NPTEL
NPTEL ONLINE COURSE
Introduction to Abstract Group Theory
MODULE – 02
Lecture – 07 - "Problems 3"

PROF.KRISHNA HANUMANTHU
CHENNAI MATHEMATICAL INSTITUTE

In this video I want to do one problem in detail which is very useful to understand basic notions of group theory, because many of the properties that we have so far learned are used in this problem, and if you understand this problem fully it is very good and it will tell you that you've understood everything that has so far been covered.

Okay, so the problem that I want to discuss in this video is the following. Show that any group G of order less than or equal to 5 is abelian, so that's the problem. So I'm going to recall some terms here that I covered in earlier videos. What is the order of a group? So recall that if G is a group and actually, if G is a finite group, G is a finite group, the order of G, which is denoted by this symbol G within bars, is the number of elements in G, okay, so order of G is the number of elements in G, so in the problem the question is to show that every group which has order less than or equal to 5, meaning any group which has 5 or fewer number of elements is abelian. And what is abelian? G is abelian if AB = BA for all A, B in G. So we say that A and B commute, so this symbol that AB = BA, in words means that A and B commute with each other, which is to say that the order in which we multiply them is irrelevant for the final answer, so G is abelian if every pair of elements in the group commute with each other.

And this is the property that groups have and not every group is abelian that also I want to recall before we get to solving this problem, if you recall the group S3, symmetric group on 3 letters is the group of bijections of a 3 element set, which we denoted by 1, 2, 3, and if you recall in the earlier video where I discussed S3 in detail, we actually listed all the elements of S3 and understood some facts about these elements, we saw that order of G was 6, and S3 was not abelian, okay. So if you go back to an earlier video you will see that we have explicitly showed that there exist two elements in S3 such that they don't commute, okay, so that S3 is not abelian and it has 6 elements, and the problem asks you to show that any group which is smaller than that, meaning having 5 elements or 4 elements or 3 elements or 2 elements or 1 element must be abelian, so the smallest group which is not abelian is of order 6 which is S3.

So now let's go ahead and solve the problem, so let's solve it, so the basic idea of the solution is the following, we are going to show essentially that, if a group has 5 elements or less there are just not too many elements, just not enough elements for a pair to not commute with each other, okay remember that if a group is not abelian it must be the case that there exists two elements that don't commute with each other, so maybe I should write this, so if G is not abelian because the definition remember is that if G is abelian if, so the definition is that G is abelian if you give me any pair of elements A, B in the group AB = BA, this must be true for all elements A, B, so what is the contrapositive of this? If G is not abelian there exist two elements, let's say A, B, in G which don't commute with each other, so such that AB is not equal to BA. And the goal for us in this solution is to show that if a group has 5 or less number of elements it cannot have just that's not is, 5 is too small a number to admit two element which have this property, which don't commute for each other, so we are going to consider 5 cases, we note that a group is a nonempty set, because a group has to contain the identity element, that's one of the properties of a group, so group has at least one element. In our problem we have to show that any group which has less than or equal to 5 elements is abelian, so we will consider cases, so first case order of G is 1, if order is 1 that means there is exactly one element in G and every group must contain the identity element so it must be E, and this is certainly abelian, why? You can see this, this is very easy to see it's abelian because in order to be not abelian there must be two elements which don't commute with each other, but the G has only one element so there is no question of having two elements which don't commute with each other, so this is okay, this is very easy.

Case 2, order of G is 2, so let's enumerate these elements, so as I said earlier every group contains E, so that must be the identity is one of the elements, okay. Now in this case there is one more element which we will call A, so that means E and A are the two distinct elements of this group, so note that in particular we have A is different from E, right, because G has two elements one is E, the other we are calling A, so certainly A is different from E.

Now if G is not abelian, again let me remind you if G is not abelian there exist two elements which don't commute with each other, in this case if G is not abelian that means E and A do not commute with each other, but that's certainly not the case, I mean E and A do commute with each other, because every element in a group commutes with identity, right, so recall that in general any element in a group commutes with the identity element. So EA is, that is part of the definition of a group that A, which are both individually equal to remember A, so G is abelian in this case also, right, because the only two elements are there and they commute with each other, so G is abelian, so in this case G is an abelian group, so we are done with order 1, order 2, we have to still consider order 3, 4, 5.

So case 3, order is 3, by the same convention as in the previous case, I am going to enumerate and give names to the elements E is one element that is the identity element, let's pick A as the second element, and let's pick B as the third element. So as before we have E, A, B are distinct elements. In other words A is different from E, B is different from E, and A is different from B, G has 3 different elements and I'm calling them E, A, B, E is the identity element, A and B are non-identity elements.

Okay now again if G is not abelian it means that there exist 2 elements which do not commute with each other, so only possibility in this case must be A and B, because A and E commute and B and E commute, the question is do A and B commute? Do A and B commute? So let's do the following so let's look at what can be AB, so what can be AB? By which I mean, remember G is a group, and I have given already names to its 3 elements, G is a group of order 3 and I have already given names to its 3 elements, I'll call the identity by E, the other two elements by A and B, but G is a group and A and B are 2 elements, so AB must be in the group, AB is an element in the group, right, because we have a binary operation on the group, A and B are there, and when you perform the binary operation on A and B the output is again in G, so AB is an element in the group which is just E, A, B, so we have 3 possibilities, AB must be E, AB must be A, AB must be B, so either this or this or this, right, AB is an element of a group which has 3 elements listed as E, A, B, so it is either E or A or B, so can it be A?

Now I'm going to invoke a very important property that we have in a group, that we discussed in an earlier video namely, cancellation property, so if AB = A multiply both sides by A inverse, so we have A inverse AB, A inverse A. Note that A inverse is also one of the 3 elements but I don't need to actually consider which it is, it's AE, A or B, I don't care what it is, it is an element in the group so I can multiply by that, right. which is going to give me by associativity I can do A inverse A which cancels and I get B = E, right, so the cancellation property directly gives this, right, because if AB = A, A is nothing but A times E then I cancel A, I have just spelled it out but this is what we have, but is B = E? Certainly B is not equal to E because they are distinct elements, so this is not possible, so this is not possible I'll say that.

So AB cannot be A, similarly AB cannot be B because the cancellation property says B is equal to BE, I cancel B and I get A = E, right, but A can't be equal to this, this can't happen, this is not the case because the three distinct elements are called E and A and B, so A can't be same as E otherwise we would not have given it a new name so this can't happen, so AB must be E, but if AB is equal to B, AB = E rather, AB = E so this means that B is A inverse, remember that if AB = E, B is A inverse and automatically BA must be E, so A and B commute.

So the point here is that, the important point, just like I said earlier that every element commutes with the identity, an element and its inverse always commute with each other, that is the point, so in this case A and B are inverses of each other and they commute, so AB = BA. If AB = BA, then G must be abelian, right, because if G remember if G is not abelian there must exist 2 elements in it which don't commute with each other, in our case G is a group of 3 elements, E commutes with A, E commutes with B, only possible violation of abelianness is if A and B don't commute with each other but we've just concluded that, A and B commute with each other so G is abelian, so we are done with case 3.

So now case 4, so that means order is 4. So let me now do the following. so I'm going to write G as, okay, so G has 4 elements right, let's call them A, B, C, the non-identity elements are A, B, C, but now I will do the following, suppose G is not, actually let me take that back, so I don't want to list enumerate this elements at this point, so suppose G is not abelian, right, suppose G is not abelian. Then by the point that I mentioned at the beginning of the proof or beginning of the solution there exist A, B in G such that AB is not equal to BA. This is the definition of group G not being abelian, but now, G has only 4 elements, that's what we are going to invoke, what would be the elements of G? E is an element of G, and A, B are second and third elements of G must be, E, A, B must be 3 distinct elements of G.

Why are they distinct? See ,because A and B do not commute with each other, neither of A and B can be E, because if A is E, B and E will commute, similarly if B is E, A and B will commute, because every element commutes with E, and A, B do not commute with each other they are different from E. Not only that, A and B are also distinct, right, because if A and B are equal, note A must be different from B. Why is that? Because if A = B then what is AB? Then AB is just A squared, but that is also same as BA, so A and B commute, right, but I am assuming that A and B do not commute, so A and B must be different, so E, A, B must be 3 distinct elements of G, but G has only 4 elements, so there is room for only one more element and I claim that must be AB.

So now what must be AB? By the previous case, we have said that AB, so what can be AB? AB has to be E, can it be E? Let's explore that, can it be A? Can it be B? Okay, so can AB be E? If AB is E, A and B are inverses of each other, right, if AB is E they are inverses of each other and hence though they commute, but that's clearly wrong because I'm assuming that they do not commute, so AB can't be E, AB can't be A because of the same cancellation property that we discussed in the previous case, B must be E, but B is not equal to E so that can't happen. Similarly in this case A must be E which can't happen, so AB, so the conclusion is, so we conclude AB must be the fourth element of G, so G must be E, A, B, AB, right because we already have 3 elements E, A, B, and AB can't be any of them, AB can't be E, AB can't be A, AB can't be B, so AB must be the fourth element, okay, but now what has to be BA, but what is BA? BA is also in the group, right, so BA can be E, but if BA is E the same problem happens, B and A are inverses of each other and hence they commute which is not possible, so BA can't be E, BA can't be A for the same reason as before, and BA can't be B, so BA must be AB, right, so again contradicting the hypothesis. So we cannot have, in other words, so is it clear? So BA must be one of the 4 elements because there is no more room in the group, group has only 4 elements and we have already identified 4 distinct elements, but BA cannot be E, because in that case they are inverses of each other and they commute, BA can't be A, BA can't be B, and BA has to be AB in which case they commute with each other, so it's a contradiction, so the hypothesis that we started with that there exist 2 elements AB such that AB is not equal to BA is wrong, in other words G must be abelian, so case 4 is also done.

So in case 4 we have concluded that G is abelian, so finally case 5, so I want to show that in the case of order 5 group, it is abelian, so what I will now do is the following. So I will use the properties that I mean the work that I have already done. So let's say E, okay, so again I don't want to start with this, so suppose G is not abelian, right, if G is not abelian, then this is exactly as in the case 4, there exist 2 elements A, B in G such that AB is not BA, okay, so now I claim that we must have that the 5 elements, recall that G has only 5 elements, of G must be E, the identity element A, B, AB and BA, why is this? Remember that A and B are elements that don't commute with each other, so they are different from E, so you have 3 elements here and just as in the case 4, AB cannot be E because if AB is E, A and B commute with each other, being the inverses of each other, so it can't be E, it can't be A, it can't be B, so AB is the fourth element, but now in the case 4 that's done and BA must be one of them, and it has to be abelian, but now we have room for one more element, BA cannot be E because B and A are not inverses of each other, it can't be A, it can't be B, and it is not equal to AB also because AB and A and B do not commute, so in other words, this is G, so G is, okay, so this is our first observation, G must be like this.

We are going to get a contradiction, so I am going to make a series of observations. So first so I'll claim that ABA, okay, so what is ABA? Remember that I want to, okay so maybe I will write it as a claim ABA is B and BAB is A, so this is my claim, so what is the proof of this? So and this is exactly as before, so I am going to systematically eliminate all other possibilities, so I'll do one of them, the other being exactly similar to this. So what is ABA? Okay, remember ABA is an element of the group, so it must be one of E, A, B, AB, or BA, so suppose, we have 5 possibilities, right, so ABA is A let's say, okay, so then just look closely at this equation, so we can read this in two ways, so we have A times BA is A, and AB times A, sorry I'm considering the case E, so I am going to consider each possibility, ABA must be an element of the group, so it is one of this 5 elements, so suppose it's E, so A times BA is E, AB times A is E, right, but this is a problem now, because if A times BA is E, then BA is A inverse and here AB is A inverse, right. This equation suggests that BA is A inverse, this equation suggests that AB is A inverse. But remember, when we discussed properties of groups in an earlier video we have shown that A inverse is unique for any element in a group, the inverse is unique, but A inverse is, both BA and AB but this means that AB is equal to BA, which is not the case, right, so ABA can't be E, so this cannot happen. Can it be, I'm claiming it's B, so let's say, can it be A? So this is not possible, correct, is it clear? AB and BA can't both be inverses of A, so ABA is not E, so that we have concluded.

Can ABA be equal to A? So I have, ABA has 4 possibilities, right, E, 5 possibilities, E, A, B, AB, BA, it has no choice, it has to be one of these 5 elements, I have concluded that it can't be A, can it be A? It can't be E, I have concluded it can't be E, can it be A? It cannot be, because if I cancel A and conclude that BA is E, but if BA is E, AB must also be E, because A and B are inverses of each other and they commute, so it can't be A. Can it be AB? If it's AB, then I cancel A, then I cancel B, I get A = E, this is also not possible, so it can't be AB. Can it be BA? It can't be, again I cancel B and A and I have A = E, right, so it can't be B, so ABA must be B, this is the only possibility left, so ABA is B, this is proved. And exactly the same proof gives me BAB = A, I have to systematically eliminate all possibilities, it can't be E, it can't be B, it can't be AB, and it can't be BA, so let me not prove that, because it's very similar to this, so I have shown that ABA = B, BAB = A.

Next I'll claim that so I think I called it 1, I'll claim 2, A squared = B squared I claim this. So claim A squared = B squared, why is this true? Remember I have shown that ABA = B, let me multiply by B on the left, what do I get? So I get BABA = B squared, I have also proved in the first step BAB = A, now multiply by A on the left, on the right, so I get BABA = A squared, right, so BABA = B squared, BABA = A squared, so A squared = B squared.

Now the third part of the proof, I want to show that there is no room for A squared, so let's say A squared, what is A squared? okay, so that's what I want to now do, A squared if A squared, so again there are 5 possibilities, right, E, A, B, AB, BA, so let me immediately rule out everything other than E. Suppose A squared is A, right, this means I cancel A, one copy of A so that means A = E, because A squared is A star A = A, so that means A = E, so that's not possible because A is the distinct element. Can A squared be B, if A squared is B, A squared is also equal to B squared, right, so B squared is B, because A squared is B squared, and A squared is B, B squared is B, that means B is E, that's not possible, so A squared cannot be B, A squared cannot be B. Can A squared be AB? If A squared is AB I cancel A on both sides to get A = B which is also not possible, A and B are distinct elements, so A squared cannot be AB. Can A squared be BA? That would give me, cancelling A, again A = B which is also not possible, so A squared cannot be A, B, AB, or BA, so A squared must be A, okay.

Now if you recall the first part what we have shown was recall BAB was A, this was proved, right, in the earlier part, BAB = A, now let's multiply by B on the left, now on the right, if I multiply by B on right I get BABA is AB, right, but BA, sorry I am multiplying by B, so BABB is AB, but what is BB? So this gives me BA, B squared is AB, but B squared is also E, if A squared is E, that's equal to B squared, so I have shown that A squared = B squared, so BA B squared is AB, but B squared is E, so BA = AB, but this is a contradiction because I have started with elements AB which do not commute with each other so AB and BA cannot be equal to each other, so again we conclude that G is abelian,, G being any group of order 5, okay.

So just to recap what we have done, we wanted to show that any group of order 5 is abelian and we have started considering order 1 which was very easy, order 2 was also very easy, order 3 was also fairly easy, order 4 was not difficult also because we easily concluded that there is not enough room, order 5 required a little bit of work but again we conclude that, by systematically using all the properties that a group satisfies, that G is abelian, so I wanted you to focus and I wanted to do this in detail because it's a very good example, it illustrates the key points of a group, and the point that you must keep in mind and I keep emphasizing in this course is that we are studying abstract groups, okay, these are groups though, many of the examples of groups that we know are familiar to us integers, real numbers, rational numbers, functions, rotations, roots of unity, complex numbers, the point is these are only examples. We want to develop a theory for abstract groups, so we cannot and we should not use any property that the specific examples have, we should only use properties that a group by definition has, namely that it has an inverse, namely that it has identity, namely that binary operation is associative, that it's closed, and those are the four important axioms, definition, they are part of the definition and after that you've concluded that there is a unique identity, there is a unique inverse for every element, using these properties we are able to, and only using these properties, so if you recall and revise what happened in this video, nowhere have we used the property that it's an integer or real number or a function, everywhere we have only used group-theoretic properties. And we have concluded that in order to achieve non-abelianess, in other words in order to produce two distinct elements that do not commute with each other you must go up to 6 order at least, and in order 6 we do have a non-abelian group, namely S3. So please go over this carefully and make sure that you understand everything here, and that will be a good way for you to make sure that you are comfortable with the basic definition and properties of groups. And I'll stop this video now, in the next video we are going to learn about subgroups of a group and study properties of subgroups, and look at various examples. Thank you.

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. PrathapHaridoss

IIT Madras Production

Funded by
Department of Higher Education
Ministry of Human Resources Development
Government of India
www.nptel.ac.in