NPTEL
NPTEL ONLINE COURSE
Introduction to Abstract
Group Theory
Module 03
Lecture 12 – "Group isomorphisms"
PROF. KRISHNA HANUMANTHU
CHENNAI MATHAMETICAL INSTITUTE

Let us continue our discussion about group homomorphisms. We defined kernels and images of group homomorphism in the previous video, so let me do one immediate proposition following those definitions.
(Refer Slide Time: 03:06)

So, before that let me recall define some well known terms. So let us say φ is a group homomorphism from G to G prime, so let's say φ is a group homomorphism from G to G prime. I define φ is 1-1 or injective is also the word, a word that we use, injective if φ of a, b is equal to phi of b implies a equals b, okay this is one way of writing this equivalently, if A is not equal to B then phi of A is not equal to φ of B, okay so this is actually nothing to do with a group homomorphism, this is a purely set-theoretic notion.
So it's injective means two distinct elements map to two distinct elements. Similarly φ is onto or another word for this is surjective if image phi, my notation was small im, okay these is also purely set-theoretic notion, image of the map is all of G prime. So this is very simple, but the proportion I want to do before continuing today is that φ is 1-1 if and only if kernel of φ is just the identity element of the group.
So remember kernel is the set of elements of the group G which map to the identity element of group G prime so 1-1-ness can be captured purely by looking at kernel of this, so what is the proof of this? So suppose we have to prove two directions right, φ is 1-1 if and only if kernel φ is e_g, so let us suppose φ 1-1 let us prove that kernel φ is eg and on the other hand let suppose kernel φ is eg and to that the φ is 1-1.
So suppose first that φ is 1-1 and let A be in kernel of φ, then by definition φ of A is eg right, kernel of phi by definition elements which map to eg, but we have

already seen that φ of eg is same as, sorry φ of eg prime right, φ of it is the identical element of G prime A being in the kernel means, A maps to eg prime.

But eg also a maps eg prime that's a property of the group homomorphism, but now φ is 1-1 and φ of A is equal to φ of eg so A equals eg. Right, if A is in the kernel A must be eg, certainly eg is in the kernel that's always true. Because kernel φ is a subgroup it contains the identity element or more directly identity element of the group maps to the identity element of the group G prime so kernel contains eg and if anything else is contained in eg sorry if anything else is contained kernel φ it is equal to eg so kernel φ is simply eg.

So that we have shown, so if kernel φ is 1-1 then the kernel of φ is eg. So the next direction,

(Refer Slide Time: 04:42)

this is the easy direction, so suppose that kernel of φ is eg, so we have now assumed that kernel of phi is eg, kernel of φ eg. So we want to show that φ is 1-1, so suppose what is 1-1? it means that if two things map two, if two element map to the same element they are equal. So suppose φ a is equal to φ of b, okay, if φ of a is equal to φ of b then φ of a times φ of b inverse equals identity of G prime, because φ of a, I am simply multiplying by φ b whole inverse.

So this is happening in G prime, φ of a times equal to φ of b, φ a φ b inverse is eg prime, but φ of b inverse remember by the properties of group homomorphism that we studied earlier, φ of b inverse is nothing but φ of b inverse φ of b whole inverse, when I write it like this I mean φ of b inverse, that is same of φ of b inverse. But again using the property of a group homomorphism this is just φ of ab inverse, φ of a times φ of b inverse is φ ab inverse and this is φ of, okay now φ of ab inverse is in eg that means, ab inverse is in the kernel φ the definition in kernel φ is that it consists of those elements which map to the identity element of G prime.

So ab inverse is in the kernel phi. But note that kernel φ is precisely eg, we have only one element in kernel phi, so that means ab inverse is eg, because eg is the only element in kernel φ, so ab inverse must be in the eg, but that means a is equal to b, because we can multiply by b. So ab inverse is eg means a equals b, so we have stated with φ of a is equal to the φ of b and concluded that a equal to b. That means, so φ is 1-1, okay so checking if a group homomorphism is injective or not, in general you have to check that no two distinct element go to distinct element, but the advantage with a group homomorphism is that all you need to check is the kernel, if kernel consist only of the identity element, it is automatically a 1-1 group homomorphism.

Okay, so a group homomorphism is 1-1 precisely if kernel is the identity, or kernel is just the identity element. Now a very important definition.

(Refer Slide Time: 07:50)

An "isomorphism of groups" is a group homomorphism, I am introducing another word for you, an isomorphism of groups is a group homomorphism φ from G to G prime such that φ is 1-1 and onto, so a group homomorphism which is simultaneously 1-1 and onto is a group isomorphism. Okay, so an immediate, so isomorphism of groups is a very very important concept of groups, it says that two groups are isomorphic when they are essentially same, if there two groups are isomorphic we will consider them as same groups.

As far as the group theoretic properties are concerned there is no difference between them, because there is a bijection between them so this is simply saying that, remember I used the word bijective earlier, bijective simply means its 1-1 and onto, so because it is bijective the sets are same and because it is homomorphism multiply two things here in one group is same as multiplying two things in the other group, so as far as the group theoretic properties are concerned they are same.

So an exercise for you which I will not discuss in great detail, if φ from G to G prime is a group isomorphism, then the map φ inverse, remember that if it is a isomorphism is a bijective map, φ is a bijective map so there is a map which sends G prime to G namely φ inverse just the set theoretic inverse function, so where does an element under G prime go under φ inverse , you simply look at a pre-image because there is exactly one pre-image it is well-defined.

The map φ inverse is also a group isomorphism, if φ is a bijective map since φ is a bijective map φ inverse can be defined. Right, that is because if b is in G prime define φ inverse b equals a if φ a is b. So you have G here G prime here, a goes to b under φ right, because it is a bijective map b has a pre image and it is exactly one, there is exactly one pre image, so I simply send b to a under φ inverse. Okay, so if a goes to b under φ, b goes to a under φ inverse.

So you can define it, because it is a bijective map, otherwise you can't define the inverse. And it is obviously a bijective map also, because if φ is bijective its inverse image is not only defined but it is bijective. So its bijective map, to check that it is a group of isomorphism we have to check that, φ inverse is actually a group homomorphism and this I will leave for you to check, so you have again in the picture I drew earlier, you have two elements b1 b2 lets say, which map to a1 a2 and you also have I want to draw a bigger diagram.

So you have b1 b2 and b1 b2 okay that's in the G prime. You have φ of this is a1, this is a2 and this is a1 a2, a1 maps to b1 under φ inverse it maps back to a1. Similarly a1 a2 map to each other under φ and φ inverse, but because φ is a group homomorphism a1 a2 maps to b1 b2 that is the property of group homomorphisms, but again by inverse definition of the inverse function this must map to b1 b2 must map to a1 a2.

So this gives you an idea of how to check that φ inverse is a group is a group homomorphism, so if you have an isomorphism of a groups which is by definition a group homomorphism which is bijective, you have an isomorphism in the opposite direction.

So group isomorphism is an important property because it allows us to consider two groups as same if their group theoretic properties are same, we do not want to think them as a different just because the names of elements are different or the way which it is represented is different. Okay, so we will as the course progresses we will look at various examples of this, but just to give you very basic idea, I want to consider one very simple example of group isomorphism,

(Refer Slide Time: 14:33)

or few of them , so let's take G1 to be 1, I, minus 1, minus I, so where I was a square root of minus 1, so remember this we discussed this came up earlier in our videos, this is the group consisting of fourth roots of unit. So this is a subgroup of C star. On the other hand let us consider G2 to be 1, a, a squared a cubed, where a is just a symbol okay, meaning it has no further interpretation, it is just a symbol, it is not a number or a matrix or an operation or a function, or permutation and so on, it's just a symbol.

And the property is, the property that it satisfies is, okay let me use e for the identity element, a to the fourth is e, so now G2 is a group, it is a group because it has identity, it is closed under the multiplication because a, a squared is a cubed is a square a cubed it is, what is a square a cubed? Just the exponential rules tell you it is a5, but a5 is a4 times a, right, and a4 is e so this is just e. So essentially what we are doing is exponents so similarly a cube power four, what is this?

Okay, this is a to the 12, and that it is a to the four cube, that's also e, a cubed to the third that's a to the ninth, so that is a to the 8 times a so that is a. Okay, so using this very important property this symbol satisfies, we can check that, this is closed, these are just examples but in general any a power i is inside $\{e, a, a^2, a^3\}$ and e is a power zero. Okay, because you can basically divide i by four and the reminder is what you get here, because a power four is e, so G2 is a group, it is an abstract group in the sense that a is just a symbol with no meaning attached to it, G1 is also a group but here there is a concrete meaning I is a square root of minus one I is a complex number. I claim that G1 and G2 are isomorphic, why is this? Let's define a function so remember an isomorphism is, when I say isomorphic so the word isomorphic,

(Refer Slide Time: 17:57)

We say G1 and G2 are isomorphic,

(Refer Slide Time: 18:13)

if there is a group isomorphism okay this is just a notation. We say that two groups are isomorphic if there is a group isomorphism from one to the other. Okay, in this now I come back to this example I want to say G1, G2 are isomorphic. So we have to exhibit an isomorphism, so let's define an isomorphism, so G1 is 1,e, 1, i, minus 1 , minus I, so send 1 to 1, I want to do from G1 to G2, I send 1 to e, I to a, minus 1 to a square, minus I to a cube. Okay and one can check easily, this is a group isomorphism, it is certainly a bijective function right, because four elements here go to four distinct element here, G2 has four elements and everything is in the image and no two elements map to same element, so it is a bisjction.

That is easy, it's just from the definition. It is also more or less easy and it is a group homomorphism, it is also easy to check this, let me not write all the details but just say how to check this, for example where does I squared go? What is I squared? Let us check that, φ of I squared is φ of I times φ of I. That is what a group homomorphism is supposed to do. But φ of I squared is φ of minus one, because I squared is minus one, what is φ of minus one, in my notation it is, in my definition it goes to I squared, on the other hand what is φ of I? It is I, this is an φ of I is a, it is a times a and that is a squared, this is okay.

I just check one more just for your clarity, what is φ of minus one times minus I, this is φ of, so I am multiplying these two elements minus one and minus I, that is φ of I. right, φ of I is a, what is φ of minus one times φ of minus I? Φ of minus one is a squared, φ of minus I is a cubed, a squared times a cube is a, so that I checked earlier. So this is also okay, this can be checked to be a group isomorphism.

So that is not difficult G1, G2 are isomorphic groups, but I want you to think about this carefully, G1 is a concrete group it is a subgroup of complex numbers non zero complex numbers which is fourth roots of unity, so it has a some meaning complex numbers have some other structure, they have some geometric meaning and so on.

Whereas second group has no structure, no meaning, other than whatever the group axioms give it. a is just a symbol and a4 is e, but G1 and G2 are isomorphic groups, so in abstract group theory, we are only interested in the group theoretic properties of a set. So in the study of abstract groups G1 and G2 are considered same, there is no difference between them, all the extra structure the G1 has is irrelevant as far as the group theory concerned, G1,G2 isomorphic as groups which is to say they essentially same.

There is no difference between them as groups,

(Refer Slide Time: 22:30)

Also note that, G2 is cyclic, G2 is a cyclic group. It is, in fact G1 is also a cyclic group, so cyclic group remember means, there is an element which generates the group in G1 case I generates the group, I squared is minus one, I cubed it is minus I, so G1 is cyclic and in G2 a generates it. So if G1 and G2 are isomorphic and both are cyclic. So it is not surprising there is in exercise I will give you and I will let you do this on your own.

If G1 is, now this is not G1 and G2, let us says G and G prime are isomorphic, then so there are two exercises G is abelian if and only if G prime is abelian, G is cyclic if and only if G prime is cyclic. Okay, being cyclic or being abelian is a very group theoretic property, so if earlier my statement that if isomorphic groups are to be thought of as same, certainly I would expect that abelianness would be care preserved under isomorphism.

So if one is abelian other must be abelian, otherwise I cannot think about them as two groups, because abelianness is necessary property of a group if one group is abelian and another group is not abelian I cannot think of them as same groups. Similarly if one group is cyclic and another is not cyclic, I cannot think them as cyclic, I cannot think them as same, so if two groups isomorphic, one is cyclic if in and only other is cyclic, one is abelian if and only other is abelian.

So again I should remark that this symbol here means, if and only if, I have been using this perhaps without saying what it is, its if and only if. That means G is abelian if G prime is abelian and only if G prime is abelian. So in order to prove this, you want to show that if G is abelian then G prime is abelian, same similarly you want to show that if G prime is abelian then G is abelian. Okay, so I will not do this exercise for now, because it's instructive to do this on your own and it is not difficult.

Online Editing and Post Production

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