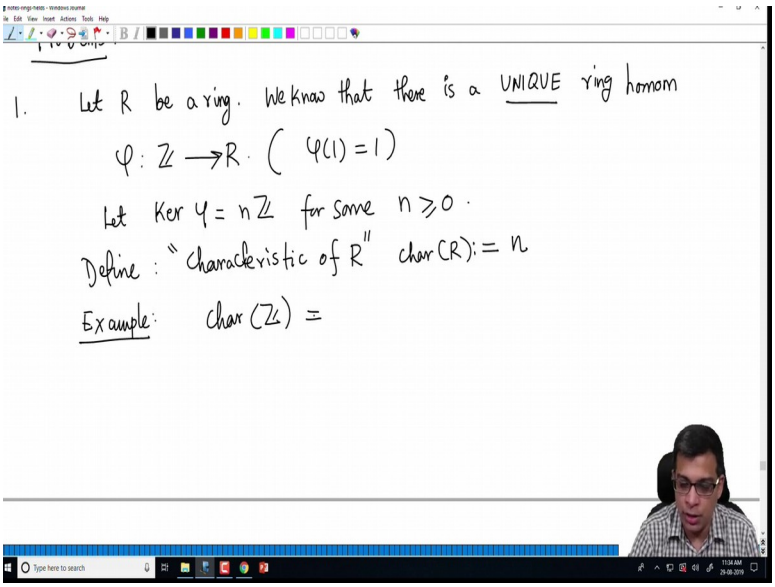
Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture – 31
Problem – 8

In the last video we considered the Eisenstein criterion which is a good way of measuring or checking whether a polynomial integer polynomial is irreducible either over the rationals or the integers. And we also did some problems on how to use it, it is not always applicable, but when its applicable, it is a very easy way of determining irreducibility.

So, that completes the topic of ring theory that I wanted to cover in this course. But, before moving to the next topic which is fields, let me do a few problems on rings in general on many of the topics that we covered in these last few weeks.

(Refer Slide Time: 00:53)



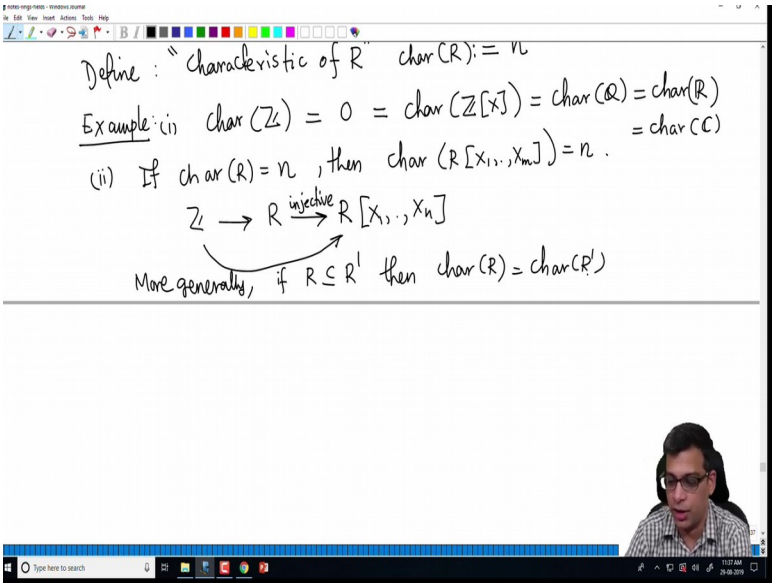
So, let me solve some problems in today's video. Some of this I may have referred to in some earlier videos, but let me do it any way again. So, let R be a ring, we know that this is really more not just a problem, but I am defining then you think and we will compute it for some examples. So, we know that there is a unique, there is very important unique ring homomorphism phi from Z to R, Z remember always represents the ring of integers.

There is a unique ring homomorphism, remember that phi of 1 must be 1. For us ring homomorphism by definition sends the unit multiplicative identity to the multiplicative identity. And, once you insist on it there is exactly one ring homomorphism right because, once you know that 1 has to go to 1, 2 has to go to 2, minus 2 has to go to minus 2, minus 1 has to go to minus 1 and so on.

So, that we have discussed earlier there is a unique ring homomorphism. So, consider the kernel of this ring homomorphism, we know that any ideal kernel is an ideal of the integers. Any ideal of the ring of integers is of the form n Z for some non-negative integer right, n is a non-negative integer. So, we define the characteristic so, this is an important word in a ring in field theory, characteristic of R which I denote usually by just char bracket R is n ok.

So, that is all; so, characteristic of R is equal to the generator, the non-negative generator of the kernel of the unique map from Z to R. So, as an example what is the characteristic of Z? What is the characteristic of Z? Remember there is a unique map from Z to Z in fact, that is the identity map, identity ring homomorphism its kernel is the 0 ideal because, it is an adjective map and hence the generator is 0.

(Refer Slide Time: 03:21)



So, characteristic of Z is 0 and that actually also is the characteristic of Z X polynomial in any number of variables, this is the characteristic of Q, characteristic of R and so on.

So, characteristic of C all this rings have the unique map from the ring of integers to these rings is injective; that means, characteristic is 0; the generator of the kernel is 0.

Similarly, we know that if characteristic this is covered here, but if characteristic of R is ok. So, maybe I will postpone this I can just say this I guess, if characteristic of R is n then characteristic of the polynomial ring over R is also let say this is m r; some other number of variables X n, then this is also n right.

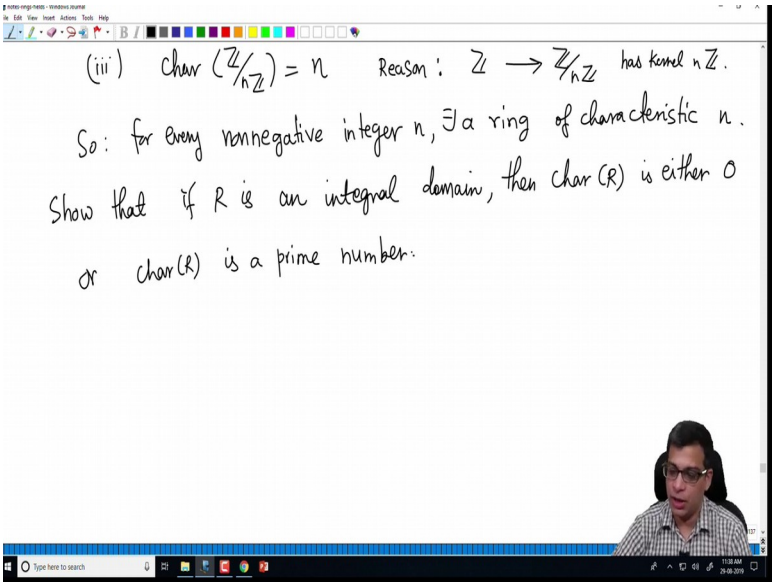
Because, if there is a the ring homomorphism, the unique ring homomorphism from this is injective. The inclusion of R in the polynomial is injective. So, the unique ring homomorphism from Z to the polynomial ring is simply the composition of the unique ring homomorphism from Z to R and then followed by the inclusion because, 1 has to go to 1.

So, this is the only one map from Z to the polynomial ring, it must be the composition of these two because that is the map from Z to that. So, this is the unique map and once you have this unique map because R to R adjoint X 1 to X n is injective, kernels are same.

Kernel of the map from Z to the polynomial ring is equal to the kernel of the map from Z to R, because if something goes to 0 under that composition it must go to 0 in the first map itself because, it second map is injective. So, the characteristic does not change if you simply add some more variables or in general if R more generally the same principle actually says that if R is a sub ring of S.

If let us say R is a sub ring of R prime and then characteristic of R is same as characteristic of R prime because, there is a unique map from Z to R. There is a unique map from Z to R prime which must be the composition of the map from Z to R and the inclusion of R and R prime.

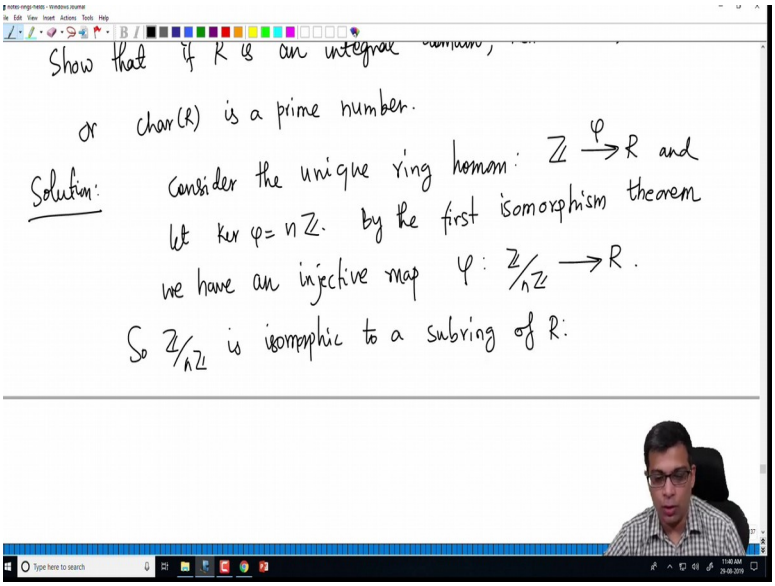
(Refer Slide Time: 06:11)



So, these are easy observations and we can also say characteristic of Z mod n Z is n right. So, this is because the reason is the unique map from Z mod Z to Z mod n Z has kernel n Z right. So, the reason is that the unique map from Z to Z mod n Z has kernel n Z so, the characteristic of Z mod n Z is n. So, in other words for every non-negative integer n there exists a ring of characteristic n this is an easy, observation because you can simply take Z mod n Z.

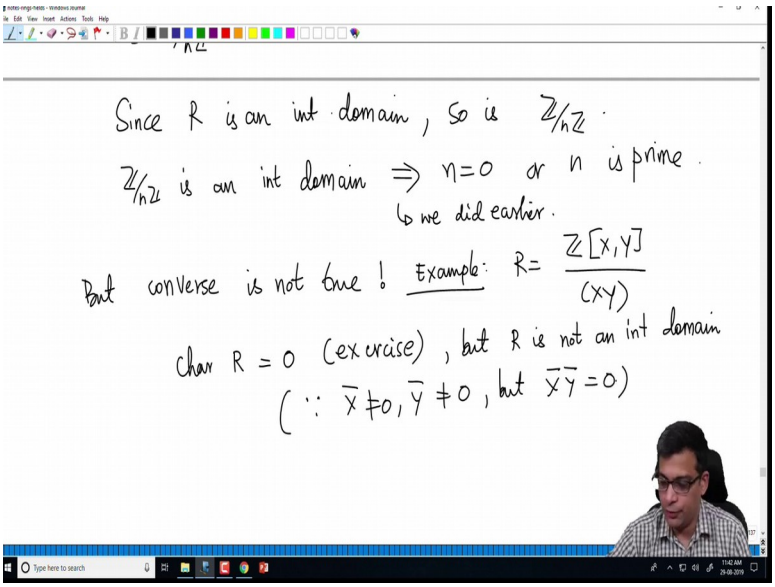
So, we have not yet gotten to the problem, but the problem now I will ask is show that if R is an integral domain, then characteristic of R is either 0 or characteristic of R is a prime number; remember characteristic is always a non-negative integer. So, for an integral domain it cannot be any arbitrary non-negative integer; it has to be either a prime number or it has to be; it has to be 0. So, 0 is also allowed and the reason is solution.

(Refer Slide Time: 07:57)



So, consider the unique map or the unique ring homomorphism from Z to R and let kernel of this phi be n Z. So, by the first isomorphism theorem, by the first isomorphism theorem we have an injective map which I will denote by also phi from Z mod n Z to R right, this is an injective map. So, Z mod n Z is isomorphic to a sub ring of R.

(Refer Slide Time: 09:03)



Now, we are given that since R is an integral domain; so, I will shorten it like this since R is an integral domain so, is Z mod n Z right. We know very well, that if you have any integral domain a sub ring is also an integral domain that is very easy to show. Because

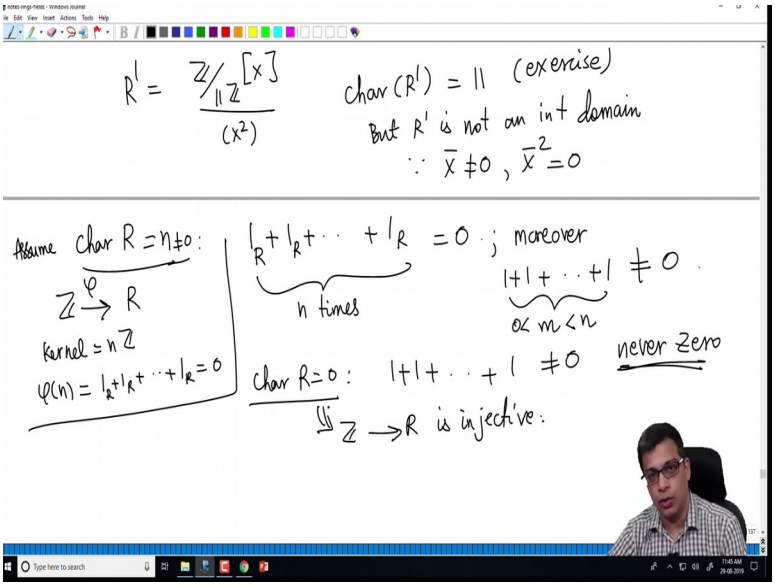
what is an integral domain? Product of two non-zero things is non-zero, but if R is the sub ring if Z mod n Z is the sub ring of R you take two things in Z mod n Z, they are also inside R and there if there both non-zero their product is non-zero in R.

So, it is also non-zero in Z mod n Z because it is a sub ring, but then if Z mod n Z is a integral domain which is what we just concluded, this implies that n is 0 or n is prime right. This is something that I discussed when I talked about integral domains, the quotient ring Z mod n Z is an integral domain only if n is 0 or n is a prime number. For example, Z mod 4 Z is not an integral domain because 4 is not prime and 4 is not 0, there you can get 2 bar times 2 bar is 0. So, this we did earlier.

So, I will not do this again, but this shows that characteristic of an integral domain is either 0 or its prime ok. So now, on the other hand; so, this solves it right, but converse is not true. What I mean is if the characteristic is prime or characteristic is 0, it need not be an integral domain. For example you consider R to be Z X Y let us say modulo the element polynomial X Y.

So, what is a characteristic of R? Characteristic of R is 0, this I will leave as an exercise. The point is Z is a sub ring of this right because, constants can be viewed has sub ring of Z X Y for sure and then you are killing X Y. So, you are not killing any integer. So, Z continues to be a sub ring of R, but is R an integral domain of course, not R is not an integral domain right because X bar and Y bar are non-zero, but X bar Y bar is 0 right. We have killed X Y so, X bar Y bar is 0.

(Refer Slide Time: 11:49)



Similarly, if you take R prime to be Z mod 2 Z let us say or Z mod 11 Z X mod X squared characteristic of R prime is actually 11 because, this is also an exercise. Z mod 11 Z sits inside this as a sub ring, but R prime is not an integral domain for the same reason right because, X bar is non-zero, but X bar squared is 0 ok.

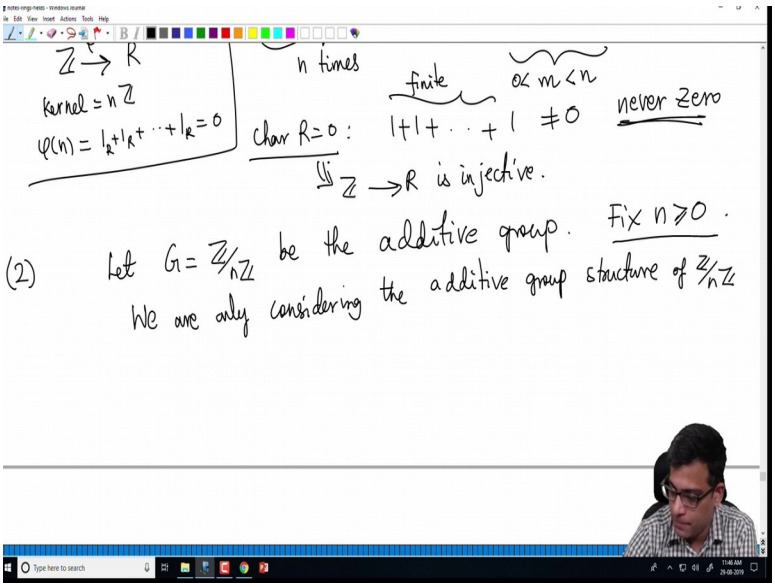
So, characteristic of an integral domain is always either 0 or a prime number, but if a ring has characteristic 0 or a prime number does not mean that ring is an integral domain ok. So, before I continue to the next problem let me basically make a remark that if characteristic of R is n, then if you take 1 R and add.

So, suppose n is not 0, assume that characteristic of R is an integer n not 0, then if you add n 1 n times you get 0 right because; that means, if you under this assumption Z mod n Z so, its inside as a sub ring of R ok. So, actually let me do it like this Z to R there is a map kernel is n; that means, n is contained in the kernel. So, phi of n is 0, but what is phi of n? Phi of n is 1 R plus 1 R plus 1 R that is 0 ok; so, that is a reason for this and not just that more over 1 plus 1 plus 1, if you take m less than n times its not 0.

So, n is the least positive integer such that 1 times 1 times 1 plus 1 plus 1 plus 1 n times is 0. In other words anything smaller it will not work, on the other hand if characteristic is 0 1 plus 1 plus 1 any number of times is not 0, is never 0 right. Because, the map from in this case the map from Z to R is injective by definition because, if the characteristic is 0 kernel is 0; that means, it is a injective map. So, when you take phi of n it is non-zero,

phi of any number is non-zero; that means, 1 plus 1 plus 1 any finitely many times it is not 0 ok; so, that is never 0.

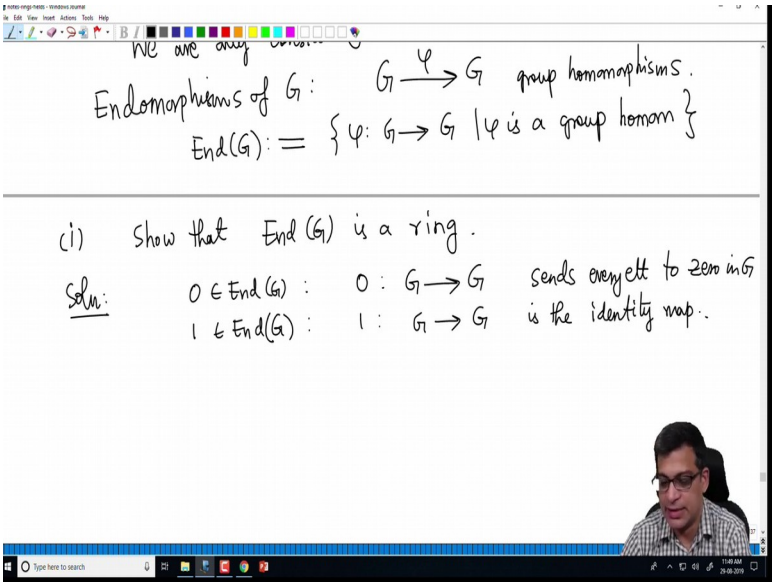
(Refer Slide Time: 14:33)



So, there is one good way of keeping track of characteristic of a ring. So now, let me do a second problem here which is actually a good way to combine group theory and ring theory, group theory that you learned in the past. And, it is somewhat confusing actually if you think about it, if you are seeing this for the first time, but let us do this carefully. Let us consider Z mod n Z be the additive group.

So of course, Z mod n Z is also a ring so; that means, we are only considering the additive group structure. So, fix an any positive any non-negative integer consider; so, fix an non-negative integer n. We are only considering the additive group structure, for now we are only considering the additive group structure of Z mod n Z ok.

(Refer Slide Time: 15:47)



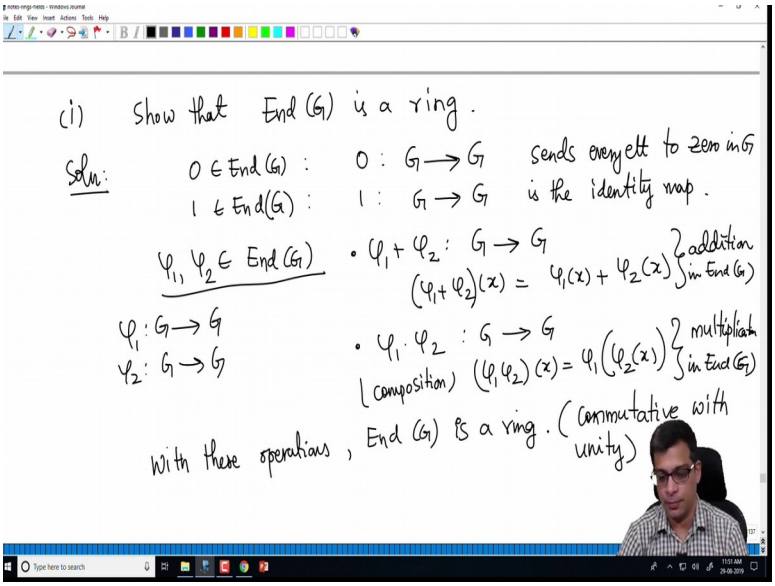
So, let us take this, I am interested in the following object. So, this is called endomorphism set for now. So, these are group homomorphisms from G to G ok. So, let us denote this by End End of G, this is by definition all group homomorphisms from. So, let me emphasise again phi is just a group homomorphism, Z mod n Z is also a ring, but I am not looking at ring homomorphisms; that means, I am not insisting that 1 goes to 1.

So, we do get lots of a new objects because, if you insist on only if you only consider ring homomorphism then there is exactly 1 because, 1 has to go to 1. There is only one element in the set of ring homomorphisms, now I am considering only the set of group homomorphism; so, they are more elements. So, first show that so, the first part of the problem is show that End G is actually a ring ok.

The solution for this is very easy, I will not do all the details because I have I want to do some other problems also. So, let me set this up and leave the actual verifications to you this part is easy, show that End G is a ring. So, what do we do? So, let us first of all 0 is there. What is 0? It is so, I will just denote by 0, it is a map from G to G sending every element to 0.

So, remember G is an additive group, it has an additive identity which we usually call 0. So, sends everything to 0, 1 in End G I claim is the identity map ok; this will make sense once we actually define addition and multiplication is the identity map; that means, it sends small x to small x. And what is addition?

(Refer Slide Time: 18:07)



So, maybe I should have said this first, if you take phi 1 phi 2 in End G what do we do? Phi 1 plus phi 2 must be another element of End G right; that means, it must be a homomorphism from G to G. And what is that? I will simply define phi 1 plus phi 2 of x, I will simply add End G so, phi 1 plus phi 2 of x will be phi 1 x plus phi 2 x. So, this is the addition in End G. What is multiplication? Multiplication is simply composition, composition of two functions because phi 1 phi 2 are both functions from G to G right.

Phi 1 is from G to G, phi 2 is also from G to G; these are actually group homomorphisms. I define phi 1 phi 2 of x to be phi 1 of phi 2 of x, this is the multiplication in End G right. So, in order to show that end G is a ring we need to say what is addition, what is multiplication.

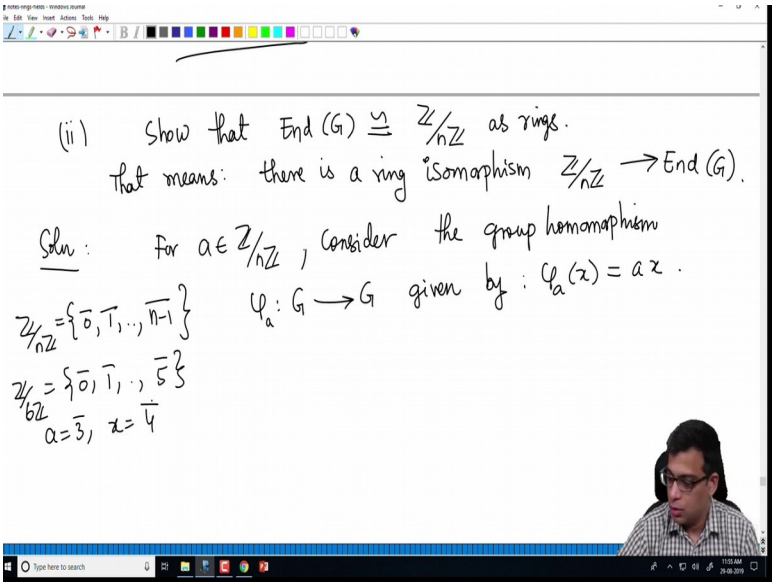
Addition is defined here by adding in the target group, multiplication is defined to be composition. So, what I will leave for you to check is with these operations End G is actually a ring. In fact, it is a commutative ring in we remember all our rings are supposed to be commutative with unity. We know that it has a unity because, remember 1 is define to be the identity map.

So, when you multiply any endomorphism with 1; that means, your composing any endomorphism with the identity map, you get that endomorphism back. So, 1 is the identity, it is actually commutative. So, this the tricky part, in general composition is not commutative right. You can compose two function f and g and in either f circle g or g

circle f in general there are different, but in this specific example its commutative. So, commutative is something you have to check, the other condition are fairly straight forward because if phi 1 and phi 2 are group homomorphisms, their sum is group homomorphism.

If phi 1 phi 2 are group homomorphism their composition is also group homomorphism, these are all group theoretic properties that one has to check. Phi 1 plus 0 is phi 1 phi 1 circle phi 2 is equal to phi 2 circle phi 1, that I told you to check phi 1 circle 1 is phi 1. And, you have to check distributive property, you have to check that under addition it is a multi it is a group that is clear because, phi 1 has an inverse right minus phi 1 phi, minus phi 1 sends x 2 minus phi x minus phi phi 1 of x. So, that is the additive inverse, not everything will have a multiplicative inverse, but that is not required for us.

(Refer Slide Time: 21:29)



So, this I will leave for you to check. So, check it is; so, even though this is the a video on problem. So, I will not do that because that is the fairly straight forward exercise. The second exercise is to show that now that by first exercise we know that End G is a ring, what kind of ring is it? We show that Z End G is isomorphic to Z mod n Z as rings; that means, there is a ring homomorphism, ring isomorphism from let me reverse the direction does not matter.

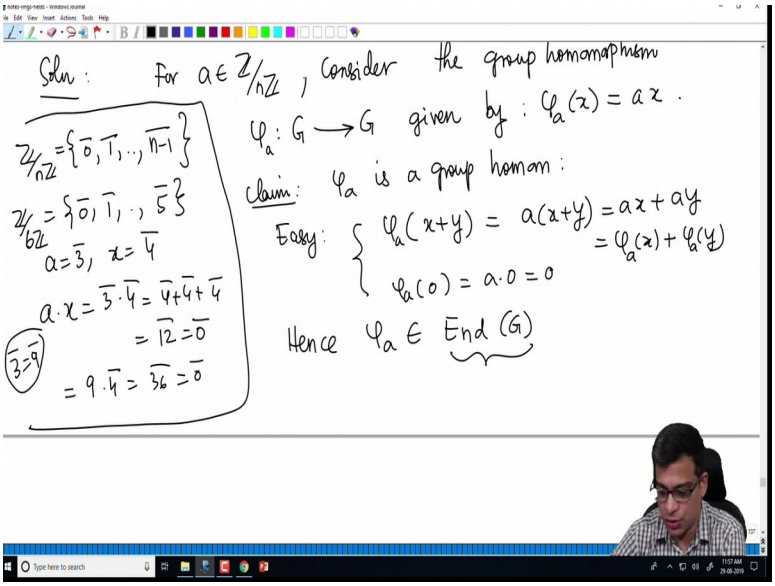
So, there is a ring isomorphism from Z mod n Z to End G. So that means, there takes so, this is the tricky part of this. What I have started with is Z mod n Z is considered as a

group only, not as a ring. I consider the set of all homomorphisms, all group homomorphisms from G to G, that actually inherits the ring structure and as a ring it is isomorphic to Z mod n Z; now Z mod n Z is being considered as a ring ok.

So, the you have to keep track of various notations here and Z mod n Z is appearing in several roles; first as a group, now as a ring. So, I am going to simply define an isomorphism and define a map and show that it is isomorphism. So, for a in Z mod n Z consider the map phi a which is from G to G, consider the group homomorphism I should write consider the group homomorphism from G to G determined by a.

What is this? So, this is given by phi a of x is ax. So, now, I need to let you what is ax, remember Z mod n Z one way of representing elements of Z mod n Z is this. So, we are implicitly using the multiplication in Z mod n Z right because though its actually group, but because its coming from integers multiplication is actually just addition. So, when I write for example, if you take Z mod 6 Z it will be 0 bar 1 bar to 5 bar, let us a is 3 bar and x is 4 bar.

(Refer Slide Time: 24:19)



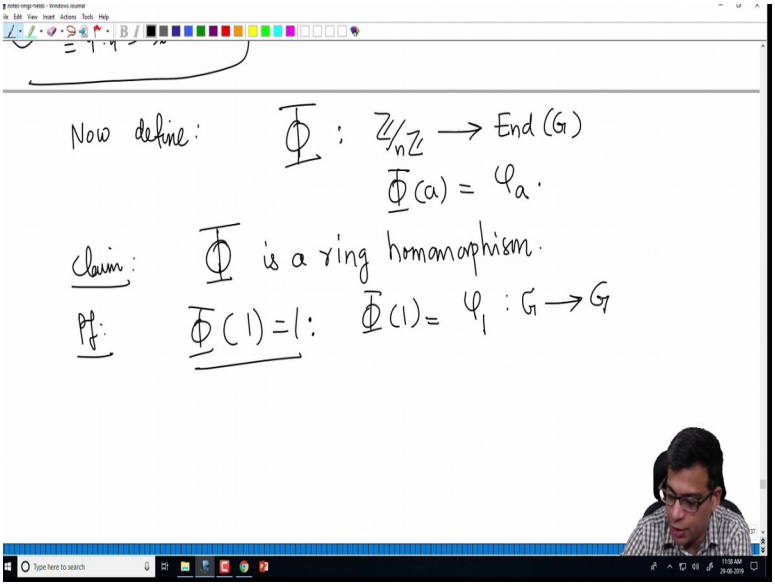
What is a times x? It is 3 bar times 4 bar which is really 4 bar plus 4 bar plus 4 bar because, 3 bar serves as the number 3 in this ring. So, multiplying by 3 means it is adding 4 bar 3 times to itself this is 12 bar which is actually 0 bar. So, this is an example. So, we can always make sense of a times x is really x plus x plus x a times, where a is an element of G. So, it is not an integer, but it has a representative in the ring of integers. Now,

if you take another representative a x does not change for example, here you can take 3 bar, but 3 bar is also 9 bar right.

So, a 3 bar is equal to 9 bar. So, I can also do 9 times 4 bar which is 36 bar which is 0 bar. So, because we are going modulo n at the end what integer I choose to represent here is irrelevant, I can choose any integer that represents here and multiply by that. So, I claim that in fact, I wrote this here, but one has to check that it is in fact, a group homomorphism. Claim phi a is a group homomorphism, this is very easy to check because this is easy phi a of x plus y is a times x plus y which is a x plus a y which is of course, phi a of x plus phi a of y. Similarly, phi a of 0 is a time 0 which is 0.

So, these are this is why it is a group homomorphism; that means, phi a is in End G, remember what is our notation for End G. These are group homomorphisms from G to G. So, phi a is one such so, it is a End G.

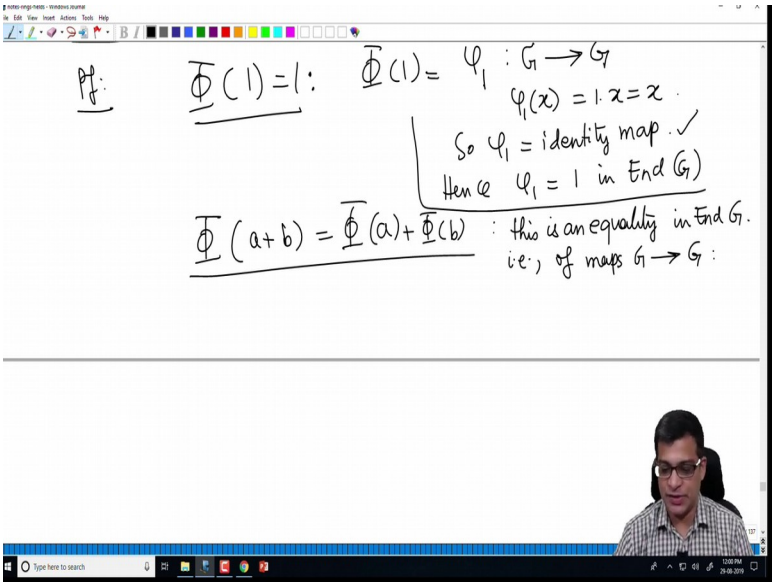
(Refer Slide Time: 26:19)



Now, define the map capital phi from Z mod n Z to End G, remember in the previous slide we started with an arbitrary element a and defined endomorphism phi sub a. Now, I am defining capital phi by defining capital phi of a is simply phi a. We have already checked in the previous slide that phi a lands in End G. So, capital phi of a is small phi sub a. So now, we claim that capital phi is a ring homomorphism.

So now, we are in the realm of rings and ring homomorphisms. So, we want to now show that it is a ring homomorphism, small phi a is a group homomorphism right. Now, capital phi is a ring homomorphism. So, in particular we want to now show that phi of 1 is 1. Why is this? What is phi of 1? So, I am proving this now phi of 1 is phi small phi sub 1. And what is small phi sub 1? It is a ring homomorphism from G to G. And what does it do?.

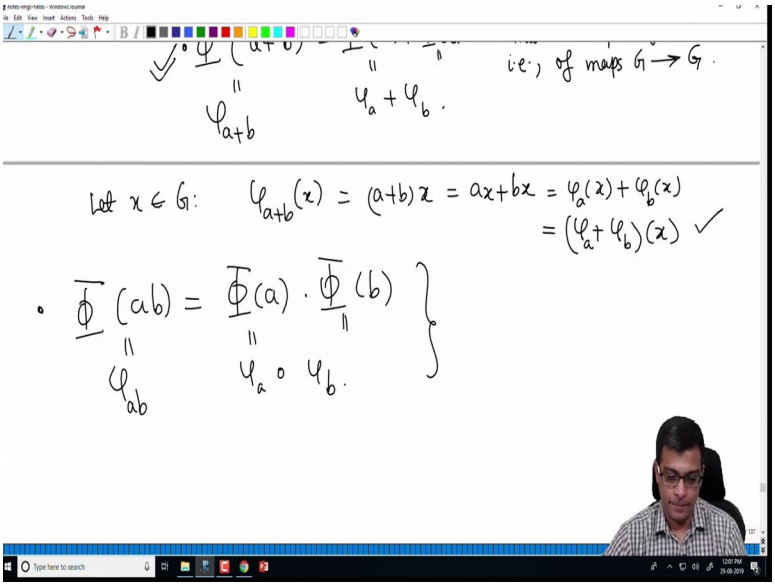
(Refer Slide Time: 27:45)



Phi sub 1 of x is 1 times x which is x right; that means, phi sub 1 is the identity map. Hence, phi sub 1 is the identity element in End G as required. So, capital phi of 1 is equal to 1, when I write 1 in the bracket here represents 1 in Z mod n Z; on the right hand side 1 represents the identity endomorphism so, we check that. What is phi of let us take phi sub a sorry phi of a plus b should equal phi of a; so, that is done, the first part is done.

The next part is to show the additive homomorphism structure, capital phi of a plus b is capital phi a plus capital phi b. What is this? So, let us check both of these sides, this is an equality of what? This is an equality in End G right; that means, this is an equality of maps of that is of maps right. So, we are supposed to check that these are same maps on G so, let us take an x.

(Refer Slide Time: 29:09)

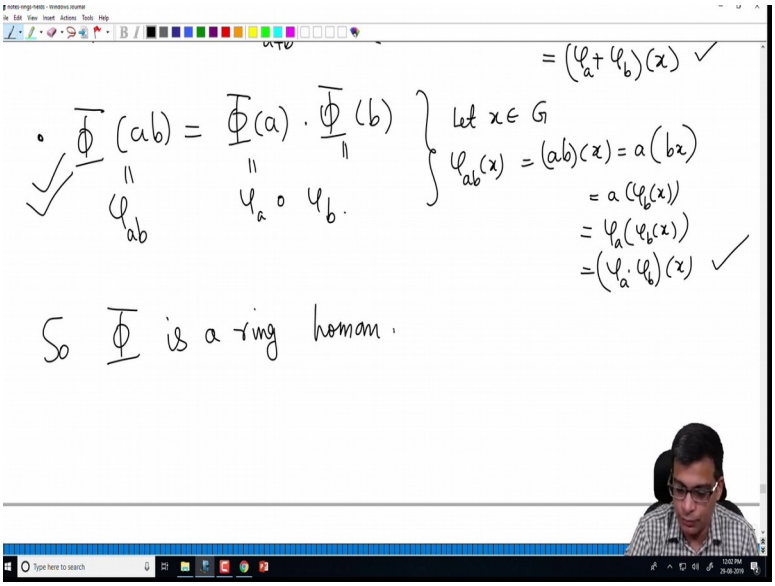


So, of course, before that let me first note that what is phi of a plus b by definition it is small phi sub a plus b. So now, and this is small phi sub a and this is small phi sub b. So, we want to check that small phi sub a plus b is equal to small phi sub a plus small phi sub b. So, let us take an arbitrary element of G and compute both sides. What is a phi of phi sub a plus b of x? This is a plus b times x, this is ax because remember a is really being thought of as an integer but, ax plus bx is actually phi of ax phi of bx.

This by the definition of addition an End G, this is actually phi sub a plus plus phi sub b of x because, when you come add to endomorphisms you just add it in the take the image and add. So, this is what we require; so, this is checked. Now finally, we have to check that phi of a b is equal to phi of a times phi of b. So, what is this? This is phi of a's small phi sub a b, this is small phi sub a, this is small phi sub b.

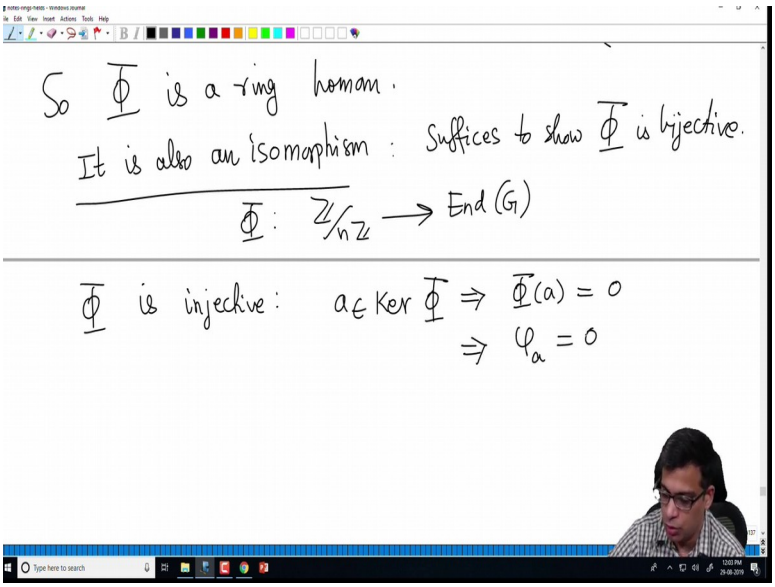
And what is a product in End G? This is actually composition, we want to check this. So, the third condition is this, I will write it as maybe I will just put a dot here, second condition is this, first condition is this. So, let us check now so, this is also an equality of maps of G to G.

(Refer Slide Time: 30:53)



So, let us take an arbitrary element x in G. What is phi ab of x? This is a b times x by definition, this is a times b of x because of the associativity of multiplication. But, this is a times phi b of x which is phi a phi b of x which is by definition phi a composed with phi b of x as required right. So, this is exactly the required equality; so, on every x they agree so, this also. So, capital phi is an ring isomorphism ok, that is good sorry ring homomorphism not yet a ring isomorphism. Now, the remaining thing is to check that it is in fact, a ring homomorphism.

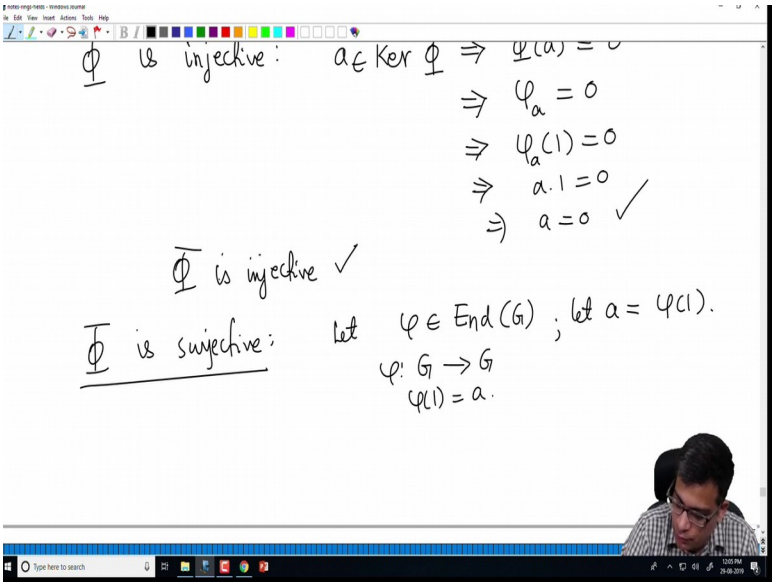
(Refer Slide Time: 31:49)



It is also an isomorphism. How do you verify that a given ring homomorphism is an isomorphism? All we need to show is that it is bijective, capital phi is bijective, but this is easy because it is also a ring homomorphism, already a ring homomorphism. We will first check that it is injective. So, capital phi is injective. Why? What is kernel?.

Suppose a belongs to remember capital phi again let me remind you is a map from Z mod n Z to End G, suppose a belongs to kernel of phi. So, to prove that a ring homomorphism is injective, it suffices to show that kernel of that ring homomorphism is 0. So, if a belongs to kernel of capital phi; that means, capital phi a is 0; that means, phis of a is 0, as an idea is a map of from G to G.

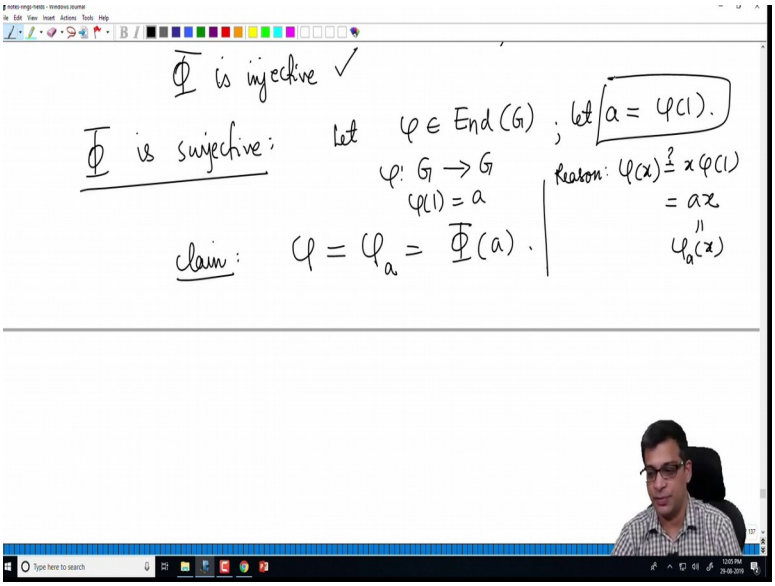
(Refer Slide Time: 32:53)



So, phi sub a of 1 is 0; that means, a times 1 is 0; that means, a is 0. So, phi is injective, now phi is an injective map from so, phi is injective from sorry. So, what is it? Phi is injective that we have shown. Now what is it that we have to show now? Phi is surjective, we are trying to show that it is bijective; so, we have shown its injective. So, we have to show its by surjective.

So, for this part let us take an arbitrary endomorphism of the group G, this is a group homomorphism from G to G. Then we claim I will not prove this. So, suppose so, before I write the claim; so, let a be phi of 1; remember phi is the phi is a group homomorphism from G to G. So, I am simply taking phi of 1 to be a; so, let us take a to be 1. The point is a now determines the entire group homomorphism phi.

(Refer Slide Time: 34:11)



So, the claim is phi is actually equal to phi sub a which is capital phi of a. Because why? The reason is phi of x is actually a times phi 1, sorry x times phi 1 which is a x, but this is also same as phi a of x ok. So, the whole point is show that phi of x is x times phi 1 and that is because, x can be written as 1 plus 1 plus 1 x times. So, because phi is a group homomorphism, phi of x is phi of 1 plus 1 plus 1 the and you can now do phi of 1 plus phi of 1 plus phi of 1 x times which is exactly this. So, this part if it is not clear just think about it for a few minutes and it will become clear to you.

So, this shows that phi is a surjective map, it is an injective map and it is a homomorphism as we verified here. So, the conclusion is these are isomorphic as a rings. So, this is a very nice problem because, it now combines everything that you know about groups and rings and it allows you to see everything in its proper place. So, if you carefully follow this video and understand this problem solution, it will be useful to you in understanding ring theory. I am going to stop this video here; in the next video we will do some more problems.

Thank you.