NPTEL

NPTEL ONLINE COURSE

Introduction to Abstract

Group Theory

MODULE – 01

Lecture – 06- "Problems 2"

PROF.KRISHNA HANUMANTHU

CHENNAI MATHEMATICAL INSTITUTE

I want to do some more examples, exercises again to illustrate properties of groups, so that you become comfortable with operating with groups.

So let me ask you a new problem, so here let's say G is a finite group, in this problem I'm working with a finite group, recall that in other words, remember what are finite groups from my earlier videos, G has only finitely many elements, so the problem is the following. So I'm giving you an exercise that I will solve in detail, so G is a finite group, I want to show that, show that for every element of G there exists a positive integer N such that A power N is identity, okay, so just a piece of notation because maybe I've not clearly defined this in the previous videos, when I write A power N will mean A star A star … star A, N times, whenever I write A power N I always mean this, because this is a short cut, so star is the operation, remember here we are working with an arbitrary finite group, and you will have to get used to thinking like this, it's not Z, it's not Q, it's not S3, it's not roots of unity, so it's not any specific thing, it's any group and the

problem should not use any specific properties of examples of groups, it must only use properties that all groups have, so here G is a finite group and star let's say is the operation, it's a shortcut, it's an easy notation instead of writing A star A star A star A always N times we will simply write A power N, so that is what I mean.

So now let's come back to the problem, it's asking you show that for any element A of G there exists a positive integer N such that when you apply A to itself n times you get the identity element, also remember E is the identity element, that is my standard notation for a group, E will stand for identity element, generally when I'm working with a general group E will stand for the identity element, so what is the solution to this? So G is a finite group, so we'll have to use that, so let's do the following, so consider, I'm going to consider the elements E, A, A squared, A cubed, A power 4, A power 5, like that and I can take A power 100, A power 101 and so on, so what am I doing this here? So I'm starting with identity that is you can think of identity as A power 0 always, that is again notation, A power 1 that means just A, A squared means A star A, then A star A star A, A star A star A star A, A star 5 times, 100 times, 101 times. Now these are all elements are, where are these living? All these are elements of G, why is that? Because, why is this? Because G is closed, I'll write G is a group, star is a binary operation on G right, so A is in G, remember A is in G that is starting point, A is in G so A squared is in G, A cubed is in G, A to the 4^{th} is in G, A to the 5^{th} is in G, A to the 100 is in G,A to the 101 is in G and so on, so these are all elements of G, but remember that G is a finite group, we are going to use this very important hypothesis, G is a finite group.

And here we have seemingly infinitely many elements, right, because you have A, A squared, A cubed, A power 4, you can keep doing this, you can do A power one thousand, A power ten thousand, A power one lakh and so on, but how do you justify this? Now G is a finite group, and these are all elements in that finite group and they are seemingly infinite but they cannot be infinite, so what is the implication here? So for some positive integers N and M, we must have, right is it clear, because this number, this elements A, A squared, A cubed are all different that will be a infinite set contain in set G which is a finite set, which is impossible, which is an absurd statement, so this cannot be an infinite set, which means there must be repetitions, if this is not infinite set then some two elements in fact many of them will collapse, so I am just saying that for some positive integers N and M and of course I have to insist that N is not equal to M, otherwise A power N is

certainly equal to A power M, so for some positive integers N and M which are different, we must have this.

Again, if not, if this does not happen then A power N is different for each N, and this set A power N, the set consisting of all powers of A is an infinite set, living inside a finite set giving you a contradiction, so A power N is equal to A power M for two different positive integers. Because N is not equal to M we can assume without loss of generality that N is strictly more than M we can assume that because one of them is bigger than the other, we will simply say N is bigger than M, then let's now play with group properties, so we have A power N equals A power M, so let's multiply this with A power – M. Okay, now again what is A power – M? If you are confused about this, I'll make a remark here, what is A power – M? It is just a short hand for, you take A power – M is by definition you take the inverse of A and write it like this, okay, so it's convenient to write this element as A power – M, so this is just notation, so this is notation, instead of writing A power -1 power M always so here what we are really doing is, so let me just, because I'm doing this for the first time, I'll just for clarity multiply both sides, so in other words I have A power N, A power M, I get A power M, but now let's see what happens, so this is now let's recall what is a definition of A power N, so this is N times, A power – 1, so this is really again star, in general the operation is star, so A power – 1 star, A power -1 M times, so that is the left hand side.

On the right hand side we have A power M, which is A times, A times A M times, star A inverse, A inverse also M times, right, so this is just expanding these terms, so but this is you can cancel this, what is the right hand side now? You have A times A inverse which is identity so that will cancel, the previous one will cancel with this and finally this will cancel, because this is exactly the same number, this is M, this is also M, this is E, this is E, and here but we are assuming remember N is strictly more than M, so we can't cancel all of them, so we can cancel M of them, so cancel M of them what will be left on the left hand side? We cancel M copies of A on the left hand side using A inverse, so then what will be left with? Is A star A, so this is, left hand side is E, right hand side is, after cancelling M copies of A from here, how many will be left with? We will be left with N – 1, M copies, okay, so that means A power N – M is E, okay.

Let's go back and see what the problem asked us to do, we asked, problem asked us to do, given an arbitrary element of the group there exists a positive integer N such that A power N is E, did we get that? Yes, we got that, because N – M is a positive integer which is a positive integer by the assumption that N is strictly more than M, and we did get a positive integers such that A power that is E, so we have solved the problem, so I hope this calculation here is clear to you, maybe just a quick calculation I mean if you in case you're confused about this, I just want to do it with specific numbers, so let's say N is 3, and M is 2, and just N is 5 and M is 3 let's say in the previous example, so that means A power 5 is equal to A power 3, I'm multiplying with if you go back and see I'm multiplying with A power -1 whole power, the smaller one which is M, so here I get A power 5 times, A power – 1 power 3 is equal to A power 3, A power -1 power 3, so that means I have a product of A 5 times so I'll cancel 3 of those, so I get A squared and here I get E, so this is just specific example so that you get understand this, so we have solved a problem, we have solved the problem which asked in a finite set this happens.

Remember that we have crucially used the finiteness hypothesis, because we want to say that this set is not finite, because it's inside a finite group, it's not finite and hence there must be repetitions, so it must happen like this, okay.

And if you can see this is not going to be true, this is not true if G is not finite, for example we take, let's say G is Z and we take the element 1 and G, so Z is under addition, okay, so I should, I should mention this because Z has, it's just a set in order to make it a group we will take the addition. If you take 1 in G remember the notation that I've been using is A power N, that is just A star A star A, N times, here the operation is addition so it's a bit confusing to think of that power notation in terms of addition, here spelling out exactly does there exist a positive integer N such that 1 + 1 + … + 1 is the identity, remember A power N is E, so that means we want A star

A star A, N times does there exist something like this, so 1 + 1 + 1, because the addition is the operation here, and the identity element is 0, does there exist something like this? Certainly not, because right, this is because 1 + 1 + 1…, N times is actually N, but N can't be 0, you're asking for M to be positive, so N can't be 0, so it's not true if G is not finite, this property is very specific to finite groups.

So just I'll end to this video with one more example which is very similar to this, so a different problem now. Let's say G is a finite group again as before, show that there exists a positive integer N such that A power N is E for all, okay, so if you read the problem carefully, let G be a finite group, show that there exists a positive integer N such that A power N is E for all A and G, what is the difference between this and the previous problem? Here I am asking you show that for a given element is A, there exists a positive integer N such that A power N equal to A, so this N has to be chosen after I get A, so it can depend on A, in the new problem I'm asking for an N which works for every element of G, so N in particular should not depend on A, but this is now easy given that we have already solved the previous problem. So solution, by the previous problem for any A in G there exists a positive integer, let me now call it N sub A, because this positive integer from the previous problem depends on A, so let's call it N sub A such that A power N sub A is 1 or rather E, okay, remember this is the content of the previous problem, there is a positive integer NA such that A power NA is E.

Now we have one such positive integer for every element of A, every element A of G, but again let's use the fact that G is a finite group, so we have NA for every small A in G, so now I simply define N to be maximum or rather let's say product NA, A and G, so this is like if G is A1 up to AR, G is a finite group right, so I'm defining it to be NA1, NA2, NAR, for every element of the group there is an associated positive integer, I'm taking the product of those positive integers, now I claim that this N will have the required property.

We claim that this N works, in other words that is A power N is E for all A in G, why? Why is this true? This is clear if you think about this for a minute, so N remember is NA1.. NAR, right, so now if you take A power N, A is equal to one of the AIs, so A power N is A power NA1.. NAR, okay, but let's say A1 = A, just for simplicity, okay, so actually let me, A1 power N, so I have A1 power this, right, because N is equal to this, but if you now think about this it is, what is this? This is A1 star A1 star A1, how many times, it is NA1, NA2, NAR times, okay, so you can now combine this in NA1 times, okay. And then combine this again in NA1 times like that, so what I am saying is, so because this number is divisible by NA1 I can break up this huge product into smaller products, each one consisting of NA1 times, but remember A1 power NA1 is identity, that is how NA1 was chosen, so this is identity, this is identity, this is identity, so the content of all this is that you can use the usual exponential rules, that means this can be written as A times NA1 power NA2, NAR, okay.

Usual exponential rules that you've learned in school say that this is equal to A1 power, the product of these two, but A1 power NA1 is E, and E power anything E is E, so this is the shortcut of the proof, okay, but the proof of this is this, because I'm using the exponential rule as a, exponents as a notation, I can't use exponential rules that I have from integers and real numbers, and rational numbers, I have to justify that, which this does. So maybe I'll leave this as an exercise for you, if A power N is identity and N divides M, then A power M is also identity, so this is an exercise which I have essentially done here, but maybe not in great detail so I would like you to all, I would like all of you to do this carefully, if A power N is identity, and N divides M, A power M is also identity.

So now given this exercise if you accept this, the problem is solved, so we did get a positive integer globally independent of elements of A such that A power N is identity. So this I'll end this video with this and in the next video I'll do one more problem in a lot of detail, and then we will continue our study of groups.