NPTEL

NPTEL ONLINE COURSE

Introduction to Abstract

Group Theory

Module 04

Lecture 19-"Quotient groups"

PROF. KRISHNA HANUMANTHU

CHENNAI MATHEMATICAL INSTITUTE

(Refer Slide Time 04:20)

Okay, so in the pervious video we have seen how to apply Lagrange's theorem and counting formula, and before that we have seen how to define cosets of a subgroup in a group. And in this video I want to introduce to you a very important notion of group theory namely quotient groups, okay this is a very important notion that is used all the time in group theory. So it is important for you to carefully understand the notion and be able to apply various theorems and properties of quotient group that we will study. So I am going to introduce to you what quotient groups are using some definitions and some properties.

The basic idea is the following you have a group, G and H a subgroup of G, in the previous video I introduced for you the notation G mod H, it was this side of all left cosets of H in G so in other words these are all elements of the form AH where A is in G, to begin with this is just a set and we computed this set in some case for example when G is the group of integers under addition and H was some subgroup of the form NZ and I think we worked out the case of 4Z in our example the set of left cosets was the finite set actually and we listed them. Similarly when G was the group of the bijections of the three element set namely symmetric group, on three letters S3 and we looked at some subgroup H and we wrote down all the cosets of that subgroup. So this is the set of our left cosets so our question is that will motivate the definition of quotient groups is: can we give a group structure to G mod H? So this is the basic question I want to address. Can we give a group structure to the set of left cosets of H in G, so in other words what is a group structure? It is a first and for most it is a binary operation so, given AH and BH in G mod H can we do perform something, can we get after performing some operation so, third left coset out of AH and BH? So this is the question.

So question is can you give a group structure to G mod H and in order to do that first we want to define a binary operation on G mod H so that when you apply that two cosets AH and BH we get a third coset. We want to do this in general now a specific example you may able to do it, but the hope is that we should be able to do this in general and not only of course this is not the end of it right we have to after giving this binary operation we have to make sure that there is a identity element that this group operation admits inverses and it is associative, these must be checked.

(Refer Slide Time 04:26)

So let us see whether we can do something like this so, I am going to recall for you the example we worked out. So lets take G to be the symmetric group on three letters and H to be the subgroup of E and (1,2) and if you recall we computed the cosets of this very carefully. So in particular we computed what is (1,3)H. (1,3) H was so I want to just write this it is something that we already did. And let me work with another element (2,3) H, (2,3) H was (2,3) and (1,3,2) we already did saw this in a previous video we have done this. So what do we do can we combine them, so what is (1,3) H what should be (1,3)H times (2,3)H? So it looks like we have to learn how to multiply sets, we know how to multiply elements, so one attempt would be, so now very generally, let me introduce to you a notion: G is a group. A,B or subsets of G not subgroups okay, so I am not taking not subgroups not necessarily subgroups. They can also be subgroups but I am not restricting only to the case of subgroups. Define because I am doing this because it seems like we have to multiply two subsets of a group here in order to multiply 1,3 H and 2,3 H we have to multiply two subsets. So let us define A dot B to be simply a times b where a is in A and b is in B, this is just the product set. Very natural definition right, in order to multiply two sets we simply take elements of the first set multiply them with the elements of the second set and you vary all the elements. So can we use this definition because cosets remember are just subsets, left cosets are nothing but subsets and I told you how to multiply subsets of a group. So using this to calculate the two cosets we are considering here (1,3) H times (2,3) H, I need to remind you again I am not claiming this a group operation this will work out, I am just saying this is an attempt. Because we need to multiply here we have to multiply sets, the goal is to multiply sets. So if you want to multiply sets, this seems like a natural definition of set multiplication,

(Refer Slide Time 08:04)

So lets just do (1,3)H times (2,3) H and as I said (1,3)H and (2,3)H are we listed them earlier, it is simply the set (1,3) lets see 1,3H was (1,2,3) product with (2,3) (1,3,2) so these are the two left cosets. So lets multiply them, you take 1,3 and multiply by you taken an element from the first set in my definition I take this to be A and take this to be B, this becomes 1,3 times 2,3, so (1,3) times (2,3), (1,3) times (1,3,2), (1,2,3) times (2,3), and (1,2,3) times (1,3,2) okay. Those are the four products we have so I take the fist element of A 1,3 multiply by 2,3 because that is an element of B, I take 1,3 and multiply it by 1,3,2, similarly I take 1,2,3 multiply by 2,3, 1,2,3 times 1,3,2, so these are the four products. Let us just simplify these and see what we get, what is (1,3) times (2,3) so I will just quickly do one these and write the rest. Remember the product in the new notation for S3 how do we multiply, so we will start with the right hand side element and go to the left. So 2 goes to 3, and 3, goes to 1, so this 2,1 what does 1 do, 1 is fixed under 2,3 and 1 goes to 3, so this is (2,1,3) 3 goes to 2, and 2 goes to 2 in this side so this is (2,1,3) similarly 1,3 times 1,3,2 is, 1 goes to 3, and 3 goes to 1, so 1 is fixed, 2 goes to 1 and 1 goes to 3, so 2 goes to 3, and 3 must go to 2, as you can check 3 goes to 2, and 2 goes to 1, similarly (1,2,3) times (1,2,3), 1 goes to 2 because 1 is fixed here and 1 goes to 2, 2 goes to 3 and 3 goes to 1 so 2 goes to 1, 3 goes to 2 and 2 goes to 3 that is fixed. Finally 1 goes to 3 and 3 goes to 1 so 1 is fixed 2 goes to 1 and 1goes to 2 so 2 is fixed, and 3 goes to 2 and 2 goes to 3 so this actually the identity element. So the last product is the identity element and this of course can be re-written as (1,3,2) so this another subset, so I am just going to rearrange these elements. E, (1,2),(2,3),(1,3,2).

So now lets stare at this earlier I taken, I have defined taken two subsets and define the product it is another subset, so here I have taken two subsets, consisting of two elements each and I multiplied them I got a subset of four elements. Now in order for this operation to be a valid group operation on the set of left cosets, when I multiply left cosets I must get another left coset, so is this a left coset? We computed the left cosets of this subgroup in the earlier video and either by looking at the list of cosets that we computed or using counting formula. Counting formula say the number of left cosets, elements in a left coset are equal to the elements of H, remember cardinality of H is equal to cardinality of AH, for every A in G, so any left coset of H must have same number of elements as H, but AH as two elements in our example so any left coset must have two elements, but this has four element so this cannot be a left coset. You can either check the explicit list that we calculated earlier or use the counting formula, not the counting formula really it is the theorem that cardinality of H is the same as cardinality of AH, this was used in Lagrange's theorem and counting formula.

So this cannot be a left coset, so this too bad, we cannot use this definition to give the definition of a multiplication of two left cosets. And however I want to now illustrate that it is actually not such a bad definition of product of left cosets, we only need to ask for a slightly stronger condition on a subgroup. We need to impose condition on subgroups,

(Refer Slide Time 13:14)

so the conclusion is this product of left coset is not a valid binary operation because product of two left cosets is not a left coset in general. So in general product of two left cosets is not a left coset, so it is not a valid binary operation.

(Refer Slide Time: 14:07)

However we will show in the next few minutes, this is a valid binary operation if H is not just a subgroup, H is a normal subgroup. If H is a normal subgroup, it turns out that this product we define here A * B = { a b / a € A , b € B } that becomes a valid binary operation provided that H is a normal subgroup, ok, this is what I want to show. But before that let me prove a proposition to achieve my goal to show the following.

Suppose that H is normal in G so, typically we denote normal subgroups by N, so in this case I will stick to H, but subsequently, when we talk about normal subgroups we will use the letter N. So what I want to first show is if A belongs to G then A H = H A, so if H is normal in G, AH=HA, in other words the left coset AH is equal to the right coset HA. Let us prove this, this is not difficult.

So I am saying in fact I am saying that if H is normal AH=HA, I am also saying the converse but I will write that later. So I am saying AH=HA, what does that mean? I want to prove that, the set AH is equal to the set HA, what does this mean what is AH? We want to show that AH as H is in H equal to HA as H is in H, so an important warning for you. We are not saying that Ah=hA, in other words if I replace capital (H) by small (h) here, I cannot say this, see this is too much to expect. This is saying that, if you recall the definition of, if this is happen for every A, this mean that H is in the center of the group if you recall the definition of center of a group, but H can be normal and not be in the center of a group. So I am not saying this, why am I not saying this, this is a weaker statement, because I am saying that AH A small h is equal to Ah small h times some other small h times A, so we only need AH to be in HA, it need not be this particular small h times A, it can be some some other h times A, so it is very important to keep in mind that to say that these to cosets are same is not same as saying A, the element A time small h is equal to the element small h times A, so now lets prove these two sets are equal, how do in general prove two sets are equal? You want to show that the first is the subset of the second, and the second is the subset of the first.

(Refer Slide Time: 18:17)

So to prove this equality choose or let Ah be in AH, so if Ah in, A capital H, lets rewrite like this write Ah is equal to Ah(A inverse) A, we can write it like this right, because by associativity A inverse and A can be first multiplied that is identity and you have Ah, so but then since, H is normal, H is normal in G, this is where we are using the normal hypothesis given A in G, and h an H, A h A inverse belongs to H, definition of normal subgroup, so this is H, I am calling it as H prime, H prime is in H, this is my definition in H here, so if you take an arbitrary element of the left coset, it is in the right coset. So AH is a subset of HA, and opposite is identical, you can do this by symmetry but let me just illustrate the point again if it is not clear to you hopefully it will be clearer after this, lets take an arbitrary element of the right coset. Then what we write, as before let us write it as A times A inverse times hA, that is same as this because of the associativity. But if Ah A inverse is in H, this is also in H, so this AH, so called this equal to H double prime, AH double time, and this is by definition of a left coset is an AH, so every element here arbitrary HA, is in AH, so HA is in AH, hence AH equals HA, so this completes the proof of the proposition. Proposition only asked you to show if H is normal AH equal HA for every A.

(Refer Slide Time: 21:03)

I want to leave this an exercise for you and this is a easy exercise that you must do: if H is the subgroup of G, and AH equals HA for all elements of the group then H must be normal in G, so if this property holds for every element then it is actually normal. That we do not need, so I will leave it as an exercise for you but you should do this and actually another exercise. If G is S_3 and H is the subgroup we considered earlier E and 1,2, is (23) times H equal to H times (23)? Okay so this is the question left coset of 23 is equal to right coset of 23? So I will give these exercises to you, you should do this, this 23 H we already computed just compute H 23 okay, this if you compute you will see that then you may ask if it is equal or not.

(Refer Slide Time: 22:19)

So now lets come back to normal subgroups, so in a normal subgroup we have AH equals HA now I want to prove the main result that we want. Proposition: Suppose that H is a normal subgroup of G, then aH, then let A,B be in G, so I am taking two arbitrary elements of G, AH times BH is by definition, this is the product of two sets that I have defined earlier. So this is the product of these two cosets that we defined earlier, namely you take something in AH times something BH and multiply, you do this for every element of AH and every element of BH, and we saw in the example of S_3 and H equal to E and 1,2 that the product is not a coset but in this case it becomes a coset. It is a coset actually AB times H, so if AH and BH are two cosets their product is also a coset. Lets prove this, this is not difficult now.

(Refer Slide Time: 23:20)

So we already know by the previous proposition, what do we know, so we know that HB equals BH, so let me write that here HB equals BH, so now lets compute this, AH times BH, see, remember just to illustrate, so will just start in the new page.

(Refer Slide Time: 24:33)

AH times BH, because of associativity, I can write this as A times HB times H, so why is this? It might be useful, it is true but it might be useful to write down this, what is AH times BH, you take something in the left coset AH it is of this form, and you take something here, so BH prime, so you take this as you vary H, in H and H prime in H, this exactly the product of two set in a group that we defined earlier. If you have two groups, subsets of a group, the product is defined to be A,B were A is in A, and B is in B, this is the definition of product of subsets that we will always use. So in this case I applying this definition to AH and BH, AH is the set A small h, BH is the set B small h prime, I just want to use a different letter because it is you have to vary all elements of capital H, so AH times BH, but this, if you associatitviy of group product, then this becomes, so I can vary a H and H prime two distinct element to may not be distinct two elements of H, then I have AH, B H prime but I put the bracket around HB, but this is precisely this, because HB, capital HB is all element small hb, and capital H is small h prime, so these two are equal, so this is okay, these two are equal.

But now by the same associativity I can write this as, first of all use the property I said earlier. HB equals BH so I can interchange, remember I cannot interchange B and small h, but HB equals some BH double prime, so that BH double prime will come here. So in other words I am saying that A,B,H double prime, H prime, H double prime H prime in H, so this part can be interchanged, switched like this. So this is what I have now again using the same this is this, again using the same associativity I can write this as AB times HH, but what is HH, if you think about it, it is nothing but H. So we claim HH equals H. Why? What is HH, it is the product H times H prime, H and H prime are in H, right, so but if H and H prime are both in H, HH prime is in H, so this is actually contained in H, HH is contained in H, on the other hand if small h is in capital H, you can write this as H times E and this is in HH, because E is in H, identity element is in H, H is in H so HE is in HH, so this means H is contained in HH, so HH is contained in H, H is contained in HH, so this implies H equals HH, when you multiply a group with itself you do not get anything bigger. You get exactly the group this is not true in general for is subset only which is not a subgroup.

So H is equals HH, because H is a group, we have used both properties here because if H and H prime are in H the product needs to be in H here, and E is in H, we need, E in order for H, H is equal to HE right, but for that we need E to be in H, so because we have used the other important property of a subgroup, it must contain the identity element. So, see now we are done because AH, BH is AH, BH, which is BH, H which is AB, HH, which is AB, H, so AH, BH is equal to ABH, which is what we claimed.

So this is the theorem, so this proposition allows us to define a group structure on G mod H, when H is normal. It turns out that there is no natural way to define group structure on G mod H, when H is not normal. This can only be done when H is normal, so what is the group structure, so from now on assume that G is a group and H is a normal subgroup. So I am going to assume that always, I am dealing with a normal subgroup of a group G, then we will give a group structure to G mod H.

So first of all, recall what is G mod H? This is the set of left cosets, as you vary A in G, so what is the binary operation? Remember the definition of a group is you start with a set and define a binary operation on the set and verify that there is an identity, every element is as an inverse and the binary operation is associative. So what is the binary operation? It is the one we discussed earlier. So define AH*BH, I am using star just to emphasize that it is a new binary operation we are defining, is the product ABH. So this is the definition of the binary operation. Now is there an identity element? It is simply H, see H itself is a left coset right, that is identity. But why is that? You take AH*H, and this is AH because A*E, is A, similarly H*AH is AH. so this is an identity element. What is the inverse of AH inverse clearly must be A inverse H, because AH time A inverse H is, by definition A, A inverse times H, which is EH which is H. Similarly A inverse times H times AH, is A inverse AH, which is EH, which is H.

(Refer Slide Time: 32:50)

And associativity finally. If you take AH times BH, then take CH, this is AB H times CH which is by definition AB, CH remember A,B,C you can multiply in any order because this is happening in capital G, so in group G the product is associative. See, as you can see, I am not writing star so if there is no star I just multiplying using this definition, so AB, CH. On the other hand what is AH, times BH times CH, this is AH times BCH which is really what I have to write here is AB times C, here I have A BC times H, but these are equal because AB times C, A times BC, so associativity is also clear.

The point is you needed a valid binary operation, that was the key step, if you have a valid binary operation it turns out the other are more or less is clear, identity element is EH inverse is are given by inverse of these elements, associativity is essentially the associativity in the group itself that will give associativity of G mod H.

You might wonder, can I can just define this without H normal. As I said if you just declare it like this, many of the properties you cannot check because AH*H would be the product, is no longer going to be AH, if H is not normal. So if you just declare it without the normality hypothesis this will not give you a group. So this is a quotient group that we wanted to discuss in this video ,G mod H with this group structure, is called the quotient group.

So the quotient group is defined, this is defined, only when H is a normal subgroup, so and quotient groups come with an important homomorphism. There is a natural homomorphism from G to G mod H. What is that? You take A and you simply map it AH, this is the set map, A going to AH because G mod H remember is the set of left cosets, A is an element, AH is the left coset. Why is this a group homomorphism? Why is phi a group homomorphism? Let's check this, we want to check phi of AB equals phi of A times phi (B). Is this true, lets write down, what is phi of (AB), phi (AB) is by definition (ABH) right and phi of (A) is (AH) phi (B) is (BH) and these two are equal by definition of the product. (AH) times (BH) is equal (ABH), so this a group homomorphism. So quotient groups must always be thought of with this structure of this particular group homomorphism, so it is a group and it admits a natural homomorphism always G to G mod H. What are the properties of G mod, phi, we can say the following. Kernel of phi, remember kernel of phi is all A in G such that (AH) is equal to the identity element of G/H, right, this is by definition the kernel, what is the identity element of G/H, so these all are A in G such that (AH) equals (EH) which is same as (AH), so I don't need to write EH, I will just write H, the identity element of G mod H remember is H, so it's all elements that map to H, but what is this? When is AH equal to H this happens precisely when A in H, this is something we have discussed earlier, so this is H, kernel phi is H. What is image phi? It is AH image phi by definition phi (A), A in G. That means this AH with A and G, this is precisely GH, G mod H. You have all the left cosets here, so its G mod H, so in other words phi is onto, so kernel phi is H and phi is onto, so I am going to summarise all this, that we learnt about quotient groups and write the following.

(Refer slide Time: 39:09)

If G is a group and H is a normal subgroup of G, then the set G mod H of left cosets of H in G is a group under the operation AH times BH equals ABH. This group G mod H is called the quotient group, it is the quotient group associated to G and H. It comes with a natural group homomorphism phi from G to G mod H such that, so we have checked that phi is a group of homomorphism, such that phi is onto and kernel phi is H. So this entire thing you need to remember, so read this carefully we can construct quotient groups whenever you have a group and a normal subgroup and the underlying set for the quotient group is simply the left cosets of H in G, so I want you to think of quotients groups as something very easy, so it is not difficult at all, because you know what is the set of G mod H, it is the simply a left cosets. A group is a set with binary operation right, so you know the set here it's just G mod H, it is the set of left cosets, what is the operation? We need to give it an operation to make it a group, it is simply you take AH and take BH multiply them, you get ABH, so that is the group operation, and it's easy to check that this group operation is closed, has identity, has inverses and it is associative. Not only that, quotient group must always be thought of along with this crucial natural group homomorphism, from G to G mod H, which has two important properties, namely that it is onto and its kernel is H, so these are the properties of quotient groups that we want to emphasise.

Online editing and Post Production

Karthik

Ravichandran