Introduction to Abstract

Group Theory

Module 04

Lecture 21 – “First isomorphism theorem”

PROF. KRISHNA HANUMATHU

CHENNAI MATHEMATICAL INSTITUTE

So now that we have learned quotient groups my next topic is to do what are called isomorphism theorems. These are all very important theorems that tell you how to understand groups are isomorphic and if groups are isomorphic then what implications do they have, and all this use the notion of quotient groups.

(Refer Slide Time: 00:37)

So the next goal is to study the isomorphism theorems for groups. So there are three such theorems, in this video I will do the first isomorphism theorem, and I will illustrate it with one example, and in future videos we’ll do the other two isomorphism theorems.

So first isomorphism theorem says the following. So there are three such isomorphism theorems, we will do the first today, first isomorphism theorem is the following. Let phi from G from G^1 be a group homomorphism, the first isomorphism says that in this situation we have the following: then we have a group isomorphism from G/ker phi to image of phi. So that’s what first isomorphism says, it’s a good time to recall what is an isomorphism.

An isomorphism is any group homomorphism which is a bijective set map, so isomorphism allows you to think of these two groups as essentially the same groups, if you have a group homomorphism kernel in this in order to even make sense remember I am saying this is a group isomorphism, so these two are groups in particular, image phi is a group, that we know because it is subgroup of G prime, but G mod kernel phi also a group because in general the quotient is only defined when you have a normal subgroup, but remember kernel phi a normal subgroup of, it is a normal subgroup. Hence we can talk about G mod kernel phi as a group, so G mod kernel phi is isomorphic to image phi.

This should remind you a problem that we solved in an earlier video where we have shown that, order of G is equal to product of order of kernel phi and the order of image phi, that is just a purely set-theoretic statement, number of elements of (G) and that required you to deal with a finite group, right because the number of elements of (G) needs to finite for that statement, is the number of elements of kernel phi times the number of elements in the image phi. But this is a very general result, this has nothing to do with finite groups and here we are only talking about isomorphisms, and in particular that problem follows from this if you think about it because this two are isomorphic groups means the orders are same, and the order of (G^1) kernel phi is order of (G) divided by the order of kernel phi.

(Refer Slide Time: 3:51)

So the proof of this theorem, let me give, it is very simple, it is essentially the problem that we solved, in the problem we have constructed a bijection, now we simply show that bijection is actually a group homomorphism, consider the function, I think I called the group homomorphism phi, so let's called function (F) I think this what we have done in that problem also, and the function is the same, what is the function? You take in element of this which is of the form of (a ker phi), so I think is probably better if I use letter like before so I am going re-write this as G/N to H^1 and what is this? This sends (aN) to phi(a), from a problem earlier we know that f is bijective, in that problem we exactly shown it is bijective .

It is certainly onto and if two cosets map to the same element that means those cosets are same. So we only need now to show that (F) is a homomorphism, because a bijective homomorphism is an isomorphism, so we only need to show that (F) is a homomorphism. What does this mean? Now in other words we have show that f(aNbN) is want to check f(aN) f(bN), you want to check this, so let us check both sides, what is f (aNbN) this is same as f(abN) because that's the product in the quotient group (aN) (bN) is (abN) and what is this? f(aN) is phi (a) and f (bN) is phi (b) right, and what is f(abN) you take any coset and map you take the element here and map it to phi of that element, so it is f (abN) will be phi of (ab). Now is this true? phi (a) phi (b) is phi (ab)? Of course it is true, this is true because phi is a homomorphism, so we have and hence (f) is a homomorphism. So we have checked it (f) is a homomorphism. So the proof is done.

(Refer Slide Time: 6:51)

So f is a bijective, bijective comes from before, that we have checked before and we checked today that it is a homomorphism, it is a bijective homomorphism so (f) is an isomorphism that's it, so (f) is isomorphism and hence we have G/kernel phi, this is my notation this symbol here arrow with symbol here , to indicate that we have an isomorphism, that's the proof of the theorem, first isomorphism theorem is proved. So its says that if you have any group of homomorphism, there is an isomorphism between the quotient group G mod kernel phi and the image group.

So why is this useful? So as I said first isomorphism theorem and more generally all isomorphism theorems are very useful in determining properties you know observing new facts about groups. So let us explore this in one example, so I am going to recall for you, what we have done in a previous video. We recall that if nZ is a subgroup of Z, actually what we should write is for any n in Z, the quotient group Z/n Z is cyclic. This I did in one of the pervious videos, where we talked about quotient groups, we explicitly calculated quotient groups for subgroups of Z, so in particular Z/nZ we concluded was cyclic, I left the last part for you to check an as exercise.

Now we will now show a sort of converse for this, we will now show that any cyclic group is isomorphic Z/nZ for some n in Z, this is the very remarkable statement right, it is okay to say that Z/nZ is cyclic, that is just a statement about subgroups of integers and quotient groups, now we are saying that you take an arbitrary subgroup cyclic group, this cyclic group can be anything, nothing to do with Z to begin with, however it is isomorphic to Z/nZ for a suitable integer.

(Refer Slide Time: 9:54)

So let me prove this theorem: if G is a cyclic group, then there exists an integer N such that, this symbol here, my notation I should remind you, we write G with this symbol to mean G is isomorphic to (G prime), that’s my notation, so I am saying that any cyclic group is isomorphic to this.

So this is very, it is to be thought of as a structural theorem for cyclic groups, any cyclic group is of this form, if you understand this group then you understand all cyclic groups right, that’s the meaning, so what is the proof? Proof is an immediate application of the first isomorphism theorem, so let’s proceed this way.

Let (a) be a generator of G, remember G is cyclic group, that means it is generated by a single element right, so G is so this is what it means, powers of (a) cover all of G, this what it means because such a thing exists because G is cyclic, we are assuming that G is cyclic group, so there is an element (a) such that its powers span or cover all of G, so you have (a) power N equals, the set (a) power N, as N various over integers is equal to G.

Now consider the function phi from Z to G, what is this function? It takes N to a power N, this is a function that we have studied in the past, in a previous video, so we have earlier that phi is a homomorphism.

(Refer Slide Time: 12:58)

A quick recall, remember we are defining phi (N) is (a) power (N) we want phi of (N + M) this is by definition (a) power N+M, this is same as $a^N a^M$ that is, if you write (a) product with (a) itself N times and M times you pool them and you get N+M times and that is phi (N) phi(M), this is not difficult at all right, so phi is a group homomorphism.

So not only that so phi is a group homomorphism, so phi from Z to G is a group homomorphism, and this is the first point, and of course phi is onto. See this is the meaning of, this is because G is cyclic, G is generated by, the point is phi maps an element in integer N to (a) power N, in general the set of elements (a) power N as N varies is not all of G, that happens only if G is generated by (a), so G is generated by (a), so phi is onto, because every element of G is form of (a) power N. Now what is kernel? Is that clear, phi is onto because G is generated by a, every element of G is a power an integer, so phi is onto. Kernel phi whatever it is, is a subgroup Z, right in general kernel is always subgroup of the group, domain group, so suppose and what are the subgroups of Z? We know that subgroups of Z are, they are the form, I should use some new letter may be but hopefully it's not confusing to use N again, though we have used N to denote the arbitrary integer right, there are of the form NZ. So suppose now coming back to specific kernel phi, kernel phi is NZ, so let's summarize what we have.

(Refer Slide Time: 15:49)

So we have a homomorphism, group homomorphism phi from Z to G such that phi is onto and kernel phi is NZ. Now let's think about what first isomorphism theorem says, what does first isomorphism say, what does it say? First isomorphism theorem says, it says, so let's see what it is, first isomorphism theorem said if phi is a group homomorphism from G to G^1 then we have an isomorphism from G mod kernel to image phi.

So we have done now, just apply that to our, so we have Z mod kernel is isomorphic to image phi, but this kernel is NZ, so Z/NZ its isomorphic to, because phi is onto, image phi is all of that, so phi is onto means, image phi is G. So Z/NZ is equal to isomorphic to G, which is exactly the theorem that I wanted to prove. So we wanted to prove that any group, any cyclic group, if G is a cyclic group there exists an integer N such that G is isomorphic to Z/NZ. We have shown that right, so this completes the proof of the theorem.

So first isomorphism theorem is a very simple statement really because its proof is clear, but it's a very powerful result, it comes up all the time, it's a very simple observation but it's always repeatedly used in various situations and using it we have proved a remarkable theorem that any cyclic groups is isomorphic to Z/NZ, why do I say it is remarkable? Because G is an arbitrary cyclic group, G could be anything, G is something that we do not know what it is, however we have identified with a very specific well-known easily understood group Z/NZ. So this is to be thought as, the conclusion to be drawn from all this is the following.

Using isomorphism theorems, we can essentially isolate the important properties of the group, cyclic groups, and think as them as Z/NZ, there is nothing more.

(Refer Slide Time: 19:18)

So let me give you one example to illustrate this. So let G be the group of 4th roots of unity, what are they? This is a group that we have seen before, this is (1,I) I being a square root of minus 1 right, complex square root of minus (1) and minus (I). We have seen before that G is cyclic, and it is of order 4, so actually by the theorem G is isomorphic to Z/nZ, so Z/4Z.

So I should have been more precise in my statement of the theorem, I wrote here G is a cyclic group then there exists the integer N such that G is isomorphic Z/NZ, but what is N actually? N cannot be arbitrary number, N has to be related to G, here N is the order of G right, so what we can conclude is why it is equal, what is the point here, so why is N equal to order of G, because if go you back and see, kernel will be NZ so, what I said is kernel is a subgroup of Z , so it is the NZ, but what is that N, it is the least positive integer such that (a) power N is identity, which is exactly the order, so N is the order of (a) which is, because (a) generate G order of (a) is cardinality of G, so in this case G is isomorphic to Z/4Z.

So to be precise what we are doing is consider the map from Z to G we send any integer to I power A, so the kernel of this is precisely 4Z, because kernel is the set of integers such as I power A is identity, in this case one, so I power 4 is one, I power 8 is one, I power minus 4 is 1 and so on.

So the theorem really written in a more precise fashion is if G is a cyclic group of order N then G is isomorphic to Z/NZ.

So let me stop the video here, we have seen a very important theorem here, called the first isomorphism theorem, and if you go back and see the statement and its proof, it’s not difficult at all, however it is always used, it is an important property of group isomorphisms that comes up a lot, so and we have seen one example of it where we have concluded that any cyclic group of order N is isomorphic to Z/NZ. So let me stop the video here, in the next videos we will study the second and third isomorphism theorems. Thank you.