to start off by first giving you some examples which I hope will motivate the definition, then I'll give you the definition and look at some properties.

Okay, so the course is on introduction to abstract group theory, okay. Groups are algebraic objects which abstract, as the word suggest, certain important features of well-known mathematical objects. So I want to do some examples which illustrate this, and in each example I want to point out the crucial piece of information that we want to retain, okay.

So the first and most important example of a group that we all know is the group of integers, so this Z is the symbol for this, so this is the set, let us start with this, it is the set of all integers, so integers are, for example these are all negative integers, 0, and positive integers so it's an infinite set, consisting of these numbers, okay.

Groups are sets along with a certain operation on them, so and the most familiar operation for us on Z is the addition, so what is this? Addition, we all know how to add two integers, and what are the properties of addition, let's try to identify this that we want to abstract out and define a group later, so what is the property of addition? So given any two integers we can add them and we get another integer, so if you add, if we add two integers we get another integer, so this is

the starting point, so we say that adding integer is the binary operation on the set of integers, so I'll define this in more formal setting later, but it simply means the word binary refers to the fact

that we add two integers to get a third integer, so for example if you add 3 and 2 you get 5, if you add 5 and -2 we get 3, so if you perform the operation of addition on two integers we get another,

the output is 1 integer, so input is 2 integers, operation is addition output is 1 integer, so that is the first property of addition.

So let's look at another important property of addition, there is a special element called 0, 0 is a special element, so what do I mean by that? So let me say 0 as a special element inside which is to say special in the following sense, if I add if N is any integers, so let us take an arbitrary element N, then if I do N+0 I get N back, which is also same as 0+N, 0 is the only integer with this property, if you add 0 to this N integer you get that integer back, no other integer has this property if you add 1 to an integer you do not get the integer back, so 0 is called the identity

element, identity element for addition, okay, so this is the second property. So remember again the first property was if you add two integers you get another integer, you have a special element that we call identity element which has the property that if you add this to any element you get the element back, you do nothing in another words.

The third important property that I want to identify is every element which in this case is an

integer, has an inverse. What is an inverse? Inverse is an element that you can add to get the identity element, so for example if you, what element do we want to add to 5? So we want to add something to 5 to get 0, what is that element? That element is obviously is -5, if you want to add something to -3 to get 0, you will add 3, more generally if you want to add –N to N you get 0, so this is an inverse, so inverse is the opposite so in some sense, if you add inverse to an element you get the identity element which I have already declared a special element called the identity

element. So every element has an inverse, so we have identified 3 properties of addition on integers, if you add two integers you get another integer, there is a special element called 0, and every element has an inverse.

Finally, I want to note the following property of addition, so remember addition is a binary operation, so in other words we can add two elements, if you add 3 and 2 you get 5, but we cannot add a priori 3 elements, how do you add 3 elements? What is the meaning of this?

Remember addition is only a binary operation, given 2 things we produce 1 output, but if you are given 3 things there are 2 possible ways of doing the addition, so if I asked you what is 3+2+5 you would first, one option is to combine 3 and 2 first, and then this now 3+2 is again an integer, and add 5 to it, so this is 3+2 in bracket, that means you apply the binary operation to 3 and 2 and for which you get 5, and then you add 5 so that gives you 10. But you can also do the following, you can first add 2 and 5, the point is to group two things together, in the first option I grouped 3 and 2, in the second option I'll group 2 and 5, so then I get 3+7 which is also 10, so I get the same answer.

So no matter how I group elements, I get the same answer which is very important, otherwise there will be an ambiguity on how to add 3 elements or 4 elements or 5 elements, so this is called associativity of addition.

Associativity means we can group things again I'll do this more formally later, but we can group, given 3 elements we can group 2 of them together in two different ways, and we get the same answer, okay, so this is the fourth property of addition on integers, so we can unambiguously add 3 elements so we can use the associativity property of addition.

So just to recall properties of addition on integers: one it is closed, so I'm going to use this word from now on, it is closed under addition which is, whenever we say a property is closed that means if I apply that property I'm within the same set so, if I take 2 integers in other words 2 elements of Z perform addition I land again in Z, there is an identity, the second property is there is an identity element, namely 0, this 0 is an identity element, every element has an inverse namely –N is the inverse of N, addition is associativite is the last property, so these are the four properties of addition on Z.

If you think about it a little bit there is another property of addition that I did not highlight now, but which we will come to later, so I'll record it here and we will come back to it later, another property of addition is, for example if I add 3+6, I get 9, which is same as 6+3, so the order in which I perform the binary operation, first 3 then 6 or first 6 then 3 I get the same answer, this is not such an important property as the first 4, but let us record this for the moment and then we will come back to it later, so this are the properties of integers, addition on integers that I want to record.

And I want you to remember that these properties while they are so obvious for addition they're not necessarily always true, for example if you take multiplication on integers, there is no inverse for multiplication if you think about it, because if you multiply, what is the inverse under operation of multiplication on integers, for example 2 has inverse 1 by 2 which is not an integer, so it's not clear that these properties always hold.

So with that let's go to the second example, which again remember I'm trying to give three examples to motivate the definition of a group, so the second example that I want to give is the following, so this is not so obvious, but I would like you to pay close attention to this, so let's take the set consisting of 1, 2, 3, okay, so these are 3 elements, so I'm not going to use any

property of 1, 2, 3 other than that they are 3 different elements of a set, so you all know what is the bijection of this set so I'm going to consider bijections of 1, 2, 3. A quick recap of the definition of a bijection, what is the bijection? A bijection is a function from {1, 2, 3} to {1, 2, 3} which is 1-1 and onto, okay. 1-1 and onto are properties of functions of sets, 1-1 means two different elements of the domain, so this is the domain, this is the codomain, two different elements of the domain go to two different elements of codomain that's 1-1, onto means every element of the codomain is equal to, an image of something from the domain so codomain is equal to the range of this function. So for example, so I'm going to use this notation to denote functions, function 1 going to 1, 2 going to 2, 3 going to 3 is a bijection, clearly, because two different elements everything in the set 1, 2, 3 is in the image, so it's a bijection, it's in fact the identity map.

On the other hand if you send 1 to 1, 2 to 1, and 3 to 2 this is not bijection, because 1 and 2 are different elements that both go to 1, so it's not 1-1, of course also it's not onto, because 3 is not in the image, so I'm not interested in functions which are not bijections, so as I said bijection is a 1-1 and onto map.

Now I'm going a define a different set, so define, which I'll denote by S sub 3, S sub 3, the 3 refers to the fact that I have 3 elements in my starting set, so S3 is the set of all bijections from {1, 2, 3} to {1, 2, 3}. So this is the set of all 1-1 and onto functions from this set to that set, so this is my set now, so I started with the set 1, 2, 3 consisting of 3 elements 1, 2, 3 and I've defined a new set now consisting of all bijections from 1, 2, 3 to itself, so I would like to define an operation on S sub 3. But before that let me first list all the elements of S3 it's not very big, for example the function that I defined earlier as an example of a bijection 1 going to 1, 2 going to 2, 3 going to 3 is a bijection let's call that F1.

So what are the elements of S3? So I'm going to try to list all the elements of S3, so the first function because these are elements are functions, I'm going to use F with a subscript to denote this elements, F1 is 1 going to 1, 2 going to 2, 3 going to 3 so that's F1, this is in fact the identity function, meaning 1 goes to 1, 2 goes to 2, 3 goes to 3.

What are the other bijections? You can also send let's call it F2, you can send 1 to 2, and 2 to 1, 3 to 3. Note that this is also a bijection, because different elements go to different elements, everything in the set is a image, 2, 1, 3 are all in the image. And if you think about it what I have done is I've just interchanged 1 and 2 while keeping 3 fixed, 1 goes to 2, 2 to goes 1, but 3 goes to 3, similarly I can interchange, I can interchange 1 and 3 so that means I send 1 to 3, 3 to 1 and 2 to 2, nothing happens to 2, but 1 goes to 3, 3 goes to 1 so this I call F3.

What are some other bijections? So F3 is done, so now F4 let's say I interchange 2 and 3, so 1 goes to 2, 2 goes to 3, 3 goes to 2, so here I do not move 1, but 2 goes to 3, 3 goes to 2 that's F4.

Are there any other bijections? There are, for example if you take if one of the elements is fixed which is to say in this, in F1, F2, 1, 2, and 3 are all fixed, in F2 3 is fixed, F3 2 is fixed, and in F4 1 is fixed, if you think about it if an element is fixed, if a function fixes either 1, 2, or 3, it must be F1, F2, F3 or F4, so the remaining bijections if there are any, must not fixed anything so, and there are such things, for example 1 can go to 2, 2 can go to 3, 3 can go to 1, neither 1 nor 2, nor 3 is fixed so everything changes, so 1 goes to 2, 2 goes to 3, 3 goes to 1, and this is a bijection.

Similarly F6 also does not fix anything, it sends 1 to 3, 2 to 1, and 3 to 2 that's also a bijection, and some thinking on your part tells you that this are all the bijections, there are only six of them, so S3 is the set consisting of F1, F2, F3, F4, F5, and F6, so I'm going to use these fixed specific definitions later, so please note that F1, F2, F3, F4, F5, F6 are the ones I define just now, so F1 is the identity element, F2, F3, F4 fix exactly one element of the set 1, 2, 3, F5 and F6 do not fix anything.

Now remember that when we look at the previous example of integers, the set was easier there, just the set of integers, but there we looked at addition, here what do you want to look at? So we want to get hold of an operation on this set, so in other words given two functions we want to produce another function, there is an obvious candidate to do this, we have all learned in school, if you take 2 functions we can compose them, in this case because the domain and codomain are the same we can always compose any two functions, so consider the operation composition of functions on S3. If you think about it, if you take 2 bijective functions and you compose them you get another bijective function, so it must be again in S3.

So let us just walk this out more concretely in a specific example, so for example if you do F2 circle F5, so remember composition is usually denoted by circle and in practice I'll just omit the circle and write this as F2, when there is nothing I'll read it as F2 composed with F5, so what does this do? Remember I apply F5 first then apply F2, F5 if you now see here, F5 sends 1 to 2,

and F2 if you look at the previous page F2 sends 2 to 1, so F5, F2 composed with F5 sends 1 to 1, because F5 sends 1 to 2, and F2 sends 2 to 1. Similarly you can just look at this 2 goes to 3 under this, and 3 goes to 2 under this.

And remember if you look back at the list of elements that we have listed in S3, this is nothing but this is same as F4, so this is an example of a, what I mean by the operation being closed, so if I take 2 functions, F2 and F5 in S3 I compose them I get another function of, another element of S3.

Now let's do F5 composed with F2, now remember I first apply F2 and then I apply F5, and if you do this as before you can quickly check that this sends 1 to 3, 2 to 2, and 3 to 1, and this is

same as F3, if you recall when I did the example of integers I did, I noted that after listing the 4 important properties I said that integers also have a fifth property, namely the order in which I apply addition does not matter, when I add 3 to 5 I get 8, but when I add 5 to 3 I also get 8, and as this example suggests as the new example suggest order does matter here, if I do F2 composed with F5 I get F4, whereas if I do F5 composed with F2 I get F3, so order in which I compose gives me different results, so however I can say that composition is a binary operation, so I'll say composition, so composition is a binary operation which is same as saying, this is same as saying that S3 is closed, see note that I've not proved this, I've only checked that the composition is closed at least for 2 elements, I have 2 composed with F5 is again a S3, F5 composed with F2 is also in

S3, but here I am saying that if you take any two elements compose them I get another element of S3, and this is an exercise that you can do and maybe later I will tell you how to do this, it's not clear but this is an easy exercise that composition of two bijections is also a bijection. This is the exercise that will make justify the statement that composition is a binary operation on S3 or that S3 is closed under composition, because if I, what is S3? Again let's recall, S3 is the set of all

bijections from the set {1, 2, 3} to itself, so if you composed two elements of it, in another words if you compose two bijections you get another bijection from 1, 2, 3 to 1, 2, 3, so S3 is closed under composition, so S3 with composition has the property that integers with addition have, so this is the first property remember.

What is the second property? There is an identity, again recall, in the first example 0 is the identity element of Z under addition, here what is the identity element of S3, it is simply F1, remember F1 is the identity function from 1, 2, 3 to 1, 2, 3, so for example F2 composed with F1 is F2. Similarly F3 composed with F1 is F3 and so on. This is clear because F1 is the identity element, so composing with F1 does not change the function at all, so there is an identity element.

Now the third property, interesting property, is there an inverse? Is there an inverse for every element of S3? There is, for example if you do F1 composed with F1 which is often for convenience of notation denoted as F1 squared, what is F1 composed with F1? If you now go back and see, if you go back and see F1 sends 1 to 1, 2 to 2, sorry actually I don't want to do F1

squared, F1 squared is simply F1 that is obvious, I want to do F2 squared, what does F2 squared do? 1 goes to 2, but 2 goes to 1, so F2 squared sends 1 to 1, 2 goes to 1 under F2 but by repeating F2 we get 1 goes to 2, so 2 goes to 2 under F2 squared, and 3 anywhere does not move under F2 so 3 goes to 3 under F2 squared also, so what I want to do is, F2 squared is F1, similarly if you

quickly check F3 squared as well as F4 squared is F1 which remember is the identity element from the previous page, remember that F1 is the identity element, and in an inverse is an element

such that when you multiply, I use the word multiply here but I should really use composed, if I compose F2 with F2 I get identity, if I compose F3 with F3 I get identity, if I compose F4 with F4 I get identity.

What is an inverse for F5? If you go back to the definition of F5 you will see quickly a simple calculation tells you that F5 composed with F6 is the identity element, because you have the definition of F5 and F6 here, 1 goes to 3 under F6, 3 goes to 1 under F5, so under F5 composed with F6 1 goes to 1, similarly 2 goes to 2, and 3 goes to 3, so F5 composed with F6 is F1, so in other words, in words F6 is the inverse of F5, and also F6, F5 is the inverse of F6, so every element has an inverse.

And the fourth property is the composition of function associative? which it is, composition of functions is associative, this is something that you perhaps have done in the past, it's an easy check that if you compose two functions and then compose the third function is same as this,

okay, so composition of functions is associative, so that comes easily here, so again the upshot here is S3 which was defined to be the set of bijections from {1, 2, 3} to {1, 2, 3} namely F1, F2, F3,

F4, F5, F6 under the composition is closed under composition there is an identity element, every element has an inverse and composition is associative, so and I want to point out that the operation here is composition, it's not addition like in the case of integers. So one more quick example I want to do, third example before we formally define groups.

Third example which is also one of the motivating examples for groups is the following, so consider an equilateral triangle, so what is an equilateral triangle, so this is a triangle with all three sides congruent, so roughly it looks like this, so I want to consider rotational symmetries of this, so what do I mean by rotational symmetries? Rotational symmetries are the following, so I

want to rotate the plane on which this triangle lives, and the rotational symmetry 1 is one where after, if I perform a rotation I get the triangle back, so rotations happen around a point, so let's say I rotate around the point in, median point of this triangle, so and rotation is always determined by an angle, so if at home you can practice this by cutting out an equilateral triangle from a paper and just rotating it, so if you rotate, let's call this side vertices A, B, C, if you rotate what rotations preserve the triangle, so this labeling is just for convenience, that's not part of the data for equilateral triangle, if I rotate what happens? So for example if I rotate by, so let say I'm rotating anti-clockwise, if I rotate by 90 degrees you can quickly see I do not get the, so this is the starting point, this is the starting triangle, if I rotate by 90 degrees I get something like this,

roughly something like this, so C will move here, A will move here, B will move here, this is not same as, clearly this is not same as, not same, 90 degree rotation, okay. So this is actually, yeah, this is not a symmetry.

So I don't want to spend lot of time on what are the rotations which preserve the triangle, but the following happens, so if you rotate by 120 degrees, or rotate by 240 degrees, of course you can also rotate by 360 degrees, which means we are not doing anything, these are the rotational symmetries of an equilateral triangle, so let us denote these by some names, so for example I call this R1, I call this R2, I call this R3, and let's take the group or the set G to be {R1, R2, R3}. I'm doing this example so that you get an idea of different kinds of groups that we encounter in mathematics, so this is the set, and this set is simply the set of all rotational symmetries of an equilateral triangle.

And as the previous two examples already indicated, we need an operation on this set, what is the operation? Operation is again composition, so operation is again composition so I can compose two rotations and if you think about it, if you compose two rotations you get another rotation, in this case it's very simple if you rotate first by R2, and then by R3 if you first rotate by 120 degrees and then by 240 degrees, remember I usually do not write the composition symbol, first rotate by 120 degrees then by 240 degrees, cumulatively I'm doing a rotation by 360 degrees, so I get R1.

Similarly if I do compose by 240 degrees, sorry 120 degrees then again by 120 degrees then I'm composing by 240 degrees, so I get R3. Similarly R3 composed with R3, if I compose by, rotate by 240 degrees then by 240 degrees so I'm rotating by 480 degrees which is rotation by 120 degrees, so it's R2, so as you can list all the possible binary operations, so composition is a

binary operation on G, so the first property is true. Second property is that there is an identity, namely R1, remember R1 is the rotation by 360 degrees or 0 degrees, performing it does not do anything so R2 composed with R1 is R2, and R3 composed with R1 is R3. Every element G has an inverse, has an inverse, as the previous page shows R3 composed with R2 is R1, so R3 is the inverse of R2, and R2 is the inverse of R1, and as again as before composition is associative, just like the second example composition is associative, composition of functions is always associative so that comes here for free, so again just like the examples 1 and 2, the third example also we have our set G on which composition is a binary operation, there is an identity element, every element has an inverse and composition is associative, okay, so these three examples I hope give you some motivation to study groups and I'll stop my first video now, in the second video we will formally define groups and look at more examples.