NPTEL

NPTEL ONLINE COURSE

Introduction to Abstract

Group Theory

Module 05

Lecture 25 –"Problem 6"

PROF. KRISHNA HANUMANTHU

CHENNAI MATHEMATICAL INSTITUTE

(Refer Slide Time: 00:55)

Before we look at some examples, I want to make an important remark. Cauchy's theorem also holds when G is not abelian, so you remove the word abelian in the theorem, so G is a finite group and P is a prime number that divides the order of G then G contains a element of order P, this is also true okay, this requires more machinery to prove and we do this in later in the course.

So after I develop more machinery required to prove this, we will prove this. In fact we will prove what are called Sylow theorems which contain this and which in fact say much more.

So let me give you quickly an example to illustrate the fact that p needs to be a prime number in the theorem. Consider the group, so I am going to consider a few two by two matrices, so one zero

zero one, minus one zero zero minus one and one zero zero minus one, minus one zero, zero one.

So G is a group of order four okay, so G is a subgroup of, here the operation is multiplication, so G is a subgroup of GL2R, so remember this all, note these all are invertible matrices. They have all determinant one or minus one, so they are invertible matrices it is subgroup of GL2. And fact that it is subgroup is clear, I will give this name, so just to, for ease of working of this, let's call this as E and let us call this as a1, let us call this a2, let us call this a3.

(Refer Slide time: 02:52)

So G is identity element that I am calling E, right, what is a1 square? a1 square is e, that is this matrix multiplied with itself, that is same as a2 squared that is same as a3 squared. What is a1a2? That is if you multiply these two matrices you will see that, it is easy to say that it is a3. a1a3 is a2, a2a3 is a1. So this is the entire group of structure on this. The data, multiplication table is completely given by this.

So G is order group in order four group, so G is an abelian group of course, and in fact we have seen in a previous video that any group of order of five or less is abelian , so this is certainly abelian and you can see that from, I should written this, that is same as a3a1 okay so that is easily verifiable from the given format, so these matrices are given you multiply these matrices, if you do not know the matrix theory, to see that how to multiply matrices and so on, do not worry about it, just think about G as group like this, with these operations, with this multiplication table, a1, a2, a3 all have, G has one element of order one and three elements of order two.

Okay, so as I said if you do not feel comfortable with matrix representation, just do not worry about it, and think about G as a group consisting of four elements E, a1, a2, a3 with this multiplication table, they are, a1, a2, a3 have order two meaning, their squares of all identity and multiplying any two of them will give you the third, in any order, so a1a2 is same as a2a1 which is a3. This is a valid group and it is a group of order four. G is called Klein four groups. Okay, it is called the Klein four group.

Is it cyclic? Is it a power of, is it the group generate by some specific element, it is not right, because it is certainly not group generated by E, is it the group generated by a1, no a1 squared is identity. So the group generated by a1 is just E a1, similarly group is generated by a2 is e, a2, because a2 is also order two, same with a3.

(Refer Slide time: 06:09)

So it is not cyclic, because it has no element of order four. Right, in order for a group of order four cyclic, it must contain an element of order four. In this case it does not, so this is another group of order four, we have seen that there is a group of order four namely the cyclic group of order four, this is not a cyclic group of order four. And it is actually an exercise which I will do maybe later, that up to isomorphism these are the only two groups of order four, both are abelian, one cyclic and the other is not cyclic. Now this is an important example to give you a various, to illustrate various points.

(Refer Slide time: 07:04)

First of all, the converse of Lagrange's theorem fails here, right, the converse of Lagrange's theorem, what is the Lagrange's theorem? If in an element, in a group, the order of an element divides the order of the group. On the other hand, here four divides order of G, which is of course, four, but G has no element of order four.

Similarly this example shows that p in Cauchy's theorem must be prime right, because four divides the order of group G, G is a finite abelian group, four divides the order of G, but G has known element of order four.

The problem is 4 is not a prime. So only if a prime number divides the order of a group, we can say there is element of that order, and that of course checks out here, because order of the group here is four, and the only prime that divides that is two, and certainly G has a element of order two.

On the other hand if G is a cyclic group of order four, say G is one, a, a2, a3. Then also G has an a element of order four, or element of order two in, namely a^2, Cauchy's theorem applies to this and says that if two divides four, two is a prime number it must have an a element of two, so it does because it a square.

So in this case there is only one element of order two, because order of a as well as order of a squared and order of a cube is two, is four rather, order of a square is two, order of e, let call this element as e, order of e is one. So the cyclic group of order four has one element of order one, one element of order two, two elements of order four. Whereas the Klein four group has one element of order one, three elements of order two.

There is always in element of order two in a group of order four by Cauchy's theorem, in an abelian group of order four. But of course every group of order four is abelian so there is no need to separately say abelian but Cauchy's theorem also say if you have 10 order 10 abelian group, it must have order two element and an order five element.

(Refer Slide time: 10:13)

So here I am doing problems. Problem one, so let's start with a couple of very easy problems, just to get started, so let us say G be a cyclic group and let H be a subgroup of G, then G mod H is cyclic okay.

So first of all recall that G is cyclic implies G is abelian, in a cyclic group is certainly abelian, implies H is normal in G, so G mod H is a group, so in order to even say G mod H is a cyclic group, first we need to know it is a group, but it is a group, so we need to know observe that it is a cyclic group.

What is a cyclic group? Suppose G is generated by A, so G is equal to A power n, n belongs to Z. So powers of A exhaust all of G, so G is every element of G, is power of A, now what is G mod H? G mod H is g times H, where g is in G, okay, these are the left cosets of H in G.

(Refer Slide Time: 12:11)

So we claim that, what is your guess, we are trying to show that G mod H is a cyclic group, if G is a cyclic group, G mod H is a cyclic group. In the other words, we have to exhibit a generator for G mod H, it is obvious to guess what? If G is generated by A, AH generates G mod H, and this is easy, because you take gH, for g in G, if g is in G right, g equals A power N, for some A. Right because A generates group G, every element of G is a power of A, so gH is equal to (A power N)H, but by the operations of cosets, this is just AH power N, so G mod H, is equal to AH, power N, N belongs to Z. Of course, we are not saying that they are all distinct elements, some of them will collapse, if it is a finite group for example, they will collapse. But that is irrelevant here, G mod H is generated by AH, so this is the solution, so if G is cyclic then, then

G mod H is cyclic. And in fact the coset of the, element, generator generates the quotient group.

(Refer Slide Time: 13:35)

Let us do one more problem which is very similar and also very easy. If G is abelian, and H a subgroup of G, show that G mod H is abelian okay. As I said this is also extremely easy, to show that a group is abelian, you have to start with two elements of the group, in this case the group we are interested in showing is abelian is G mod H, so let us take two arbitrary elements, AH, and BH. These are a two left cosets, what is the AH times BH. By definition of the group operation on the quotient groups, this is ABH, but AB is equal to BA, because your group is abelian and this is same as AH, okay, so this is okay, this is also a trivial exercise, let us do one more interesting exercise.

(Refer Slide Time: 14:39)

This is slightly more work, so more interesting. Suppose G, let ZG be the centre of G, okay, if G mod Z is cyclic show that G is abelian.

In order to first solve the problem, let's first we call what is the centre, remember ZG is all elements A in G, which commute everything else in G. So A in G such that that Ag is equal to gA to all g in G, so this is the centre. So now we are assuming that G mod ZG is cyclic, we want to show Z is, G is abelian here, okay, in order to show abelianness as in the previous problem we have to take two arbitrary elements, and to show, we want to show, show that AB equals BA, right let us keep this in mind, we want to show AB = BA.

So now since G/Z(G) is cyclic, it has a generator, right it is generated by some element of G/Z(G), right so this G/Z(G) is a cyclic group it is generated by an element of that, say g Z(G), so an element of this simply a left coset, so take a left coset and suppose that it a generator, that means everything in G mod Z(G) is a power of this, so in particular we have AZ(G), see AZG and BZ(G) are elements of G/Z(G) so they are generated by gZ(G). So it is some g(Z(G) power I and BZ(G) is some Z(G) power J, for some integers I and J, okay that means because gZ(G) generates it these two elements are power of it, so that means AZ(G)=(g power I) Z(G) and BZ(G)= (g power J)Z(G), this is the meaning of coset multiplication. But now let us pull this relation back to the group G. So this means, so what is this mean? That means A times something lets x, in the center is equal to g power I times something, where x and x prime are in the center, right because A times that, as cosets they are equal, that means A times an element of this is equal to an element of this, so A times x will be equal to this.

(Refer Slide Time: 19:07)

So I can rewrite this as A= g I power X for some X in Z(G), okay so this X and X prime I am interchanging so it is actually this X here is this x prime times x inverse because X and X prime are in the center, X prime times X inverse is also in the center, so I am renaming everything to call it X. Similarly we have B = g power J times Y for some Y in the center, so far fine, right, A = g power I times X for some X in the center, similarly B = g power J times Y for some Y in the center. Now let us go ahead and calculate AB, now that we have written everything in terms of elements of capital G and not as cosets, let us write AB.

So this is g power I X g power J Y, but now what is X and Y, X and Y are in the center, so they commute with everything, so this is same g power I, g power j, X, Y right, this is g power I +J, XY, on the other hand, what is BA? This is g power J, Y g power I, X again using the fact that X and Y are in the center, AB=BA, so I am using the fact that g power I and g power J is g power I +J and X and Y are in the center. So this shows that because A and B were arbitrary elements of the group and they commute, G is abelian okay.

(Refer Slide Time: 22:00)

So if G mod is the center cyclic, G is abelian.

So the next problem and this is the problem that I used in the proof of Cauchy's theorem. It says the following. Let G be a cyclic group. Suppose that, which is finite so this is finite cyclic group. Suppose that M divides, M is a positive integer, suppose M is a positive integer that divides the order of G, okay, so then show that G contains an element of order M. So that is the problem, so solution, so this is problem 4 I think okay.

Solution is the following. So suppose that G is generated by A right, so G is finite cyclic group okay, so G must be of the form E, A, A^2 , A power (N – 1), where N is the order of A as well as order of the group, right so G is like this so G has N elements and order of A is N. And if M divides consider the element A power N /M.

(Refer Slide Time: 24: 01)

So consider this element, A power N/M. See that because M divides N and M is a positive integer remember M is a positive integer, N by M is also an integer so A power N by M is a valid element of the group, it is A multiplied by itself N by M times, so A power N by M power M is of course A power N which is identity, remember as I have repeatedly said in the past, you can apply the usual exponential rules to group operations.

So A power N by M, if you call this element B, B power M is E, can we say order of B is M? If so, we are done, right, because we are trying to show that G contains an element of order M, if order B is M we are done, but actually we cannot right away say this, in order to say order of B is M, you have to say, no not yet we can’t say this yet, what is order of B? Order of B is the least positive integer D such that B power D is E, right, certainly M is a candidate for it B power M is E, but we have to rule out the possibility that something less than M has this property.

(Refer Slide Time: 27:04)

So if B power D is E, so let us say, for suppose for some D < M, we have B power D is equal to E. Then let us see what are the consequences of this, B power D is E, this means A power N/M, so remember A power N/M is DB, power D is E, right this means A power (ND /M) is E but if D is less than M , ND/M is less than N correct, because D by M is less than 1, but this contradicts, we have a power of A equal to E but that power is less than N, we have a contradiction, we have contradicted the fact that order of A is N, right.

(Refer Slide Time: 29:40)

Because order of A is N means N is the smallest positive integer such that A power N is identity, but here we are getting A power (ND/M) is E and ND/M <N. So this a contradiction and only assumption that we could have possibly made incorrectly was that D is less than M, so we must have, so A power M identity and A power D is identity implies that D is at least N, so order of B power M I, sorry I should not have said A power M, B power M is identity where B is A power N/M, B power M is identity and no smaller power of B is identity. So order of B is exactly equal to M and this completes the solutions of the problem because we want to show G contains element of order M and we have shown that because B is that element okay.

I will only remark one more time that we have seen the example of Klein 4 group, where you have a group of order 4 yet the group does not contain an element of order 4, of course this is also illustrated by the symmetric group on three letters S3, S3 has 6 elements, but it not cyclic.

So it has no element of order 6, so the statement that G contains an element of order M if M divides the order of G is simply false if G is not cyclic. So let me remark, it is crucial that we assume G is cyclic in this problem, because example take G to the Klein four group or G is S3, this has order of 4 and this has order 6, but they are not cyclic, not cyclic, and they have no element of order 4 or order 6 respectively, okay. I will stop the video here, hopefully these problems gave you some idea of how to apply various results that we have learned and you should try to do more exercises that I have been giving in the videos using these ideas. Thank you.

Online Editing and Post Production

Karthik

Ravichandran

Mohanarangan

Sribalaji

Komathi

Vignesh

Mahesh Kumar

Web Studio Team

Anitha

Bharathi

Clifford

Deepthi

Dhivya

Divya

Gayathri

Gokulsekar

Halid

Heamvathy

Jagadeeshwaran

Jayanthi

Kamala

Lakshmipriya

Libin

Madhu

Maria Neeta

Mohana

Mohana Sundari

Muralikrishnan

Nivetha

Parkavi

Poonkuzhale

Poornika

Premkumar

Ragavi

Raja

Renuka

Saravanan

Sathya

Shirley

Subash

Suriyaprakash

Vinothini

Executive producer

Kannan Krishnamurty

NPTEL Co-ordinators

Prof.Andrew Thangaraj

Prof. Parthap 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