NPTEL
NPTEL ONLINE COURSE
Introduction to Abstract Group Theory
Module 04
Lecture 18 – "Problems 5"
PROF. KRISHNA HANUMANTHU
CHENNAI MATHEMATICAL INSTITUTE

Okay so in the last few videos, we have learned about cosets of a subgroup in a group. We have learned about how cosets partition a group and using that idea we've proved the first important theorem of the course which was Lagrange's theorem. And remember that Lagrange's theorem says that when that G is a finite group and H is a subgroup of G, then the order of H divides the order of the group.
(Refer Slide Time: 00:46)

So recall I am going to start with this, Lagrange's theorem says the following. So if G is a finite group, and H is a subgroup of G, then we have the order of H divides the order of G. And in fact we proved this by using counting formula, which is a more precise statement about the orders of G or H. So not only does the order of H divide the order of G we have this counting formula, remember the symbol [G: H] stands for index of H in G which is the member of left cosets of H in G.

So the ratio of the order of the group divided by the order of H is precisley the number of left cosets, so this is a very important formula and Lagrange's theorem is a very important theorem. And in order to explain how we use this, let me do two problems in this video, so I want to illustrate the use of these results.

Problem one is let P be a prime number, and let G be a group of order P. So P is a prime number and G is a group of order P. Show that G is cyclic. So recall that a cyclic group is a group which is generated by ,cyclic means generated by, a single element. And I will recall this definition again in the solution, so if a group has order a prime number,
(Refer Slide Time: 03:18)

then it is a cyclic group. So let us see how to solve this, so because G has order a prime number and 1 is not a prime number, since1 is not a prime number, G contains an element a, which is different from E. This is because if G does not contain any element different from E, then order of G is 1. Because G is just the set consisting of E, but then order of G is 1, at the same time we know order of G is prime number, so it cannot happen.

Now consider the subgroup H generated by a, so remember H is all elements of this form: E, A, A, A square, and so on. And because it is a finite group it will stop somewhere, and the inverses of A will also be included in this, so I am not going to write A power – 1 and so on, because some A power positive integer will be equal ton A power -1. Now Lagrange's theorem says what? Order of H divides order of G.
Now order of G is a prime number. And order of H divides it. But because P is a prime number, only numbers that divide a prime number are 1 and that prime number. So order of H is either 1 or order of H is P. Clearly order of H cannot be 1, why cannot this happen, because H contains A and E which are distinct, so H cannot be order 1 group, so this must be the case, but if H is order P, and G is also order P, this means H equals, but note that H is cyclic by definition. It is a group generated by,

it is a subgroup generated by a single element, so it s a cyclic group by construction. And H is equal to G, so G is cyclic, that's all.

So we have solved the problem. If you have a group of order, prime order it is cyclic automatically. You might wonder what about groups that are not of prime order, so does there exist a group of order 4 that is not cyclic. See, 4 is not a prime number so the problem here is nothing to say about a group of order 4.
It however says that order of group order two must be cyclic, a group of order three must be cyclic, group of order five must be cyclic, seven, eleven and so on. But four we don't know, does there a group of order 6 is not cyclic?
(Refer Slide Time: 07:11)

We know a group of order 6 that is not cyclic. We know that because we can take S3 which remember in our new notation has this form. This has order 6 but elements have all order 1, 2 or 3. So this is, I will leave this as an exercise for you, it is a very easy exercise, it's something you should do, we have done enough to conclude that it is not cyclic. But I haven't explicitly talked about a group of order 4 that is not cyclic, that I will come back to later in the course. So this is anyway a digression, the problem was to show that any group of order equal to a prime number is cyclic. And we have used it becomes immediate, the solution is immediate if once you use the Lagrange's theorem, Lagrange's theorem is very powerful. The point of the problem is to illustrate that.

One more problem I want to do, because to illustrate more about cosets, so let us take a group homomorphism, phi is a group homomorphism. Show that order of G, ok so again assume G is

finite, so whenever we talk about order we have to assume it is finite. Show that order of G is equal to product of the order of kernel phi and image phi.

Remember kernel phi is the set of elements G which map to identity element of G prime. Image phi is simply the image of the function. All element of G prime that have pre-images in G. So show this, so this is also a problem which illustrates important features of group homomorphisms, as well as application of the notion of cosets.
So I am going to give a name for this, so let N equal kernel phi, so recall that we defined group of homomorphisms, we showed that kernel of a group homomorphism, and image of a group homomorphism are subgroups. Not only that, after I defined normal subgroups. I showed that kernel is a normal subgroup. So we know that N is a normal subgroup of G, and we also know that image, let H prime, the image of phi. Instead of writing kernel φ, image φ all the time, I am giving those names. Image φ is a subgroup of, H prime is a subgroup of G prime and in general it is not a normal subgroup, as you should think of an example.
(Refer Slide Time: 11:13)

So we want to show that order of G is equal to product of order of N and order of H prime . So what I will do is, we will show the following, before that I want to recall for you, if A and B are in the group G, φ of A is equal to φ of B, if an only if, B is An, for some n in N, why is the, this was done by us but let us quickly recall this, so I will write it separately, φ of A is equal to φ of B. That means φ of AB inverse, let me write this as A inverse B is E G prime. This is because φ of A inverse times B is

φ A inverse, times φ of B, φ of A inverse φ of A whole inverse, so these are inverses of each other and multiplying them by you get identity element of G prime. I have done many examples of this, so I am not going to write down the details. But this A inverse B goes to G prime by definition A inverse B belong to N. That means B belongs to AN. This is exactly the statement, and note that if this happens, if B is in AN, A inverse B in N. If A inverse B is in N by definition φ inverse A inverse B is E G prime. And if φ of A inverse B is EG prime then φ of A must be equal to φ of B. So these are implications, go backward also.

So this is the if and only if statement, this is the statement that AN equals BN. So if B is equal to AN, A must be equal to the left coset. Recall that AN is the left co set, A times small n for all small n, BN is B times small n for all n. Remember that if B is equal to An, An is an element of A capital N, B is an element of B capital N, because you can take small n to the identity element, so B is certainly in BN. So AN and BN have a common element mainly b, hence they must be equal cosets. Remember if two left cosets are either identical or they have nothing in common. So we will use this to solve the problem. Now lets us recall the problem.

We are trying to show that cardinality of G or namely the order of G is equal to order of N times of order of H prime. So this is the product of two numbers. So why is this true? I want to say that I will take the set of, consider, so I will write it here, the set of left cosets of N in G. This is denoted by, so I am introducing new notation for you and this anticipates our definition of quotient groups later, G mod N, that is how you read this, G mod N is the set of left cosets, for now it is simply a set.

So consider a map, consider the function from the left cosets to H prime, H prime you remember the image of phi. What is the left coset? What is the function I want to consider? I take element AN left cosets are of the form AN and I will map it to φ of A, so this is the function. I am defining the function AN going to this, this is the function F. So F of A is just φ A.
(Refer Slide Time: 16:07)

I claim that, we will show that F is bijection. What does this mean? So first we want to show f is onto. Why? So you give me any element of H prime, in order to be onto, a function has to have a pre-image for every element in H prime. So you give me an element of H prime. What is an element of H prime?

Remember H prime is the image of phi. So let φ of A be in H prime. H prime is the image, so it only contains element of the form φ (A) where A is in G. Then what is F of AN? F of AN is precisely φ(A). By definition F of A N is the function which the, F send AN is φ A. So if φ A is in H prime F of AN is φ A, so every element of H prime is in the image. So F is on to, now we will show that F is 1-1, what is the meaning of 1-1? If two elements under F map to the same element, those two elements are equal.

So suppose that F of AN is equal to BN, so take two cosets which have the same image under F, this means if φ A is equal to B, because F AN is by definition φ A, f BN is by definition φ B. And then I checked earlier that if φ A is equals to φ B, then AN equals BN. By the above argument, we conclude, because φ A equals φ B implies AN= BN. So we have concluded that F is 1-1 also, F is onto, F is 1-1 also, we checked. So F is a bijection between two sets, what does it mean? F is bijection between G

mod N and H prime.

If you have a bijection between two sets, the two sets must have the same number of elements, the number of elements in G mod N is equal to the number of elements of H prime, which is what we denote by order H. But what is number of elements in G mod N. Number of elements in GN is being the set of left cosets, number of elements in G mod N is precisely the number of left cosets of N and G, which we do not buy this symbol [G: N]. [G: N] is equal to the cardinality of H prime. But what is [G:N] by counting formula, which I recalled at the beginning of this video, counting formula says G mod N, is equal to order of G mod order of N, which is equal to order of H prime, which implies order of G is equal to order of N times order of H prime, as desired. This is exactly what we wanted, the problem asked to prove that order of G is equal to order for kernel φ times of order of image φ, kernel φ was denoted by N, image φ was denoted by H prime, so order of G is equal to order of kernel φ times order of H prime, so that completes the solution.

So in these two problems I hope you understood how to use the counting formula and Lagrange's theorem and using these we are able to conclude very strong statements about groups, so I will stop the video here and in the next video I am going to start with my definition of quotient groups.

Online Editing and Post Production

Karthick

Ravichandaran

Mohanarangan

Sribalaji

Komathi

Vignesh
Mahesh kumar

Web Studio Team

Anitha
Bharathi
Catherine
Clifford
Deepthi
Dhivya
Divya
Gayathri
Gokulsekar
Halid
Hemavathy
Jagadeeshwaran
Jayanthi
Kamala
Lakshimipriya
Libin
Madhu
Maria Neeta
Mohana
Mohana Sundari
Muralikrishnan
Nivetha
Parkavi
Poonkuzhale
Poornika
Premkumar
Ragavi
Raja

Renuka
Saravanan
Sathya
Shirley
Sorna
Subash
Suriyaprakash
Vinothini

Executive Producer

Kannan Krishnamurty

NPTEL Co-ordinates

Prof. Andrew Thangaraj
Prof. Prathap Haridoss

IIT Madras Production

Funded by
Department of Higher Education
Ministry of Human Resource Development
Government of India
www.mptel.ac.in
Copyrights Reserved