NPTEL
NPTEL ONLINE COURSE
Introducing to Abstract Group Theory
Module 09
Lecture 45 – “Problems 10”
PROF. KRISHNA HANUMANTHU
CHENNAI MATHEMATICAL INSTITUTE

Okay, so, in this video I will continue my applications of Sylow theorems and problems based on Sylow theorems. But before that let me do actually a couple of small results that don’t use Sylow theorem. But, they are useful applications for group actions. So, let’s say this is a problem I want to solve today.
(Refer Slide Time 00:33)

Let’s say G is a group and p is a prime number and let’s say G has order p^e. Okay, in other words order of G is a power of p and let’s say e is at least 1. Okay, show that the center of G is non-trivial. Okay so, I will explain what this means.

So recall the center of G, which is denoted by Z(G), is all elements of G which commute with all other elements. So, the problem is asking us to show it is non-trivial.

So, we want to show order of Z(G) is at least 2. Okay, so remember this need not be the case. I will only say this, you can check this on your own. If G is S3 for example, the symmetric group on 3 letters, center is thriven. Of course, the symmetric group doesn't have this property that its order is a prime power. So, if you have this, prime power groups have non-trivial order. So, for this we consider the action of G on itself by conjugation.

Okay, so this is something we have seen before. So, in particular, we look at class equation. What is the class equation? It says that cardinality of, order of G, which I am assuming is P^e, is the sum of orders of conjugacy classes. But remember one conjugacy class is just {e}, this is the orbit of e. Conjugacy classes are orbits of elements under conjugation action. So, the class equation looks like, $p^e=1+|C2|+|C3|+\ldots+|Ck|$.

(Refer Slide Time 02:47)

Now we further apply group actions. So, what does counting formula say? Counting formula says order of G is stabilizer of some element times orbit of that element. Again this is p^e so we can certainly say that the size of a conjugacy class or size of an element, orbit of an element divides p^e. But what are the numbers that divide p^e? So, orbit of g must have size p^i for i = 0, 1, 2 up to e, it can be zero, of course.

Now let's go back to the conjugacy class equation. You have $1+|C2|+|C3|+\ldots+|Ck|$; using the counting formula I can say that, each of these is a power of p even 1 is a power of p. So, this is some $p^{a2} +p^{a3}+\ldots+p^{ak}$, correct.

(Refer Slide Time 04:33)

Suppose a2 is positive, a3 is positive, ak is positive, suppose they are all positive. Then, p^e will be $1+p^{a2} +p^{a3}+\ldots+p^{ak}$, and this whole thing is divisible by p, because if they are all positive.

That means p divides 1 because p divides p^e, p divides this sum, so p divides their difference which is 1. But this is absurd.

But, where did we go wrong? We went wrong in assuming that all the a_is are positive. So, some a_i is equal to 0. So, say a_2 is 0. That means what? $|C_2| =1$.
(Refer Slide Time 05:39)

But what is C_2? So a_2 remember is the, $|C_2|$ is p^{a2}, $a_2=0$. So, $|C_2|$ is 1. This implies C_2 which is the conjugacy class or orbit of some element g has only one element. But, what is orbit of g? It is all elements like this. But of course orbit definitely contains g. But that means aga^{-1} is g for all a in G. That means, ag = ga for all a in G; that means a belongs to the center. Sorry, this is not 'a' that I can conclude is in the center, a is varying so I can conclude g is in the center and remember g is different from e.

(Refer Slide Time 06:42)

Because I am taking the second thing that appears in the class equation, these are distinct orbits, e already is taken care of when we wrote 1. So C_2 being the order of g and g must be

different from e. So we have produced an element g in the center which is different from e. So that concludes that the center is non-trivial. Okay, so that solves the problem.
(Refer Slide Time 07:30)

So, if you have a group whose order is prime power, such groups are called p-groups, we have shown that the center is non-trivial. So, p groups have non-trivial center.

Now I am going to consider a special kind of p-group. Suppose G has order p or p^2, where p is prime then G is abelian. So it is not true that p-groups are abelian, all we know is that their center is non-trivial. So, there are non-identity elements in the center. But if it is either p or p^2 the center is everything, in other words is an abelian.

So, if $|G|=p$ then G is actually a cyclic group, implies G is abelian. There is nothing new here we have seen this before.
(Refer Slide Time08:35)

So assume $|G|=p^2$. So we want to show G is abelian. Equivalently we want to show Z (G) = G. Note that by the previous problem we know that the center is non-trivial. So, center must be bigger than just the identity. But now we want to show that it is all of G.

What are the possibilities for the center? So, center is a subgroup

(e) $\leq$ Z (G) $\leq$ G, which is between (e) and G. By the previous problem it is not equal to (e), so it is either G or it is strictly between. So suppose, if possible, Z G) $\neq$ G.

So, you should think for a minute if it is not clear to you, why the center being all of G implies G is abelian. This is just the definition of what a center is.

So suppose the center is not equal to G. So choose x ϵ G, x not in the center Z(G), right. If x is not in the center, if center is not all of G there must be something that is not in the center. Let's consider the conjugacy class of x, that means C(x) = $\{gxg^{-1} \mid g \epsilon G\}$. Okay so, this is called the centralizer of x, recall, and it is a subgroup. And I will let you do that easily, check that it is a subgroup of G. Because identity certainly has this property, if two things have that property their product has this property and if something has this property inverse also has this property.
(Refer Slide Time11:00)

Now, this is easy check. It is also easy to check that center will always be contained in the centralizer, because center, remember is all elements which commute with everything. So, if something commutes with, sorry this is actually, I made a mistake here so, actually let me erase all this, I got confused. I am not looking at the conjugacy class. I'm looking at the centralizer.

Consider the centralizer of x, I will call it C(x). This is by definition {g ϵ G| gxg^{-1} =x}. Okay so, this is a subgroup of G and this contains the center Z(G). That is what I want to say. Why is this? This is all group elements which commute with everything. C(x) is the group elements which commute with x so, Z (G) contains C(x). So, what do we have?

We have (e), we have Z (G), we have C(x), we have G. The reason we need p^2 is this, so this is order 1, this we are assuming is order p because it is strictly between G and ZG and this is p^2 and C(x).
(Refer Slide Time 12:49)

Remember, C(x) contains x because x certainly has this property: xxx^{-1} is x. So, Z(G) and Z(G) does not contain x, that is our assumption. So this implies Z(G) is contained but not equal to centralizer. So, this must be p^2.

That means, so C(x) = G, all of G itself, that means g x = x g for all g ϵ G right, that is the centralizer. It is all elements which have g x = x g, but that is all of G, so g x = x g for all G.

But this in turn means that x ϵ Z (G), this is a contradiction right, because we chose x to be not in Z (G). So this shows that any group of order p^2 or any group of order p is abelian.
(Refer Slide Time14:13)

So, now using these two facts which do not require Sylow theorems at all, these two problems, I am going to do a third problem which does use Sylow theorem.

So, let's say G is a finite group and p divides |G| and as always p is a prime number. Okay, in fact, suppose that p^e divides |G| then G has a subgroup of order p^e. Okay so this is the problem.

This looks very much like first Sylow theorem but with some difference, the first Sylow theorem is the key statement we will use but we have to do some more work because the first Sylow theorem says that, you take the largest power of p that divides |G| then there is a subgroup of that order. Here, I am not assuming that p^e is the largest power. So, how do we do this? So, first without loss of the generality we can assume G is a p-group, that is $|G| = p^{n.}$

(Refer Slide Time15:56)

Why is this? Meaning why can we assume this? So, write G as some, I think maybe I should not use e here. Let's say, suppose G is a finite group and p^i divides G then G has a subgroup power of p^i.

(Refer Slide Time 16: 20)

And here I can assume that I claim this. So, write like this, like we do in the Sylow theorem, so p does not divide m. Sylow I implies G has a subgroup order p^e, say H is the subgroup of G of p^e . Now, if $i \leq e$, if we show, take $i \leq e$, if we show H has a subgroup of order i, then G also has a subgroup right, the same subgroup which is the subgroup of H is also a subgroup of order p^i for G also. So, it's enough to show that H contains a subgroup of order p^i. So, we can restrict our attention and this, in order to make this assumption we need the Sylow theorem, in the rest of the proof we do not need. So Sylow theorem is needed for this reason.
(Refer Slide Time 17: 52)

So, assume now that G is, we can from now on assume $|G|=p^e$ and $i \leq e$, we want to show G has a subgroup of order p^i.

Okay, just to quickly recap why we can make this assumption: G need not be a p-group but it will have, its order will decompose like this, Sylow I says that G has a subgroup of order p^e and if you prove the problem for that subgroup, we have solved the problem for the given subgroup, given group G. So we might as well assume that G is a group of order p^e.

Now by a corollary of first Sylow theorem, we can assume that. No, not corollary of the first Sylow theorem, by the first problem of this video, the center of the group is non-trivial, right. We have shown that a p-group has non-trivial center. So, take, it has non identity element. So I can always choose an element, let's call this x, of the center such that order of (x) = p.

And in order to do this I used the corollary to the first Sylow theorem. Remember there is an element of the center which is not identity, order of the center is also a power of p, in other words, the center is also a p-group because order of the center divides p^e. So, the order of the center is also a power of p. So an element will have order a power of p. So, by taking a suitable power of it, we can assume that it has order p. So look at Corollary to Sylow I that we have done in that video for producing such an x and now let H be the subgroup.

So I am starting with a new notation here. Whatever I called earlier H is gone now so, G is a group of order p^e and H be the subgroup generated by x. So, H is the subgroup generated by x so $|H| = p$, of course, because order of x is p.

(Refer Slide Time 20:40)

More than that, H is in fact normal in G. Why is that? Because x is a central element, x is in the center. So how do you show something is normal? Take an arbitrary group element g and an arbitrary ring element, it will be some x^n and multiply by g^{-1}. But remember x is in the center right, we have chosen an element x of the center. So, x^n also is in the center so $x^n gg^{-1} = x^n$, this is of course in H. So H is normal in G.

(Refer Slide Time 21:28)

So, in particular we can consider the quotient group G/H. Right, if you have a normal subgroup of a group you can consider the quotient group and look at the map from G to G/H, the natural map so, g going to the coset gH.

What is the cardinality of, order of |G/H|? By the counting formula this is the ratio, p^e this is p so, so this is p^{e-1}, okay. Now, by induction, so I am going to basically solve this problem by induction. So we use induction. $|G/H| = p^{e-1}$ which is less than p^e.

So, we can assume by induction that G/H has a subgroup, say K^1, such that the $|K^1| = p^{i-1}$. So, I am going to construct, my goal is to construct a subgroup of order p^i for G.
(Refer Slide Time 23:05)

I am going to construct, I am going to use induction hypothesis to suppose that G/H, which is a group of order less than p^e has a group of order, subgroup of order p^{i-1}.

So, what is the picture: we have G, G/H, K^1, which is the subgroup, this has order p^{i-1}, this has order p^{e-1}, this has order p^e. How do I get, so this is the picture how do I get the K that I we want, the group of order subgroup of order p^i? Okay so, naturally your guess would be, I take φ^{-1} (K^1), call that K.

So, let K be phi inverse (K^1). It is an easy exercise that I may have discussed when I talked about homomorphisms, inverse image of a subgroup is a subgroup. So, K is a subgroup of G. We claim that K is the desired subgroup, we claim that $|K|=p^i$.

So remember our goal is to construct, given than G has order p^e and $i \leq e$, we want to show G has a subgroup of order p^i. We use induction and go to a smaller group which is G/H and apply induction to that to guarantee that there is a K^1 for, which is a subgroup of G/H which has order p^{i-1}.

(Refer Slide Time 24:45)

And I am simply taking the inverse image, K will be the inverse image. So, it is a subgroup, that is trivial. We want to show that in fact, its order is p^i. So, why is that? This is very easy now. So remember, we have G to G/H, K is here and K to K^1, we have a map.

(Refer Slide Time 25:08)

Because K, this is phi, this is phi restricted K. And because K is the inverse image of K^1, K maps to K^1. So, what is the kernel of this map? Remember what is the kernel of phi first? Kernel of phi is of course H, right. kernel is the inverse image of identity element. So K^1 contains the identity element, so its inverse image will contain all of the kernel, so K contains H. We have this also, so kernel of phi restricted to K, I claim, is also H. Because how can something go to 0 here or the identity element here?

If it goes to identity element here, it already goes to identity element here, so it is in H. So, if something is in H it is already in K, so kernel of this is H. And of course phi restricted to K is also onto, it is onto right, because phi itself is onto. So, this is also onto.

So forget this now, focus your attention on this map and apply counting formula. It says that, or the first isomorphism theorem really, first isomorphism theorem says that K mod kernel of this map, which I am denoting by phi restricted to K, is isomorphic to K^1.

But that is same as, because kernel is H, this implies that now the counting formula says that |K| by |H| is $|K^1|$, which remember is p^{i-1}. So $|K| = p^{i-1}$ times |H|, but the order of H is p, okay.

(Refer Slide Time27:04)

So thus we have produced a subgroup K of G of order p^i. Okay, remember this was the problem. Problem was to show that if you have a group G such that p^i divides the order of G, then there is a subgroup of order p^i. So now, first using the first Sylow theorem, we have reduced to the case that G has order p power e; that was the crucial restriction and that needed Sylow's first theorem.

Then we used the fact that, for such p-groups the center is non-trivial and to get hold of this x which made all the proof work. And then, we go to G mod the subgroup generated by x, use induction to show that that has the right subgroup and we take the inverse image and then a quick application of first isomorphism theorem and counting formula says that the inverse image has the desired property. So, this proves the problem and this completes the video and the course.

I wanted to cover the standard things that are done in a group theory course: so we have done Lagrange's theorem, cosets, quotient groups, Cauchy's theorem, group actions which is the most important topic here and using that we have done the Sylow theorems. So this is the material that is covered in any standard course in group theory and if you understand this course fully, then you know the group theory that is expected in a B.Sc or a M.Sc course. 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
Laksmipriya
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 Krishnamurthy
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
www.nptel.as.in