NPTEL

NPTEL ONLINE COURSE

Introductions to abstract

Group Theory

Module 02

Lecture 11-“Properties of homomorphism”

PROF-KRISHNA HANUMANTHU

CHENNAI MATHEMATICAL INSTITUTE

So let’s continue our study of group homomorphisms. Last video we defined group homomorphisms and looked at various examples of group homomorphism. I am going to study further now. I am going to start with some basic properties of group homomorphisms.

(Refer Slide Time: 00:34)

So properties of group homomorphisms, okay, so some of the most important properties are the following. So maybe I will write this as a definition, proposition rather. Proposition: Let φ from G to G prime be a group homomorphism, it sends, in other words, φ of AB is equal to φ of A times φ of B for all AB in G. Then we have two statements φ of EG is EG prime, so just to clarify here E always stands remember for our identity element in a group.

But here I have two groups G and G prime, so I am going be denoting which identity I am talking about by looking at the subscript, E sub G is the identity element of G, E sub G prime is the identity element of G prime, so what I am saying is that in a group homomorphism, the identity element of the first group goes to the identity elements of the second group, further we have if A belongs to G, if A is an arbitrary element of G then φ of A inverse, that means I first take the inverse of A and apply φ to it, I get the same answer as first taking image of A and taking the inverse image, okay, so just ready this carefully, I first take inverse image, sorry I first take the inverse then take φ or I first take the image and then take the inverse image.

(Refer Slide Time: 02:48)

I get the same answer so inverse and then φ is same as first φ and then the inverse, so these are the properties of group homomorphisms. So let us prove this, this is very easy, the condition that φ of AB equals φ A times φ of B guarantees this, that is a powerful condition that guarantees this. Note that EG times EG is EG, right, this is in G, this operation is taking place, this is an equation in G, that is because anything commutes with EG, so in particular anything when you multiply by EG you get it back so in particular EG times EG is EG, so apply φ to both sides, okay, now because φ is a group homomorphism, φ of EG times φ of EG is φ of EG times φ of EG, φ of EG times EG is equal to φ of EG, I am not changing the right hand side here, φ of EG is same as, I am keeping it as φ of EG.

But the left hand side becomes this, because of the group homomorphism property, okay, now let's look at this, this is in G prime this is an equation in G prime, we started with an equation in G applied φ to it and translated completely to G prime so now what does this mean? You have two elements, so you have an element actually in G prime that you when multiply you get it back, so we trying to show that φ of EG is EG prime.

But whatever it is, I can multiply by, both sides by, both sides of this by, the inverse of φ of EG. What do I get? This is an element of the group G prime, so we have two elements multiplying to this element, they all happen to be same element, and you can multiply by the inverse of this, so φ of EG inverse times φ of EG times φ of EG is φ of EG inverse times φ of EG, correct? So that is what we have when you multiply out you get this.

But then what is, what is this, because again the group is associative we can combine these two and that will cancel because that is inverse of this, so we get, φ of EG on the left hand side and what is φ of EG inverses times φ of EG this is an element inverse times itself. So this is nothing but EG prime, this is a property of inverse in a group, φ of EG is some element, I am multiplying by its inverse this is some element in G prime, I am multiplying by it's inverse so I get EG prime so this proves the first property that I said, so the identity element of group G maps to the identity element of the group G prime, right. Second property is similar and easy, so let us say that we have we have already shown that so we know that A time so let A, B in G then A times A inverse is EG right, this is the definition of inverse so apply φ to both sides so φ of A time A inverse is φ of EG by part one it is already shown to be EG prime φ of EG is EG prime, now the group homomorphism property says that φ of A times φ of A inverse is EG prime.

(Refer Slide Time: 06:50)

So φ of A times φ of A inverse is EG prime, but remember inverse is the unique element which has the property that φ of A times it is EG prime, so by definition of inverse, we must have φ of A inverse is φ of A inverse the whole inverse because φ of A when you multiply with this element here you get the identity element so this element must be the inverse of φ of A which is denoted by φ A whole inverse.

So this is, remember, the second property, φ of A inverse is φ of A whole inverse so this proves two, so the proof is complete, in other words, identity must go to identity under a group homomorphism and inverses must go to inverses, this is useful to keep in mind because it tells you quickly if a map is a group homomorphism or not, if it doesn't send identity element to identity element, it cannot be a group homomorphism.

So, if you recall, one of the examples I did in the previous video was sending a function from Z to {1, -1}, φ of A is, let us say 1, if A is odd, -1 if A is even, and I asked you to check that this is not a group homomorphism. That was left as an exercise for you. Now let's do this exercise using the proposition that we proved today. Remember the other way if you send even numbers to 1, odd numbers to -1, that was a group homomorphism.

But if I interchange this it is not a group homomorphism. In fact, what is the identity element of Z? This is my notation right, E is always the identity element and I am denoting the group by the subscript. Remember Z is a group under addition so the identity element is 0. Right, and zero is even, so under this map, φ of 0 is because, even numbers goes to -1, φ of 0 is -1, but what is, you call this group G prime, what is EG prime?

Certainly 1, because this is a group under multiplication with 1 as identity, so the zero element does not map to the identity element. So, φ of EG is Z rather is not equal to EG prime. So, φ is not a group homomorphism. We do not need to check anything more, you simply send, you simply check that the identity element does not go to the identity element it cannot be a group homomorphism. Okay, so similarly inverses go to inverses.

So however I want to make a point here, if the identity element goes to the identity element does not mean that it is a group homomorphism. The proposition does not say that if this condition is satisfied if EG goes to EG prime, it is a group homomorphism. It only says that if you have a group homomorphism,

(Refer Slide Time: 10:55)

identity element goes to identity element. So, neither of these are sufficient conditions for homomorphism. There only necessary conditions. They must be true, but if they are true it does not mean that it's a group homomorphism.

Okay, so now that we have this, let me define some important subgroups associated to, important subgroups associated to a group homomorphism. Okay, so there are two.

So let me work now with an arbitrary group homomorphism. Let us say φ from G to G prime is a group homomorphism. So we define two subsets first and we will check that they are group homomorphisms, sorry we define two subsets first and check that they are subgroups. So "kernel of φ", okay this is the word, kernel of φ and it is denoted simply by Ker (φ), is the following. So, you define Ker (φ) to be all elements of the group such that φ of A is the identity element of G prime. So this is all elements of the group such that φ of A is EG prime, exactly the subset of elements which map to EG prime, so and similarly let me define this first. Image of phi, so this is the subset of G remember. Kernel is a subset of G. Image φ

(Refer Slide Time: 13:14)

which I will denote by image phi is the following. Image phi is equal to, simply the image of the function φ, so this is just a set-theoretic notion, I am taking all elements of G prime, this is inside G prime clearly. All elements of G prime which appear as the images of the elements of G under φ. So, the proposition now is kernel φ is a subgroup of G, it is a subset of G by definition but in fact it is a subgroup of G and image φ is a subgroup of G prime.

This is true for any group homomorphism. So if you start with any group homomorphism φ, kernel is a subgroup of G, image is a subgroup of G prime. What is a proof? It is again fairly straight forward, let me check 1. What is a subgroup? If you recall from a previous video, subgroup is a subset of the group which is closed under multiplication, which has inverses and which has the identity element, Okay.

So first of all is it closed under, kernel φ is closed under the binary operation of G. So, let's check this. Kernel φ is closed under the binary operation of sorry G not G prime of G because if, A and B are in kernel phi, this means φ of A and φ of B are both EG prime, by definition. Kernel φ consists of elements which map to the identity of G prime, but then what is φ AB? This is by definition sorry not by definition by the property of a group homomorphism, is same as φ of A times φ of B which is EG prime times EG prime which is EG prime. So that means AB is in, right, because AB maps to EG prime so AB is in the kernel phi. We started with two elements in the kernel and concluded that their product is in the kernel. Kernel φ contains EG. This is very easy, right, because what is φ of EG? This is by the previous proposition this is EG prime. So that means EG is in the kernel φ.

Finally kernel φ is closed under inverses, the third property, that we require for a group, subgroup, is it closed under inverses? Yes, because if a belongs to the kernel φ that means φ of a is EG prime, by definition it is EG prime. By the previous proposition, φ of a inverse is φ of a inverse by the previous proposition, right and this, sorry, so let me write it like this,

(Refer Slide Time: 16:59)

Φ of a inverse which, by the previous proposition, is φ of a inverse which is EG prime inverse which is EG prime, right. φ of a inverse is by the previous proposition inverse of φ a, φ of a is EG prime, it is EG prime inverse, inverse of identity itself okay, so that means a inverse is in kernel phi. So we have checked three properties: kernel φ is closed under binary operation of G, it contains the identity element and it contains inverses, so kernel φ is a subgroup of G.

Now let us check that image is the subgroup of G. I am going to show that image is of subgroup of G. Similarly, exactly as before image φ is closed under binary operation of G prime, right, now we are claiming that image φ is a subgroup of G prime, so it must be closed under the binary operation of G prime. What are two elements of image φ? If you recall, image φ is φ of a, a in g, for all elements a of G, we take φ of a, so two elements of image φ would be φ of a times φ of b. Let’s say they are both in image φ. But that means, φ of a times φ of b, by the property of group homomorphism, is same as φ of ab, but this is by definition in image φ, because this is the image of ab, product of φ of a and φ of b is the image of ab.

So if you start with two things in image φ, their product is in image φ. Image φ contains EG prime, it must contain EG prime in order to be a subgroup but it does, because φ of EG by the previous proposition is EG prime. So EG prime is in the image, recall again that image is the image of the function, EG prime is an image of an element. So it is contained in the image, it is the set theoretic image. Image φ is closed under inverses, this is also easy, let’s say φ of a belongs to image φ. Then what is φ of a, whole inverse? By the previous proportion, this is same as φ of a inverse.

(Refer Slide Time: 20:01)

Right, φ of a, whole inverse is φ of a inverse, but φ of a inverse again is by definition an element of the image. Because it is image of a inverse, so image φ is a subgroup and this proves the proposition. So we have shown that kernel and image of subgroups G and G prime, so this is an important, these are two important subgroups attached to any group homomorphism. So it’s a good exercise now for you, to work out the kernel and images in all the previous examples that we discussed of group homomorphisms. I won’t discuss all the examples, but if you consider the map from Z to Z, φ of a being na, so we have fixed n, this is the first example of a group homomorphism that we studied, you fix an integer n and send an integer a to n times a, the kernel of φ is all integers such that na is zero, because zero is the identity element of Z.

But this is precisely zero, so the kernel is just zero. Remember kernel, being the subgroup of the group, contains the zero elements always, so in this case it is exactly zero element. So this is a sub group of the first Z, what is the image of Z, phi? This is all na, where a is in z, and this is precisely the group nZ that we discussed, subgroup of Z obtained by multiples of a, so this is a subgroup.

And if you take the determinant homomorphism from GLNR to R star, what is the kernel of this? Remember φ of A is determinate of A, kernel of a is the set of matrices in GLNR, such that φ of A which is the determinate of A, is 1. So this is a subgroup by the previous proposition and this is called the “Special Linear Group” denoted SLNR, okay, Glnr is called the "General Linear Group". Special linear group is a group of invertible elements with determinant 1. That's the kernel. What is the image of φ?

(Refer Slide Time: 23:31)

Image of φ is the set of real numbers which are obtained as determinant of A, for an invertible matrix. So image consists of all determinants as you vary the invertible matrix in Glnr, what is this? It's certainly a subgroup of, by the previous proposition, it is a subgroup of the multiplicative group of nonzero real numbers. But I claim in fact, it is all of nonzero real numbers, why?

I claim that image of the determinant map is all of nonzero real numbers. In other words, given a nonzero real number, r let's say, there exists an invertible real n by n matrix A such that determinant of A is r. Note that if I show this, then I have justified saying that image of φ is R star, because if there is such a matrix, it is in Glnr, so A is in Glnr, that is to say it is an invertible real n by n matrix and its determinant is r. So r would be in the image, so if I want to show image of φ is R star I need to verify this, but what is such a matrix? I simply can take, I will take a diagonal matrix, I will put r in the first left hand side position and I will take ones everywhere, I will take one everywhere else on the diagonal, zeros off the diagonal. This is certainly an invertible matrix because its determinant is r and r is non zero. It is an invertible matrix, it is size N by N, it has real entries. So this matrix will have determinant because determinant of a diagonal matrix is the product of diagonal entries, determinant of A is r. So the image of the determinant homomorphism is all real numbers, non-zero real numbers of course, we want non-zero real numbers.

(Refer Slide Time: 26:03)

Just one more example I want to do, this is also something we discussed in the previous video. If you take, G is an arbitrary group, fix an element of G and consider group homomorphism from the integers to the group by sending n to A^n this is a group homomorphism was something we checked earlier, what is the kernel of φ? This is all integers such that φ of A, in this case A^n is identity of G. This is a subgroup of Z. This is a subgroup of Z, so this is all integers such that A power n identity is a subgroup of Z. What is the image of φ? This is A^n so remember this is φ power n as n varies over integers, this is by definition image of φ, but what is φ power n? This is just A power n has n varies over integers. In other words, this is just A-3, A-2, A-1, A0 which is EG, A, A^2 if you recall and you remember now from a previous video we gave a name for this group.

This is simply the subgroup generated by A, this is the subgroup generated by image of φ is the subgroup generated by A. Let's look at kernel slightly more carefully, so now what is kernel of the same example, in this same example what is the kernel of φ? So kernel of φ, as I wrote earlier, is all integers such that A power n equals EG and if you recall again from a previous video we have already classified all the subgroups of the integers.

(Refer Slide Time: 28:38)

What are they? Recall we earlier classified, so remember this is a subgroup of Z, we already classified all subgroups of, what are they? They are of the form, they are multiples of a fixed integer, so we have already used n and a here, so I am going to use BZ, right, they are of the form BZ. BZ, being all multiples of a fixed B, so BZ is BN, where N varies over, so they are of the form BZ, where BZ is this, so every subgroup of integers is like this.

In particular, kernel is also like this, so in our example kernel φ being a subgroup of Z is of the form kernel φ is BZ for some integer, in fact, B is a non-negative integer. See if you go back and see the video where classified subgroups of Z they are of the form BZ, for a non-negative B. We can always if, ok, I don't want to repeat the proof, but we first rule out the case that it is a zero subgroup, in which case it is of the form zero times Z.

Otherwise there are some numbers in it, nonzero numbers, hence there must be some positive number in it and we take the smallest positive number and show that all elements of this subgroup are multiples of it, so B is either 0 or positive. So now this B is actually something that you are familiar with, B as an exercise note that B is nothing but the order of, recall that, from before what is order of A? So we have two possibilities.

So what is order of A? We first look at multiple of A, so we look at E, A, A squared, A cubed, we keep looking at this, either you will never hit E again the identity element or you will hit E somewhere. It is the first place you hit E if you hit E. So order of A has two possibilities, it is either, okay, maybe I should write like this, if A power n is e for some positive integer,

(Refer Slide Time: 32:38)

n, then order of A is the smallest positive integer m such that A power m is E, this is such that. Okay, so S.T. always stands for "such that". So if A power n is identity for some positive integer n, I am going to simply look at the least positive integer which has that property. If A power n is not equal to E for any positive integer n then I will simply define the order of A to be infinity, and now I claim that looking at the map, the group homomorphism which sends integer n, A power n in a group G, we noted that kernel is of the form BZ, it is all multiples of B, so kernel of remember φ, is all integers n such that A power n is identity. And we saw that it is BZ, for some integer which is non-negative. So it's either 0, in which case kernel φ is zero, kernel φ is the zero set and in this case A power n cannot be equal to A for any positive integer, so order of A is infinity.

So actually I should not say this, so this is not right, B is nothing but the order of A is not quite true. B is related , I should write B is related to order of A, if B is 0 then order of A is infinity. If B is not 0, so B is positive, then kernel of φ is BZ and now the order of A is actually B. So in this case order of A is B because remember kernel is BZ and B is positive, so the smallest positive integer such that A^n is B, so order of A is B.

So if the kernel of this map is kernel of this map is zero if kernel of this map is zero then order of A is infinity and kernel of this map is nonzero then order is equal to the generator of the group, so B is related to order of A. So these are some of the properties of group homomorphisms and I am going to stop here in this video and in the next video I am going to talk about, so in this video we have looked at basic properties of group homomorphisms, namely that they send identity element to the identity element, inverses to inverses, we looked at two very important groups associated to a group homomorphisms, namely the kernel and the image and we worked out what these are in some of the examples of group homomorphisms that we looked at. In the next video I will continue my study of group homomorphisms and define isomorphism of groups. Thank you.