NPTEL
NPTEL ONLINE COURSE
Introduction to Abstract Group Theory
MODULE – 02
Lecture – 08 - "Subgroups"

PROF. KRISHNA HANUMANTHU
CHENNAI MATHEMATICAL INSTITUTE

Okay, so in this video I am going to talk about subgroups of a group, we have seen some examples of these already so I am going to define these and then we will look at examples and properties. So a subgroup of a group is simply, when I'll say it words first, a simply a subset of a group which has the properties of a group which has the properties of a group.

So let's fix a group, let's say G is a group, a subgroup of G, so let's say subgroup H of G is a subset of G, so to begin with it's a subset of G which has the following properties, which has the following properties. One, H is closed under the operation of, so this means remember that if A and B are in H this implies AB is in H. Remember this is really not always true, because if A and B are in H they are in G, so AB is in G, but here we want it to be in H again, so it's a condition on H, so it must be closed under binary operation of G, the identity element must be in H, and, three, if A is in H then A inverse should be in H, okay, so this is the subgroup, so that's all, so that is the definition of a subgroup.

The third condition here is saying that if an element is in H it's inverse is also in H, again remember that inverse is in G but it need not be in H, we want it to be in H, so I will only remark here, an easy remark, if H is a subgroup of G, then H is also a group under the same operation as, so if you focus your attention only on H it's actually a group because it has a
binary operation, same as the one of G, it has identity element, it has inverses, but the group has another property, right which is associativity, but remember that associativity comes for free in this case, because associativity holds in G, so if you get 3 elements A, B, C in G you can group them in any of the two ways to get the same answer, hence if 2 element, 3 elements are given in H, associativity holds automatically for them because they are elements of G, so it's also a group, we do not need to check for associativity separately, so some immediate examples and non-examples really.

Z is a sub group of Q under addition, so this is obvious, right, because under addition Q is a group to begin with, Z is closed under addition, it has 0, and it has inverses, okay.

So similarly Q is a subgroup of R or C again under addition. Q star which is remember nonzero rationals is a subgroup of R star or C star, these are nonzero reals, these are nonzero complexes, this is under multiplication. I am not checking this in detail but it's very clear, right, Q star is subgroup of R star because it is closed under multiplication, it has identity, it has inverses.

What about Z star? Is not a subgroup, for example of Q star, nonzero integers do not form a subgroup under of Q star under multiplication, because it is closed under multiplication, it has identity but it doesn't have inverses. See, note that the reason is same as the reason that we saw in an earlier video that Z star is not a group, so it can't be a subgroup of Q star.

Okay, so some more interesting examples, let's take the subset of Z consisting of even integers, so in other words H is 2N as N varies over Z, right, even integers are divisible by 2, so they are always multiples of 2 so you can write them as 2 times N, as N varies over Z. Is this a subgroup? Is this a subgroup of Z? Let's check one by one, what are the properties? Is even integers closed under the binary operation which is of course, I haven't emphasized here because it's clear generally I am considering Z under addition, so I take Z under addition and take H to be the even integers.

Are they closed under the addition of integers? Yes, if you sum two even integers it is even integer, right, is the identity element in the set H, yes, because 0 which is the identity element is an even integer. Similarly if N is an even integer it's inverse, what is the inverse under addition? It's minus, okay so minus of an even integer, it is yes, it is a subgroup and the reasons I'll not write this, but I'll just say that 0 is an even integer, sum of even integers is an even integer, negative of an even integer is an even integer, so even integers form a subgroup.

What about odd integers? So take the subset of odd integers, is it a subgroup, certainly it's not a subgroup because it's neither closed nor does it have an identity element, because you can have sum of two odd integers, and you get an even integer 3 + 3 is 6, 3 is odd but the sum of 3 and 3 is 6. Similarly 0 is not there so because 0 for example is not odd, so odd integers do not form a subgroup but even integers do.

What about this set 3N, N in Z? Earlier we took 2N which is the even integers, right, that's a subgroup we saw, what about odd, multiples of 3, so these are all multiples of 3, so this set is actually -6, -3, 0, 3, 6, 9, 12, and so on. That is this set, this is also a group, this is a subgroup of Z, because 0 is there, sum of any two things here will be again a multiple of 3, if you take 2 multiples of 3 and sum them, for example 3 + 6 is 9, which is also a multiple of 3 but more generally if you do 3N + 3N it will be 3 times N + M, so it is closed under addition, and negative of multiple of 3 is also a multiple of 3, so it is a subgroup of Z, more generally AZ which is by definition all multiples of A is a subgroup of Z for any A in Z, okay, so maybe I'll write that as a theorem or, let me wait for the theorem but why is the previous statement true? AZ is a subgroup for any A in Z, it's exactly the same reason as it is for 2Z and 3Z, remember this is nothing but 3Z, and even integers are nothing but 2Z, so all multiples of 2, so this 2Z is just my notation, more generally AZ is the collection of all multiples of A, it's a subgroup of Z for every small A, because if you take 0, N as 0, 0 is inside that so let me just check by one by one, so AZ is closed under addition, why? Because if you take AN + AM this is a multiple of A, this is a multiple of A, you are adding them you get A times N + M which is also multiple of A, so that is okay, AZ contains 0 certainly, because 0 is A times 0, remember AZ is all multiples of A, so you can take AN for every N in Z so in particular when you take N = 0 you get 0. And similarly AZ is closed, contains inverses that is because inverse of AN is A times – N, so that's also inside AZ, so AZ is, so these 3 points imply that AZ is a subgroup of Z. Now the theorem that I want to write and prove is that every subgroup of Z is of the form AZ for some positive integer, okay, so for some integer not positive, but some non-negative integer A, okay, so this is the theorem so I am, earlier before the theorem I showed that A times Z is a subgroup for every small A, but now I making the converse statement, I'm saying that every subgroup of Z is of the form AZ, this specific kind of a subgroup, this requires a proof, right, these look like specific kinds of subgroups, but why should every subgroup of Z be of that form, so let's prove this.

So how do I prove this statement? I am going to prove that any subgroup you give me of Z must equal AZ, where A is some nonnegative integer, so let me prove it by first starting with an arbitrary subgroup of Z, let's say H is a subgroup of Z. So we are going to first assume that, consider the case that H is 0, that's certainly a possibility right, 0 by itself is a subgroup of Z, if H is just 0, then is it of the form AZ? Yes, it is of the form 0, Z because this is 0 times N, N in Z that means this is just 0, so remember I'm allowed to take any nonnegative integer A, I'm going to take 0 in this case, if H consists only of the zero element it is 0Z which is of the required form, so that case is done.

So now, so suppose that H is not just the zero element, so H contains an integer N, right, which is different from 0 because H is a subgroup of Z, it is not just the single element 0 that means it contains a nonzero integer, yes, so it contains a nonzero integer. I claim that in fact H contains a positive integer, why is this? Why? Okay, so I first said that H contains an integer N nonzero, so let N nonzero be an element of H, I know that there is a nonzero element because remember I have assumed that H is not zero, H = 0 case I have already settled, so H is not equal to the single element 0, so it contains an element N of which is different from 0. If N is positive we are done, we are done in the sense that we are done with this statement, I'm trying to prove that it contains a positive integer, so N itself is positive we are done, if N is less than 0 remember N is different from 0 so N is either strictly more than 0 or strictly less than 0, if N is less than 0, – N is positive, right, if N is less than 0, – N is greater than 0, but I claim that since N belongs to H, – N also belongs to H, why is this? This is because H is a subgroup, this is where we have used the fact that H is a subgroup, remember if you recall the definition of a subgroup, if A belongs to H, A inverse belongs to H, the inverse of A belongs to H. In my example, I'm working with Z under addition so inverses are negatives, if N is H, so N is an H, -N is also in H, so if

N is negative, – N is positive. So I have justified this statement here that H contains a positive integer N.

Now define or let A be the smallest, this is a very important argument, you should pay close attention to this, this comes up a lot in algebra, so I have first said H contains a positive integer, now I'm going to take this smallest positive integer contain in H, remember that H contains perhaps lots of positive integers, but there will always be a smallest positive integer because any set of positive integers has a smallest element, so if you take the set of positive integers in H it will contain a smallest element, so I take A to be the smallest positive integer in H, so how do I get A? So I'll start with 1, is 1 in H, if not I'll go to 2, is 2 in H, if not I'll go to 3, if 3 is not in H I'll check with 4, otherwise I'll check with 5, because H contains a positive integer at some point we will reach a number which is in H, the first time we reach that is the smallest positive integer that's in H, so I'll call that A.

Then we claim that H must contain only multiples of H, A is my claim which also proves the theorem, so why is H = AZ? So now let, let's say B is a positive integer in H, so let's say, let me write it like this, let B in H and assume, okay, so let's say B is in H and assume B is positive, so I am going to consider this case. By the choice of A, what is choice of A? A is the smallest positive integer contained in H, B is some other positive integer contained in H, so by choice of A, we have B greater or equal to A, B could be A of course, but it can't be smaller than A.

So now we divide B by A, so you all know division, what does it mean? So if I divide B by A, I can write it like this, B = some A times some P + Q, so if I divide an integer by another integer, I'll have some reminder, what is the properties of this P and Q? P is in some, P is some Z, element of Z and Q the important property is Q is strictly between, sorry, Q is nonnegative but it is strictly less than A, see remainder is always less than A, correct, because if Q is more than or equal to A, I can further divide, okay, so I can keep dividing until the remainder is strictly less than A, so I have this.

Now this equation will translate to B – AP = Q, now let's observe this closely. B is in H, that is by hypothesis, A is of course in H because A was chosen to be, remember that A was the smallest positive integer contained in H, so we claim A is in H, B is in H again using the properties of a subgroup, so note that A is in H, so –AP is in H, because H is a subgroup, – AP, what is –AP? So actually if you want to do step by step, if A is in H, why is – AP in H? –AP remember is P times –A, I can write it like this, that means it's – A + -A + -A, P times. A is in H, so –A is in H, that is the property of a subgroup, if –A is in H, P times you add –A to itself that's also in H, so that's the proof for this. Similarly B is in H, that is also given, hence B –AP in H. So A is in H, -AP is in H, and B is in H so that B + -AP is also in H, so B – AP is in H, then Q is in H, right because B –AP =Q, so Q is in H. But now let's see something interesting happens, Q is in H but Q is strictly less than A, Q is strictly less than A, can Q be positive now? It cannot be, Q can't be positive, because Q is strictly less than A and A is the smallest positive integer in H, and Q remember is the conclusion at this point, is Q is in H, so Q can't be, if Q is in H and it is positive, and it is less than A, that violates the choice of A, A was chosen to be the smallest positive integer, so Q must be 0. Then if Q is 0 the remainder is 0, if Q is 0, this is 0, so B = AP, so if B is AP this means that B is inside AZ, see I have started with an arbitrary element of H which is positive and concluded that it is a multiple of AP, a multiple of A, I don't care what P is, it's just a multiple of A, that's what I am interested in, so every positive number in H is a multiple of A.

What about negative integer? So if, let say B is a negative integer, if B is in H and B is less than 0, consider –B which will be positive, -B is in H because B is in H, and H is a subgroup, -B is in H and by what we have already shown which is that every positive integer is a multiple of A, –B is a multiple of A for some P, but then B is A times –P, so B is also a multiple of, in other words, so we have showed that, shown that every element of H is a multiple of A, hence H is contained in AZ, remember AZ is the set of all multiples of A, every element of H is a multiple of A, so H is in contained in AZ, but clearly, because, two reasons, H is a subgroup and A is in H, A is in H because remember A is the smallest positive integer that's in H, so A is in H, H is a subgroup so twice A is in H, thrice A is in H, and hundred times A is in H, so all multiples of, positive multiples of A is in H, because A is in H, -A is in H and all positive multiples of –A are in H, so entire AZ is contained in H, so AZ = H, remember that's what we are trying to prove, so this completes the proof. This completes the proof of the theorem that we have every subgroup, so I think the theorem is here, what is the theorem, so let's see, every subgroup of Z is of the form AZ for some nonnegative integer AZ, for some nonnegative integer A in Z.

So this is very strong property of subgroups of Z, so I want to just make one more remark as I said this is an important proof, okay so in this proof as I said the proof is very important to understand, and just to make emphasize my point what we have really done is you take the integers, 0 is here, and I'm looking at a subgroup of Z, I have taken the smallest positive integer, so A is the smallest positive integer in H, so that means there is, between 0 and A there is nothing in H, so as you go from 0 to the right first time you hit H is at A, okay, so then next time you hit H is 2A, so there is nothing in between A and 2A that can be in H, that is because if there is something in between by subtracting A you land here, but then we know that there is nothing between 0 and A in H.

Similarly at the, next one is 3A, next one is 4A, so H must be only multiples of, so similarly between –A and 0 there can't be anything in H because if there was something here in H, it's negative will come here and that will violate the property that A is the smallest positive integer, so in some sense H must be just this made up of this multiples of A, okay, and nothing in between these multiples can be in H, so this is exactly what we have done. So subgroups of Z are particularly simple in this way.

One more remark. Every group has two obvious subgroups, right, no matter what the group is, it has two obvious subgroups. You can take E is a subgroup of G, definitely it's a subgroup of G because it is closed under the binary operation, there is just one element so if you apply E squared E cube it's all E, so it is closed under the binary operation, the identity is there inverses are there, so it is subgroup. Similarly, this is called the trivial subgroup, okay, so it is trivial but it has just E. G is also a subgroup, G is a subgroup of G also, because it is certainly a group, so and it's closed under the binary operation by definition it has inverses, it has identity, so it is the full group, so these are not interesting, so typically we are interested in subgroups which are neither the trivial subgroup or the full subgroup.

Online Editing and Post Production

Karthik

Ravichandran

Mohanarangan

Sribalaji

Komathi

Vignesh

Mahesh Kumar

Web Studio Team

Anitha

Bharathi

Catherine

Clifford

Deepthi

Dhivya

Divya

Gayathri

Gokulsekar

Halid

Hemavathy

Jagadeeshwaran

Jayanthi

Kamala

Lakshmipriya

Libin

Madhu

Maria Neeta

Mohana

Muralikrishnan

Nivetha

Parkavi

Poonkuzhale

Poornika

Premkumar

Ragavi

Raja

Renuka

Saravanan

Sathya

Shirley

Sorna

Subash

Suriyaprakash

Vinothini

Executive Producer

Kannan Krishnamurthy

NPTEL CO-ordinators

Prof. Andrew Thangaraj

Prof. Prathap Haridoss

IIT Madras Production

Funded by

Department of Higher Education

Ministry of Human Resources Development

Government of India

HYPERLINK "http://www.nptel.ac.in" www.nptel.ac.in