NPTEL

NPTEL ONLINE COURSE

Introduction to Abstract

Group Theory

Module 05

Lecture 24- "Cauchy's theorem"

PROF. KRISHNA HANUMANTHU

CHENNAI MATHEMATICAL INSTITUTE

So in this video I am going to prove an important theorem, a special case of important theorem called Cauchy's theorem.

(Refer Slide Time: 0022)

So this is a good application of the concept of quotient groups, so this is useful to you will understand in proof why is it is useful to look at quotient groups. So Cauchy theorem says that so this is the following, so let G be a finite abelian group. So it is a finite group so meaning it has only finitely many elements and it is an abelian group meaning any two elements in G commute with each other. Suppose that a prime number P divides the order of G.

So P is a prime number that divides the order of G, then G has an element of order P, so then G has elements of order p. So this is Cauchy's theorem. We will first prove this and then look at why this is a surprising statement. If G has an element of order p it is a strong condition on the group, so and it is important to note that P must be a prime number. So all this we will see after we prove the theorem and see where we use the prime number hypothesis.

Again let us see the statement. G has an element of order p what is an element of order? Order of an element, recall order of an element A is the least positive integer d such that A power d is identity. So there is such an element in the group G. so we are going to consider the size of the group, so we will prove this in two cases, we will consider two cases. So the cases are the following.

Case1: G contains, G does not contain a subgroup H such that 1 is strictly less than order of H which is strictly less than order G. So remember G is a finite group so I can talk of order of G, is the number of elements, so suppose G does not contain a subgroup H which has this property. That means cardinality of H is strictly greater than 1 means H contains elements that are different form identity element. And order of H less than order of G means H is a proper subgroup.

(Refer Slide Time: 04:02)

If G does contain such an element, so then I will first solve this problem in, prove the theorem in this case. So choose an element A in G such that A is different from E, E is the identity element. Why is there an element A such that A is different from E? Such an element exists because cardinality of G is greater than 1. Why is cardinality of G is is greater than 1? Because I am assuming that a prime number p divides the order of G, so if cardinality or order of G is 1 certainly no prime number divides it, prime numbers are

2, 3, 5, 7 and so on, so order of G is at least 2, that means there is an element A which is different from E.

Consider the subgroup generated by A. Now what are we considering in this case? This case we are assuming that that G does not contain a subgroup H which is non-trivial and proper, because A is different from E, by hypothesis A is different from E by choice. So the subgroup generated by A cannot be identity and hence it has to be all of G, because G does not contain any subgroup that is non-trivial and proper, if A is the subgroup generated by A, then it is non-trivial because A is different from E, so it must not be proper so it is equal to G. On the other hand, so in particular G is cyclic group. What is the order of, note that if you have a cyclic group generated by A, order of G is equal to order of A.

Because, this is because, G is nothing but E, A, A^2 , A power (order of A)-1, you take powers of A and go all the way up to (order of A)-1, the next power which is A power order of A will be E, so this is G, how many elements are here? Order of A many elements are there, so that is the order of G. So now and what are the assuming? We are assuming that P, we assume we know, P divides order of G which is order of A.

So now we have to exhibit an element of order P, so if P divides order of A, so I am going to, so best way to complete now is through the following exercise, so I will leave it as separate exercise and do this later in a separate video or may be in the same

video, but it will interfere with the proof of Cauchy's theorem. So I don't want to spend time on this, if G is a cyclic group of order N and M divides N, then G contains an element of order M.

So this is not a difficult exercise at all and this is a very general, so M, N are positive integers. And it has nothing to do with primeness, so G is a cyclic group of order N and M is another number that divides N, then G contains an order of element M so this so this is sort of a converse to Lagrange's theorem, which I proved earlier, what is Lagrange's theorem? It says that G has a finite group and we have element its order divides the order of the group.

I am saying now that if I am further assuming G cyclic and a number divides the order of group then there is an element of that order.

(Refer Slide Time: 09:56)

Now the by the exercise, G contains an element of order P, because G is cyclic, that is what we have concluded, G is a cycle group, so and P divides the order of the group, so G has an element of order P, so if the group is assumed to be cyclic, very strong statement is known, much stronger than Cauchy's theorem, it says that if P is a prime number, and P divides the order of the group, and G is abelian, that is the version of the Cauchy's theorem that we are doing now, there is an element of order P. But the exercise is saying that if G is cyclic, life is much simpler, for any M dividing the order of the group, there is an element of that order.

So I will do this exercise later, but we are done, assuming that exercise. So now let us go to case two, so in case two what is the complement of case 1, case 1 was there is no subgroup of G which is non-trivial and proper, so case 2 would be there is a subgroup of G which is non-trivial and proper, so there is a subgroup, H of G, which is non- trivial and proper, that is H is different from the trivial group, that is H is different from G also, so we have 1 strictly less than order of H which is strictly less than order of G, okay.

Now I am going to use induction on G, so what does the theorem say, theorem says that if G is a finite abelian group and a prime number divides its order then G contains an element of that order, so what would be the base case of induction, because I want to take an order, which is divisible by a prime number, order of G is two, G is a and e and order of G is divisible by two and order of a is two, so only prime that divides the order of G is two and there is an element of order two, this is okay, base case is proved.

(Refer Slide Time: 12:56)

So now I can assume that up to some number all groups of that order which are abelian and if a prime number divides them, there is an element of order p. So now we know that order of H is strictly less than order of G, so suppose that P divides order of H, this is not necessarily true but suppose it is true. We only assumed that P divides order G. Suppose that P divides order of H.

Then by induction because the order of H is strictly less than order of G and we are looking, induction hypothesis is that anything which has order less than the order of G the theorem goes, now H is an abelian group, G is abelian that implies H is abelian, abelianness is inherited by subgroups, any two elements of G commute with each other, so any two elements of H also commute with each other, so H is abelian, its order of H is G and P divides order of H, so by induction H contains an element of order P.

(Refer Slide Time: 14:51)

So this is the induction statement, but if H contains an element of order of P then so does G. That is immediate right, if H contains a of order P, then a belongs to H, order of a is P, implies a belongs to G, H is a subgroup of G and order does not change, order of a is order of a, so G contains the element of order of P, so this is the easy case, if P divides order of H then we are done.

So, suppose that P does not divide order of (H), this can happen right, P divides order of (H) or P does not divide order of (H), but now recall counting formula, that we learned while proving Lagrange's's theorem. It says that order of (G), is equal to order of H times order of (G/H), the index right, now since we have assumed that G is abelian, every subgroup is normal right, in an abelian group, G/H is a group and note that order of G/H is the index of H in G, (G:H). Now if you look carefully at the counting formula, the order of G is equal to order of H times order of G/H right, and what is the hypothesis? Hypothesis is that, P divides order of G.

And hence P divides order of H times order of G mod H, and a property of prime number says that, P divides order of G mod H, see P divides order of G, P does not divide order of H, so P divides order of G mod H, this is a property of prime numbers, if P is a prime number and it divides the product of 2 numbers, it must divide one of them, and it does not divide H, is our hypothesis so P divides order of G mod H and, note that order of G mod H, is equal to order of G mod order of H, which is less than, order of G, also because H is a nontrivial group, this is because order of G, order of H is greater than 1, so induction hypothesis is okay, so in order to make sure that, induction hypothesis is applies to G mod H, we need to check that G mod H is abelian group, is that clear?

If G is abelian, G mod H is abelian, this is a very easy exercise, that I will do later in a video, G mod H is abelian, order of G mod H is less than order of G, and P divides, order of G mod H, that is what I noted here, so induction hypothesis applies to G mod H. So I want to emphasise a very important point here that, I need to assume that G is abelian okay, that is why I state in the original theorem, that G is abelian.

Because if G is abelian only you can consider G mod H for an arbitrary subgroup H, otherwise G mod H is not a group, it is just a set of cosets. So now what does the hypothesis say? Induction hypothesis so, by the induction hypothesis, G mod H contains an element of order P, right, because G mod H is an abelian group, its order is divisible by P, and its order is less than order of G, so it contains an element of order P, but what are elements of G mod P,

they are left cosets of H in G, so say gH in G mod H has order P, right.

This means gH power P is equal to H, because that is the meaning of order, gH power P is H and gH is not equal to H. If order of gH is equal to P implies this, P is the smallest positive number such that gH power P is identity which is H, in G mod H identity is H, so gH power 1 because remember P is strictly more that 1 always, P is a prime number so gH cannot be H and gH power P is H. But what is gH power P that means g power P H is H, right

(Refer Slide Time: 21:12)

and of course gH is not equal to H, that means g power p is H and g is not in H this is the meaning when you pull the element back to G. g is an element of G, it is p-th power is in H and itself it is not in H okay.

(Refer Slide Time: 21:17)

So g power p is in H and g is not H. Now let us denote by m the order of H, okay, so I am just giving it a name. Let m the order of H. Then what we have is by Lagrange's theorem applied to H and what is Lagrange's theorem? It says that if you have a group and an element in it, order of the element divides order of the group.

(Refer Slide Time: 22:08)

Order of g power p divides order of H which I called m, okay. If order of g power p divides m and this is something I have showed before, g power p whole power m is equal to e. This is the exercise that, this came up in several places, if g is an element of group G and order of g is let's say a and then g power an is e for all n right, so if here m is divisible by order of g power p, m is order of g power p times something.

So g power p power m is identity. This means we have g power pm is identity. I also remarked numerous times, that usual exponent rules apply to taking powers in elements of groups. So this is remember I can always switch the exponents. So, g power p whole power m is identity means g power m whole power p is identity. So now can we say, that order of g power m is p, can we say this?

See not quite, right, because what is order of g power m? This is this least positive integer such that g power m power p is identity. We have certainly g power d, least positive integer, d such that g power m power d is identity. We know that g power m power p is identity, but what if there is a smaller number, we can certainly say is that order of g power m divides, okay so this is also an exercise this is sort of converse to this exercise that I wrote in the box here.

That also we have repeatedly discussed, if you have an element of order is 3 only we have that a power will be equal to identity if you take multiples of 3. Right, so recall if order of g is a and g power n is identity, then a divides n, using this we conclude that order of g power m divides p, because g power m power p is identity, so order of g power m must divide p. Right, this is discussed in various previous videos.

So, now hopefully you remember, otherwise go back and see some of the videos that talk about this. But now p is a prime number so we are going to use this fact now, and I think this is the first time we using that p is a prime number right.

(Refer Slide Time: 26:41)

So p is a prime number, so actually it is not first time, we have also used it here. To say that if p does not divide order of H if p is does not divide order of H, it divides order of G mod H, here also we used. So p is a prime number so only numbers that divide p are 1 and p, so order of g power m is 1 or order of g power m is p. Right, I have observed here that order of g power m divides p, but p is a prime number so order of g power m is 1 or order of g power m is p.

Because only numbers that divide P are 1 and P. But order of g power g is 1 means what? g power m is identity, an element has order 1 if and only if it is identity, but if g power m is identity that means, if g power m is identity, apply Lagrange's theorem, so now I will do, so g power m is identity let us say. So I want to say that this is not possible, why? The reason is this is not possible because g power m is identity right, suppose g power m is identity, this implies order of g okay, so if order of g power m which we know either 1 or P if the order of g power m is 1 then g power m is E if which I clam is not possible.

So why is that? If g power m is E then certainly gH power m is g^m H which EH which is H so g power H, g H power m is H, but

recall how did we pickup gH, order of gH is P, that is the way we constructed, we chose, because by induction hypothesis applied to G/H it contains an element of order P so gH was that element, so gH power m = identity and order of gH = P that means P divides m by the same exercise as before if order of g is A and g power N is E then a divides N.

But P divides m, this is not a good thing right, because then P divides what is m, m was order of H, so we simply called the m the order of H, somewhere I wrote that right, we let m be the order of H but we are assuming the P does not divide order of H, because if P divides order of H we would not even do all this, if P divides order of H we are done right away, so does not divide order of H is our assumption and now we are getting the P divides order of H so g power m cannot be equal to E, so this is not possible. So order of g power m is P and we are done because remember we want to exhibit is the element we are looking for, g power m is the element we are looking for.

We want to exhibit, this completes the theorem proof of the theorem, we want to exhibit an element of order P. Just to recap, so this is, you have to carefully follow the proof that I gave, I am going to spend 2 minutes recalling the proof how we did this.

The Cauchy's theorem says that if G is a finite abelian group and P is a prime number that divides the order of G then G has an element of order P. The first which is easy is that G has no non-trivial proper subgroups, then we conclude immediately the G is cyclic. And by this exercise which I will do later we are done.

So the interesting case is, there is a subgroup of H of G which is non-trivial and proper. Then using abelianness of G, we have that H is normal which we use later. So we know that order of H is greater than 1 and less than order of G and we use induction, if p divides order of H, so by the counting formula, p must divide either order of H or order of G mod H.

Because P divides order of G and P is a prime number. If P divides order of H immediately by induction H contains and order P element so G also contains an order P element, the same element. Otherwise G mod H contains an order P element. Let us call that gH, then we played with that element and concluded that an element that is related to it is the element we are looking for.

Okay, so the last part of the proof is somewhat tricky perhaps, so you have to carefully read the proof and listen to my proof once more if needed to make sure that you understand, okay, so this complete the proof of Cauchy's theorem.

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

HYPERLINK "http://www.mptel.ac.in"www.mptel.ac.in