NPTEL
NPTEL ONLINE COURSE
Introduction to Abstract
Group Theory
Module 06
Lecture 37 – "Cayley's theorem"
PROF.KRISHNA HANUMANTHU
CHENNAI MATHEMATICAL INSTITUTE

In this video we are going to prove one of the important theorems in group theory called Cayley's theorem. Let me write it down and I will prove it, it's an important theorem because it tells you something about structure of groups and the proof is fairly easy given that we have understood already some facts about group actions, ok.

Cayley's theorem is the following. So let G be a finite group of order n, that means G has an exactly n elements. Then it says, then G is isomorphi c to a subgroup of Sn, okay. So it says simply, this is the theorem: if G is a finite group order n G is isomorphi c to a subgroup of Sn. Recall that Sn is the symmetric group on n letters.

So I said this is a structural result about groups because symmetric groups are very general in this sense, every group finite group can be put inside in a symmetric group. So if you study symmetric groups and all their subgroups you would have studied all groups, that is the point of Cayley's theorem. Every finite group is isomorphi c to a subgroup of Sn where n is the

order of the group.

So for the proof we are going to consider the action of G on itself by left multiplication, ok, so when I defined actions, group actions on a set S, I gave you several examples, two of those the examples where group acting on itself, so the group is G, the set is also G in these examples. And there were two important actions that I highlighted at that point of a group on itself, one is by left multiplication, and the other is by conjugation ok. So in this proof we are going to apply the action of G on itself by left multiplication.

This means if you have G, so here the set is also G and then gs is simply gs, which is the, gs is simply the product of g and s in G, right. So this the product inside the group G, so let's use this. Now how do I use this? So I am going to fix g in G, first fix small g in G.

Consider the function G to G, because this function is dependent on g, let me call this phi sub g, consider the function defined by I will take small s, phi g of s is gs, so remember G is playing two avatars here one is as a group the other is as a set. Here I am thinking of G as a set, I am fixing a group element g, I am giving you a function on the set to itself, its a function from the set G to the set G. Because it is determined by small g, I am going to denote the function by phi subscript g.
So what does it do? It takes an element small s and maps it to gs. We claim that phi g is a bijection. See certainly phi g is a well-defined function right, it takes an s and maps it to gs, so there is

no problem phi g is a well-defined function.

Now let's take this function and we want to show it's a bijection so in another words we have to check it's 1-1 and it's onto. So why is it 1-1? What is one 1-1? 1-1 means if two things so it's a function G to G, if s1 and s2 map to the same thing then s1and s2 must be equal. So let phi g of s1 equals phi g of s2, suppose that happens.

This implies, what is phi g s1? that is gs 1, what is phi g of s2? that is gs 2 gs 1=gs 2. Remember g is the element of capital G s1 is also element of capital G but s1 is being thought of a set element of the set G so I am using small g to denote the group element and small s1 and small s2 to denote the element of capital G when it is being considered as a set. gs 1=gs 2 but this is a product in the group, that means s1=s2.

The cancellation property in a group, so s1=s2, so phi gs 1=phi gs 2 means if two things go to the same thing, they are equal to each other. This shows that phi G is 1-1, right. Two distinct elements go to the same thing means they are equal.

So now it remains only to show phi g is onto .Why is phi g onto? What is the meaning of being onto? It means you give me any element of the target space there exist s something that maps to it, right. You are given this, there exists such an element. So now let me give may be given an element s in capital G, so which element maps to this? So then phi g of g inverse s, let's consider g inverse s, right. If s is in G, g inverse s is also in G.

So what is phi g of g inverse s? By definition this is g times g inverse of s, by associability this is g(g inverse)=g(g inverse s)=(g g inverse)s which is s, right. So if you give me an arbitrary element of s, g inverse s maps to this under under phi g, so phi g is onto. So phi g is 1-1 and onto so phi g is a bijection, right.

So this is the claim we made, we claimed that phi g is a bijection which I proved. G has n elements right, that is the hypothesis, the hypothesis is that G is a finite group of order n, that means it has exactly n elements. What is Sn? Sn I said is the symmetric group on n letters.

So Sn is the group of bijections of this set {1,2,…..,n}, right. But really the fact that we are calling the elements 1, 2,…, n is not important, Sn is the group of bijections of a set with n elements, remember Sn is the group of bijections of an n element set, for the convenience when working with symmetric groups it is convenient to call the elements 1, 2, 3, up to n, but it need not be those, Sn is the group of bijection for any element, n element set. G is one such, G is an n element set, so Sn can be identified with bijections of G, because Sn is a group of bijections any set with n elements and G is a set with an elements, I can naturally think of Sn as a group of bijections.

So it cannot be identified with bijections of G, I should write can be identified with the group of bijections ok, so if you wish you can call the element of G as 1, 2, up to n because it has n

elements you fix some order take the first element call it 1 second element is 2 right that's what we are doing here. Sn can be thought of bijections of G but phi g is a bijection of G, so now we have a function, lets call it capital ø from G to Sn, what does it do? It takes a g and sends it to phi g that I defined earlier, remember what is phi g for a fixed small g, phi g is the function from G to G and sends s to gs, which I have checked is a bijection so phi g we already checked that phi g is a bijection of G, so phi g is in Sn because Sn is for the purposes of this theorem we are thinking of Sn as a group of bijections of G itself, so phi g, being a bijection of G, is an element of Sn. So I am sending g to phi g. Now ø, capital phi a function from a group to another group, so now I claim that phi is a group homomorphism, ok.

So this is, you have to be careful here, so what is the function phi? It sends an element to another function, the function sends an element to another function, that's what capital phi is doing because Sn is really functions of G to G and a small g under the function capital phi goes to the function small phi g. So capital phi is a function that takes an element of the group G and sends it to a function which is what we are calling by phi g.

So I am now claiming that phi is a group homomorphism, that is, capital ø(g1g2) =ø(g1) composed with ø(g2). And remember the composition on Sn when Sn is being thought as bijections of capital G, the binary operation there is the composition, so you apply, you take two elements of capital G, g1 and g2, we want to first multiply them and apply phi then phi of g1 as a function

composed with phi of g2 will give you the answer, so this must be true for all g1, g2 in G ok.

(Refer Slide Time 13:09)

So let's check this. So now we are saying that two functions are equal, because capital ø(g1 g2) is a function. We are saying that, ok first let me say, the left hand side LHS and the right hand side RHS are both functions right, what are they really, they are functions from G to itself, to G because they are both in Sn which we are considering as all functions bijective functions from G to G for the purpose of this theorem. Sn is all bijective functions from G to G, this we can do right because G has n elements, so this is valid and now LHS and RHS in this equation are both functions from G to G.

So in order to be equal, so we are saying that these two functions are equal, identical as functions. When do we say two functions are equal? Two functions are equal if they agree on every element of the domain which this case is G. So let us choose an arbitrary s in G, again G here is really playing the role of the set, so I am taking an element small s, let's take an element s in G, see what LHS and RHS do to s.

(Refer Slide Time 15:30)

Let's do LHS is ø(g1g2), that's a function from G to G right, what does it do to (s)? What does it do to s? ø of (g1g2) remember is phi (g1g2), because ø as a function from G to Sn sends a small g to phi g, that's the function capital ø, so ø(g1g2) is ø of small phi of (g1g2) and then apply to s, it is this. But what is this? Small phi was defined way back in the beginning of the proof.

Small phi of g is (gs) applied to s, so, small (φ) g1, g2 of (s) g1g2s. This is what LHS does to small (s). Now what does RHS do? What is RHS?

(Refer Slide Time 16:43)

RHS is (φ) g1 circle (φ) g2, this composition applied to (s), composition of functions says that this must be (φ) g1 applied to (φ) g2 applied to (s), that is the definition of composition. But what is (φ) g2? (φ) g2 is small (φ) g2 (s), right, capital (φ) g2 is small (φ) sub g2. This is (φ) g2, g1 by the way, here small (φ) g2 of (s) is by definition of small (φ), is g2 (s). But this is equal to (φ) g1 of g2 (s), and this is equal to g1g2s. Now are these equal? Of course they are equal because this is the associativity in the group, so LHS=RHS as functions. Remember we are working with an arbitrary(s) so and LHS and RHS agree on that arbitrary (s), so they are equal as functions.

So this proves that capital (φ) is a group homomorphism, so this justifies that statement that capital (φ) is a group homomorphism. Now I want to claim that it is not only a group homomorphism, it is an injective group homomorphism.

(Refer Slide Time 18:27)

So I want to say (ϕ) of g is 1-1, (ϕ) is 1-1. Earlier we have showed that small (ϕ) is 1-1but remember now we are saying capital (ϕ) is 1-1, small (ϕ) was in fact 1-1 and onto and hence became an element of symmetric group. Now I am saying capital (ϕ) is 1-1, it is generally not onto, it is only 1-1. Why is it 1-1? Because it is a group homomorphism capital (ϕ) is a group homomorphism we checked already, it is enough to check what? A group homomorphism is 1-1 if and only if the kernel of capital (ϕ) is the identity element of G, remember a group homomorphism is 1-1 if and only if its kernel is identity, so this what I am going to check. So suppose, so clearly (e) belongs to kernel (ϕ), remember this requires additional statement, because this follows immediately from the fact that (ϕ) is a group homomorphism.

So it sends identity to identity so, we need to check the opposite inclusion. So suppose g belongs to kernel (ϕ), kernel (ϕ) is a subgroup of (G), let us take a small (g) in it.

(Refer Slide Time 19:59)

This means (ϕ) of (g), which is what, small phi of g, remember capital (ϕ) is defined to be small (ϕ) sub (g). So this is, small (g) is in the kernel means its image is the identity element of S_n. What is the identity element of S_n? S_n is the group of bijections

of G, it is identity element means it is identity function. So, (φ) g is the identity function from G to G. Identity element of the symmetric group is the identity function. So (φ) g is the identity function. Hence, phi g of (s) =s for all s in S, this is the conclusion of g being in the kernel of capital (φ).

(Refer Slide Time 21:16)

But what is phi g of s? φ g of s is by definition (gs). So gs=s for all s for all s in S. In fact, this is a very strong condition, gs=s remember implies (gs) s inverse=s s inverse implies g=e, this is the cancelation property, right. We can cancel s, that is the point.

So, g=e, isn't that what we wanted? We said that kernel is identity only, we started with an arbitrary g in kernel (φ) and we concluded that it is equal to e. So, capital (φ) is1-1.

(Refer Slide time 22:10)

Now lets us take stock of where we are so, now situation is, capital (φ) from G to S_n is a 1-1 group homomorphism. It is a 1-1 group homomorphism. Now, we recall a point that I made after proving the first isomorphism theorem, if you have a 1-1 group homomorphism or injective group homomorphism, G can be identified with a subgroup of S_n.

So by the first isomorphism theorem, remember first isomorphism says that a group homomorphism if you have G mod the kernel is isomorphic to the image. So G is, in this case the kernel is trivial right because it is injective, to the image. By the first isomorphism theorem G is isomorphic to the image.
(Refer Slide Time23:13)

But note that the image of (ϕ), in general the image of a group homomorphism is always a subgroup of the target group. In this case it is a S_n so image of (ϕ) is a subgroup of S_n and G is isomorphic to it. So, this completes the proof of Cayley's theorem.

Remember what was Cayley's theorem? So that was the beginning of this video. Cayley's theorem said that if you have a finite group of order n, then it isomorphic to a subgroup of S_n , which is exactly what we have just proved.

G is isomorphic to the image of (ϕ) and image of (ϕ) is a subgroup of S_n , so G is isomorphic to a subgroup of S_n so, this is Cayley's theorem and this is a structural statement, not always very useful and the reason that it's not always very useful is because S_n is a very complicated group, okay.

So, one thing that we have noticed in that video when we talked about S_n is the size of S_n keeps increasing by larger and larger

numbers because S3 has order six, S4 has order 24, S5 has order 120, S6 has order 720 and so on. So S_n is a very complicated group, so knowing that every group is a subgroup of S_n is not in practice very useful, however it is a good structural statement.

It says that every group can be thought of as a subgroup of S_n. So I am going to remark here something that we have proved earlier.

(Refer Slide Time 25:15)

Re call that a cyclic group is isomorphic to a quotient of the form. So compare this statement, cyclic group is isomorphic to quotient of the form. So, here also we are relating an arbitrary cyclic group to a well-known group like Z. So how do we show this?

We take the map from Z to G sending 1 to the generator of G. Because G is a cyclic group this is onto and kernel is always of the form NZ for some N, for some N, I should write here. So, by the first isomorphism theorem Z mod NZ is isomorphic to G. So this is also a structural theorem, we are relating an arbitrary cyclic group to something well known.

Cayley's theorem does the same. It relates in fact an arbitrary group any finite group not just a cyclic group, any finite group is actually can be put inside S_n, think of it like this, it can be, it is isomorphic to subgroup of S_n, so that means you can put it inside S_n.

But the reason why this is very useful? That cyclic groups are of the form Z mod NZ is that Z is very simple group to understand, so Z mod NZ is a very simple group and to say that every cyclic group and to say that every cyclic group is of that form is very nice.

Whereas S_n is a very complicated group, so knowing that every group is a group of S_n is not in general that useful, okay. Nevertheless this is an important theorem in group theory because it says that every group sits inside Sn. So in theory you know that subgroups of S_n exhaust all finite groups, that is what it means. If you list all the subgroups of the symmetric groups for all N, then you have listed all groups.

And that is a strong theoretical statement, and it is sometimes useful to, if you work with an arbitrary group G, it sometimes, to give it a concrete shape, and you can do that by putting inside S_n, and we have done a lot of analysis of S_n, it has a cycle decomposition, it has every element can written as a product of disjoint cycles, every element is the a product of transpositions, there is even and odd permutations.

So now knowing that every group is isomorphic to a subgroup of S_n, you can really think of elements of G as cycles, because G is sitting inside Sn and as far as group-theoretic properties are concerned, they are preserved under the isomorphism, so G can

be replaced by whichever group it is isomorphic to which is a subgroup of S_n and work with whatever we know about S_n. So in some cases it is a good result, because it helps us give a concrete shape to an abstract group. And that is why Cayley's theorem is an important theorem in group theory, so let me stop the video here in the next video we will continue our study of group actions, thank you.