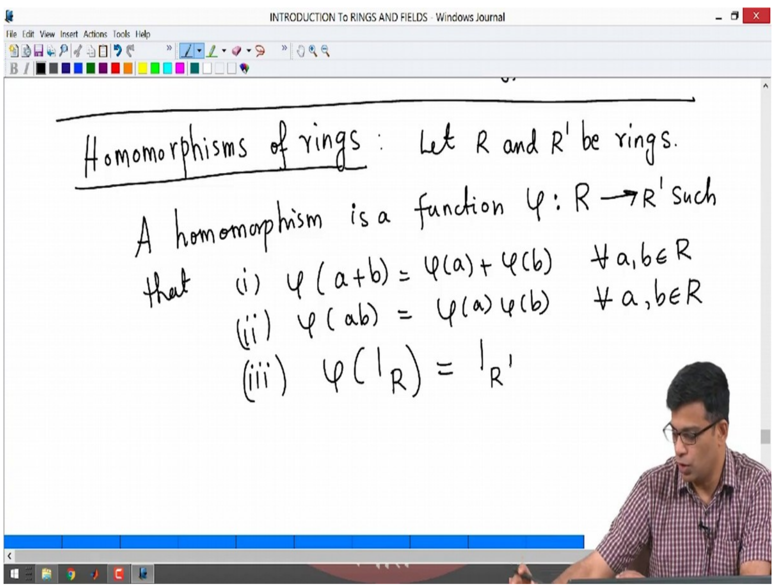
Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 06
Homomorphisms

In this video, we are going to introduce a very very important notion in a ring theory called "Homomorphisms" ok.

(Refer Slide Time: 00:25)



So, the next thing for us to do is homomorphism of rings ok. So, the goal is to study homomorphisms of rings. So, what are these? So, let us take two rings, so let R and R prime be rings. So, whenever you learn a mathematical object it is in order to understand these you need to study functions between them.

So, given the situation we have various different properties of those functions. When you studied groups we studied homomorphisms of groups, when you have you know metric spaces you have continuous functions. Similarly, for rings we have their own notion of functions. So, what is that?

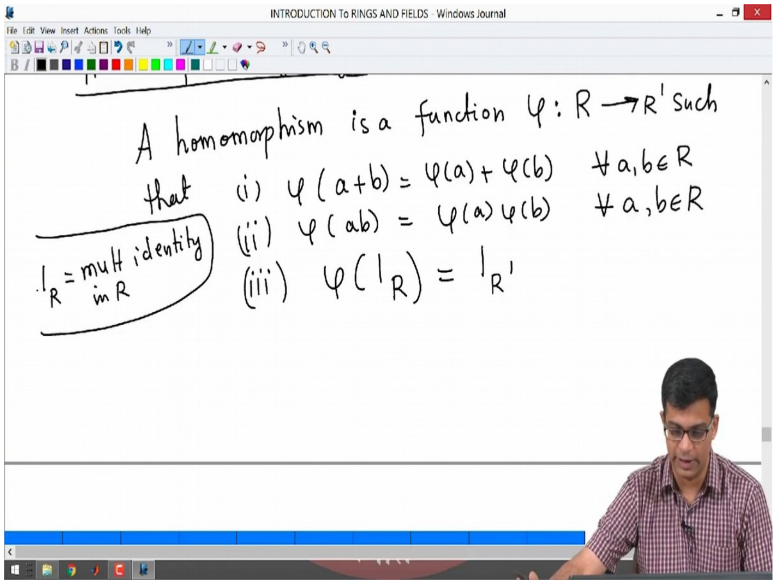
So, a homomorphism is a function; a homomorphism is a function let us call it phi from R to R prime such that it has the following properties. Because, R is abelian group under addition, R prime is an abelian group under addition it must to begin with have the property that it is an abelian group homomorphism. So, that can be captured by simply saying such that, so we have the following functions properties phi of a plus b should be equal to phi of a plus phi of b.

So, if you take two elements in ring R, for all a b in R if you take phi of a plus b it should be phi of a plus phi of b. The second property is if you multiply them first in R and then take the image that should be same as taking the image and then taking the a then multiplying inside R prime. So, here you have to be careful here.

See plus that I have on the left-hand side is plus in R, plus that I have on the right-hand side is plus in R prime. Similarly, when I write a b here I am multiplying in R, here I am multiplying by multiplying in R prime because R and R prime are rings they have their own multiplication and addition. So, these properties look very similar to group homomorphism properties.

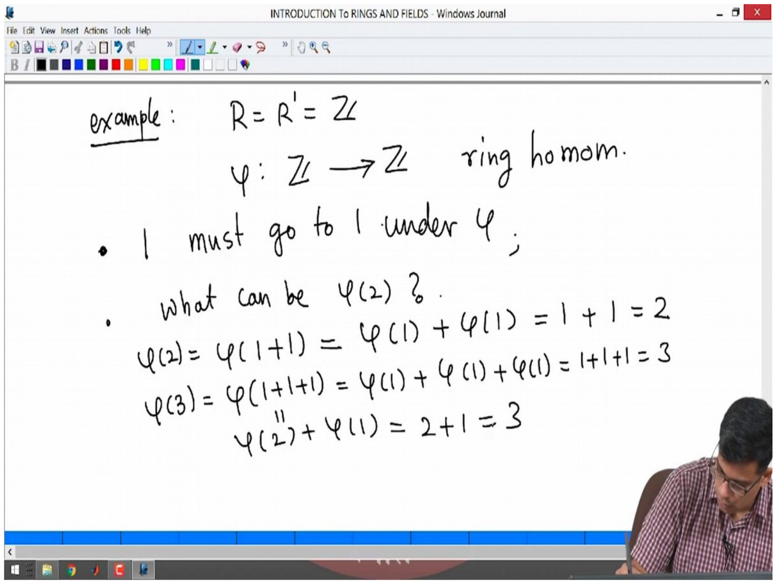
The third and very important property for a ring homomorphism is phi 1 R should be 1 R prime. So, I am going to do this just once, so that you are familiar with 1 being an identity element of R versus 1 being in element identity element of R prime.

(Refer Slide Time: 03:23)



So, this is the multiplicative identity in R and similarly 1 R prime is the multiplicative identity in R prime. So, in general we will not do this. We will just use 1 always to denote multiplicative identity in whatever ring we are considering. But just to understand what the third property is saying I want the multiplicative identity of the first ring to go to the multiplicative identity of the second ring. So, using these three properties we have homo; so, given these three properties we have homomorphisms of rings.

(Refer Slide Time: 04:07)

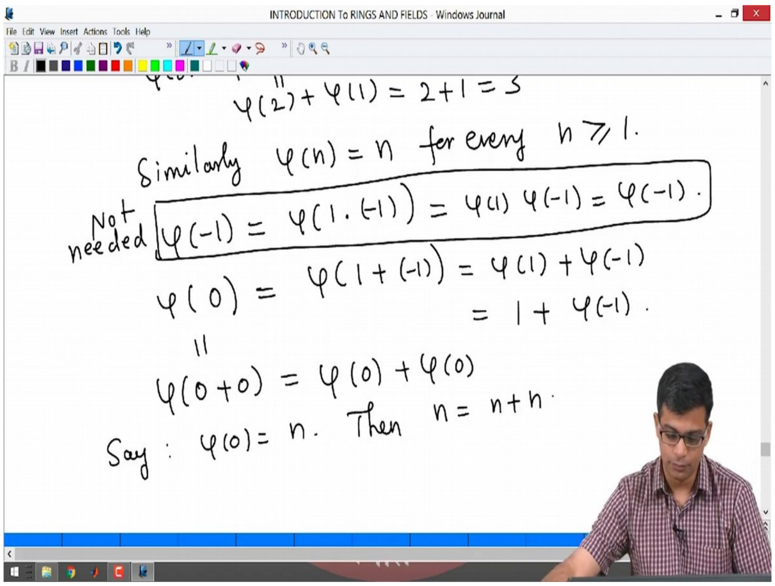


So, first as an immediate example, let us look at R and R prime both are the equal to the ring of integers. So, R and R prime are equal to Z. What is a ring homomorphism? So, I want to write like this. So, I want a ring homomorphism. So, let us try to build up a ring homomorphism using the three properties. We are already told that 1 must go to 1. So, there is no choice. So, 1 must go to 1. The integer 1 must go to integer 1 under phi ok. So now, then what about, so this is already forced on us. Now, what can be image of 2?

What can be the image of 2? Now, let us look the properties of a ring homomorphism. Phi of a plus b should be phi of a plus phi of b. So, phi of 2 remember phi 2 is phi of 1 plus 1 because 2 is 1 plus 1. But phi of 1 plus 1 by ring homomorphism property should be phi of 1 plus phi of 1, but phi of 1 is supposed to be 1 so, 1 plus 1 is 2. So, in other words, there is no choice for phi of 2 also, right phi of 2 must be 2. What about phi of 3? Phi of 3 is equal to phi of 1 plus 1 plus 1 because 3 is 1 plus 1 plus, this is obvious, but the ring homomorphism property says that this should be phi of 1 plus phi of 1 plus phi of 1.

Though I have written for two elements here, phi of a plus b you can clearly see that generalizes to any number of finite number of elements phi of 1 plus 1 plus 1 should be phi of 1 plus 1 plus phi 1 which is in turn phi of 1 plus phi 1 plus phi 1. But this is 1 plus 1 plus 1 which is 3. Of course, I can also write this as phi of 2 plus phi of 1 and I have already showed that phi of 2 must be 2. So, this is 3. So, you can clearly see that similarly phi of n is equal to n for every n greater than 1.

(Refer Slide Time: 06:31)



So, now, let us look at negative numbers. So, what is phi of minus 1? What is phi of minus 1? So, phi of minus 1 should be whatever it is, write phi of minus 1 is equal to phi of 1 times phi of minus 1 because minus 1 is 1 times minus 1, but because of the third property of ring homomorphism or the second one in the list that I wrote here, phi of a b is phi of a times phi of b. So, phi of 1 times minus 1 is phi of 1 times phi of minus 1 ok.

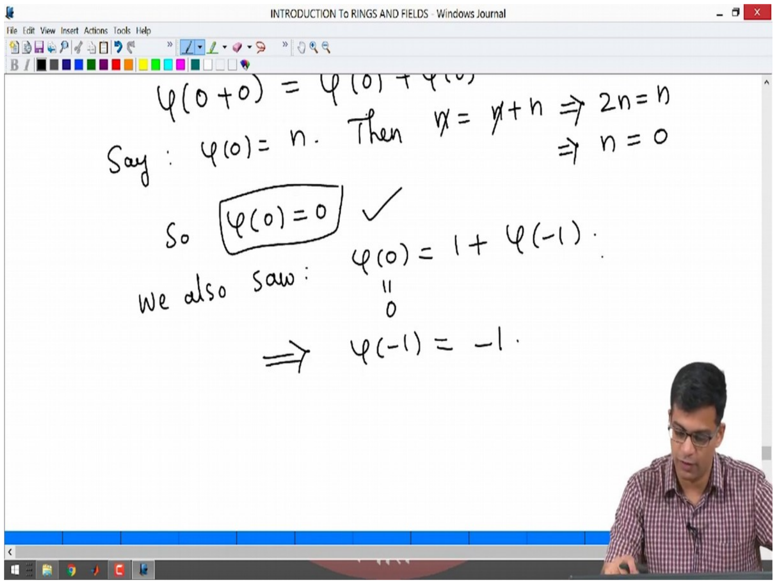
So, this tells me nothing actually, right. So, this is just phi of minus 1 ok. So, this is actually not useful in order to compute phi of minus 1 because phi of minus 1 is phi of minus 1, there is no information that we have. So, let us do one more thing. Let us try to find out phi of 0 first. What is phi of 0? So, I will write this as phi of 1 sorry phi of 1 plus minus 1. So, this is actually you can skip. So, this I made mistake this is not necessary. It is not needed.

Let us do phi of 0. So, 0 is 1 plus minus 1, right. So, phi of 0 is phi of 1 plus minus 1, but again by the property of ring homomorphism this is same as phi of 1 plus phi of minus 1 ok. So, and phi of 1 is phi of 1 is 1, so this is 1 plus phi of minus 1. So, now, I want to show that phi of 0 is 0 ok. So, let us use; let us see if I get this. So, phi of 0 equals phi of 0 times 1. So, I am going to use the. So, phi 0 is on the one hand 1 plus phi of minus 1. Now, phi of 0 is phi of 0 times 1 because 0 is equal to 0 times 1.

And this is equal to by the property of a ring homomorphism phi of 0 times phi of 1, ok. So, this is also. So, actually let me not do this. Let us do the following. Phi of 0 is phi of 0 plus 0, right, phi of 0 is phi of 0 plus 0 because 0 is equal to 0 plus 0. Phi of 0 plus 0 is phi of 0 plus phi of 0. So, phi of 0 is equal to phi of 0 plus phi of 0. But now what integer has this property?

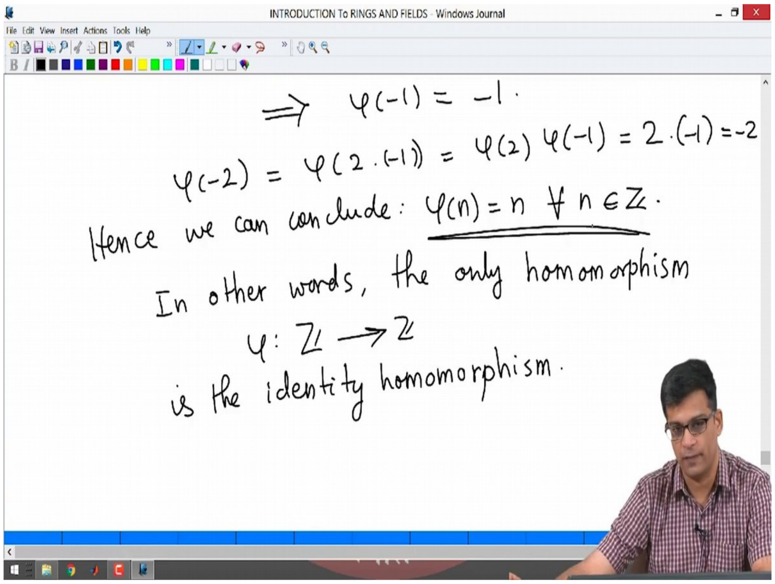
We have some integer let us say phi of 0 is equal to sum n ok. So, then we have n equals n plus n, right n is equal to n plus n. But once n is equal to n plus n that means 2 n equals n, that means n is 0, because if you have any integer which twice that is equal to itself n must be 0, right. So, in other words all we are doing is cancelling that, so, n is equal to 0.

(Refer Slide Time: 09:57)



So that means, phi of 0 is 0 ok. So, this I should have said first. Phi of 0 is 0 once you have the property that phi of a plus b is equal to phi of a plus phi of b, phi of 0 is 0. Now, let us come back here. So, we have also notice that, we also saw phi of 0 is equal to 1 plus phi of minus 1, right. So, now that we know what is phi of 0 which is 0, so we can also find out phi of minus 1. So, phi of minus 1 is minus 1 because phi of minus 1 is 0 minus 1, so phi of minus 1 is minus 1. What about phi of minus 2?

(Refer Slide Time: 11:05)



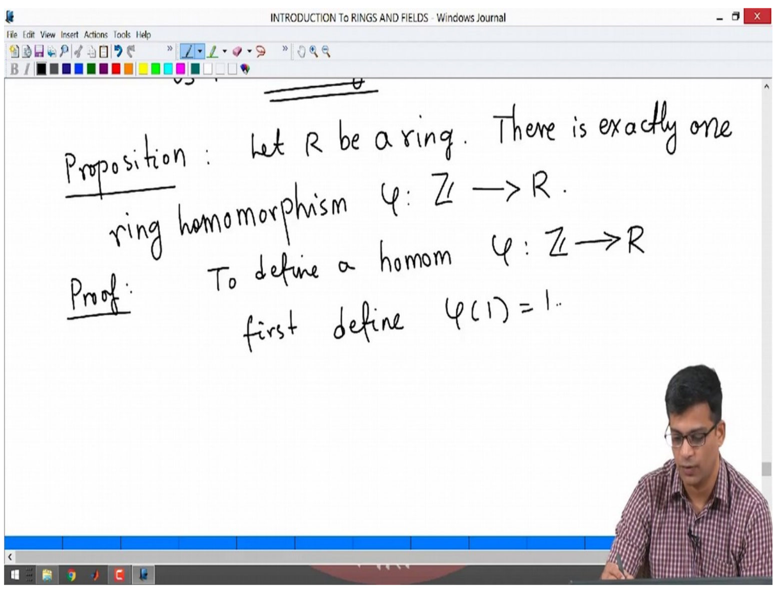
Now, we can simply use multiplicative property of this. So, phi of minus 2 is 2 times phi of 2 minus 1, right because minus 2 is 2 times minus 1. This is same as phi of 2 times phi of minus 1 by the multiplicative property which we have not used yet. Now, phi of 2 I have already showed is 2 and phi of minus 1 I have already showed is minus 1, so this is minus 2. So that means, phi of minus 2 is minus 2. So now, we can conclude, hence we can conclude. Earlier I said phi of n is equal to n for all positive integers n, right. Now, I am able to conclude this is true for all n, phi of n is equal to n for every n in Z.

In other words the only homomorphism from Z to Z is the identity homomorphism ok. So, this is a very interesting property that you should actually spend some time thinking about it, because we have lots of group homomorphism from Z to Z, right. Group homomorphisms from Z to Z if you think about it will have both the properties 1 and 2 that I have written here, a plus b will go a phi a plus phi of b and that will automatically imply that phi of a b is phi of a times phi of b.

But the third condition we do not have for a group homomorphism, that allows us to send 1 to 2, that will give you homomorphism, that allows us to send 1 to 3 that is another group homomorphism. **But for a ring homomorphism 1 must go to 1,** so it is very rigid. So, ring group homomorphism are rigid 1 has no choice, but to go to 1. And once you insist that 1 has to go to 1, all you are left with is the identity group homomorphism. So, the only ring homomorphism from Z to Z is the identity homomorphism. So, ring homomorphisms are very special and part of their speciality comes from the requirement that 1 must go to 1.

So now, this is one example which is very important. Let us slightly generalize this example to make a very important, find out an important property about rings. So, this is another example ok.

(Refer Slide Time: 13:49)

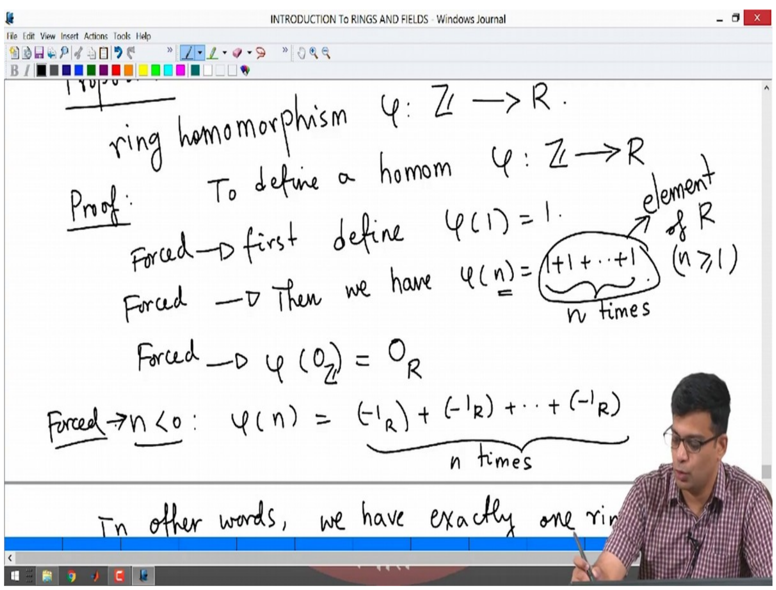


So, this is really a proposition, I will write it like that. So, this is a proposition. So, what is a proposition? Given for, let R be a ring. So, the previous example said that there is exactly one homomorphism from Z to Z, namely the identity map. Now, if you replace Z by any ring R and look at the homomorphism from integers to R, the same idea as before shows that there is exactly 1 homomorphism.

So, let R be a ring there is exactly one ring homomorphisms, ring homomorphism from Z to R. This is a very crucial statement in ring theory and it tells you that integers are somewhat special among all the things. They are special because there is always a homomorphism from Z to R and there is in fact, exactly 1. So, that is saying two things here, there is a homomorphism and there is exactly 1 we are saying. So, that gives Z as special place in the world of rings.

So, what is the proof of this? So, now, to define a homomorphism is easy. So, remember here R is an arbitrary ring, we are not going to use any property of R other than its ring theoretic properties. To define a homomorphism of from Z to R simply ok, so first define I should say first define ok. So, remember there is no choice for us. The identity element of Z, you multiplicative identity element of Z must go to multiplicative identity of R which I will denote for convenience of notation I will just denote both by 1. We will only keep in mind that 1 here, in the bracket stands for 1 of Z, 1 here stands for 1 of R. So, there is no choice 1 has to go to 1.

(Refer Slide Time: 16:19)



So, then we have phi of n is 1 plus 1 plus 1 n times for n positive ok. So, again this is forced on us. So, what I am trying to arrive at in this proposition is, once you define 1 equal to phi of 1 equal to 1 which we have no choice about we must define it like that, every other integer has a natural image.

There is no choice for them also. For example, if n is a positive integer; remember in order to define a map from Z to R homomorphism from Z to R, I need to tell you what is image of every integer is. I have defined 1 will go to 1 because we have no choice, now I am taking care of positive integers.

If I have a positive integer its image must be simply 1 of R plus 1 R, the identity element of R added n times. This is the property of a ring homomorphism, right. So, phi of n must be that whatever that element is, that is a ring element now ok. And, what about phi of negative integers? If n is negative and on the other hand if first of all n equal to 0 what should be, I will simply define it to be 0. Again, there is 0 here stands for two different 0s, 0 of the integers will be denoted by 0 sub Z that must go to 0 sub R. Now, I have defined phi for positive integers and 0.

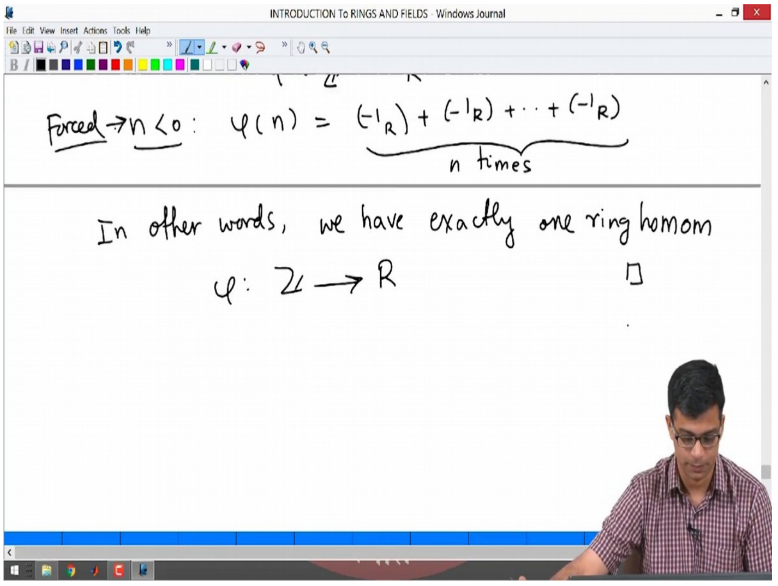
What will it be for negative integers? I will simply define it, I have to define it remember using the ring theoretic, ring homomorphism properties. So, I will define it to be minus 1; minus 1 in the ring R, plus minus 1 because 1 is a ring element its additive inverse is denoted by minus 1, I will add it n times. So, there is no choice again about this.

So really, I have done both existence and uniqueness of a ringhomomorphism from Z to R because 1 must go to 1, that forces n to go to 1 plus 1 plus 1 plus 1 n times. It also forces 0 just like we have checked earlier, 0 must go to 0 because 0 plus 0 must go to 0, phi of 0 plus 0 is same as phi of 0; that means, phi of 0 plus phi 0 plus phi of 0, but in a group that implies that phi of that element is the 0 element. So, the proof for this is exactly here.

So, what I have described here. In this box, that proof carries over. So, this is also forced. So, this is forced. These are all forced, by which I mean forced by the the ring homomorphism properties. 1 must go to 1, that is forced. Once 1 goes to 1 phi of n for positive n must go to 1 plus 1 plus 1 n times that is forced, 0 must go to 0 that is forced, and so is this, right.

I have already told you again here because phi of minus 1 is phi of 1 time a phi of 0 is phi of 1 minus 1 which is phi of 1 plus phi of minus 1 phi of 1 is 1 and phi of 0 is 0. So, phi of minus 1 will be minus 1. Similarly, phi of minus n will be minus 1 plus minus 1 plus minus 1 n time, so, this is also forced.

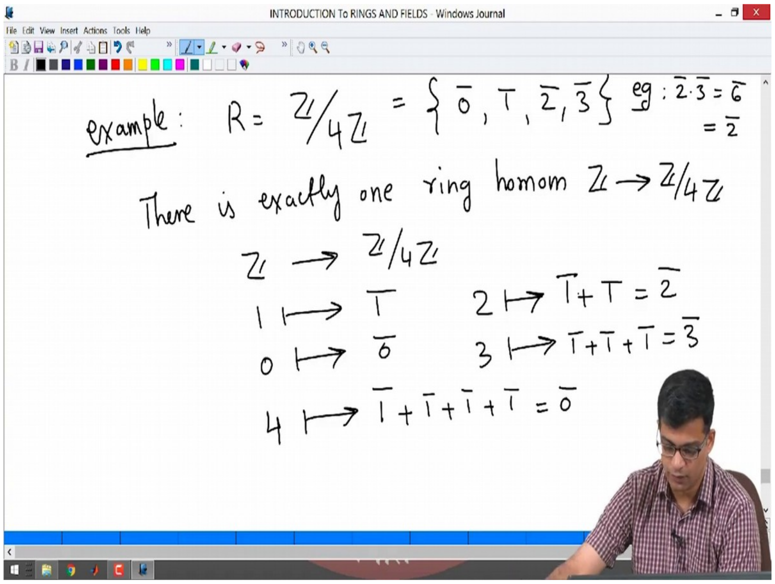
(Refer Slide Time: 20:15)



In other words, we have exactly one ring homomorphism, right. So, we have exactly one ring homomorphism from Z to any ring R. So, I essentially this finishes the proof of the proposition, I have defined a ring homomorphism and I have at each step showed you that there is no choice we have.

So, we cannot send 1 to any other element, right 1 has go to 1. We cannot send 2 to any other element, 2 has to go to 1 plus 1, 0 must go to 0, minus 2 must go to minus 1 plus minus 1. So, there is no choice and this particular choice gives you a valid homomorphism. So, in other words, we have a ring homomorphism and we have exactly one ring homomorphism.

(Refer Slide Time: 21:11)



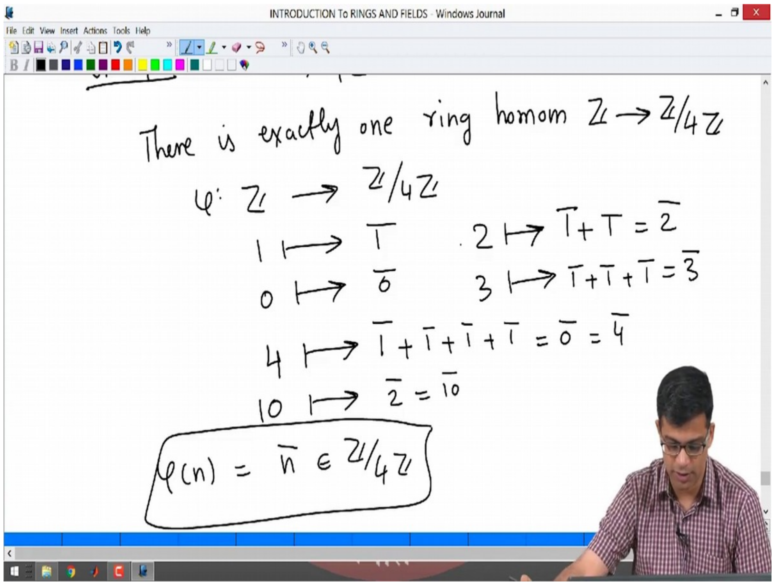
So, to illustrate this point and to also give you some subtleties about this, let us look at the example of R. Let us say I take Z mod 4 Z. Remember, last in previous video we told you how to give a ring structure, we learned how to give a ring structure to this cosets, right

So, you think of Z as an abelian group, 4 Z is a subgroup of the abelian group and you take the quotient group, it will have 4 elements and on which you know how to multiply ok. I have told you how to multiply. So, here for example, 2 bar times 3 bar is 6 bar which is actually 2 bar ok. So, this tells me that in using this idea you can multiply any two elements here and that makes this a ring.

So, by the proposition before there is exactly one ring homomorphism from Z to Z mod 4 Z ok. Let us explicitly write it down, let us explicitly write it down so, Z to Z mod 4 Z. As we said 1 must go to 1. What is 1 of R? So, R has 4 elements here, so 1 bar is the multiplicative identity. 1 bar must go to 1 bar, of course, 0 must go to 0 bar, 2 bar must go to sorry 2, the integer 2 must go to remember image of 1 plus image of 1, so 1 bar plus 1 bar which is 2 bar. Where will 3 go? 3 will go to 1 bar plus 1 bar plus 1 bar which is 3 bar.

Now, Z has infinitely many elements, I need to tell you what is the image of 4. Where will 4 go? It will go because of the previous proposition, it will go to 1 bar plus 1 bar plus 1 bar plus 1 bar, but this actually the zero element of the ring, right because 4 times if you add 1 bar you get 0, that the residue of 4, residue class of 4 which is 0.

(Refer Slide Time: 23:27)



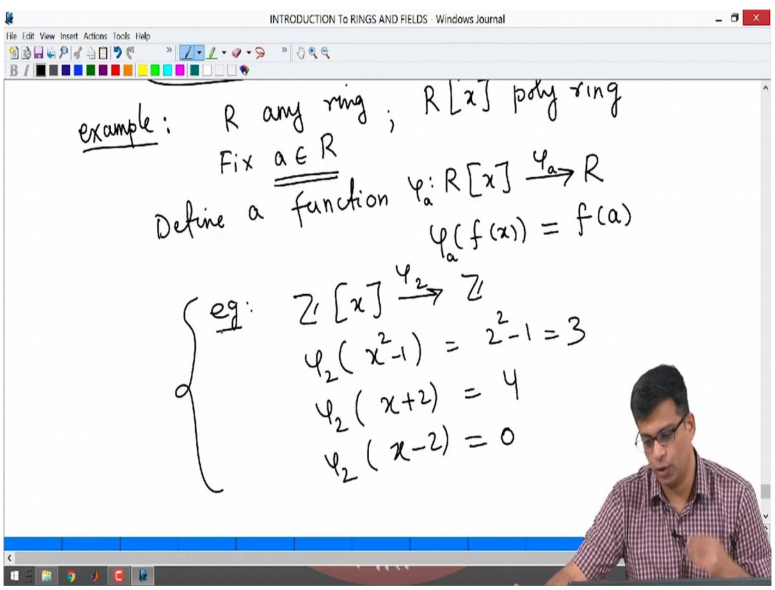
Similarly, where will 10 go? Now, you get the idea. So, 1 plus 1 bar you add 10 times that will simply be 2 bar. So, in other words if you think about this phi of n is actually just n bar in Z mod 4 Z, right. So, here member n 2 bar is same as 10 bar, 0 bar is same as 4 bar. So, this is the ring homomorphism.

And again, it confirms to you that there is no choice in defining this ring homomorphism, we are forced to have this. 1 bar must go to 1 bar sorry, 1 must go to 1 bar, 0 must go to 0 bar, 4 must go to 0 bar, 2 goes to 2 bar, 3 goes to 3 bar and so on. So, this is the unique ring homomorphism from Z to R Z mod 4 Z. So, I am also trying to do this example for the following reason.

When I write here for an arbitrary ring homomorphism from Z to an arbitrary ring R, n goes to positive n goes to 1 plus 1 plus 1 n times, you might think that is equal to n itself, but that is that will not be. So, what I want to say is that this is not really n, n really only stands for an integer. This is a ring element. Whatever you get, in different situations you will get different things.

So, in the case of Z mod 4 Z, if you take 4 and see where it will go, it will be 1 bar plus 1 bar plus 1 bar plus 1 bar that is not really 4, there is no element called 4 in Z mod 4 Z, ok, so that is a 0 bar. So, you have to be careful when you do this, it is not n as we know an integer n, it is just the multiplicative identity added n times. So, here multiplicative identity is 1, added 4 times for 4 you get 0 actually the 0 element. So, you have to be careful about such subtleties when dealing with arbitrary rings. And, I will just do one more example to illustrate another important class of ring homomorphisms ok.

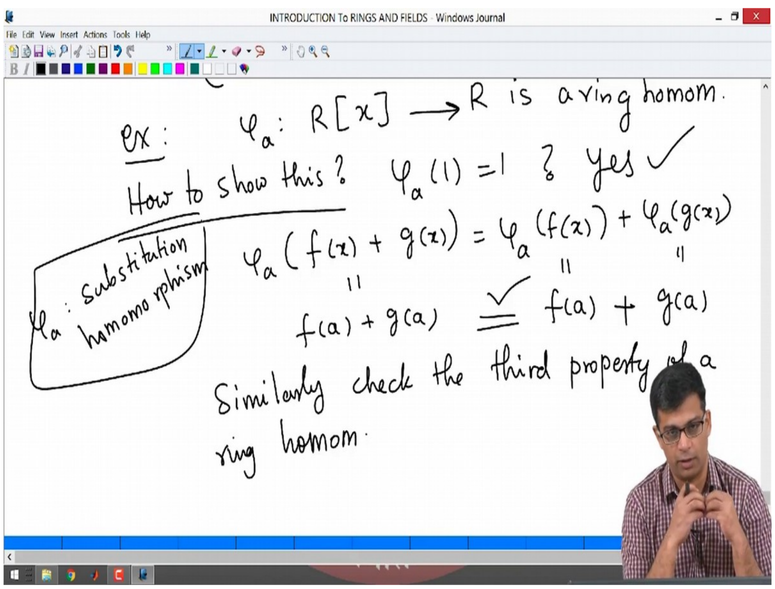
(Refer Slide Time: 25:51)



So, here for this purpose let us take R any ring and consider the polynomial ring R[x] that we discussed in a previous video, and let us fix an element of R. Let us say fix an element of R, let us call it a. So, define a function from R[x] to R by sending let us call this phi, phi of f of x, f x is a polynomial in R[x] I send it to f of a. So, I have already told you in a previous video, we can evaluate a polynomial at any element of the ring. So, in other words I am simply replacing x by a.

For example, if I take Z[x]. So, this is a special case of this example I have a map from Z[x] to Z[x], Z[x] to Z. Let us denote this by phi sub a, because a determines this map, right. So, this is phi sub a. So, here let us look at phi sub 2. So, phi sub 2 of x squared minus 1 will be simply 2 squared minus 1 that is 3, phi sub 2 of x plus 2 will be 4, phi sub 2 of x minus 2 will be 0, right. So, you understand. You take a polynomial replace x by that element a and you get a ring element that is this map. So, this is an exercise now.

(Refer Slide Time: 27:35)

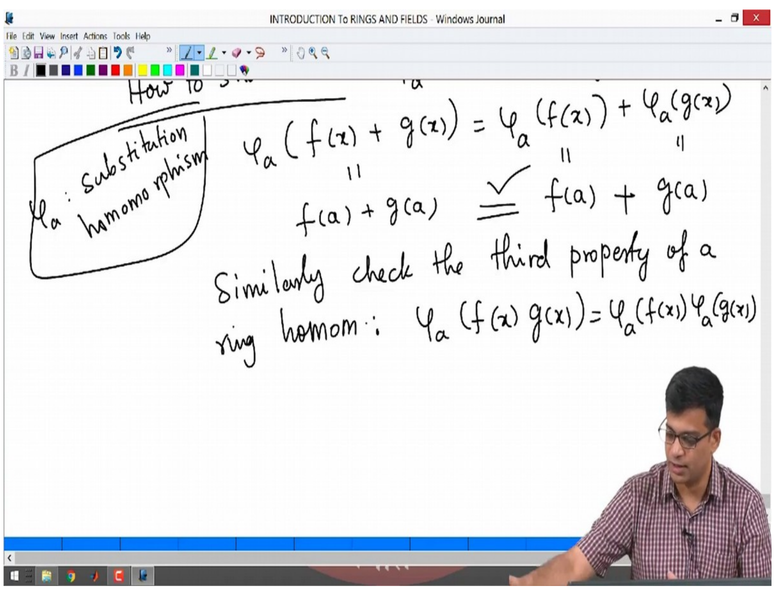


Now, going back to the general case, phi a from R[x] to R is a ring homomorphism ok. So, let me just quickly tell you, instead giving you a full proof of this which I leave you for you to do, how to show this. I will suggest, I will give you some hints and I will ask you to finish the proof how to show this.

There are 3 properties to check, right. So, you take first of all is phi of a 1 1? This we need, right. Take the constant polynomial 1, substitute x equal to a, do you get 1? We get 1, this is because there is no x in 1. So, when you plug in a, there is nothing that changes. So, phi of a is, phi of a phi of 1 is 1. What about phi of a of f x plus g x? So, I claim that this is same as phi a of f x plus phi a of g x. So, this is by definition f a plus g a, because you are taking this polynomial given by the sum of these two substituting by a. This is f a, this is g a ok so, these are equal.

Similarly, so essentially, I have done 2 of the 3 properties. Do similarly check the third property of a ring homomorphism ok. So, this is an important ring homomorphism for us. This is called “substitution map” because that is what it is, right. So, phi a is called substitution homomorphism and it is an important homomorphism for us. It is a way of going from a polynomial ring to the ring itself, underlying the base ring, by substituting a specific value for every x.

(Refer Slide Time: 29:51)



So, this is the ring homomorphism. I will leave the last check for you, phi of a phi of f x times g x is phi of f x times phi of g x ok. In fact, I will be happy even if you can check this in a particular example. Even if for a Z[x] to Z[x] and phi 2 you play with two polynomials of your choice and check that this third property of a ring homomorphism holds. So, this tells me that phi a is a ring homomorphism and we call this a substitution homomorphism.

So, some of the important examples of ring homomorphism that we covered in this video after defining ring homomorphisms are, some of the examples we discussed are: we showed that there is a unique homomorphism from Z to any ring R and in particular there is a unique homomorphism from Z to Z and which is identity homomorphism. And we also talked about homomorphism from polynomial ring R[x] to R, given by substituting a specific element.

I am going to end this video here. In the next video we will look at more examples of ring homomorphisms and their properties.

Thank you.