NPTEL

NPTEL ONLINE COURSE

Introduction to Abstract

Group Theory

MODULE – 01

Lectwure – 02- "Definition of a group and examples"

PROF.KRISHNA HANUMANTHU

CHENNAI MATHEMATICAL INSTITUTE

So in the previous video we saw some examples of sets with operations, we haven't yet define what a group is, so these were sets with operations, for example the first one was integers under addition, the second one was the set was the bijections from {1, 2, 3} to {1, 2, 3} under composition, and the third example was rotational symmetries of an equilateral triangle, so in all these examples we saw that the binary operation at certain properties.

So hopefully those examples motivated the definition of group, go ahead and formally define a groups, so this is the definition of a group, which is the object that we will study in this course, okay, so this should now be clear after the examples that we have done, so a group is a set, let's say G, we denote groups by usually G, with a binary operation, so what is a binary operation? So it is a function from G x G to G, so it is just a mathematical way of writing, what we discussed in the previous video, so given two elements of the group, so G x G is the set Cartesian product of two sets, so elements are pairs of elements of G, there is a way to produce another, just for clarity let me use star as my operation, though in practice we will not use this, so star is the binary operation.

So remember that binary operation definition already includes the statement that the operation is closed, because you take two elements of the group G, perform the star operation you get a third element of the group, g1 star g2, satisfying the following properties, remember that the examples that we studied in the previous video, the operation had four properties, namely that it is closed or that it is a binary operation, that's already listed here, so the remaining three properties are there is an identity element which is denoted usually by e, what is the property of the identity element? g star e is equal to e star g and you must get g back, so remember this is exactly the identity element that we studied, 0 was the identity element for the operation addition on integers, but we want to insist that whether you compose g with e or e with g you get g back, so that is the first property.

Every element g of the group set G has an inverse, which is, if g is an element there is something called g inverse, we denote this by g inverse, so the inverse is denoted by g inverse that's just convenience, what is the property of g inverse? g star g inverse is same as g inverse star g and you should get the identity element back, okay, so remember that first identity element must be there then inverse can be defined.

And what is the third property of the binary operation? Star is associative, which is to say that g1 star g2, star g3 must equal g1 star, g2 star g3, this is true for all elements g1, g2, g3 in G. This is true for every triple of elements of the group, so then we say that the operation is associative, so remember we always have to emphasize that a group is a set G along with a

binary operation, a set itself is not a group, binary operation is important to define a group, so we say the correct way to say this is G, star is a group, that's all, so a group is a set along with a binary operation star which admits an identity every element of the set has an inverse and the operation is associative, so G star is a group, so again let me emphasize star is important.

So examples, let's look at examples, remember that in the previous video we looked at some examples, and my goal has been always to abstract the key properties in those examples, and the key properties in this examples was the operation was closed namely it is a binary operation, there is an identity element and every element has an inverse and it is associative, so I have abstracted out those properties and defined a group, this is what we now call an abstract group, so "abstract" refers to the fact that it is not specific, it's not integers that you are used to, it's not functions that you're used to, it's not real numbers that you are used to, the set along with the operation has no structure other than that imposed by this operation and these properties, that's why it's an abstract group, so integers with addition is a group, this is our first example in the previous video.

Similarly S3 along with composition is a group this is composition, so plus is the addition of integers, S3 with composition of functions. Similarly I defined rotational symmetries of an equilateral triangle that we call G earlier and again there the operation was composition, so these three are examples of groups.

And as I said the operation is important to this, but whenever if there is no confusion, in other words if the operation is clear from context .we write G is a group, instead of, okay, so it is simpler sometimes to write that G is a group instead of specifying the operation because sometimes we don't need to specify the operation if you are looking at an example or a problem, operation is clear from the context, okay, so I want to today discuss more examples. We have

already three examples, I want to discuss more examples so that we have a collection of groups in mind before we study properties of these groups, let's first look at some more examples.

Some obvious ones to begin with, so let's take Q, these are standard notations that I'll use throughout the course, so this is the set of rational numbers, and under addition this is a group, just like integers under addition is a group, rational numbers under addition is a group, and the proof is similar, remember a group is a set with binary operation. In the case of Q the binary operation was addition, so you can add two rational numbers, keep in mind that if you add two rational numbers you get another rational number so it is a binary operation on the set of rational numbers, there is an identity element namely the 0 element, so that's an identity element, every element has an inverse, what is an inverse of 1 by 2? It's -1 by 2 so addition on rational numbers has an inverse, and addition certainly is associative, so Q with addition is a group. Similarly R which is the set of real numbers, as I mentioned these are going to be my standard notations, Z refers to integers, Q with this bar here refers to rational numbers, R refers to real numbers, and just like before R, + is a group, exactly for the same reasons, you can add two real numbers, you get another real number. Similarly if you take the set of complex numbers, it's also a group under addition.

As you can see, unless you mention a possible binary operation the question of a group does not arise, so you have to mention what the operation is, so under addition which is very familiar to us, Z, Q, R, and C are all groups. Now let me ask you something, so let me study possibility of groups under multiplication, so usual multiplication so, is for example, Z a group under, we have seen this in detail in the previous video, it is a group under addition, but now I'm asking, is it a group under multiplication, remember multiplication is a operation that we can perform on integers. First property, is it closed? Here you have to ask yourself if I multiply two integers, do I get another integer, yes, that's okay, so of the required 4 properties the first property is okay, multiplication is closed, because multiplying two integers, so if we multiply two integers, we get another integer, so that's okay. The second property is, is there an identity? Okay, so this is where things get tricky, is there an identity element for multiplication? Think for a second, it looks like there is, how about 1, the integer 1? So it looks like it is a multiplicative identity, so if you do 3 times 1, this dot here for me is the symbol for multiplication, is 3. Similarly 5 times 1 is 5, 100 times 1 is 100, so is 1 multiplicative to identity? Actually it is not, it's almost a multiplicative identity but if you do 0 times 1, you get 0, so yeah, so actually it is a multiplicative identity, that's not a problem, so 1 is a multiplicative identity.

What about inverses? So here is where we have a problem, as I mentioned in the first video briefly, what is an inverse of 2? What is the inverse of 2? Remember, inverse of 2 under

multiplication, so here I am interested in multiplication, additive inverse is -2 that was okay, because under addition Z is a group and 2 has inverse, if you recall 2+ -2 was 0, but what is the multiplicative inverse? You have to remember that definition of an inverse in a group, what is the definition of an inverse? It is an element which has the property that if you perform the binary operation you get the identity element, we agreed that, 1 is the multiplicative identity, so which number can you multiply with 2 to get 1, so 2 times something should give 1, so what is that? Certainly that has to be 1/2, but 1/2 is not an integer, okay, so in other words inverses do not exist in Z for multiplication, they do exist for addition, so inverses do not exist in Z for multiplication, so Z under multiplication ,this is multiplication, is not a group, okay, so Z under addition is a group, but Z under multiplication is not a group, okay, so fine. Z is not a group, because inverse is do not exist 1/2 is not an integer, okay.

Now let's enlarge our set, so what about Q, under multiplication? Q under addition of course as we saw earlier is a group, what about under multiplication? See here the problem of the integers does not arise because 2 has an inverse now, namely 1/2, so 1/2 which was not an integer earlier is nevertheless a rational number, so 2 has an inverse, remember inverse is must exist in the set, again I go back to the definition of a group, every element g of G has an inverse, g inverse which is again an element of the group G of the set G which has this property, for integers that is not the case under multiplication. For rational numbers 2 has an inverse, but there is still a problem, what is that problem? What is that? 2 has an inverse, but 0 does not have an inverse, why? Because if you do 0 times anything and remember to be an inverse of 0 we must multiply with something to get 1, but this is not possible, because if you multiply anything with 0 you get 0, you can never get 1, so Q under addition, sorry Q under multiplication is not a group. Again Q under addition is a group, but Q under multiplication is not a group because it seems very close to being a group, because it is closed under multiplication certainly because if you multiply 2 rational numbers you do get

another rational number, there is an identity element namely 1, and almost all elements have inverse, in fact every element other than 0 has an inverse, and certainly multiplication is associative always, so but still it's not a group because one element has no inverse, but if you remove 0 from it, let's denote Q star to be the set of nonzero rational numbers, in other words in the notation of sets this is R, okay, so let me denote like this, this is Q – the element 0, if you take nonzero rational numbers under multiplication they form a group, is it clear? Because remember the only problem that we encountered in making Q under multiplication a group is that 0 has no inverse, 0 does not have an inverse, but I've removed 0 here, 0 is not in Q star, so we don't ask for its inverse. Now if you take a rational number if r is in Q star, inverse of r, remember which we denote by r inverse is simply 1/r, so it is now well defined because r is not 0, so Q star is a group, so I'll let you go back to the definition and think a little bit if needed to convince yourself that Q star has all the required properties, there is an identity element namely

1, every element has an inverse and multiplication is definitely associative, okay, so Q star under addition, multiplication is a group.

And similarly R star which is as before set of nonzero real numbers, similarly C star set of nonzero complex numbers are both groups under multiplication, because star means we have removed 0, these are nonzero real numbers, nonzero complex numbers, and just like in the case of rational numbers if I remove 0, multiplication becomes a group because every nonzero

element has an inverse under multiplication, identity element is still 1, multiplication is definitely associative, so these are groups, but I want to remark that Z star which is the set of, if you define it like this nonzero integers, Z star under multiplication is not a group, because here there was a problem with even nonzero integers having inverses, not just the integer 0, because even 2 does not have an inverse, so Z star is not a group, but R star, C star and Q star are groups under addition, I also want to discuss more examples coming from this rational numbers, real numbers, and complex numbers.

So quickly another example, if you define Q+ this is my notation, for positive rational numbers, similarly R+ positive reals, are they groups under multiplication? If you think about it, are groups under multiplication, because remember the multiplicative identity is 1 which is a positive real number or rational number, so 1 belongs to Q+ and 1 belongs to R+, so I'm defining R+ to be positive reals, Q+ to be positive rationals, we will keep using these in the course, they contain 1, and inverse of a positive real number is again a positive real number, inverse of a positive rational number is again a positive rational number, so and associativity comes for free because multiplication of numbers is associative, and closed also comes for free because if you multiply positive numbers you get positive number, so these are different examples of groups.

And I also remark once more that Q+ or R+ or Q star or R star or C star are not groups under addition, they are groups under multiplication but not under addition because what is the identity element for addition? As we have seen earlier it is the 0 element, but 0 is not in Q+ because it's not a positive rational number, it's not in R+, Q star, R star, C star do not contain 0 because obviously they are defined to be nonzero rationals, reals, and complex numbers, so they are not groups under addition, but they are groups under multiplication. These examples make it very clear that group operation is very important, obviously the name itself suggests that before you want to understand a some set is a group or not, the sets have no meaning, unless you ask for what is the operation, so under addition these are not even groups, under multiplication they're groups, okay, so it's important to keep in mind that when we specify a group we specify, we must specify a group operation, okay.