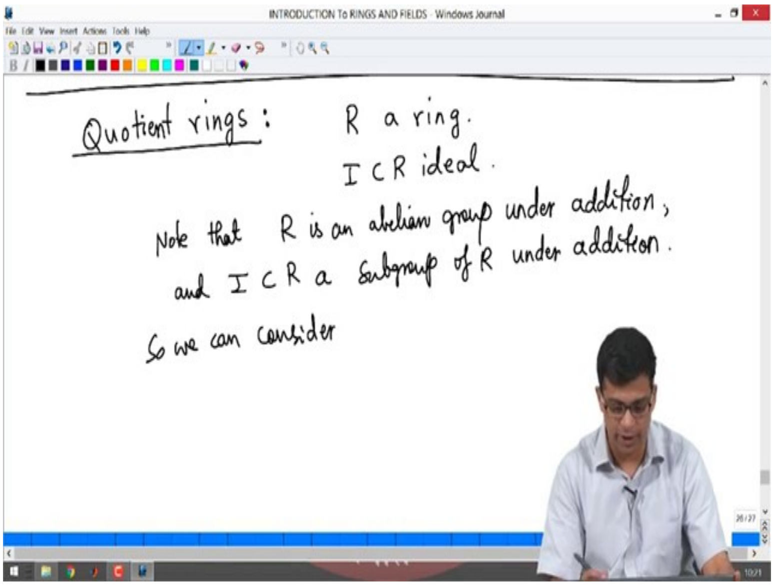
Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 11
Quotient rings

So, let us continue now. So, in the last few videos we have done some examples and exercises, hopefully which gave you some idea of how to work with rings. So, in this video I am going to start with a very important operation in ring theory called quotienting.

(Refer Slide Time: 00:29)



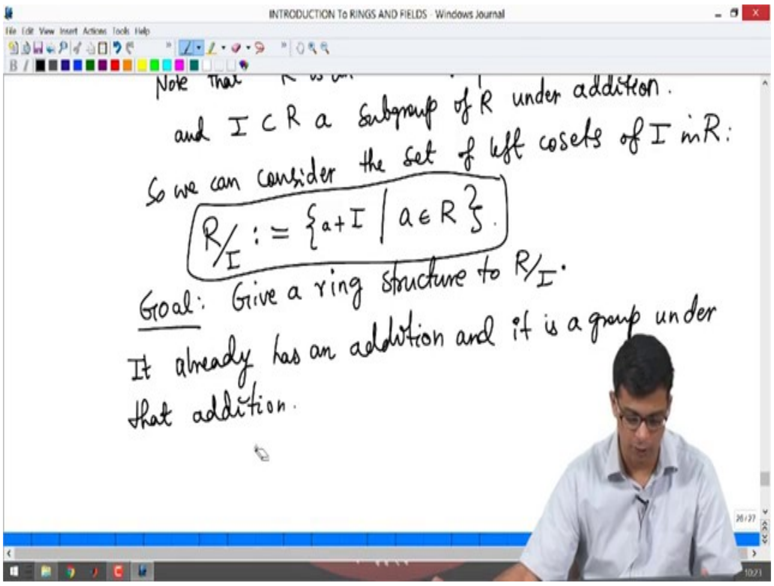
So, I want to introduce to you what are quotient rings. So, this is very similar to the notion of quotient groups that you have studied in group theory course. So, what are quotient rings? So, here I take a ring R so, before I start this let me give you a quick recap of how do we define quotient groups. So, here in the case of groups we have a group G and we want a normal subgroup H and, then we want to give a group structure to the set of left cosets of H in G and that was called G mod H and in order to give a group structure to that we needed H to be normal.

But, here we do the same, we will first consider the additive group R. If R is a ring remember under addition it is an abelian group because it is abelian we do not need to specifically now ask for normal subgroups because every subgroup is normal. So now, we want to consider subgroups of the additive group of R and take the quotient group.

But in order to give a ring structure to the quotient we need additional properties on the, on that subgroup we started with and that simply happens to be the ideals. So, all we need is an ideal.

So, ideal will do the job for us. So, I is an ideal. So, the set R mod I will be exactly what you are used to in the case of groups. So, consider R mod I ok. So, let me write first, note that R is an abelian group under addition and I, I is more than a subgroup, but it is certainly a subgroup under addition ok, it is a subgroup under addition. So, we can consider basically just forgetting the multiplication on R and the additional property of an ideal we forget for the moment or we do not need that for the moment.

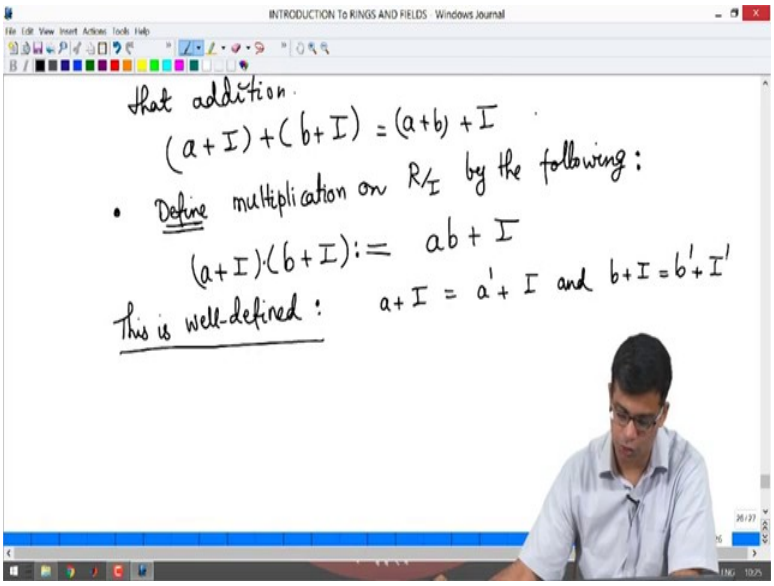
(Refer Slide Time: 02:59)



We can consider the set of cosets and I will write left cosets of I in R. So, we will denote this as usual by R mod I. So, these are left cosets so, these are things of the form aI, a in R. So, my goal is to make this ring. Our goal make or let me write give a ring structure to give ring structure to R mod I that is my goal; what it already has. What it already has is, it already has an addition and it is a group under that; till this point it is nothing new, this is exactly group theory.

R is a group under addition, abelian group under addition, I is a subgroup. So, R mod I the set of left corsets is a group. So, let me recall what is the operation here. So, the operation of addition is aI, sorry. So, actually I wrote something wrong here. Yes, I take that back. So, go back to this, it is not aI right. I am not taking a cosets under multiplication I am taking cosets under addition so, a plus I. So, as I told you when I define R mod I do not look at multiplication, I do not need or I do not refer to multiplication of I.

(Refer Slide Time: 04:55)

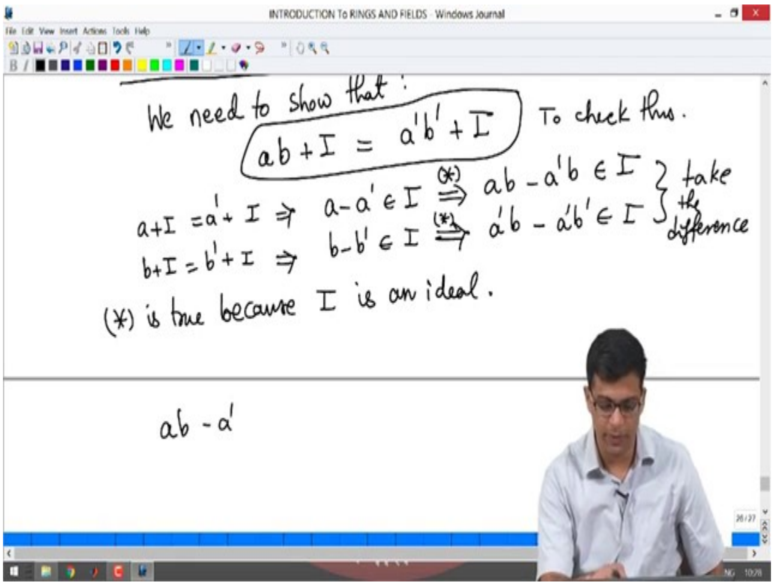


So, how do I add two cosets? It is simply a plus I plus b plus I is a plus b plus I. So, under this, I R mod I is a group. What now I want to do is give define multiplication so, this is a group. So, define multiplication by the following. What is that? I take a plus I and I take b plus I ok, now this is there is one natural thing to do here. I take one coset a plus I, another coset b plus I and I define it to be a b plus I.

So, this is natural to do still we have to check various things, we have to check first of all that it is well defined. So, this is my definition. This is well defined, we need to check that. Why? I need to check that this is well-defined because a plus I is a coset remember, I can take one representative you can take another representative. So, it looks like a if I take a as a representative, you take a prime as a representative, you do a b, I do a b, you do a prime b. But, a b and a prime b should give you the same coset otherwise this is not well defined.

So, what do I have to do? So, to check well-defined, I have to do the following. Suppose a plus I is same as a plus a prime plus I and b plus I is same as b prime plus I prime. So, what do I have to show?

(Refer Slide Time: 06:53)



We need to show this is the usual thing that one has to deal with when one works with cosets right. Because, a coset can have several representatives and there is no unique choice, right; whatever we define operation that we define we need to ensure that the choice of the representative plays no role. So, in other words we need to show that a b plus I is equal to a prime plus b prime a prime b prime plus I.

If I show this then I would have checked well-defined as because, because no matter what I choose, a plus I or a plus I or a prime I plus I or b plus I or b prime plus I, I would get the same result.

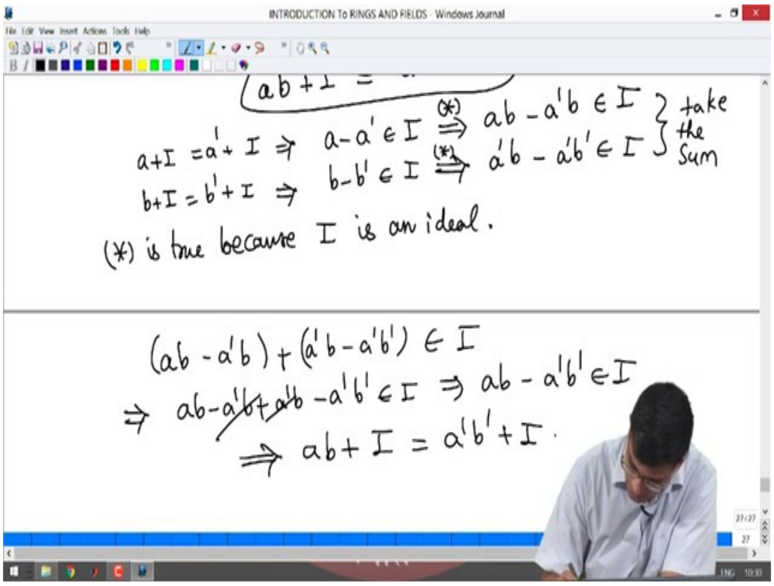
So, how do I check this? So, we want to check this, this is exactly the well-definedness. Now, let us use the fact that a plus I is a prime plus I prime I, this means a minus a prime is in I. This is a property of left cosets, right? Left cosets have this property that if two elements of the group have this are in the same coset; that means, their difference is in that subgroup. Similarly, b plus I is equal to b prime plus I implies b minus b prime is in I ok. So, now what I will do is I will multiply this with let us see, I will multiply this with b.

I claim that a b minus a prime b is in I. Why is this implication true? This implication is true so, let us say star, star is true because here is where we will introduce the, we will need the additional property of an ideal. It is not merely a subgroup right, it has a property that you take an element of I, multiply by any ring element, it lands again in I, that property is used here; a minus a prime is in I, b is an arbitrary ring element I multiply by that so, a b minus a prime b is in I.

Similarly, I multiply the second one by this is also because of star, by a. I multiply this by a. So, a b minus a b prime is in I. So, what I have is a b minus a prime b is in I, a b minus a b prime is in I. So now, take the difference, I is an ideal. So, if two things are in the ideal their differences in the ideal.

So, a b minus a prime b sorry so something is wrong here. So, actually I will do a prime times this. So, b minus b prime is in I, a prime is a ring element, I multiply by a prime it is also in the ring; it is in the ideal. So, a prime b minus a prime b prime is in I.

(Refer Slide Time: 10:27)

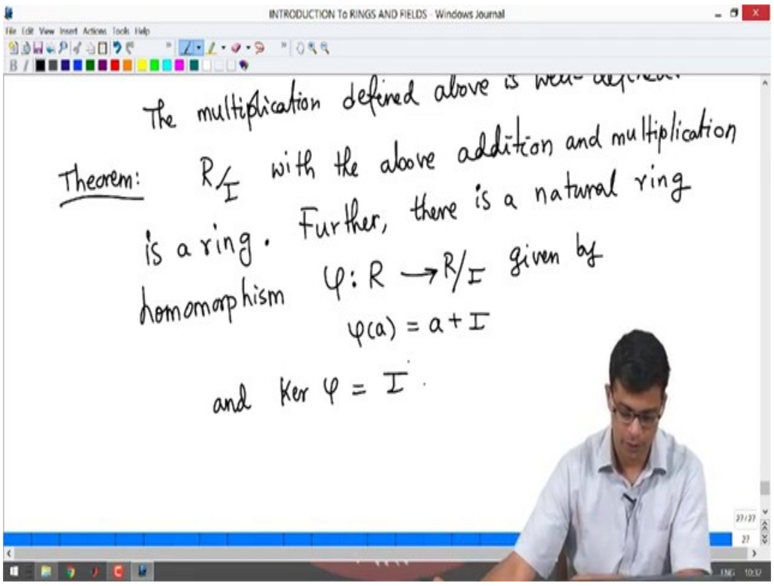


So, now I take the difference. So, I get a b minus a prime b minus a prime b minus a prime b prime is in I. Because individually they are in I, their differences is in I but this means a b minus a prime b minus a prime b plus a prime b prime is in I. So, of course, I cancel this now. So, yeah, I am sorry actually I take the sum, I got confused. So, I take the sum, not the difference so, I take the sum. So, I put plus here so, again two things are in I their sum is also in I right. So, I can take a b minus a prime b plus a prime b minus a prime b prime.

So, now I cancel a prime b a prime b this is in I; that means, a b minus a prime b prime is in I. This tells me that a b I plus I is equal to a prime b prime plus I ok, that is what I needed to prove; a b plus I is equal to a prime b prime plus I.

Two cosets are equal; a plus I is equal to b plus I remember if and only if a minus b is in I that is what we have using all the time. In order to show a b plus I is equal to a prime b prime plus I; I need to show that a b minus a prime b prime is in I which is what I have shown here ok.

(Refer Slide Time: 11:59)



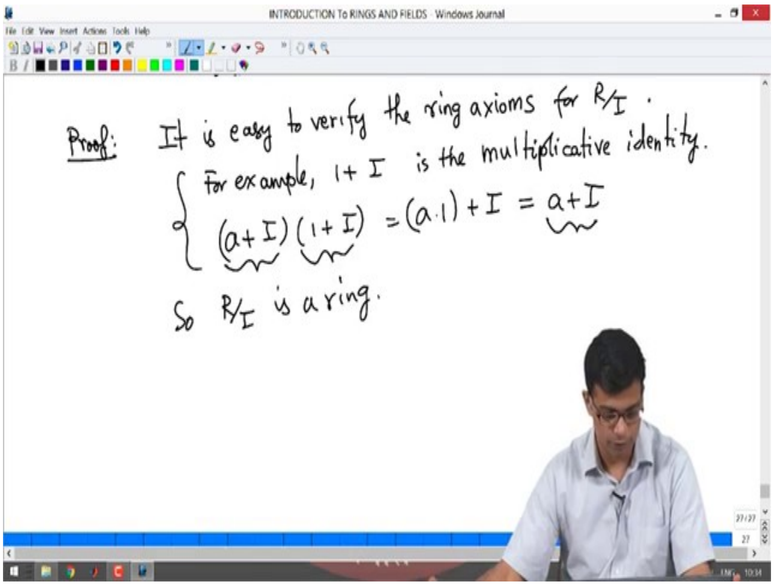
So, the multiplication defined above is well-defined because I do not need to worry about which representative I pick. You pick a representative, I pick a representative and our when we you multiply your representatives I multiply my representatives, we get the same answer. So, multiplication above is well defined.

So, now the theorem is: R mod I with the above addition. So, I will write the full statement of the theorem here and we will give a sketch of the proof with the addition and multiplication defined above; with the addition and multiplication is a ring, that is the first point.

So, we have addition that makes it in abelian group, I just defined a multiplication which I said is well-defined and it makes it a ring. Further there is a natural ring homomorphism phi from R to R mod I, given by phi of a is equal to a plus I and there is a natural homomorphism like this, in other words I am saying this homomorphism and kernel phi is precisely I. This is a fundamental theorem in ring theory because in order to study rings we need to construct quotient rings and quotient rings are connected to the original rings via this theorem.

So, R mod I is a ring to begin with and whenever you think of a quotient ring you have to also think of this natural ring homomorphism from the ring to the quotient ring and the that ring homomorphism has the property that its kernel is I.

(Refer Slide Time: 14:15)

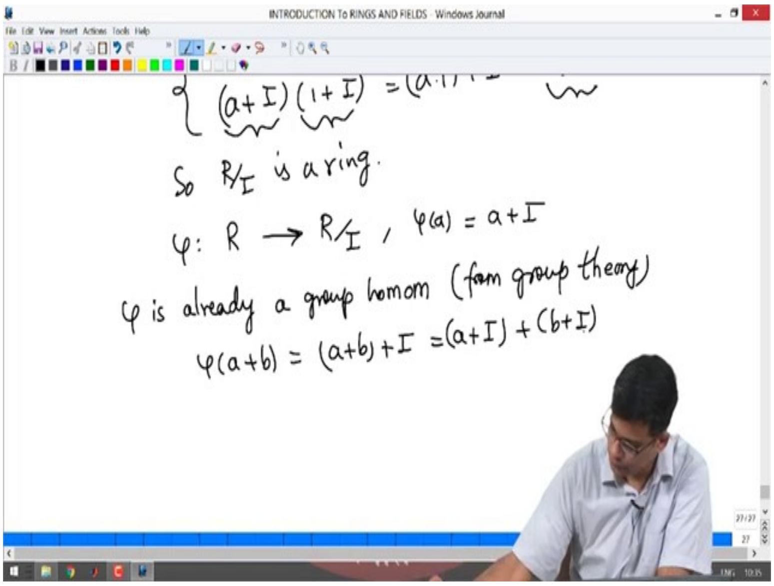


So, I am going to give you a proof, but not of the fact that R mod I is a ring ok. So, that is a fairly simple check. It is easy to verify the ring axioms for R mod I. So, in other words multiplication is commutative, multiplication and addition are distributive. See we do not need to worry about anything about addition right because R mod I is already an abelian group under addition that comes just from group theory. All we need to do is the new data which is multiplication satisfies the ring axioms, which I will leave for you for example, what is the, I will only mention this.

What is the ring multiplicative identity for the ring R mod I? It is simply 1 plus I; 1 plus I is the multiplicative identity. This is actually easy to check because a plus I is an arbitrary quotient ring element. If you multiply by 1 plus I by the definition of multiplication I gave it is a plus a times 1 plus I which is a plus I.

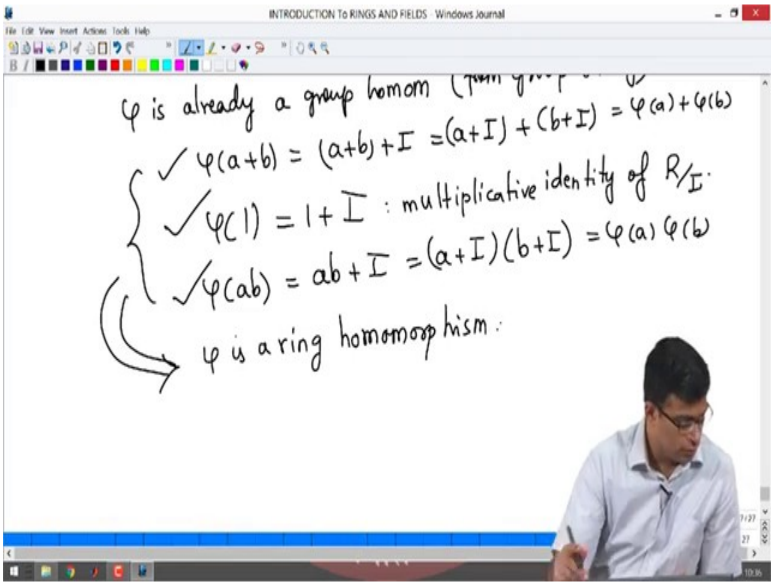
So, you multiply something with 1 plus I you get that back. So, 1 plus I is the multiplicative identity, the other things are fairly easy to check. So, R mod I is ring; so, I will not prove this ok. The first part of the theorem I will not prove, that it is a ring.

(Refer Slide Time: 16:05)



On the other hand let us prove that we have already given a map R to R mod I, phi of a is a plus I, this is also easy to check. Why is it; why is it a ring homomorphism? So, what we need to check? Phi is already a group homomorphism. This is from group theory right, because, R mod I is constructed as the left additive cosets of I. So, it is a group and this is a group homomorphism which anyway by you can check directly phi of a plus b is a plus b plus I by definition of phi which is a plus I plus b plus I which is phi a plus phi b.

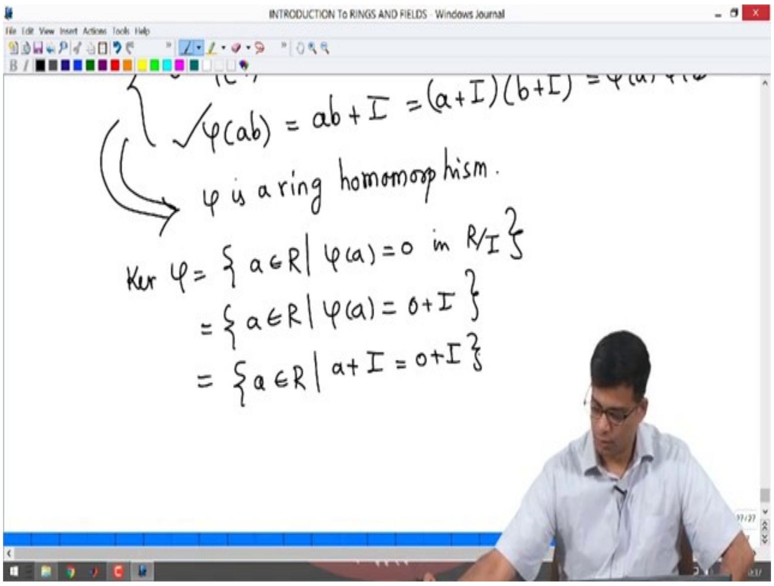
(Refer Slide Time: 16:59)



What is phi of 1? Remember phi of 1 must be 1, but phi of 1 is 1 plus I which is the multiplicative identity. The second property of a ring homomorphism is that the identity element of the domain ring has to go to the identity element of the codomain ring. Here R is the domain ring, R mod I is the codomain ring, 1 is the ring identity element of R, 1 plus I is the identity element of R mod I. So, 1 goes to 1 plus I by definition so, that is fine.

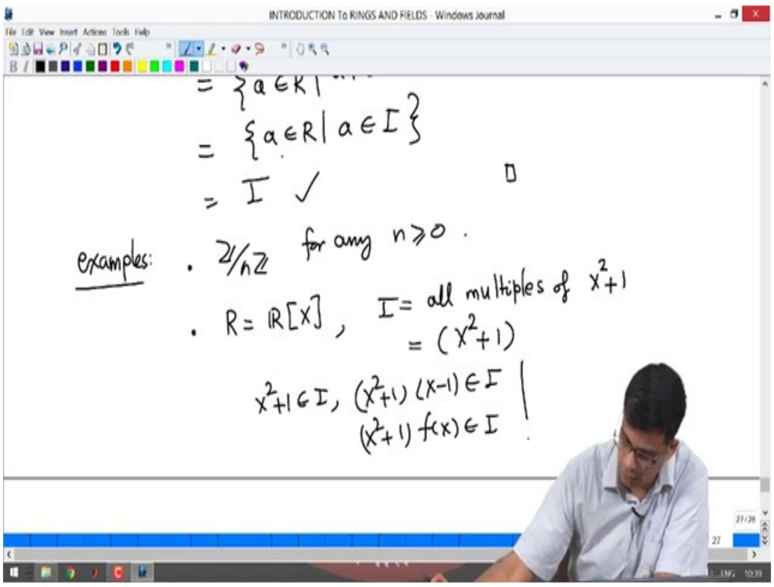
Finally what is phi of a b? Phi of a b is by definition a b plus I by definition of the map, phi is a b plus I. But, by definition of the multiplication in R mod I a b plus I is same as a plus I times b plus I which is same as phi a phi b. So, phi is a ring homomorphism, all these properties imply that phi is a ring homomorphism. So, now the last thing, what is the last thing in the theorem? Kernel of phi is identity.

(Refer Slide Time: 18:25)



So, what is kernel of phi; is all elements a in R such that phi a is 0, in R mod I right because, phi is a (Refer Time: 18:36) from R mod I. But this is same as a in R phi a is equal to what is the zero element in R mod I? Zero element is additive identity right, R mod I has additive identity 0 plus I right phi a is equal to 0 plus I. But what is phi a? So, this is a in R such that a plus I, because a plus I is equal to phi of a by definition is 0 plus I.

(Refer Slide Time: 19:07)

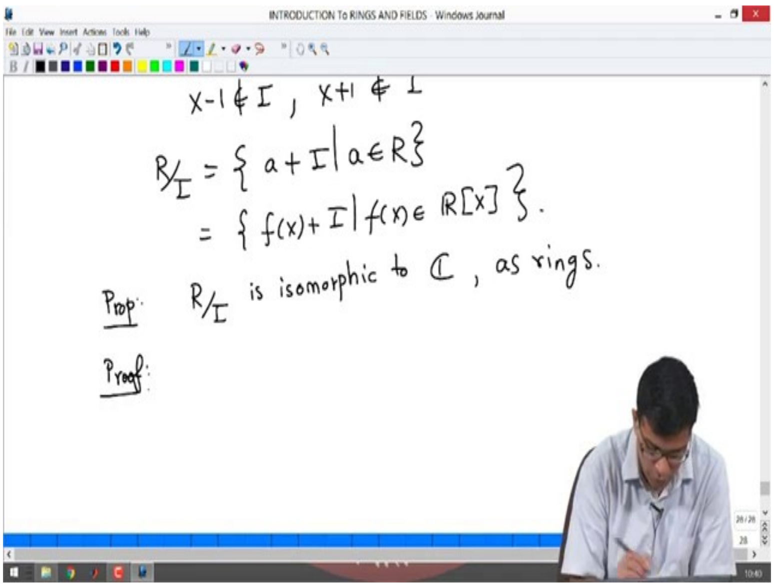


So, in other words this is a in R such that a plus I is equal to 0 plus I. When are two cosets equal? I mentioned this earlier, if the difference of these two elements is in I; that means, a is in I a minus 0 is in I so, a is in I. What are elements in R such that a is in I? This is precisely I. So, kernel of phi is equal to I. This is the last point of the proof. So, the proof is finished. So, quotient rings are very important for us. Quotient rings come equipped with a natural ring homomorphism from R to R mod I, whose kernel is I.

So, now let me do some examples to work with this. The first example is something you have already seen, you can take Z mod nZ for any n right; because nZ is an ideal Z mod nZ, this we are already familiar with ok. So, let us look at something more, something different and this will also anticipate something that I want to do next. Let us take R to be the polynomial ring in one variable. So, let us take R to be the polynomial in one variable and the ideal I to be all multiples of the polynomial x squared plus 1. So, this is denoted by x squared plus 1 around round brackets.

For example x squared plus 1 is in I, x squared plus 1 times x minus 1 is in I, x squared plus 1 times any polynomial in general is in I.

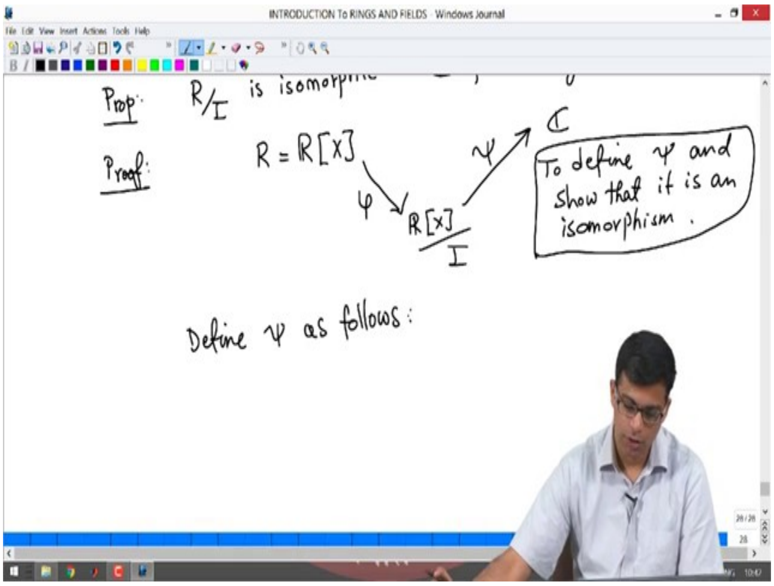
(Refer Slide Time: 20:57)



But what are not in I? x minus 1 is not in I right because x minus 1 cannot be written as a multiple of x squared plus 1 just for degree reasons. Similarly x plus 1 is not in I. So, these are elements which are multiples of x squared plus 1. So, R mod I to is by definition elements of R plus I, in our case R is the polynomial ring. So, I will write this as f x plus I, where f x is in the polynomial ring.

So, what I want to do is prove that this is familiar to you, this ring is familiar to you; in the process of proving this you will understand more about quotient rings. So, I will prove a proposition R mod I that I wrote here is isomorphic to the ring of complex numbers or the field of complex numbers, as rings or as fields it does not matter. So, R mod I is isomorphic to C. So, in other words I want to produce a ring isomorphism from R mod I to C.

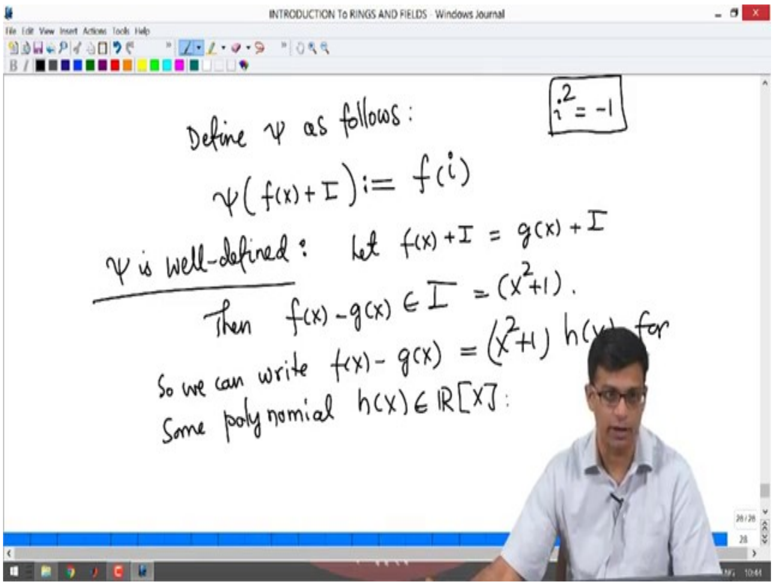
(Refer Slide Time: 22:27)



What I will do is the following. So, this is the picture. We have R so, this is useful to keep in mind. So, remember R is R x, the standard or the natural map we have from R x to I, right. So, there is always a natural map that I defined by phi. So now, I want to define a map to C that is why I call it psi. So, I want to define psi and show that it is an isomorphism is my goal. So, I want to define psi and make it an isomorphism.

So, what I will do? So, what I will do is choose, define psi like this, as follows. So, take an element of R x mod I. What is an element of R x mod I?

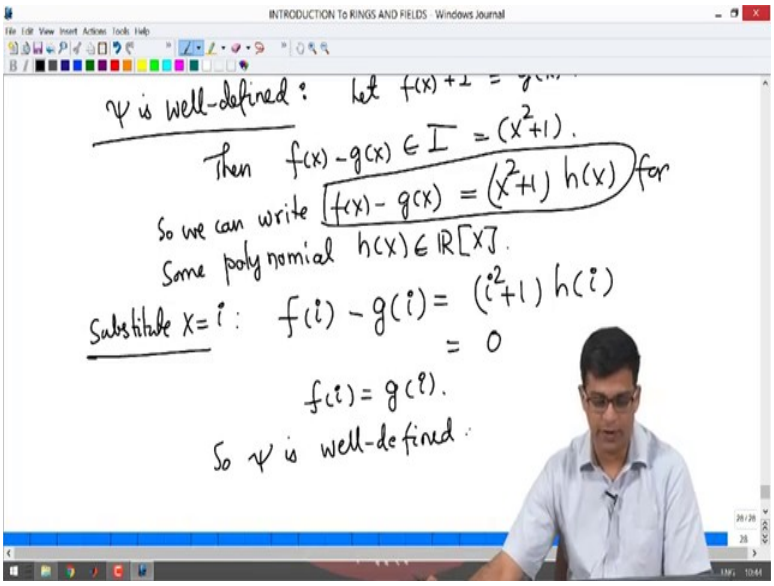
(Refer Slide Time: 23:37)



It is an element of the form f x plus I. So, psi of f x plus I, I define it to be f of i, where i is, of course, a square root of minus 1. So, remember again I am taking an element in the quotient ring, I am just evaluating the corresponding polynomial at x equal to i. So, again the question is, is it even well defined, is psi well defined? That must be proved right because for this coset f x plus I may be you choose g x as your representative and then you are image will be g of i, I choose f x my image will be f of i. So, f of i and g of i should be equal to each other for this to be well defined.

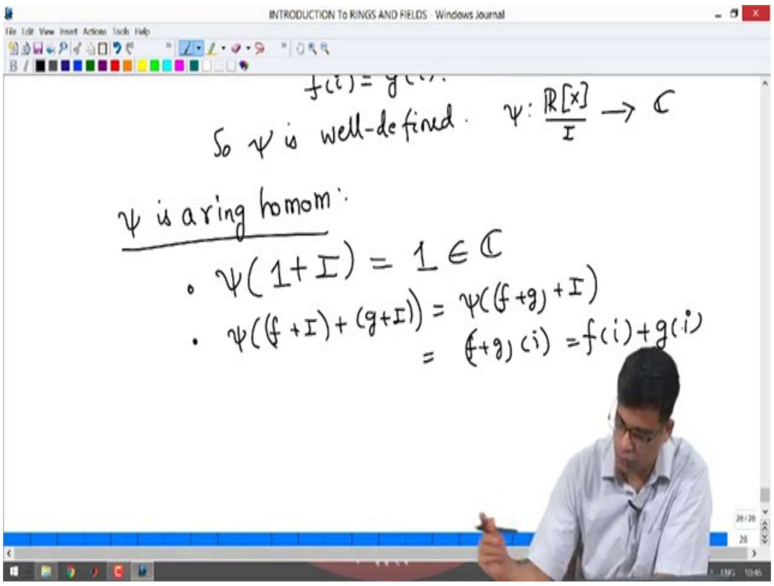
So, what we need to show is, let f x I be equal to g x I right; that means, f x minus g x is in I; by definition of equality of cosets if two cosets are equal their difference of f and g is in I. But what is I? I is x squared plus 1. So, we can write f x minus g x is equal to x squared plus 1 times h x for some polynomial h x in R x. See all this is happening now in R x not R x mod I. So, everything here is from this point onwards is happening in R x. Now, let us look at this equation here and substitute x equal to i.

(Refer Slide Time: 25:43)



So, what do I get? I get f of i minus g of i is equal to i squared plus 1 times h of i. But what is i squared plus 1? i squared plus 1 is minus 1. So, minus 1 plus 1 is 0, this is 0. It does not matter what h of i is. So, f of i minus g of i is 0. So, f of i equals g of i. So, this proves that psi is well-defined.

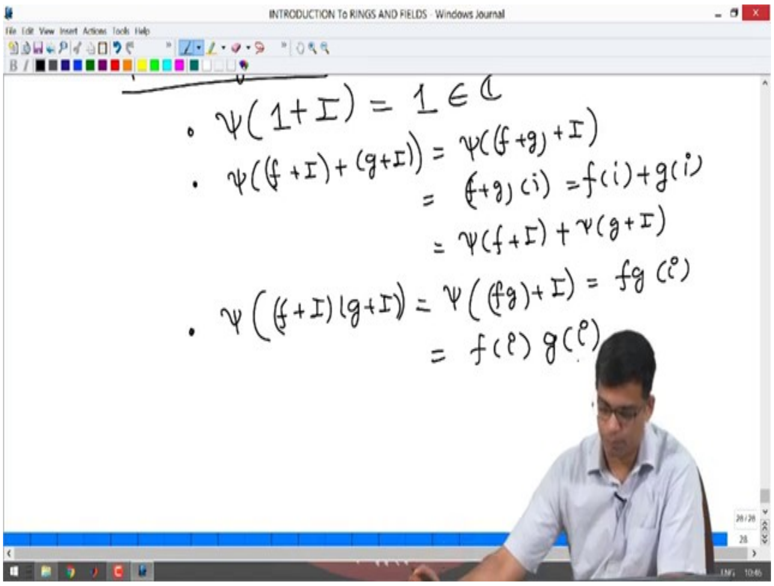
(Refer Slide Time: 26:27)



So, we have a well-defined map at least from R x mod I to C. So, now next step is to show phi is ring homomorphism. This is actually very easy because psi of, what is 1 plus I? Remember identity element of R x mod I is 1 plus I. And, what is psi of that? It is the polynomial 1 evaluated at I which is 1. So, psi of 1 is 1, remember psi of f x plus I is f of i. So, if f x is constant it is just that constant; 1 plus I goes to 1.

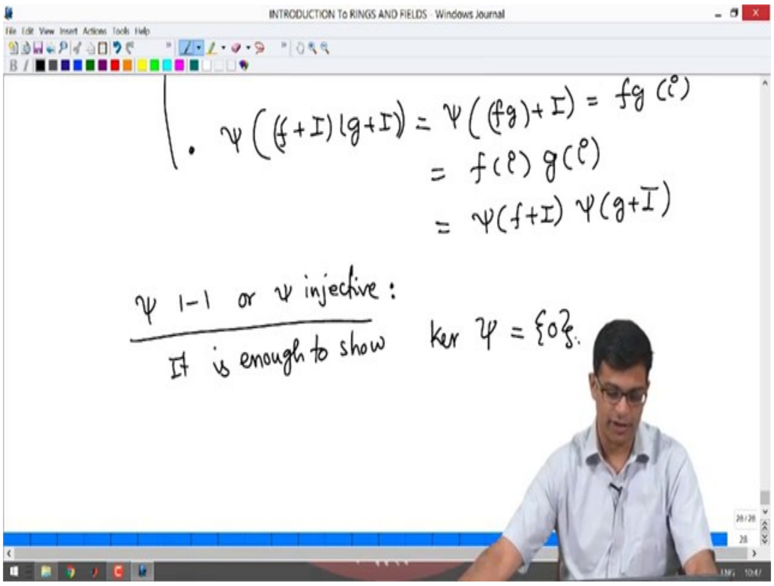
What is psi of f plus I plus g plus I? This is psi of f plus g plus I by definition of addition in R mod I, this is f plus g of i. So, this is f of i plus g of i, again usual polynomial properties.

(Refer Slide Time: 27:43)



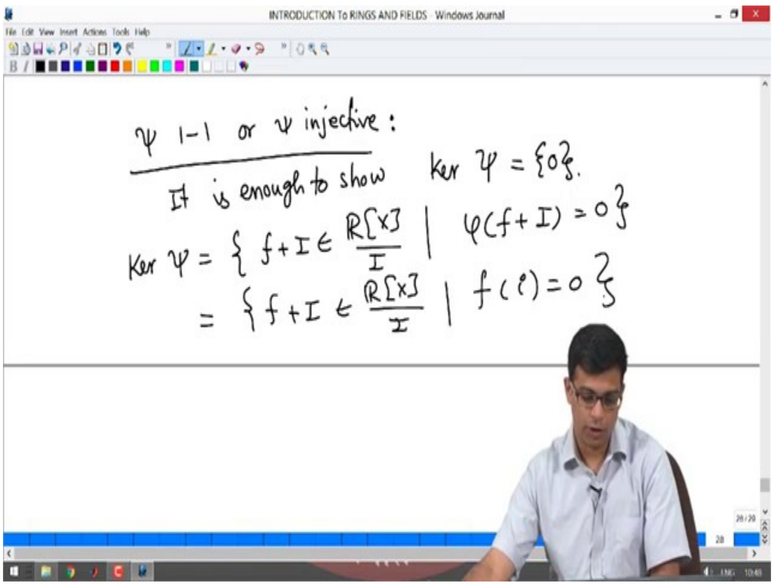
And, this is psi of f plus I plus psi of g of I; g plus I. And finally, psi of f plus I times g plus I is by definition of multiplication, psi of f g plus I which is f g of I by definition of psi which is f of i times g of i by definition of by properties of polynomial rings polynomials.

(Refer Slide Time: 28:11)



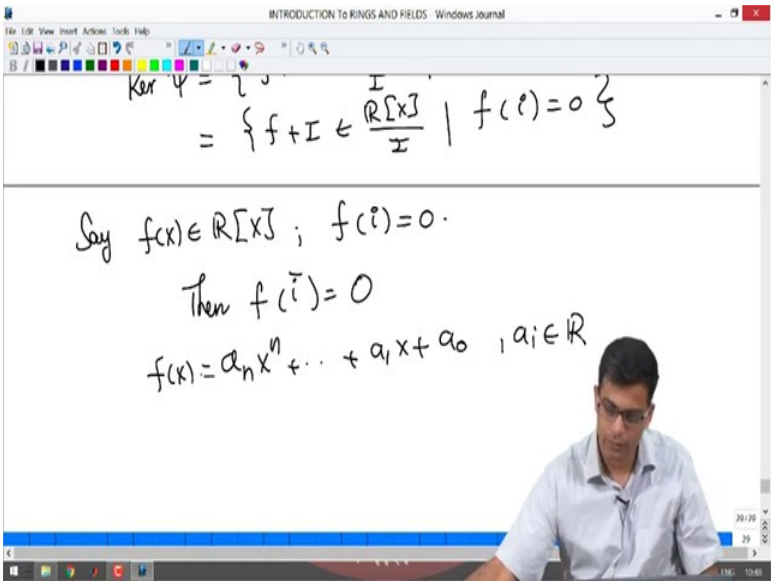
And this is psi of f plus I times psi of g plus I. So, these three properties imply that psi is a ring homomorphism and what is an isomorphism of rings? I told you this before; an isomorphism of rings is one which admits ring homomorphism which admits an inverse ring homomorphism or equivalently psi is 1-1 and onto. So, 1-1 means injective; we will show that it is injective and it is on to. So, it suffices to show it is enough to show kernel psi is 0, right. Because, remember in an earlier video I did a problem in which we said that a ring homomorphism is injective if and only if its kernel is 0.

(Refer Slide Time: 29:13)



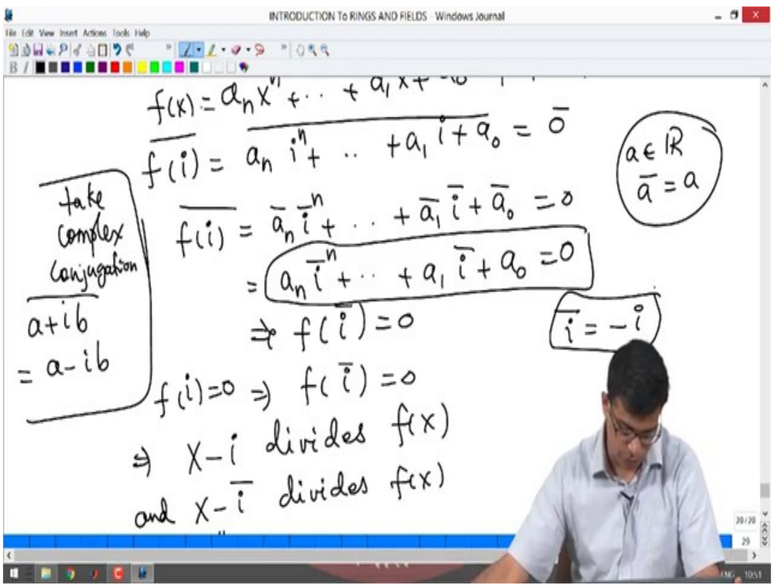
So, what is the kernel of psi; is all elements f plus I in R mod I in R x mod I such that phi of f plus I is 0. But that means, all elements f plus I in R x mod I such that f of i is 0.

(Refer Slide Time: 29:43)



If f of i is 0 so, now I will do some simple calculations. So, f is a polynomial over real numbers, f of i is 0, then I will quickly finish this, but you can do this easily. Then f of i bar which is actually minus i. So, I will write it here: say f x is in this f of i is this, then f of i bar which is also 0. See this is because f has real coefficients, see f is let us say a n x n plus a 1 x plus a 0 where, a i's are in R.

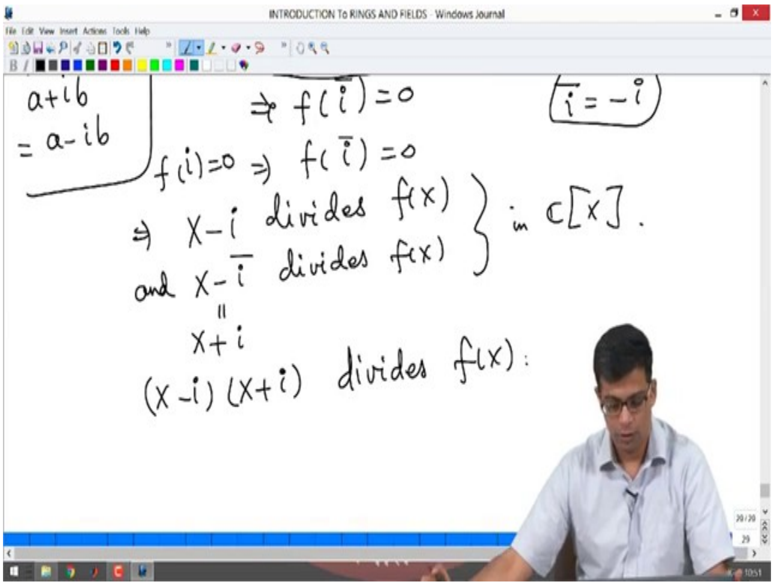
(Refer Slide Time: 30:27)



f of i is a n i power n dot dot dot a 1 i plus a 0 this is 0, but now take complex conjugation which is what bar is right, take that. So, f of i bar is this whole bar, but complex conjugation is also a ring property homomorphism. So, this is, but 0 bar is 0 right, but a n's are real numbers.

So, a n bar is just a n. So, a n i bar power n a 1 i bar plus a 0, is 0 because if a is a real number a bar is a. What is complex conjugation by the way? a plus i b is equal to a minus i b; conjugation of a plus i b is a minus i b. But this means right, because this if you look at this all we have done is that replaced x by i bar. So, f of i bar is 0. So, f of i is 0 implies f of i bar is 0.

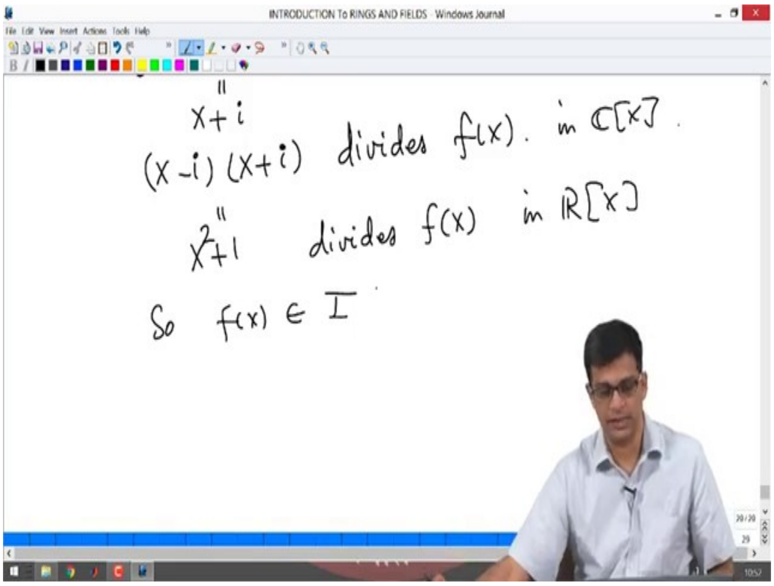
(Refer Slide Time: 31:53)



But that means, x minus i in an earlier video we showed that so, this f of i is 0, if i is f of i is 0 then x minus i divides f and if f of i bar is 0 then x minus i bar also divides f x, but x minus i bar is x plus i because i bar is minus i. So finally, what we have is that x minus i divides f x, x plus i divides f x.

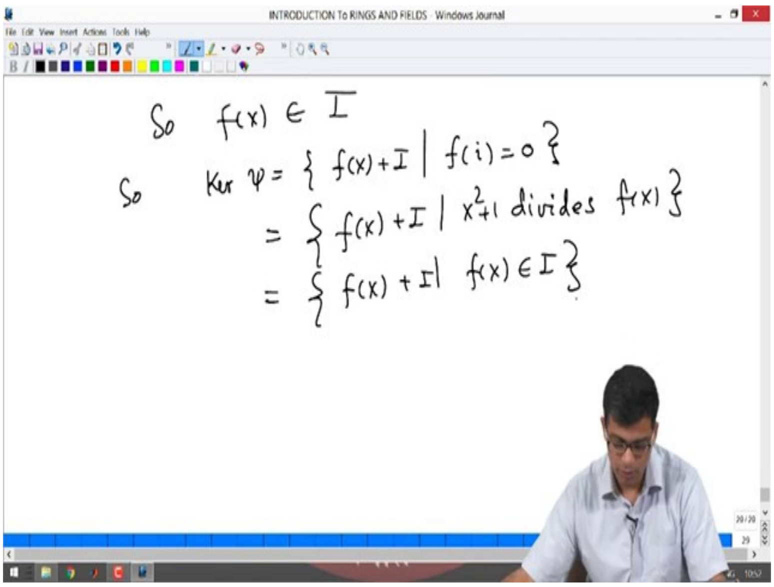
This is if you want in C x. Inside C x I have x minus i and x plus i divide f x, but that means, x minus i times x plus i divides f x. So, because x minus i and x plus i have nothing in common, no factors in common. This is a point that I will mention again when we talk about unique factorization domains; x minus i times x plus i divides f x in C x.

(Refer Slide Time: 33:07)



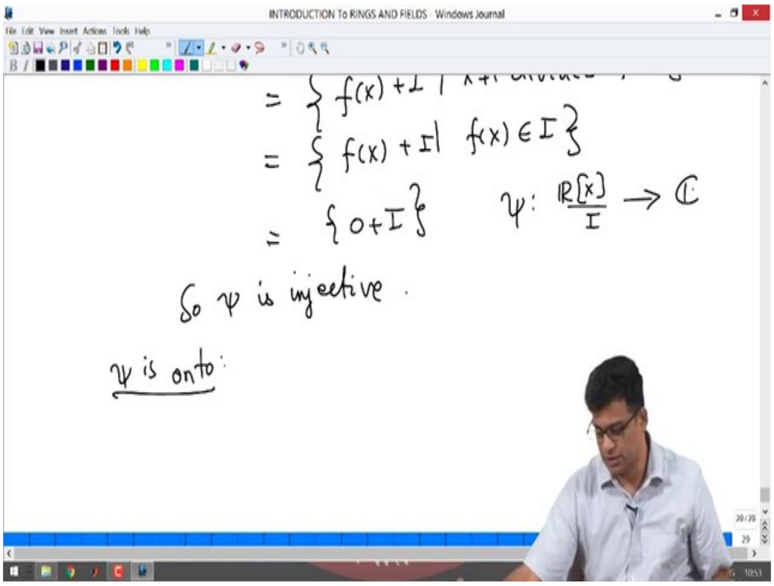
But x minus i times x plus i is actually equal to x squared plus 1. So, x squared plus 1 divides you can say in R x because now, x squared plus 1 is in R x and f x is also in R x. So, if they if this divides x squared plus 1 divides f x in a larger ring, it also divides it in the smaller ring; that means f x is in I. So, ok, this is a long proof but it is important to understand this.

(Refer Slide Time: 33:43)

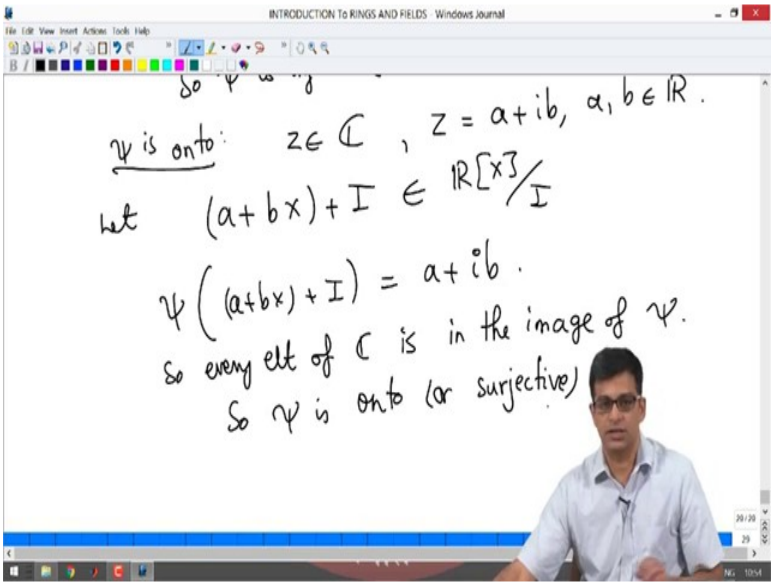


So, what we have just shown is that kernel.

(Refer Slide Time: 34:25)



(Refer Slide Time: 35:07)



(Refer Slide Time: 36:17)