NPTEL
NPTEL ONLINE COURSE
Introduction to Abstract Group Theory
Module 08
Lecture 40- "Group action on subset"
Prof. KRISHNA HANUMANTHU
CHENNAI MATHEMATICAL INSTITUTE

Okay, in this last part of the course we are going to study the Sylow theorems,
(Refer Slide Time: 00:21)

which is the last topic. Sylow theorems are very important part of finite group theory, they are standard theorems and they are very useful in understanding finite groups. Before we state, there are three Sylow theorems, I will state them and prove them in next few videos. Let me first recall what we have learned in the previous videos.

So our setup was a following. So G is a finite group, so we are going to recall first. So remember our setup is G is a finite group, S is a set okay, so most of the time we will deal with finite sets and the assumption is G acts on S, right. So there is a map from G cross S to S, you have a an element g and an element s, we map it to what we call g dot s. So sometimes we just write it as gs. And it has usual properties 1 dot s is s, and (g1g2)s is g1(g2s).

Okay, so these are the properties of group action. So now and the most important thing that we have learned,

(Refer Slide Time: 01:56)

in the video when we talked about group actions was the counting formula. Remember, so let say small s is an element of capital S. So S is the set on which G acts, so then the stabilizer of s, we have defined stabilizer of s denoted by Gs or sometime I will denote it by stab(s), and that is all group elements which fix s or stabilize s, remember that this is a subgroup, subgroup of, this is a subgroup of G. So this is a subgroup of G and the other important set that we have attached to small s is orbit of s which are denoted by Os, it is a subset of s given by gs, g belonging to G, right. So this is the orbit, this is a subset of S.

These are the two things that we attached to a particular element, so these are attached to a small s, and the counting formula says the order of G is equal to order of the stabilizer times the order of the orbit, meaning number of elements. So you take the order of the subgroup Gs and multiply with the order of the orbit or the number of elements in orbit you get the order of the group. And remember how do we do this, we observed that this follows, remember this follows because, this follows from the bijection between, this follows bijection between G mod Gs and Os.

So we take a coset and map it to Gs. So this was the proof of the counting formula. And another important property of group actions is,

(Refer Slide Time: 04:27)

equivalence classes, so the action of G on S partitions S into disjoint orbits, right. So if S is a finite set, then we can write the order of S or the size of S or the number of element of S as the sum of sizes of disjoint orbits so let us call this o1, o2, …, ok, where o1,..,ok are distinct orbits. Remember that orbits, two different orbits are always disjoint, so the two orbits are distinct, so they are either disjoint or same.

So you can always use this, these are the two important equations that we have attached to a group action. We have the counting formula which says something about the order of the group and then we have something about the order of set, and the most important actions for us in the context of the Sylow theorems.

(Refer Slide Time: 05:54)

So we are interested in the action of a group G on itself. Remember that the two equations that I recall for you are general statements, whenever a finite group act on a finite set S they hold. But we want to focus in these videos on the group G acting on itself. So in other words the set is also S, the set is also G and we are interested in the two important actions are the following.

So one, G acts on G by left multiplication, remember this means the action is given by g dot let me use the letter s, so g and s are of course in G but I want to distinguish between the group element and element when thought of as a set. So this is just action, so multiplication on the left. The other important,

(Refer Slide Time: 07:16)

action on G on itself is by conjugation. So here g acts on s by conjugation so gs is defined to be gs, g^{-1}. We checked in our earlier video that these are the actions of G on itself. So this gives the important class equation, this was the other important thing that we have learned about group actions. The action of G on itself by conjugation gives us the class equation. What is the class equation?

So we can write the order of G as order of conjugacy classes. So c1 through ck are conjugacy classes, distinct conjugacy classes of G. Recall that conjugacy class remember what is conjugacy class? Conjugacy class is simply orbit its an orbit for G acting on itself by conjugation. Okay, so I won't go into details because we have discussed this, except to say that,

(Refer Slide Time: 09:09)

there is a class equation for every finite group, we can compute in principle class equation of any finite group. I will recall for you, for S3 order is 6 and there are three conjugacy classes of orders 1, 2, and 3, so this is the class equation of S3. Okay, so now this is all for recalling.

Let me now go to the new stuff. So I want to in this video setup the Sylow theorems, first Sylow theorem and prove it.

So for that in these three theorems that we will call Sylow theorems, we are going to repeatedly and alternately use G acting on itself by conjugation sometimes, by left multiplication sometimes.
(Refer Slide Time: 09:59)

So suppose, so now suppose, G acts on itself, consider the action of G on itself by left multiplication, so one of the first of the two operations I mentioned of a group on itself. So this is the action of G left, on itself by left multiplication.

So now I want to define we want to define an action of G on subsets of S. Okay, so we know that G acts on itself by left multiplication, using that I want to define an action of G on subsets of S so S is actually G on subsets of G. So suppose let A be a subset, so I want to stress here, it is only a subset in general, not necessarily a subgroup. So it is just a subset. It is some collection of elements of G. And let small g be an element of the group.

Define g dot A, the definition of g dot A is very natural, so it is ga as a various in small a varies in capital A. So I will leave it as an exercise for you,
(Refer Slide Time: 11:33)

and this is very easy exercise, so if you recall or define the power set of G. So this is P of G is the set of all subsets of G, so the above action, so what I defined earlier defines an action of G on the power set. Right, so I define g of A to be ga, g times small a, as a varies in capital A. So now you can define this for any subset so I claim that it is an action of G on this new set namely the power set. What are the conditions to check?

Identity times any subset itself, that is clear, because if g is identity, g times a is just a and similarly the associativity property holds, which is trivial to check. So we have in action of the group on the power set, so now let us fix a subset of G.

What is a stabilizer of A? Let us explore this, what is the stabilizer of A? Okay, so remember stabilizer is, so I am going to use this notation, stabilizer of A is all group elements such that gA is A that's all.

So stabilizer is this, so I want to stress here that gA equal to A, means, what does it mean? So the set gA as a is in A, which is exactly gA is A. So in other words, if a belongs to a then ga also belong to A. This is the meaning of small g stabilizing capital A, so it must have the property that if small a belongs to capital A, then small ga belongs to capital A. Then we say that it stabilizes capital A, in particular it is not necessary that ga is equal to a, right that is not necessary, ga is equal to a, need not happen.

We do not need ga to be a, so it is not necessary. We need that ga is again in A, so certainly g times capital A equal to capital A doesn't mean g times small a is equal to small a.

So with that, now suppose that, so now let's go back to the general situation, G is a group acting on itself by left multiplication, okay, so now we are in the general situation that G is a group acting on itself by left multiplication and I have extended that action to subsets of G. So now let's look at following situation.
(Refer Slide Time: 15:52)

Suppose that you have again, G acts on itself by left multiplication and A is a subset of G, we have extended the action of G to subsets as above. Okay, now I am going to consider, let the stabilizer be, let H be the stabilizer of A, so remember this means it is all elements which fix the set A, not an element of A, they do not fix an element of A. They are allowed to interchange elements of A, you take an element of A small g maps it to some other element of capital A.

Okay, now I am going to prove that, so this, I am going to prove a small lemma here which I will use later. So the lemma is the order of H divides the order of A. So whenever I use this vertical bars I always mean order of that set, meaning the number of elements of that set. Okay, so and also I must tell you again that in the all the videos from now on G is a finite group. So we assumed that G is a finite group, okay so what is the proof of this?

So I want to show that order of H divides order of A, and the

reason is remember H is the stabilizer of A, so let small a be in capital A. Then since H stabilizers A, ha is in A for every h in H. So the set in the other words, the set ha as h varies in capital H is contained in capital A,right. So the, I want to call like this, I want to write like this, the H-orbit of a is completely inside A, is that clear? The H-orbit of small a is completely inside A. What is H-orbit?
H-orbit is simply what I wrote earlier. So ha, small ha, as small h in H. H-orbit is simply the orbit of A as you take elements of capital H, I am calling H-orbit as opposed to orbit, because I am, now I have a different group right, earlier I am considering G-action now I am considering H-action, so orbits are dependent on the group which is acting.
So to stress that here I am looking at the action of capital H, and I am talking about H-orbit, so the point is capital H is the stabilizer of A, so if small a is an capital A the H-orbit of small a is completely inside A. So in other words,
(Refer Slide Time: 19:10)

hence, A is the union of H-orbits right, because remember H-orbits are of course H-orbits are disjoint. And a must be the union of, why is this, why is it a union of H-orbits? Because if a belongs to A then the H-orbits of a, let us denote by H-orbit is completely contained inside A. So what is H-orbit? I am going to write it as ha, because it is small h times small a, as small h varies in capital H, this is simply the right coset. Right, this is right coset of a.

So H-orbit, if small a is a capital A the entire right coset is in capital A. So A must be a union of Ha, of course Ha will be same for different a's perhaps, Ha maybe equal to Hb, but they cover A, there is no problem. Now also we know that cosets are disjoint, so we can write A as, in fact, we can write A as a disjoint union of cosets.

So, right, we can write A, as some Ha1, disjoint union Ha2, disjoint union H(ar), so because again remember cosets which are equivalence classes for a group action are either same or they are disjoint. So A is union of Ha, because every small a is a some Ha, namely it is in Ha and they cover A of course.

Hence they cover A, the important point is Ha is, all of Ha is in capital A, so we have this. And once you have that, we just identify the distinct ones among them and write it like this. So A is a union of Ha1, Ha2, H(ar), so in particular the order of A is equal to order of Ha1 plus the order of Ha2, and so on up to the order of H(ar). Okay, now let's see, what is the order of Ha1? Order of Ha1 is just order of H. Similarly order of Ha2 is order of H, order of H(ar) is order of H again. So this is the order of H times r.
(Refer Slide Time: 22:02)

So order of A is equal to r times order of H. This means exactly that H divides order of H divides order of A, right. This is the meaning of dividing and here we are only using the fact that, so we used if you have Ha remember if you take a coset of a

subgroup, left or right it doesn't matter, the order is the same because it is a group property.
Small ha as you vary h, will be, there will be as many elements as there are elements of capital H. So this is an easy exercise that we have done in the previous videos, so this prove the proportion right, so let's recall the proportion or the lemma I called it. If you have G acting on itself by left multiplication and you take a subset of the group G and its, the subset is called as A and H is the stabilizer of A , then the order of H divides the order of A.

Okay, this is important for us when we do proofs of Sylow theorems later on. So now let us go ahead and start our discussion of Sylow theorems. So now our goal is to study.
(Refer Slide Time: 23:31)

So we are going to prove Sylow theorems. Okay, there are three Sylow theorems. I am going to state them and prove them one by one, but they all have to do with the following setup.

So G let G be a finite group. So I am going to, Sylow theorems are very important theorems to understand something about the finite groups. So we understand this in the following way.

So let p be a prime number, so we are going to write suppose the order of G is n, so we are going to write n as p^e times m, where p and m are co-prime. Remember that "co-prime" means p and m have no common factors because p is a prime number it simply means that p does not divide m, so this only means, in this situation, p does not divide m.

Okay, we can always write any number like this. So n equals p^e, power p power e times m. See for example if n is 6 and p is 2, we can write 6 as 2 times 3, if p is 3 and n is equal to 6, we write 3 as 2, 3 times 2. But if n equal to 6, so here e equal to 1 and m equal to 3. So write 2^1 here also e equal to 1 but m equal to 2. Now on the other hand if n is equal to 6 and p is equal to 5, how do you write this? It is 5^0 times 6, so e is zero, m is 6.

So e is, in this description, e is always non-negative. Right, and m is always at least 1, so n is at least 1. So its a finite group, so it must have at least 1 element. So we have this situation, so we simply look at how many times p appears in n, it may not appear at all like when it is 5 and n is equal to 6, or if n is 12 and p is 2, we have 12 equals 2 squared times 2, so e is 2 and m is 3. So we simply look at how many times a prime appears.

So now Sylow theorems are really statements about special subgroups of a group G and these subgroups are described by the element p.
(Refer Slide Time: 26:35)

So the important definition for us in this is: A, so G is a finite group as above, a "Sylow p-subgroup" of G is a subgroup of order p power e. So we of course write, it is important to write this, so the order of group is written as $p^e m$. So a Sylow-p subgroup of G is a subgroup order p^e, where p^e is the largest power of p that divides the order of the group G, okay. So a Sylow-p subgroup is a subgroup of order p power e.

So as an example, a Sylow-2 subgroup of S3 is a subgroup of order two. And if you recall our study of S3 in the previous videos, S3 has 3 Sylow-2 subgroups, because it has three elements of order two, each of them generates a subgroup order 2, so there are three Sylow-2 subgroups of S3. On the other hand, S3 has only one Sylow-3 subgroup, so I want you to get used to these notations, what is a Sylow-3 subgroup of S3? What is the order of Sylow-3 subgroup? Remember 6 is written as 3^1 times 2, so a Sylow-3 subgroup has order 3. And there is only one subgroup of S3 which has order 3.
(Refer Slide Time: 29:26)

And S3 has no Sylow p-subgroups if p is not equal to 2 and p is not equal to 3. Because if p is not equal to 2 and p is not equal to 3, that prime does not divide the order of S3, which is 6. So p^e will be p^0, so there is no subgroup of that order, so we only consider this, so this is the convention. We only look at Sylow-p subgroups, if p divides e, p divides order of group, in other words in my notation small e is positive.
On the other hand if G is a group of order 100, a Sylow-5 subgroup of G, let us think about it, what is, see 5 is a prime divide 100, so it Sylow 5-subgroups can be studied.

So what is a Sylow 5-subgroup of G? What will its order be? It will be order 25. This is because 100 are equal to 5^2 times 4, 25 times 4. So a Sylow 5-subgroup will have order 5 squared.

Similarly a Sylow 2-subgroup of G has an order, now 4, because 100 is 2 squared times 25. So Sylow 2-subgroup will have order 4, 2 squared. So we look at the largest power that divides the order, not just, for Sylow 2-subgroup it's not 2, its 4. Similarly Sylow 5-subgroup it is 25.

So these are Sylow p-subgroups of a finite group G and the Sylow theorems are statements about their existence, their properties, how many there are and so on. So I will stop this video here, in the remaining videos we are going to state Sylow theorems and prove them and then look at some examples and exercises. 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