NPTEL
NPTEL ONLINE COURSE
Introduction to Abstract
Group Theory
Module 08
Lecture 41 – "Sylow Theorem 1"
PROF. KRISHNA HANUMANTHU
CHENNAI MATHEMATICAL INSTITUTE

So let us now continue our study of Sylow theorems, so with whatever background I gave in the last video, let me now start, go ahead and start with the first Sylow theorem. So there are three Sylow theorems.
(Refer Slide Time: 00:32)

First Sylow theorem is the following. So let G be a finite group, let p be a prime number such that, let p be a prime number such that p divides the order of G. So we write the order of G, so we write the order of G, let us call it small n, as p^e times m, where because I am now assuming that p divides the order of G, e is positive and p does not divide m, okay.

So remember that this means that we have taken out the largest power of p that is available in the order of G.

So then this is the set up, as in the end of the last video, I set it up like this. Then so actually this data is not relevant for the statement, so the statement is, let G be a finite group, let p be a prime number that divides the order of the group, then G has a

Sylow p-subgroup. So then G has a Sylow p-subgroup. So this is a very strong theorem in the, you should recall first of all, recall Cauchy's theorem.

So if you recall, one of the theorem that I did in previous weeks was Cauchy's theorem. So there I assumed that if G is an abelian group, finite always as always, and a prime p divides order of G then G has an element of order p. So this was the Cauchy's theorem. So the first Sylow theorem is a vast generalization of this thing because first of all I am not assuming G it is an abelian group and in fact we are saying much more than that it has an element of order p.

Because we are saying that in fact it has a subgroup of order p power e. As a corollary after proving this, I will prove that first Sylow theorem will definitely imply that any group of order, any group whose ordered is divisible by p has an element of order p.
(Refer Slide Time: 03:41)

(Refer Slide Time: 03:42)

So first Sylow theorem is a, it is not, I mean it is a vast generalization, so I mean it generalizes Cauchy's theorem to arbitrary finite groups and makes a stronger statement than saying that there is an element of order p. So my goal today is to

prove that G has a Sylow p-subgroup, remember Sylow p-subgroup is a subgroup of order p power e. So the proof of Sylow theorem, so rest of the video will be focused on the proof of Sylow theorem.

And as I mentioned in the previous video, this proof as well as the proofs of next two Sylow theorems, depend critically on action of G on itself and its subsets. The two actions we consider are left multiplication and conjugation. So now I am going to consider the following set, so earlier I talked about G acting on the power set of G, G acting on the set of all sets of subsets of G. Now I am not interested in all subsets.

I am interested in only subsets of cardinality p power e, so let capital S be the set of subsets of G of order p power e. So remember background, always we assume that n can be written as, n is the order of group, and that is written as p^e power m, p power e times m and p does not divide m, this is our set up. So let us look at the subsets of order p power e, so in other words S is all sets A and I again stress these are subsets only, not subgroups.

The cardinality of A is p power e. G acts on S by left multiplication. So remember in the previous video, I said g acts on subsets of G by left multiplication, there I defined G (DOT) A to be g times small a, as small a varies over capital A. Now I am introducing a further restriction here, I am not looking at all subsets but I am looking at subsets of order p power e and all you need to verify here, to verify the G acts on S, is that, it is an easy exercise actually to verify this. If A has p power e elements

then gA has also p power e elements. So in fact I should state this exercise better.
(Refer Slide Time: 06:45)

So in fact I should state: order of A is order of gA. So if order of A is p power e then order of gA is also p power e, and this is repeatedly used in all the videos that we have done, because this is related to the statement that two cosets of a subgroup have the same number of elements, but here even if A is not a subgroup the statement holds, because the set of elements ga will be distinct if a is distinct.

So in other words if a and bare distinct ga and gbare distinct. So the number of elements of A is equal to number of elements of gA. So in other words if you take a subset of order p power e, apply a group element to it you get another element of order p power e, so G acts on this set S. So I am not interested in the power set of A, I am interested in the subsets which have p power e elements.

So now I am going to recall for you a fact, what is the order of S? So this is a simple combinatorial argument that you may have seen earlier or you can think about it and convince yourself, so I am not going to prove this because this takes me on a tangent. So you have n elements, small n many elements in capital G, and you want to construct a group of, a subset of order p power e, so the number of ways for doing this is simply n chose (p power e).

So this is n chose (p power e), that you have studied I am sure in other courses. So the number of elements of capital S is n chose (p power e), in other words number of subsets of group G which have cardinality p power e, precisely n chose (p power e), and what is n chose (p power e)? It is n factorial divided by (p power e) factorial times n – (p power e) factorial. So this if you cancel out n – (p power e) factorial what you will have is n times n -1 times n-2 upto n-pe+1.

Because n – pe factorial will be cancelled from this and you will have p power e factorial, so (p power e), (p power e)-1, (p power e)-2 and 1 the last term will be 1. Which is, of course (p power e) – (p power e)+1. So this is the number of elements of capital S. In fact, this is the first fact. The second fact is.
(Refer Slide Time: 09:34)

Fact two is that p does not divide the cardinality of S, so this is also not difficult at all but and I will give you a very quick argument about why this is true. So remember that order of S is this, right order of S is this. So there are in the numerator and denominator, there are same number of elements. So think of order of S as n by (p power e), n-1 by (p power e)-1, n-2 by (p power e)-2. n- (p power e)+1 by (p power e)-(p power e)+1. So I am just, because there are exactly same number of factors in both numerator and denominator, I am going to write it like this.

So if I show that p does not divide each of them then we are

done but here of course why does p not divide? I mean that these are not necessarily integers, but I claim that the same factor of p divides n-i and (p power e)- i for any i from 0 to (p power e)-1. Because that is the last factor, so each factor can be that of as n-i where its n-0 here n-1 here, n-2 here, n- in bracket, so this can be written as, so there are (p power e)-1, actually (p power e) factors here n-0, n-1 and n-2,…

So same the factor divides, so if p divides n three times I claim that it also divides p power e three times and then same thing happens everywhere. So there cannot be after you cancel all the things and all the factors and compute cardinality of S, there cannot be a p in its order and this is easy to see because suppose i can be written as p power i, sorry, let us say p power r times I don't know so k.

So let us say write i, as so here of course t could be 0 also. So then n-i is (p power e)m, remember n is (p power e)m - (p power r)k. So you can factor out and remember r must be strictly less than e because i is strictly less than p power e, so r is strictly less than e. So I can factor (p power r) and what I will have is (p power e-r)-k, so r is the largest power that divides, of p, that divides n-i. Similarly (p power e)-i will be (p power e)- (p power r) times k. Again we have (p power r)(p power e-r)-1, okay.

So then if you write it like this, then (p power r) is the largest power of p that divides both n-i and (p power e)-i. So this forces capital S not to have, the order of S not to have any factor of p. Because in each of these ratios the same p appears, so when does p divide order of S? It divides it when one of this factors has a p remaining, after you cancel p in both numerator and denominator it should have some p left but that does not happen because if p power 2 divides n-1 and p power 3 does not divide

it exactly same happens (p power e)-1 so then that is all. So it turns of that, there is no factor of p in S, so I got to use this.
(Refer Slide Time: 14:23)

(Refer Slide Time: 14:24)

So the key fact for us, to be used later is, p does not divide, so just if you understand this that is great, but I want you to now take, spend a minute thinking about this argument why p does not divide order of S. But please remember that if you don't understand, it will not affect the rest of the proof. So if you don't understand don't get worried about it forget it for the moment, accept this is a fact and try to follow the rest of the proof.

And if you don't understand why this statement is true. You can go back and read the proof, listen to the proof again carefully or ask questions. So in the rest of the proof I am not going to use any of these calculation, I am only going to use this fact: p does not divide order of S. So let us only use this. So let us accept this, so now we are ready to prove Sylow first theorem.

So what we have is: G acts on S by left multiplication. And what is S? S is the set of all subsets of capital G which have order p power e. So it acts on S. So now we have the orbit decomposition of S. What does it say?

Order of S is order of orbits order of the first orbit some, I don't know, it doesn't matter, so this is some k orbits. So where O1

through Ok are distinct orbits for the action of G on S. So any time you have a finite group G acting on a finite set S we have the orbit decomposition in hence order of S is the sum of the orders of individual orbits.
But now by the above fact, p, which is the fixed prime number we are dealing with, p does not divide order of S. Now look closely at this equation: order of S is equal to order of O1+ order of O2+ ... (dot, dot, and dot) + order of Ok; p does not divide the left hand side, so p cannot divide all the terms on the right hand side, right. Because if p divides order of O1 and order of O3 and so on up to order of Ok, p will divide everything in the right hand side, so p will divide the sum also. But then that violates the fact that p does not divide order of S.
(Refer Slide Time: 17:45)

(Refer Slide Time: 17:46)

So there exits an order orbit Oi such that p does not divide the order of Oi, right. This is clear because if p divides all orders p divides the sum. Then p divides order of S which cannot happen, so there must in other words the statement that p divides all orders is wrong. Then that means p does not divide some order, so p does not divide orbit Oi. So say remember, what is Oi? These are orbits of elements of S. So let us say it is orbit of A, so A is in S, so p does not divide orbit of A, that is the conclusion for us.

P does not divide orbit of A. Now let H be the stabilizer of A and our claim now is H is the desired subgroup. We claim that H is a Sylow p-subgroup of G. Note that being stabilizer of A or some element of capital S, remember A is an element of capital S, capital S is a set of subsets, so an element of capital S is actually a subset of G. So A is an element of capital S, H is a stabilizer so H is definitely a subgroup.

The thing to prove here is we know that H is a subgroup of G. We need to show that it is a Sylow p-subgroup. What is the meaning of Sylow p-subgroup? We want to show that its order is equal to p power e. In the last video I defined Sylow p-subgroups for a group G and in our context it is exactly subgroup of order p power e. So in order to claim prove the claim which is that H is a Sylow p-subgroup we need to only show that order of H is p power e.

So now I am going to use another small lemma that I proved in the previous video. So what we know is the following. By the lemma in the previous video, by the lemma in the previous video, order of H divides order of A. So if you go back and look at the previous video this is exactly the lemma that I proved, if G is a group acting on subsets of G and you take a subset and you look at its stabilizer, order of the stabilizer divides the order of the set.

(Refer Slide Time: 20:52)

(Refer Slide Time: 20:53)

So H divides and what is the order of A? Order of A is p power e because A belongs to remember A belongs to capital S which is the set of all subsets of p power e, so order of H divides order of P power e, sorry order of H divides p power e, so order or H is a power of p, so if you have a number dividing p power e, p is a prime number so it must be a power of p. So only number that divide p power e are powers of p.

So this is because p is prime. Of course this is not true if p is not a prime so if some number divides p power e it must be a power of p by itself. We also have the counting formula. What is the counting formula? It says that order of G, remember G acts on S, use counting formula for the G action on S and the element A in S. I recalled earlier in the video the counting formula it says the order of the group is product of order of the stabilizer of A and the orbit of A.

And what is the order of group? It is p power e times m, order of the stabilizer which I called H is some power of, let's say p power i, let us say p power i is the order of H. So remember I concluded that order of H is a power of p, so it is one p power i and whatever is orbit of, order of the orbit. So and it is some number so let us call it so may be number m not m so let us call it r.

So p power e times m is equal to p power i time r. But remember the assumption on orbit of A, orbit of A is such that p does not divide the size of orbit of A, so by choice of A p does divide the order of orbit of A, so in other words p does not divide r. So now let us look at this carefully. So we have p^e m is equal to p^i r, and what do we know? p does not divide r, so remember integers can be factored uniquely. So you have p appears e times on the left hand side.
(Refer Slide Time: 23:58)

So p appears e times on the left, so it must appear e times on the right also. It appears i times her and it does not appear in r. When I right "appear" what I mean is when I factor r into product of primes p is not one of them. So this implies these two facts imply that i equal to e, so because the p must appear e times on the right hand side also and r cannot have any p's in it. So i must be equal to e.
So the order of the stabilizer is p power e, so we are done with the proof the first Sylow theorem.

Recall the first Sylow theorem says if you have a group G finite group G and a prime number p divides it, p must, G must have a Sylow p-subgroup and we have produced it. Because we have produced it because H is a Sylow p-subgroup of G, so this completes the proof. The proof is very clever and you would not normally think of proving it like this.

So what happened is we have looked at the set of all subsets of

G containing p power e elements. Of course some of them will be subgroups but we didn't directly prove that one of them is a subgroup, what we showed is that stabilizer of one of them will have order p power e. That is what we have shown. So there is an orbit whose order is not divisible by p and stabilizer of that element must have order p power e. So this proves the first Sylow theorem and an important corollary of this is the following.
(Refer Slide Time: 26:13)

(Refer Slide Time: 26:14)

So let G be a finite group and let p be a prime number that divides order of G then G has an element of order p. So that is my statement. This is exactly the generalization of Cauchy's theorem that I promised when I talked about Cauchy's theorem. Here I am removing an important word here I am not assuming that G is an abelian group. We have already proved that if G is a finite abelian group and a prime divides that order of that group then that group has an order p element.

Now I am not assuming that the group is abelian anymore ,any finite group has this property. Why is this?
By first Sylow theorem, G has a Sylow p-subgroup say H. So G has a Sylow p-subgroup, say H. So in other words order of H is equal to p power e and we write n as p power e m always p does not divide m, n is the order of G. So now let us chose any

element of H what can be the order of a?

By Lagrange's theorem the order of the element divides p power e, order of the element divides the order of H which is, because a is in H, Lagrange's theorem. Lagrange's theorem implies order of a divides order of H which is p power e. So this in particular means order of a is equal to p power r, for some, I am going to assume that a is not identity, so r is between 1 and e. So it can't be 0, because if r is 0, p power 0 is 1, order of a is 1 means a is e. So A is p power r, order of A is p power r. Now how do I construct an order p element?
(Refer Slide Time: 29:00)

(Refer Slide Time: 29:01)

So now consider b is equal to a power (p power r-1), so I am taking b to be a power p power r-1 which is of course an element of H which is an element of which is a subset of subgroup of G. So I claim that then we claim order of b is p. This is easy because what is b power p? b power p is a power p power r-1 power p, and this obviously implies, this is equal to a power p power r, because order of a is p power r this is e. So b power p is e, right.
So now that doesn't immediately prove that order of b is p, because b power p is e means so order of b divides p. This is something we have learned way back in the beginning videos. If an element has certain power of an element is identity then order

of that element must divide that power, but only numbers that divide p, p being a prime number are 1 and p, so order of b is 1 or order of b is p. If order of b is p we are done.
Can order of b is 1, can order of b be 1? Order of b 1 means what? Only element of order 1 in any group is the identity element. That means b must be equal to e, that means a power p power r-1 is equal to e, that means order of a divides p power (r-1) but order of a is p power r. That is by assumption, right, a was an element of order p power r. Hence p power r divides p power r-1, this is absurd. Obviously p power r cannot divide p power r-1, so order of b is, p power, p and b is the element we are looking for, so this proves the corollary.

So as I said this corollary generalizes the Cauchy's theorem and says that for any finite group, no longer needed we are assuming it to be abelian, if a prime number divides the order of the group then that group has an element of order p. And this is an immediate corollary of the first Sylow theorem, so Sylow theorem is way more than just saying that corollary. So it is saying something stronger because it says that G has a subgroup of order p power e.
So this hopefully gives you an idea of the power of Cauchy's theorem and the next two Cauchy's theorems say further about this, so first, sorry this says something about the power of Sylow theorem and the next two Sylow theorems say further things about Sylow p-subgroups. We know now that there is always at least one Sylow p-subgroup, so in the next two Sylow theorems we will study more properties of Sylow p-subgroups, Thank you, I will stop the video here.

Online Editing and Post Production

Karthik
Ravichandran
Mohanarangan
Sribaliji
Komathi
Vignesh
Mahesh Kumar

WebStudio Team

Anitha
Bharathi
Catherine
Clifford
Deepthi
Dhivya
Divya
Gayathri
Gokulsekar
Halid
Hemavathy
Jagadeeshwaran
Jayanthi
Kamala
Lakshmipriya
Libin
Madhu
Maria Neeta
Mohana
Mohana Sundari
Muralikrishnan
Nivetha

Parkavi
Poonkuzhale
Poorvika
Ragavi
Raja
Renuka
Saravanan
Sathya
Shirley
Sona
Subash
Suryaprakash
Vinothini
Executive Producer
Kannan Krishnamurty
NPTEL Co-ordinators
Prof. Andrew Thangaraj
Prof. Prathap Haridoss
IIT Madras Production
Funded by
Department of Higher Education
Ministry of Human Resource Development
Government of India
WW.nptel.ac.in