NPTEL
NPTEL ONLINE COURSE
Introduction to Abstract
Group Theory
Module 03
Lecture 15 – "Problems 4"
PROF. KRISHNA HANUMANTHU
CHENNAI MATHEMATICAL INSTITUTE

In the previous videos we studied homomorphism of groups. And we looked at when groups are isomorphic. So I am going to do some exercises in this video to help understand these concepts and so that you get comfortable working with homomorphisms. So as a problem consider the following.

(Refer Slide Time: 00:36)

So the problem asks to describe all group homomorphisms from the group of integers to itself. So, in other words, we are interested in describing group homomorphism from the group of integers under addition remember always, when I write Z, it is always under addition, to itself. So how do you do this? So, let's look at what can possibly be a group homomorphism. So, suppose that phi is a group homomorphism from the integers to integers. And if you recall from the properties of homomorphisms that we have already studied, we know for example that the identify element under a group homomorphism must map to the identity element. In the case identity element is 0. So, this is guaranteed, this is forced by a group homomorphism. But now suppose that $\varphi(1)$ is some integer. So, $\varphi(1)$ remember is some integer, so I am going to call it A. Okay, then what is $\varphi(n)$ for another integer n. So group homomorphism properties will tell us that $\Phi(1+1)$ is equal to φ

(1) + φ (1), this the definition of group homomorphism. And what is φ (1+1) that is just φ (2) because 1+1 is 2. On the other hand, I have declared φ (1) is a, so, this is a + a, what is a + a, a is an integer. So this is just 2a. So φ (2) is 2a. What is φ (3), 3a. The same reasoning, so in general φ (n) is na, if n is positive right, because φ (1) is a, φ (2) is 2a, φ (3) is 3a, φ (4) is a + a + a + a 4a and so on.

(Refer Slide Time: 03:20)

Now what about negative integers? Qhat is φ (-1), again another property of group homomorphism that you recall from the previous video. Φ (-1) must be – φ (1). I am writing in this in the addition notation here. What we learned earlier. What we wrote earlier was φ (a inverse) = φ (a) inverse, right that means the symbol is less important here. The concept is image of the inverse of a, a inverse this is the symbol of inverse of a, image of the inverse of a is the inverse of the image a. This in this case inverse of 1 is minus 1. So minus 1 map to inverse of the image on 1 so, which was a. So φ (-1) is –a, so, that means φ (-2) by the same logic as before, is minus 2a. So, you have φ (-n) is – na so for all integers now.

Not just positive integers. For all integers n we have φ (n) is na right, so let's take a minute to think about what this means. I have only prescribed what is φ(1), right and I called it a, it is some integer I called it a. But then I have no choice on what the other images should be, once I determine what φ(1) is, I am forced to have φ(n)=na. How do you express this phenomenon, so what we can write is, φ is determined by φ(1), which is to say that once you fix φ(1), or once you give it a name, a, every other

image of φ is determined. Because once φ (1) is a, φ (n) is na. So φ is determined by φ (1). All you need to specify in other words all you need to specify to give a group homomorphism form Z to Z, we only need to define what should be the image of 1. Right, because if I define what image of 1 is, a homomorphism will have to be fixed once you determine what phi of 1 is. Because once you defined φ (1), φ (n) is automatically defined. This is the power of a group homomorphism. Once you define what phi of 1 is, all other images, all the other infinity integers, images are determined. Now the next question is, what are the possible choice is for φ (1)? So first point is this. That to give a homomorphism from Z to Z, we only need to define φ (1). We do not sit down and see what is φ(1) and what is φ(2) what is φ (3) what is φ(-1) we do no need to do that. We only need to say what φ (1) is, others will follow automatically from the definition of a group homomorphism. So, now all we need to do is define φ (1) but what can be φ (1) ?
(Refer Slide Time: 07:11)

Can φ (1) be any integer? It can be any integer. Because, in the calculation that we discussed earlier a was an integer. I can put a to be any integer. I have a valid homomorphism after I define φ (1) to be a. So for any integer a, define a group homomorphism φ from Z to Z by setting φ (1) = a. Once you set φ (1) =a as I have already noted every other φ (n) is determined and give me any integer a, I can put φ (1) =a, right, so then φ is homomorphism. This is what I am claiming. This exercise that we have done, no matter what a is I can declare φ (1) to be a and

once φ (1) =a, φ (n) will automatically be na.
Right so, for any n, so this is the homomorphism that is determined by a. To answer the original question, remember what was the original question, describe all group homomorphism from Z to Z, and we have done that. So what are the group homomorphism from Z to Z? The group homomorphisms are determined by the image of 1. And image of 1 can be any integer, so this is the answer to the question. The group homomorphisms from Z to Z are determined by image of 1 and image of 1 can be any integer. So, you have group homomorphism Z to Z are determined by integers again. So, they are determined by Z again.
(Refer Slide Time; 10; 03)

That is the solution to this problem.
So, now I will ask you a question to continue this problem. Which of these homomorphisms are isomorphisms? Recall that isomorphisms are group homomorphisms that are bijective set functions. Okay, so which of these homomorphisms are bijections is what I am asking now. So I am going to use the letter a as a subscript to denote that φ (a) sense want to a. so φ(a) is the homomorphism from Z to Z sending 1 to a. And the previous problem we have solved by saying that all group homomorphisms from Z to itself are of the form of φ(a). So, which of these are bijections? So for example if you take a to be 2.
What is φ (2) from Z to Z. It sends 1 to 2 and so on right, it sends just I will write it for clarity for you. Where does it send 2, it will send it to 4, because φ (2) must be φ (1+1). And so on.

And φ (n) in general so I will write that here. Φ (n) in general is simply 2n. Is this a bijection? Think about for a minute. Recall that bijection are 1-1 and onto. Bijections are injective and surjective. Those were the words I used I introduced in a previous video. Is it 1-1. It is 1-1 but not onto. That is because
(Refer Slide Time: 12:28)

it is not onto because 1 is not in the image of, clearly right, because φ (2) sends an integer n to twice the integer n, 2n. Is there any integer n such that 2n equals 1? There is not because no integer multiplied by 2 is 1. So, 1 is not in the image. So, φ (2) is not onto. So, similarly, φ (a) is not onto for a greater than or equal to 2, right, because for the same reason φ (a) sends n. to an, and a is greater than equal to 2 an cannot equal to 1 for any n, right, so it sends an integer to a times this. If a is at least two, it cannot equal 1.
So, it is not onto. What about a less than or equal to minus 2, for the same reason, it is not onto, for a less than equal to minus 2. Right, because again minus 2a can never be equal to minus 2n can never be equal to 1, minus 3n can never be equal to 1. On the other end φ (1) is simply the identity map. Right, because φ (1) of n is n. So, it is bijecitve. And it is an isomorphism. What about φ (-1)? φ(-1) sends n to minus n, and this already we know is a homomorphism and you can clearly check that this is also an isomorphism.
Because every integer is in the image, it is onto. Because, is 10 in the image? yes because -10 maps to 10. Is 100 in the image? yes -100 maps to 100. Is it 1-1? It is certainly 1-1. All φ (a)s are 1-1, okay, that we have discussed. Kernel of Φ (a) is 0, so it is

an isomorphism. What about φ(0)? So we have addressed all integers greater than or equal to 2 or less than or equal to minus 2 and 1 and -1. What about φ(0)? Φ0 (n) is just 0. So, φ0 is the zero map. Which is to say, φ0 sends everything to, so, that is every integer to 0.
(Refer Slide Time: 15:51)

So, certainly φ0 is not an isomorphism right, because it is not onto and it is not 1-1. So, we have determined that only 2 of these φ (a) are isomorphisms, Φ (1) and φ (-1). So let me summarize the whole problem as follows. Every group homomorphism from Z to Z is one of the, this is the answer to the original problem. Determine all group homomorphisms from Z to Z. They are the form φ (a) as a varies in Z. These all are the homomorphisms. So φ (a) as a belongs to Z is the set of all homomorphisms.
Φ (a) is an isomorphism if and only if a = 1 or a = -1. This is the second problem that we did. It is an isomorphism if only if a is 1 or -1. Φ (a) is injective if only if a is not 0. This I didn't explicitly say. But this is an exercise for you. It is, the reason that φ2 was not an isomorphism was that it is not onto, it is 1-1, because what does φ (2) do? Φ (2) sends n to to 2n. If 2n is 0, we have already discussed in an earlier video that a group homomorphism is injective if and only if the kernel is 0. The trivial subgroup, if 2n is 0, then m must be 0. So, kernel is 0.
(Refer Slide Time: 17:59)

And φ (a) is surjective, when is it surjective? It is surjective if only if a=1 or a=-1. Remember that for any other integer, it is not surjective. So, the summary of this problem which you should carefully understand, this is an important example of group homomorphisms and the properties that we have learned about group homomorphisms and this description is hopefully giving you a clearer understanding of all group homomorphisms from Z to Z.
(Refer Slide Time: 18:40)

Okay, so, let me do one more problem, and I will do the solution also. So that you understand how to apply the notions of group homomorphisms that we learnt. So let G be a group, so this the second problem of this video. Let G be a group and let a be an element of G. Let G be a group, let a be an element of G. Suppose that order of a is r. So, what is order of a? I am going to recall it here. Order of a is the smallest positive integer n let's say d such that a power d is the identity element. This was our original definition of order. It is the smallest positive integer such that a power that is the identity element. Here I am saying that order of a is some integer r. So, obviously it is a positive integer. In other words, I am saying that some power of a is identity, some positive power and now suppose that a power n is also identity, for some other positive integer n. Then show that r divides n, so this is the problem. Okay, so the problem is saying that if order is given to be a number r. and a power n is identity for some other number n, all positive numbers, then r must divide n.
Okay, what is the solution of this? I am going to recall for you,

another description of the order that I gave after I defined homeomorphisms. Consider the homomorphism from Z to G which sends some integer m to a power m. In an earlier video, already we saw that φ is a group homomorphism. That we already saw in a previous video. We also saw that if you consider the kernel, so kernel of φ is rZ, where r is the smallest positive integer such that a power r is identity. Remember in general there is another possibility kernel of φ may be either rZ, or kernel of φ is 0. This is is also possible in general because there may not be any kernel of this map. That means a power m may never be identity for any positive integer. Okay, so this is a possibility in general. But in our problem kernel φ is not {0}. I should really put as a set.

Because kernel φ is 0 is a possibility general. But in our problem it is not possible. Because in our problem remember we are given that order of a is r, where r is a positive integer. Order has to be either 0 or positive integer always. And in this problem we are given that order is a positive integer. So kernel φ is not 0 because r belongs to the kernel. So, note that r is a positive integer. So, kernel is non-zero. That does not happen. So kernel is this is not going to be a case in our problem. Kernel is rZ. So in general, kernel is in generated by the order of a, okay. Now let us look at the problem more carefully. So r is order of a, and a power n equal to identity for some integer n. Since a power n is identity we have that n belongs to kernel φ. Because what is φ? Φ sends to n to a power n. So φ (n) is a power n which is identity, so n belongs to kernel φ. But kernel φ as we discussed earlier is rZ. So, n belongs to rZ. So, n belongs to rZ. What does it mean? Then n=r times m, for some m, right, because remember recall what is rZ? rZ is the set of multiples of r. It is r, 2r, 3r, –r, -2r, -3r, and so on. If n belongs them then n is the

form.
(Refer Slide Time: 25:34)

So n is the multiple of r. So, r divide n, which is exactly what the problem asked us to do. It asked us to show that r divides n, which is what we have showed. Okay, so keep in mind that, if an element has order r and a power n is identity the r is divides n. Basically what happens is that if you take a and you write multiples of a, not multiples, sorry, powers of a. So you have a power 0, which is identity then you have a, a2, a3. There are two possibilities either you will never 1) we never encounter e in this sequence right, so it keeps going, a power 100 and a power1000 so on. So, there are all distinct and e is never there. Clearly the group must be infinite in this for this case to occur. The other possibility is 2) e occurs, I mean of course when I say e never occurs e certainly occurs at the beginning. We never encounter e in this sequence after a power 0, we do have e in this, but if this sequence actually starts with a, not with a power 0. In this sequence either e appears or e does not appear, if e does not appear they are all distinct. And the group in particular must be infinite. Or e occurs in this sequence and order of a is the first place where e occurs. Again I am not considering this. Let me not even put that in the sequence. I keep looking at a, a2, a3, a4, a5 and so on. And the first time I see e, if it is a power r, then r is order of a. And the point is the sequence then repeats. So suppose a power 5 is identity. So the sequence is a, a2, a3, a4, a5, a, okay, which is e as I said I am assuming this. So example and then what is a power 6? this is just a power 5 times a. So, this is just a. So, the 6^{th} element again a. Then a2, a3 this is same

as a7, this is same as a8, a4 is a9, a5 a10 which is also again equal to a. So, the sequence is just
(Refer Slide Time: 29:16)

repetitions of this, so this block keeps repeating. This segment keeps repeating forever. So what we are saying is if a power100, a power some number is e, that number must be a multiple of 5. So this is e. In this block e must appear at the last spot in each block. And that spot is the multiples of 5. So this is the 5^{th} position, 5^{th} position, this is the 10^{th} position, this is the 15^{th} position. This is the 20^{th} position.
Okay, so the problem is essentially encapsulating the detailed data that we have just discussed. If a power n is e, then it must be a multiple of the first time uncounted e in the sequence. And let me quickly illustrate both of these possibilities, both of these possibilities occur, for example if you take G to be Z and a to be 1. Or let's say 3. If you take 3, if this sequence again we remember in the general case we use the multiplicative notation a, a2 a3. But when we are dealing with integers we use additive notation. So the sequence will be 3, 6 twice, and two times and 9, 12, 15, 18 and so on. So, we never encounter 0.
This is the possibilities number 1 here. So this is a sequence of distinct integers never containing 0. So this is the first possibility. On the other hand, if you take G to be is some other group. For example, if you take G to be the group of 4^{th} roots of unity, 4^{th} roots of unity, that we encountered before, and you take a to be I. So, you start with I, then you take I2 which is minus 1. But once you come to I power 4 it is 1. So, this is the segment that keeps repeating. So the next I to the 5^{th} will be I

again. I to the 6th will be minus1. I to the 7^{th} will be minus -I. and I to the 8^{th} will be 1 again.
(Refer Slide Time: 32:10)

So this will be repeated. So the segment that keeps repeating is I, minus 1, minus I and 1. So, then you repeat this. And then you repeat this. You repeat this forever and in particular we know that order of I is 4 because 1 is appearing in the 4^{th} spot, 8^{th} spot, 12^{th} spot, 16th spot and so on. So, this illustrates for you the point of this exercise. Okay so let me now end this problem by doing a related problem,
(Refer Slide Time: 32:43)

which exactly uses this and this also makes use of the notion of group homomorphism. So let's say G to G prime is a group of homomorphism, let us say, I take an element in G, suppose that the order of a is r, so you could have simply written is as order of a is r. The problem is, what can you say about order of φ (a)? So, the problem is if you have a group homomorphism and an element is fixed which has some finite order, what is the order of the image? Can you say anything about the order of the image. Order of a is r, what is the order of φ (a). How is it related to r in other words, that is the question.
(Refer Slide Time: 33:49)

So, solution is the following. Let's recall that order of a is equal to r implies, a power r is identity. Now let me, this is the identity of the group G, that is because a is inside G. Now let us apply φ to both sides. Right, so φ a power r is equal to phi of eg. Now continuing here and using the properties of group homomorphism, φ (a power r) is just phi of a whole power r. And what is φ (eg), that is eg prime right, because the identity element under a group homomorphism maps to identity element. So φ (a) whole power r is eg prime. By the previous problem which I have written here, what is the previous problem in any group if a power n is e, then order of a divides n. So here φ (a) power r is eG prime. So, order of a order of φ (a), whatever it is, divides r. That is all we can say. So, what can you say about order of φ (a)? We can say that order of φ(a) divides r.

So this gives you a restriction on the possible images of elements of a group under a group homomorphism. If an element has order 5, its image has to have an order that divides 5. So it has to be either 1 or 5. So in particular, if φ is a group homomorphism, let me shorten it like this, group homomorphism and a is an element of G has order 5 then φ (a) has order 1 or 5. Right, it is an immediate consequence of the problem, because whatever is the order of φ (a), must divide 5. 5 being a prime number, it is either 1 or 5. So and as a supplementary exercise, this is a trivial exercise that I have repeatedly used. Let G be any group and let a be an element of G.

Then order of a is one if and only if a = e, okay, so this is easy for you to do. Only element which has order 1 is e, okay, coming back to this example φ (a) is order 1 or order 5, so in other word φ (a) is either identity element or its order must be 5. So, this is very useful to keep in mind, order of any element

must divide the order of the element. Order of phi of a must divide the order of a.

So, I just recall for you, what is order of r is a. So order of φ (a) divides order of a, okay. So let me stop the video here. And hopefully this gave you an idea of how to work with group homomorphisms and apply various properties that we have learned, so in the next video I will continue with my study of cosets that I have introduced, study of equivalence classes that I have introduced in a previous video. Thank you.