NPTEL
NPTEL ONLINE COURSE
Introduction to Abstract
Group Theory
Module 08
Lecture 43 - "Sylow Theorem 111"
PROF. KRISHNA HANUMANTHU
CHENNAI MATHEMATICAL INSTITUTE

So, let us continue now. In the previous two videos we looked at the first and the second Sylow theorems. The first one said that a group, a finite group G has a Sylow p-subgroup, if p divides the order of the group. Second Sylow theorem said that any two Sylow p-subgroups are conjugate.
(Refer Slide Time: 00:32)

The third Sylow theorem says something about the number of Sylow p-subgroups. So let us prove this, let us first state this.

Let G be a finite group. The set up is as in the first two Sylow theorems. So, let G be a finite group and let p be a prime that divides order of G. So we write order of G as $p^e m$, where p does not divide m okay, as always. Let small s be the number of Sylow p-subgroups.
So, as I said the third Sylow theorem is a statement about the number of Sylow p-subgroups. Let us call it s, remember s it at least 1, by the first Sylow theorem. Then the third Sylow theorem says two things. (1) s divides m. Okay, so remember m

is the factor of, in the order of the group, which does not contain any p, after removing all the factors, largest power of p that is available. So, s divides m and (2) s is of the form ap+1 for some a in natural numbers.

Okay, so that means when you divide s by p, you have remainder 1. So, let us go ahead and prove this. Proof is again a clever use of group actions as the first two Sylow theorems work. Here also we cleverly use a group action on a suitable subset. So, here I am going to consider the set, the useful set here is capital S is the set of all Sylow p-subgroups. So this is, H is a subgroup of G and order of H is p^e, that is the set S.
(Refer Slide Time: 03:14)

Now we want to consider a G-action on S. So, remember G acts by two things on itself or subsets, either by left multiplication or by conjugation. Here if you take left multiplication it won't give you an action, why? Remember S is not just subsets, S is not the set of subsets. It is a set of groups; it is a set of subgroups. So, if you take left multiplication, you are no longer going to be in the set because if you multiply a subset, subgroup by an element on the left you will have a subset not necessarily a subgroup.

So, if you consider the action of G on S by left multiplication it will not give you an action because our set now consists of subgroups. So, we are going to consider the action by conjugation. Remember as I said in the previous video, conjugation preserves this set. So, in other words if H is an S, then g and g is in G, gH is also, gH by definition is $gH\ g^{-1}$. So here it is not the left multiplication, it is the group action, g. H is also in S, because gHg^{-1} is a subgroup and its order is also p^e.

So, it is an action. So, now this is the goal for us. Now by the second Sylow theorem, so first of all let us fix some element of H, S so. Let H be in S. So, that is H is a Sylow p-subgroup of G.

What is the orbit of S, sorry orbit of H? What is the orbit of H under this action? Remember the proof in this case completely depends on the action of the group G on this set S by conjugation. What is the orbit of H? It is all gHg^{-1}, as g varies is in the group, gHg^{-1}. Now remember $gHg^{-1}$are all Sylow p-subgroups that is okay. But by the second Sylow theorem this is all of S, correct?

Because every, any two Sylow p-subgroups are conjugate. So you take any element of S, namely a Sylow p-subgroup. It is conjugate to H because any two conjugate; any two Sylow p-subgroups are conjugate by second Sylow theorem. So, there will be a suitable g such that gHg^{-1} is that Sylow p-subgroup.

So, the orbit of H is all of S. What is the stabilizer of H? Stabilizer of H is all group elements such that $gHg^{-1}$is H. Under the action you must get back H. This is what we called the normalizer, if you recall from one of the earlier videos, this is the normalizer of H. So, let us denote this by N (H) and for simplicity I am just going to call it N, okay.
(Refer Slide Time: 06:42)

So now the counting formula gives me the following. Counting formula applied for, applied to this particular G action on S and for the element H. It says that cardinality of G is equal to cardinality of stabilizer of H times the orbit of H. This is the counting formula. This is p^e times m; this is equal to, what is the stabilizer of H? This is the order of N, N was my notation for the normalizer and orbit of H is S, right.

Orbit of H by the second Sylow theorem is all of S. So hence, p^em is equal to capital N times capital s. So, capital N order capital N times remember our notation was number of Sylow p-subgroups was called s, right in the definition. In the statement of the theorem small s denotes the number of Sylow p-subgroups. Capital S the set of Sylow p-subgroups. So, order of S is small s; so p^e m is s times order of N.

Now what we have is the following. Normalizer of a subgroup H will always contain the subgroup. So we have this because remember normalizer is all elements such that $gH\ g^{-1} = H$, if some element is already in capital H, certainly it will contain, it will be contained in the normalizer so, we have this. Then I claim, so we have the index of N in G divides the index of G in H, H in G. Why is this?

I will quickly tell you why. What we have is the counting formula for the subgroup of a group tells me that, this is one of the original counting formulas. Order of the group is the index times order of the subgroup. But remember this is also equal to the index of N in G times order of N. I am applying the counting formula first to H and then to N.

(Refer Slide Time: 09:22)

But since, H is in N, Lagrange's theorem says what? Lagrange's theorem says that order of a subgroup divides order of the group. So order of H divides order of N. So we can write order of H times some, let us say L is order of N for some L in natural numbers, positive integer.

So, now let us recall this, so order of G is index of H times order of H, which is the index of N times order of N. But order of N is order of, so I am going to rewrite this as index of N and instead of N order of N, I am going to use this, order of H times L.

So, now I will look at the, this term and this term and cancel H, order of H. So, index of H is equal to index of N times L. So, index of N divides index of H. Okay, index of N divides index of H. Now let us look at the counting formula that we had earlier. What is the index of N?
(Refer Slide Time: 11:15)

So I want to understand, by the counting formula we have order of G is equal to s times order of N, right. So this implies s is equal to order of G divided by order of N, which is index of N. But what I have just concluded is, index of N, so is that clear? We proved earlier that order of G is equal to small s times order of N. So, small s is order of G divided by order of N which is by

definition the index of N, not by definition but by the counting formula, is index of N.

But we know that index of N divides index of H. And what is the index of H? This in turn is the order of G divided by order of H, but H is remember a Sylow p-subgroup. So, this is $p^e m$ by p^e, this is m. Okay, so s is the index of N so, s divides m and I think this gives (1), I called it (1), (1) of the theorem.

Remember the statement of the Sylow theorem is that if you call small s, the number of Sylow p-subgroups it divides m and it is of the form ap+1.

So, I have just proved the first part of it. Right, this gives the first statement of the theorem.

To prove the second theorem, second part to prove (2) I am going to consider a different action by a different group. To prove (2) we consider a different action. So, here I want to consider, we look at, so earlier I looked at the action of the group G on the set of all Sylow p-subgroups that gave me the statement (1). To prove statement (2) I will look at the action of H, H is a, so we actually fix. So, fix a Sylow p-subgroup, call it H, and we look at the action of H on the same set as above.
(Refer Slide Time: 13:58)

So, S being all Sylow p-subgroups of G, right. So as in the previous, part (1) of this theorem, S was the same set, I am only

changing the set the group which is acting. I do not consider the action of G, all of G, I only consider the action of the group H. So, Sylow p-subgroups the set remains the same. And I am going to call this set H, see H is an element of this right? So, H1 is called, I am just going to take H as H1, H2, H3 and remember there are s of them. Small s is the number of elements of capital S.

So, we look at H action on S, H action on S by conjugation. So, only difference from the first part is, instead of looking at the action of G on S by conjugation, we look at the action of H on S by conjugation.

Okay, so now what is the, so I am going to figure out what is the orbit of H? First I am going to understand what is the orbit of H. What is orbit of H? So, orbit of H, so orb of H is all gHg^{-1}, but now where is g?

Because so maybe I should call what is the H-orbit of H. Remember I am no longer interested in the action of G, what happens outside H is of no concern for me. I am only interested in the H-orbit of H. What is the H-orbit of H? It is all groups of the form gHg^{-1}, where g is in H. But this is exactly H. Right, because if g is in H, $gHg^{-1}$is H. So, orbit of H is just the singleton H. Now choose some let any i be any number bigger than 1.

What is the orbit of (Hi), is what I want to think about, and for that I will suppose that {Hi} is an H-orbit of H, of S rather. Remember I am looking at capital H acting on capital S by conjugation. Suppose that some Sylow p-subgroup, different

from H, so (i) is greater than 1, different from H, let us say Hi forms an orbit by itself. What can we say about Hi is what I want to understand.

(Refer Slide Time: 17:04)

But if {Hi} is an orbit by itself, then what we have is h times (Hi) times h^{-1} is equal to (Hi) for all h. Right, this is the meaning of capital {Hi} being an H-orbit because H orbit of (Hi) is all elements like this, all subgroups like this but it is just (Hi). The singleton {Hi} is an H orbit, that means H times small h times (Hi) times small h^{-1} is equal to (Hi) for every h in H. That means small h is in normalizer of Hi for all (i). Right small h is in normalizer of Hi for all i, because what is a normalizer?

Recall, I am going to call it Ni which is the normalizer of (Hi) is by definition all g in G such that gHi $g^{-1}$is Hi. If you go back and see in the earlier part of the video, normalizer was defined to be this. Now if h times (Hi) times h^{-1} is (Hi), then h belongs to the normalizer. So, H for small, for every, sorry, it is for all iH in capital H. That means capital H is in normalizer of (Hi). So, capital H is in Ni. So, now we have two things.

So, we have H and (Hi) are both subgroups of Ni, right. Because I concluded here that H is in Ni and I definitely know that (Hi) is in Ni, that is not a problem. (Hi) is in Ni, H is also in Ni, so they are both subgroups of Ni. Moreover H and (Hi) are in fact Sylow p-subgroups of Ni. Why is that?

What are Sylow p-subgroups of Ni? You look at the order of Ni, you look at the largest power of p that appears in it and you look at those subgroups of that order. Remember Ni is a subgroup of N, so order of Ni divides order of N.

So, the largest power of p that appears in Ni cannot be more than e which is the, so in fact what we have is also some Ni is $p^e m$ prime, because remember what we have is Hi is contained in Ni, contained in G. So, this has order, Hi as order p^e, G as order $p^e m$. So, order of Ni must be divisible by pi by Lagrange's theorem and in turn, it must divide $P^e m$. So, it must be some m prime. Right so Sylow p-subgroups of Ni are also subgroups of order p^i.

H and Hi remember are subgroups of order p^i. They are both subgroups of Ni and they both have the order p^i, so they are both Sylow p-subgroups of Ni.

So, by the second Sylow theorem, so just to repeat, the largest power of p that appears in Ni, is also p^e. So, Sylow p-subgroups of Ni are subgroups of order p^i and we have shown we know that H and (Hi) are both subgroups of N and both have order p power; they are both subgroups of Ni and both have order p^e. So, they are both Sylow p-subgroups of Ni. Now what does the Sylow second theorem say? It says that any two Sylow subgroups or conjugate.

(Refer Slide Time: 21:30)

So, H and Hi are conjugate in Ni. So, here I am only focused on applying the theorems to Ni, not to G. So, apply the second Sylow theorem to Ni. Ni is a finite group; H and (Hi) are subgroups of Ni which are both Sylow p-subgroups. So, they are conjugate in Ni. That is, there exists g in Ni, such that gHi g^{-1} is H, right. This is the meaning of being conjugate. But if g is in Ni, recall what is Ni; Ni is the elements g such that gHi g^{-1} is equal to Hi.

This means gH g^{-1}, gHi g^{-1} is Hi but this is also at the same time equal to H because gHi g^{-1} is H that is the assumption that, that is the consequence of the second Sylow theorem because they are conjugate but g being Ni forces gHi g^{-1} to be (Hi).This is the definition of Ni. That means H is equal to Hi.

So, the upshot of all this is: if {Hi} is an orbit, is an H-orbit in S, then Hi equal to H. Okay, so if Hi is an N orbit, Hi is an H-orbit of S then it is H. what we have shown is H is an orbit by itself that is okay but if Hi is an orbit by itself we must have that Hi is equal to H. So, it is the only singleton orbit of S, so written differently H is the only singleton orbit in S. Singleton orbit means an orbit consisting of a single element. It is only singleton orbit of S.
(Refer Slide Time: 23:54)

Now consider orbit decomposition of S. So, we have the size of S which remember was denoted by small S is order of O_1+ order of O_2+ …+ order of O_k. And let us assume that order of O_1, sorry O_1 is orbit of H. H was the fixed thing that we had dealt

with. Okay, so that is H. So, order of O_1 is 1 +order of O_2 + order of O_k. So, here of course I am looking at H-orbit decomposition and by what we have done above by the above argument, order of O_i is at least 2 for all i from 2 to k, right. So every other orbit has at least two elements because if it has only one element, it must be H. So, it has to, and that we have already accounted for. So, they are all at least 2.

But now apply counting formula. What we get in the counting formula? Here we are looking at the H action. So, let us say O_i is the orbit of Hi. So, if that applied counting formula applied to that says order of H is stabilizer of $O_{i,}$ sorry stabilizer of Hi times the size of O_i. But what is the order of H? H is a Sylow p-subgroup, so order of H is $p^{e.}$

So, this means order of O_i divides p, this is great, order of O_i divides p because p^e is stabilizer of Hi times order of O_i. So order of O_i divides p. But for i at least two, we have two facts: order of O_i is at least two by this argument and it also divides p. Okay, so it cannot be 1, so they are all at least two. So, now let us look at the orbit decomposition of S and I am going to write it like this.

(Refer Slide Time: 26:41)

Small s is the order of S which is $O_1+O_2+O_k$ but we agreed that order of O_1 is 1 + order of O_2 is something times p. Right, something times so let us say order of O_i is p times let us say $A_{i,}$

that Ai is at least 1. So, it is p times A_2, p times A_3, so order of O_3 is p times A3, order of O_k A_k is p times A_k. So, 1 times + p times (A_2 + A_3+ $A_{k)}$ and you call this A, and this is exactly the statement that we made, this gives (2).

So, the proof is complete. Right, so we have shown that the number of Sylow p-subgroups when you divide by p leaves a remainder of 1. So, let us quickly recap this. The argument was we look at; we fix a Sylow p-subgroup. So, let's see where we started with this. So, we fix a Sylow p-subgroup and then look at the action of that Sylow p-subgroup on the collection of all Sylow p-subgroups by conjugation and after some work we concluded that the only singleton orbit is H itself. Any other orbit must contain at least two elements.
So, the orbit decomposition looks like this: s equals 1+ the remaining orbits. But the remaining orbits must divide p because of the counting formula. So, all the remaining terms are divisible by p and 1 is left so s itself must be of the form 1+ ap.

Okay, so let us again look at the example of S3 with that we have seen before. So, here of course order of S3 is 6 which is 2 times 3. So, the number of, let us denote by s2, the number of Sylow 2-groups, subgroups and s3 is the number of Sylow 3-subgroups.
(Refer Slide Time: 29:26)

The third Sylow theorem says so, let us first do s2. So s2 divides 3 and s2 is 1+3A or 1+2A right. But, and what is s2? So, third Sylow theorem says this. But we know what s2 is. What is s2?

We already seen right there are 3 Sylow 2-subgroups, that does three satisfy this? Yes of course it does because 3 divides 3 and 3 is of the form 1+2 here.
What does third Sylow theorem says about s3? We know of course we know s3 is 1 so, let us see if that is confirmed by Sylow theorem, third Sylow theorem. s3 should be a divisor of 2 and s3 must also be 1+3a. So, 1 satisfies this. Correct, because 1 divides 2 and 1 is of the form 3A, 1+3a.

Okay, so this says that, this just confirms what Sylow theorem says but I want to stress one fact here. Sylow theorem does not tell you exactly what the number of Sylow p-subgroups is. Okay, it only gives you a range of possibilities. You have to further investigate the group to determine which possibility occurs. See as in this example, before you knew this, suppose you did not know this, we can say that even if we did not know anything about s3, we can say s3 must be 1.

Why is that? Because s3 divides 2 that leave only 2 possibilities, it is either 1 or 2. Right, but it also at the same time must be of the form 1+3a but 2 are not of the form 1+3a. So, we can say s3 must be 1. This immediately come, no matter what the group is, even if you did not know that is S3, s3 must be 2. On the other hand s2 can be 1 or 3, why is that? Because remember the conditions are s2 divides 3 and s2 is 1+ 2a.

Certainly 1 divides 1 has these properties because 1 divides 3 and 1 is of the form 1+2 times 0; and 3 also has this property, 3 divides 3 and 3 is of the form 1+ 2 times 1.

So, Sylow theorem only says that s2 can be either 1 or 3 and in the example of the symmetric group, the option 3 is achieved. Of course my notation is confusing here because the group and also S_3 so I hope you do not get too confused about this. So, if the group is S3 then s2 is 3.

(Refer Slide Time: 33:07)

On the other hand let us take the group to be, if we take the group to be Z mod 6Z, this is also group of order 6. Then s2 is actually 1. This is an exercise for you; Z mod 6Z has exactly one Sylow 2-subgroup. Okay, so in this case s2 is equal to 1 is achieved.

So, just to recap Sylow theorem is not a conclusive answer to, third Sylow theorem is not a conclusive answer to the question of how many Sylow p-subgroups exist because it only gives you a range.

As this is example of order 6 suggests sometimes that range contains only one element like in this case; if you have a group of order 6 we know that there must be only one Sylow 3-subgroup that we can say because that number has to divide 2 and at the same time be of the form 1+3a.

On the other hand, when you look at Sylow 2-subgroups there are either 1 or 3, and as you can see in these two examples, both options are achieved.

So, the Sylow third, third Sylow theorem is not very precise, it gives you a range of possibilities. Sometimes that range is very small, in fact it can be even 1 possibility, sometimes you can further study the group to eliminate some possibilities. But as it is third Sylow theorem is very useful. So, I will stop the video here in the next video I will look at some applications of Sylow theorems and solve some problems. 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
Lakshimipriya
Libin
Madhu
Maria Neeta
Mohana
Mohana Sundari
Muralikrishanan
Nivetha
Parkavi
Poonkuzhale
Poornika
Prem Kumar
Ragavi
Raja
Renuka
Saravanan
Sathya
Shirely
Sorna
Subash
Suriyaprakash
Vinothini
Executive Producer
Kannan Krishnamurty
NPTEL Coordinators
Prof. Andrew Thangaraj
Prof. Prathap Haridoss
IIT Madras Production
Funded by

Department of Higher Education
Ministry of Human Resource Development
Government of India
HYPERLINK "http://WWW.nptel.ac.in" WWW.nptel.ac.in