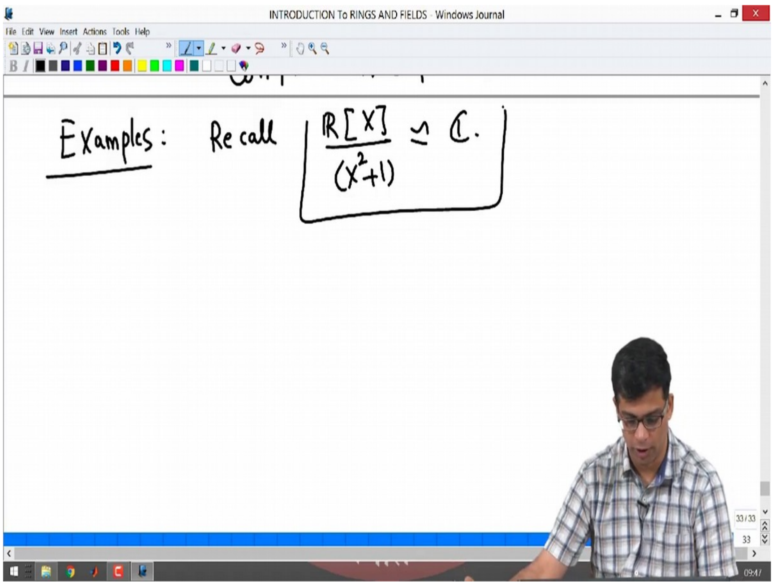
Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 13
Examples of correspondence theorem

In the last video we looked at an important theorem about quotient rings. We have three parts there, one is that image of a ring homomorphism is a subring which was fairly easy, second part was called the first isomorphism theorem it says that if you have a ring homomorphism from R to S it is an onto homomorphism. Then R mod kernel phi is isomorphic to S. And the third part of the theorem was we had a bijective correspondence between ideals in the ring R that contain the kernel and ideals in the ring S ok.

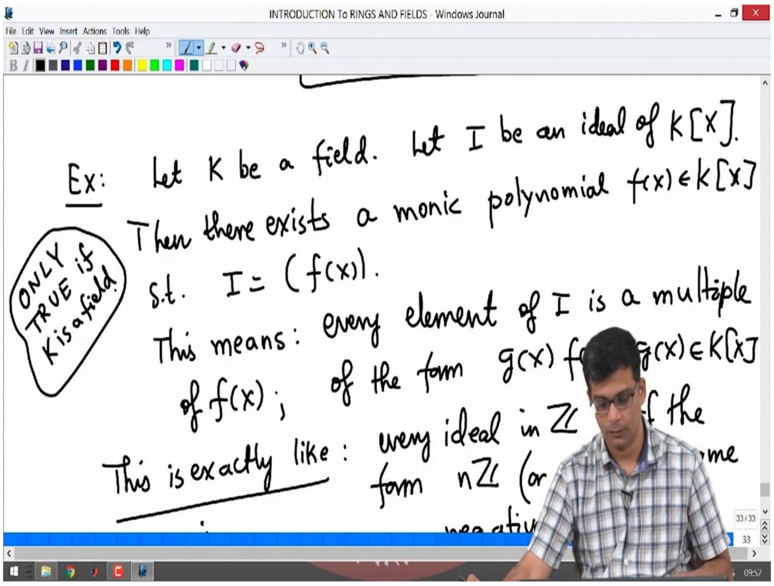
(Refer Slide Time: 00:46)



So, I want to do some examples in this video to illustrate the application of the previous theorem.

Let me start with the example that I did a few videos ago about R mod x. So, if you have. So, recall I have showed in an earlier video that there is an isomorphism between these two rings ok. So, let me re prove that today and as I said this is an important isomorphism. If you understand this isomorphism you really have understood important things about ring theory. So, this is something that you have to carefully think about and understand.

(Refer Slide Time: 01:30)

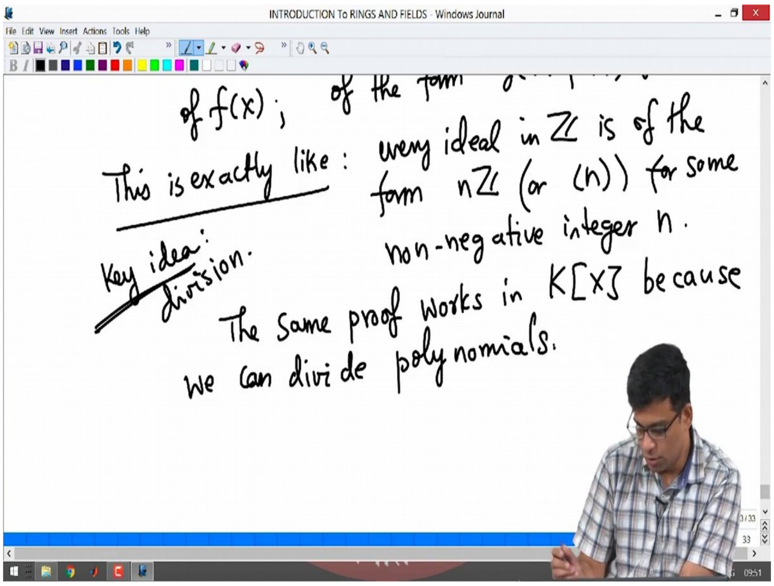


But in order to prove this in a different way. So, I am going to use an exercise which I mentioned earlier, but I have I have not solved this, but the solution is exactly similar to another theorem that I have done earlier. So, let K be a field remember a field is a ring where every non zero element is a unit; in other words, it has a multiplicative inverse. So, then every ideal in and let us consider let I be an ideal of K x remember K x always stands for the polynomial ring over K in one variable.

So, I is an ideal of K x then there exists. So, then there exists a monic polynomial f x in k x remember what is monic? Monic simply means that its leading coefficient is 1. So, if it is a polynomial of degree 10; that means, x power 10 is the largest power of x that you see there the coefficient x power 10 is 1 there exists a monic polynomial f x such that, I is equal to the ideal generated by f x. So, this notation I have used before this simply means that this means in the ring of integers we know what this means. This because there it was if you put brackets around 2; that means, the, it is ideal generated by 2; that means, every elements of that set is a multiple of 2; it is the same thing here.

This means every element of I is a multiple of f x; that means, it is of the form g x times f x where g x is an arbitrary element of k x, right. So, an ideal generated by a single element is by definition that element times any element.

(Refer Slide Time: 03:51)



So, why is this? So, this is the exactly like the statement I proved: every ideal in Z the ring of integers is of the form nZ or n in other words for some non-negative integer right.

Remember this I have proved this in some video in a video few videos ago, here the key idea was division algorithm. So, division. So, we started with an ideal if it is the 0 ideal it is already of the form 0 times Z, if it is not the 0 ideal it must contain some non zero number, then it must contain a positive integer, because ideal is closed under the taking inverses. So, if it contains non zero elements. So, it contains positive elements.

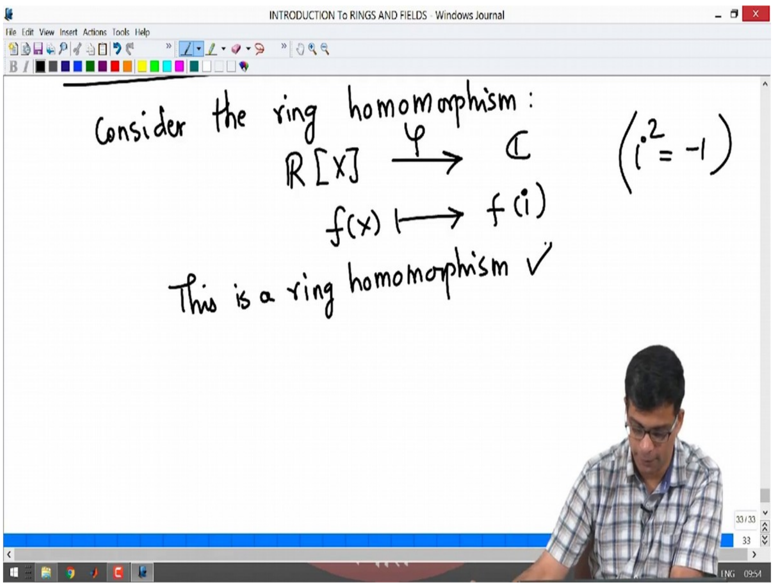
And then we simply take the least positive element of I and then we use division algorithm to argue that everything is a multiple of that. Because we can divide by this least element, the reminder is a number strictly less than this element. So, it cannot be there if it is positive. So, it must be 0 in other words reminder is 0. The same the same proof works in k x because we can divide polynomials also just like we can divide integers.

Remember though that to divide polynomials we, to divide by a polynomial f, we need that the leading coefficient of f must be a unit, but in a field every non zero element is a unit and leading coefficient is by definition non-zero. So, we can always divide by any polynomial, any non zero polynomial if a f x non zero polynomial we can divide by that polynomial in a field in a polynomial ring or a field. So, that is why we cannot divide in general in R x and we do not have such a statement for R x, where R is an arbitrary ring.

This is only true if K is a field in other words if K is just a ring this is not true as we will do in examples later. So, in other words we want to show that there is something. So, what would be the analogue of least positive element? What you do is if the ideal in k x is not zero. So, I will not do this, I will leave it for you to do because it is exactly similar: you take an ideal if it is 0 you are done because it is generated by the 0 polynomial. If it is not 0 take the polynomial, non-zero polynomial which has the least degree, in other words. In fact, take take a monic, take the monic polynomial with the least degree and then divide by it, argue that reminder must be 0 ok.

So, let me not say anything more about this, in a future problem session I will try to do this in details. So, I am going to use this. So, in particular in R x if R is the field of real numbers every ideal is generated by a single element. So, let us the apply this.

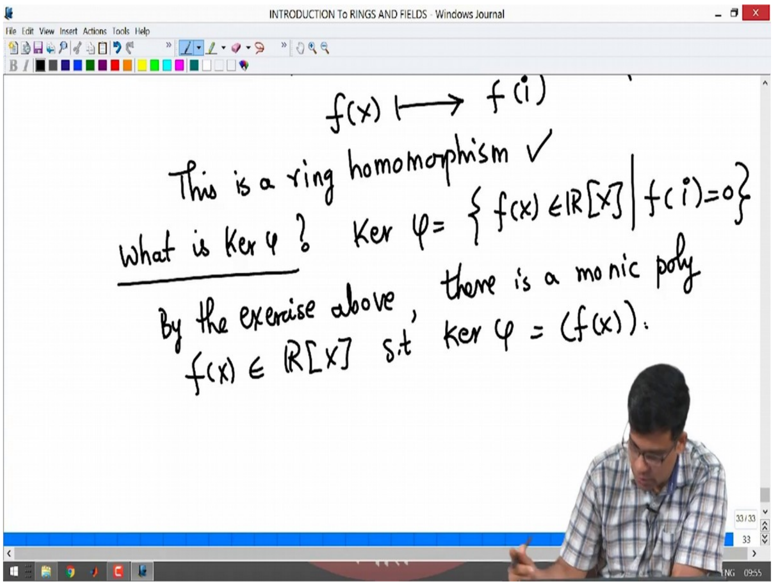
(Refer Slide Time: 07:27)



So, consider the ring homomorphism. So, I am going to reprove the statement that we proved in a previous video. So, consider ring homomorphism from R x to C which takes f x to f i. So, i as always is a square root of minus 1 so, imaginary number.

So, what is this function? f x goes to f i, this is a ring homomorphism is an is easy check. In fact, I think I discussed such examples when I defined ring homomorphisms. So, this is ring homomorphism I will not do this in detail. So, this is a ring homomorphism let us assume that. What we are doing is take a polynomial with real coefficients and you evaluate it at the imaginary number i. So, you plug in x equal to i you then get a complex number. So, it is an element of c. So, this a ring homomorphism.

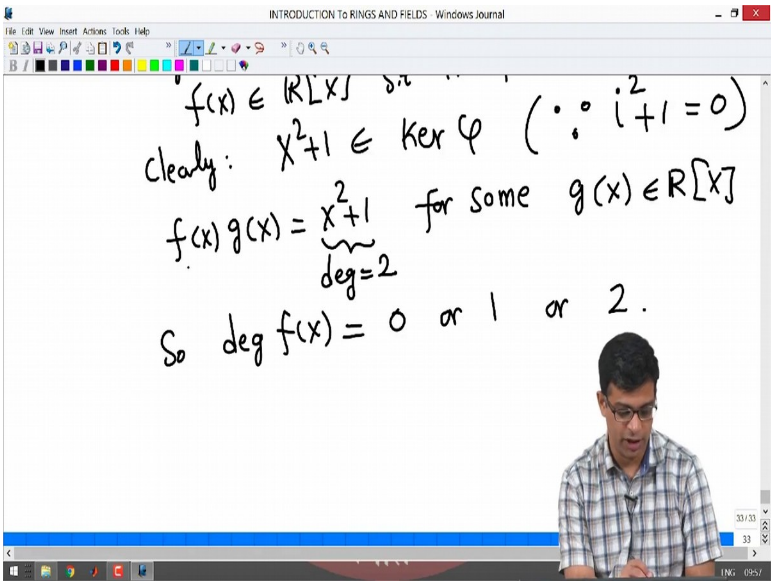
(Refer Slide Time: 08:33)



What is the kernel of this? What is kernel of phi? So, that is what the question is kernel phi is all elements in the polynomial ring R x.

So, this f x in a R x. So, f of i is 0 ok. So, now, I know, because of the or the rather the exercise that I mentioned here, every ideal in a kernel phi is a, every ideal in the polynomial ring R x is generated by a single element. So, by the exercise above there is a monic polynomial f of x in R x such that kernel phi is the ideal generated by f of x. So, in order to determine kernel phi I just need to find out f of x; let us search for f of x.

(Refer Slide Time: 09:41)

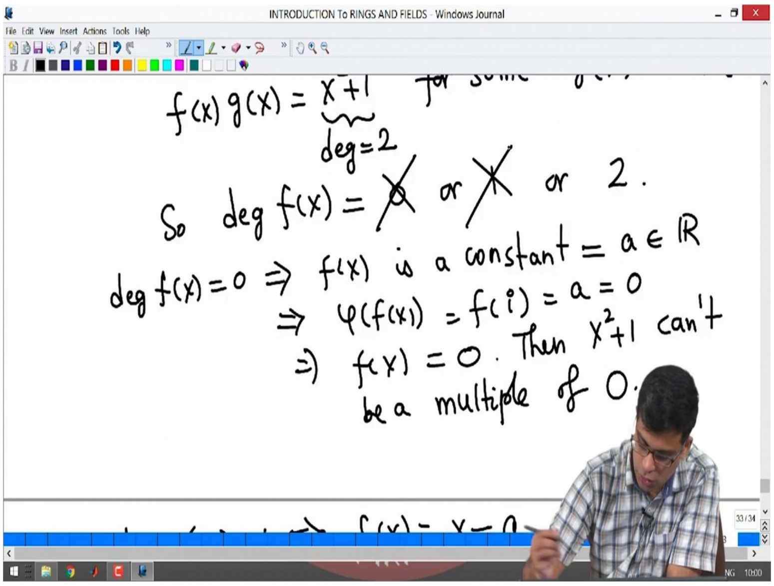


So, what are some elements of the kernel? Certainly you know that by definition of I x square plus 1 is in the kernel write this is because I square plus 1 is 0. So, if you take x squared plus 1 and substitute x equal to i it become 0.

So, x squared plus 1 is the kernel. So, that already means that f is the generator of the kernel f x. So, in other words f x times g x is x square plus 1 for some. Remember this is the definition of the ideal generated by f x, every element of the ideal is a multiple f of x; x is squared plus 1 is an element of the kernel. So, it must be a multiple f of x, these already means because this is degree 2.

So, degree f is 0 or 1 or 2, that means because if you have a polynomial that divides a polynomial of degree 2 its degree must be less than or equal to that right because degree of the product is the sum of the degrees degree f x plus degree of g x is 2; so, degree f x 0 1 or 2.

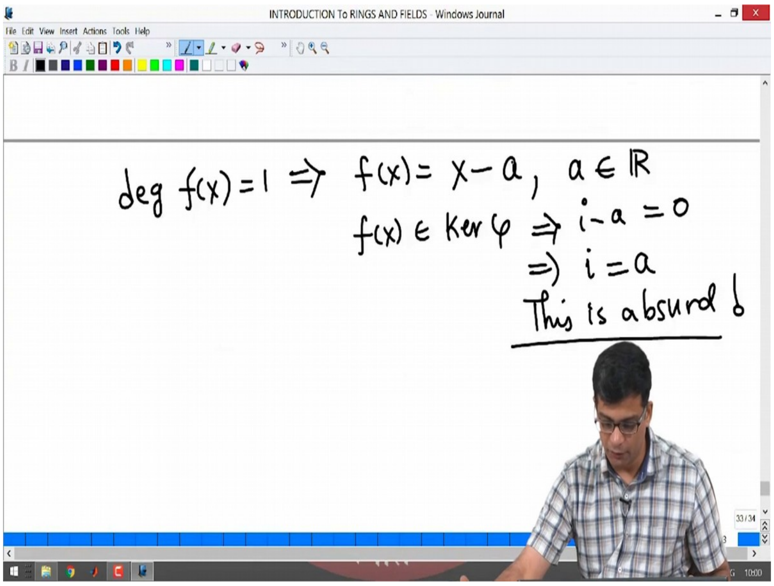
(Refer Slide Time: 11:07)



So, now let us look at the possibilities; can degree f x be 0? Remember what is the meaning of this? Degree of f x is 0 means f x is a constant, but then what is phi of f of x? So, f x is a constant; let us call it a in R right it is a degree 0 polynomial means it is a constant a, but then this is just a, but because if there is no meaning to substitute for x in a constant polynomial. Under the function phi under the function phi a constant simply goes to the constant itself ok.

So, there is, in other words, a goes to a, but because f is the generator of the kernel in particular f is in the, f is generator of kernel and in particular f is in the kernel phi of, f x 0; that means, a is 0; that means, f x = 0, but now this is a problem right because f x 0 how can x plus 1 b? A multiple of 0 x square plus 1 then cannot be a multiple of 0 f x x plus 1 cannot be a multiple of 0 right because a; obviously, any multiple of 0 is 0. So, in other words 0 is not a possible degree for f of x ok. So, the proof hopefully is clear. So, f x cannot be degree 0.

(Refer Slide Time: 12:48)

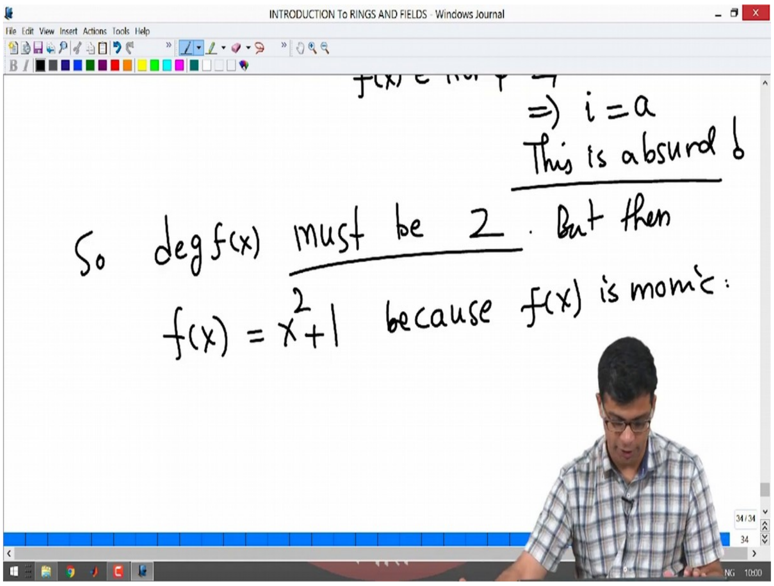


Now, let us see degree of f x is 1, can this be possible? Remember f x is a monic polynomial by choice, there is a monic polynomial f x such that kernel phi is all multiples of f x.

So, if f x is monic; that means, f x is degree 1 and monic means a a f x is the form x minus a, what is what are degree 1 polynomials? The highest degree of x is 1. So, x plus x minus a or x plus a in general you can have coefficient, but because its monic coefficient is 1, but then remember f x is in the kernel as I mentioned earlier. So, this implies x minus a in the kernel, but; that means, i minus a in the kernel.

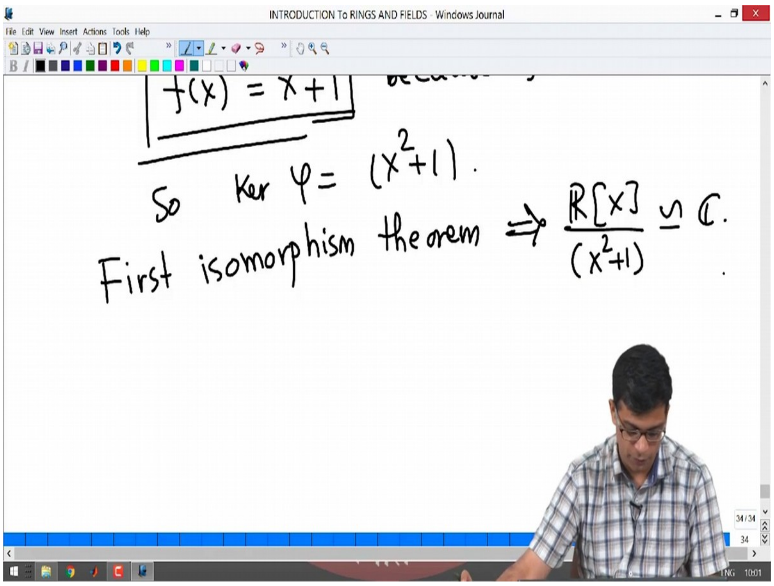
So, i minus a is equal to 0 right because x minus a under phi mapped. So, i minus k, but; that means, i equal to a, but this is also absurd right, why is it absurd? This is absurd because a is a real number, i is a imaginary number, i is not a real number. So, a real number cannot be equal to i. So, 1 is also not a possibility.

(Refer Slide Time: 14:04)



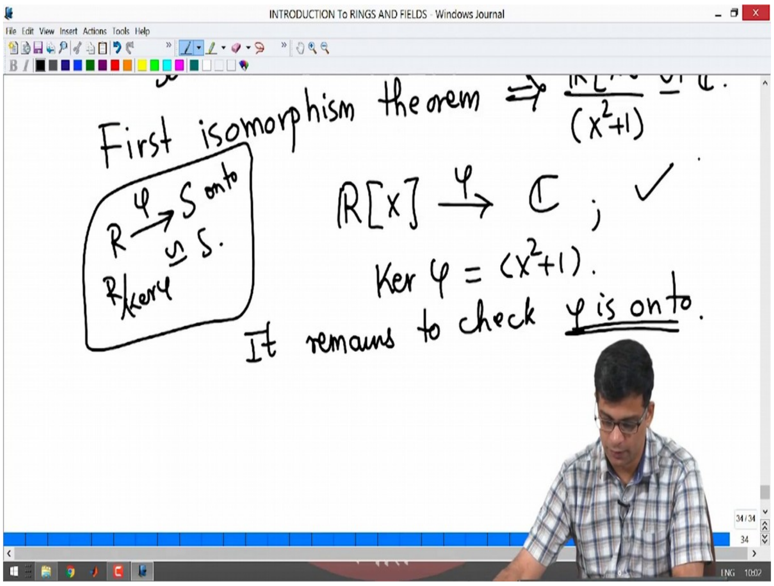
So, degree of x must f x must be. So, degree of f x must be two; that means, f x is equal to x square plus 2; x square plus 1, but then x is degree, f x is equal to this because both are monic it is a degree two polynomial that divides x square plus 1 that mean it must be x square plus 1 times a constant. Remember degree of f plus degree of g here is 2. So, degree of f x 0 means degree of g is 2 degree of f x 1 means degree of g is 1 degree of f x 2 is what we just established; that means, degree of g is 0 that mean is a constant, but f x a monic polynomial x square plus 1 monic polynomial. So, g x is must be 1 ok.

(Refer Slide Time: 15:05)



So, f x is x square plus 1; that means, kernel of phi is precisely x square plus 1. So, now, isomorphism theorem says, what does it say? Precisely that R x mod ok. So, I will write this here, but there is one additional fact to be verified.

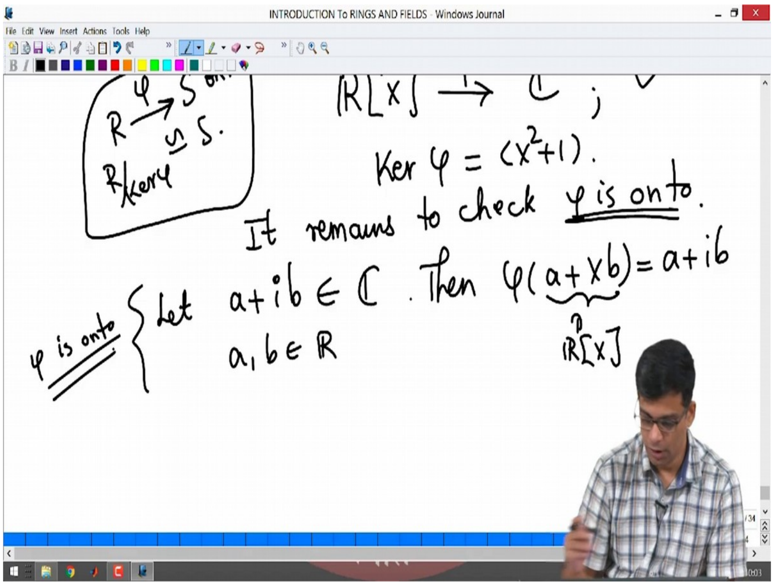
(Refer Slide Time: 15:34)



So, first isomorphism theorem says from the previous video if you have a ring homomorphism R to S, R mod kernel phi is isomorphic to S; however, remember this must be onto ok. So, in our situation we have R x to C we have this, we have kernel of phi is x squared plus 1 so, R x mod the kernel isomorphic the image. So, it remain to check in other words. So, I cannot yet say this, right, I have to check phi is on to, but I claim that is trivial because if ok.

So, let me first say that phi is onto we have this the missing phi is here is that phi is onto. If it is onto we have this because of the first isomorphism theorem, but why is phi is onto, why is phi on to?

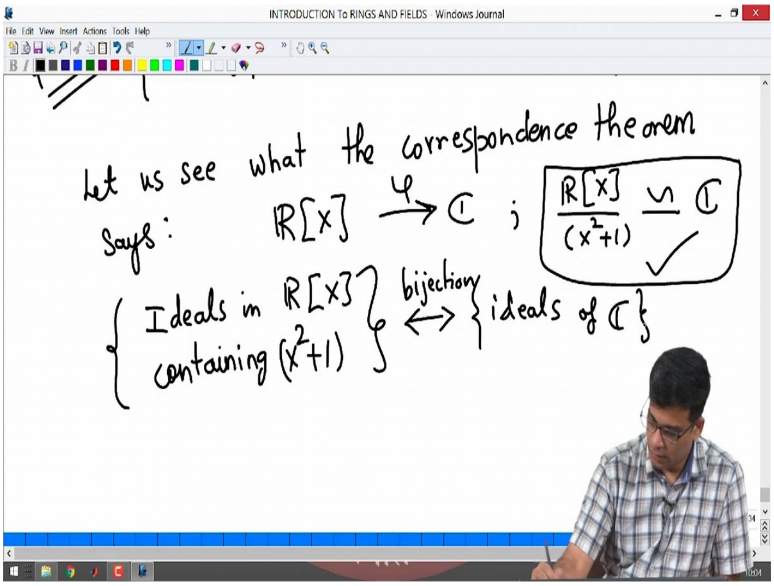
(Refer Slide Time: 16:32)



So, let us taken arbitrary element of the complex numbers a plus i b, then remember; that means, a b are real numbers then phi of a plus x b is a plus i b right because remember a plus x b is a polynomial in R x because a b are real number and its images is obtained by plugging in x equal to i and do you that you just get x a plus i b. So, phi is onto.

So, phi is onto R x to C the map phi from R x phi is onto. its kernel is x square plus 1. So, we conclude R x mode x square plus 1 C. So, this is another proof of this important isomorphism of rings that I did in an earlier video ok, but now it uses the first isomorphism theorem. Now that is one application first isomorphism theorem let us apply the last part of the theorem from last video.

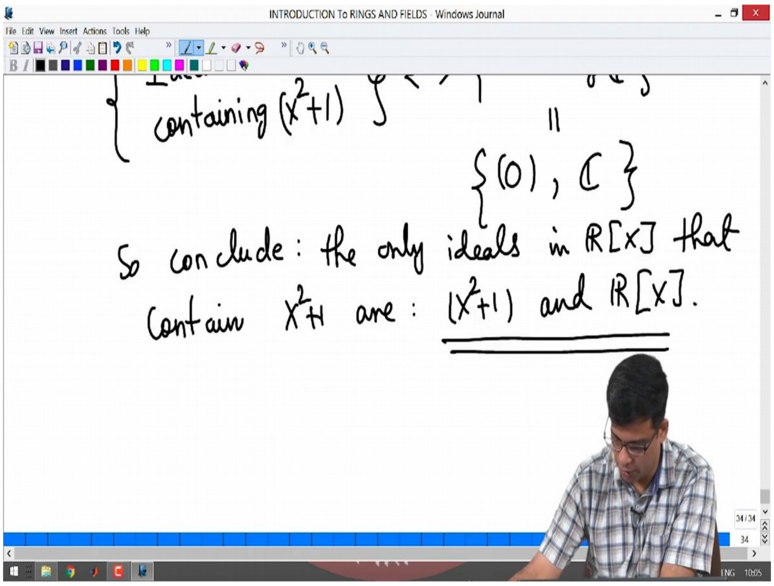
(Refer Slide Time: 17:29)



So, let us now apply what the correspondence theorem says. Let us see what the correspondence theorem says, correspondence theorem says. So, we have R x to C which is phi we have already established R x mod x square plus 1 is isomorphic to C. So, this is done now, what does the correspondence theorem say? It says that ideals in R x containing kernel phi are in bijective correspondence with ideal in C.

So, let us in write it in detail: ideals in R x containing x square plus 1 are in bijective correspondence with ideals of ok. So, now, this is what the correspondence theorem says, but what are ideal of C? There are exactly two ideals right.

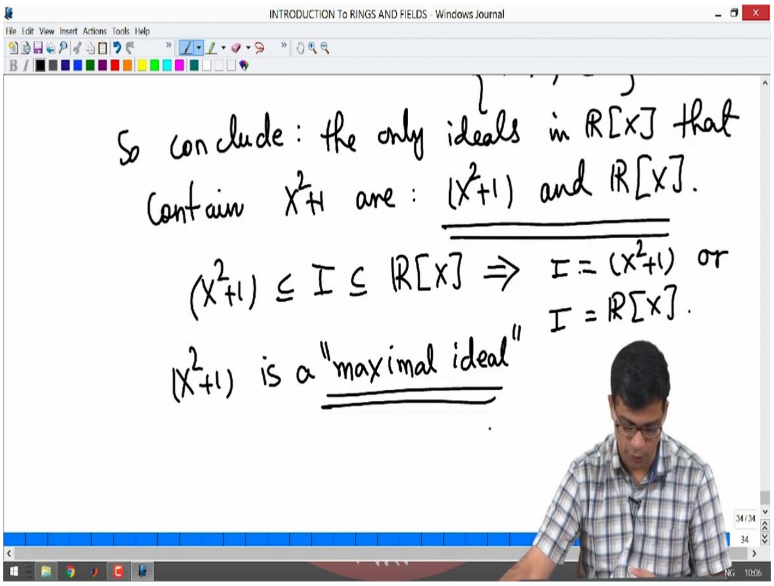
(Refer Slide Time: 18:47)



So, remember C is a field, any field as a exactly two ideal; so, namely the 0 ideal and C. So, there are only two ideals here. So, we can conclude the only ideals in R x that contain x square plus 1 R there are only two ideals because this set has two elements. By the bi-jection between this set and this set this set has two elements right and what is this set? Ideals in R x containing x squared plus 1.

So, there are only two ideals containing x squared plus 1 and there are two obvious ideals that contain x squared plus 1 right x squared plus 1 itself and R x there is no other ideals. So, this is a point I want to emphasize.

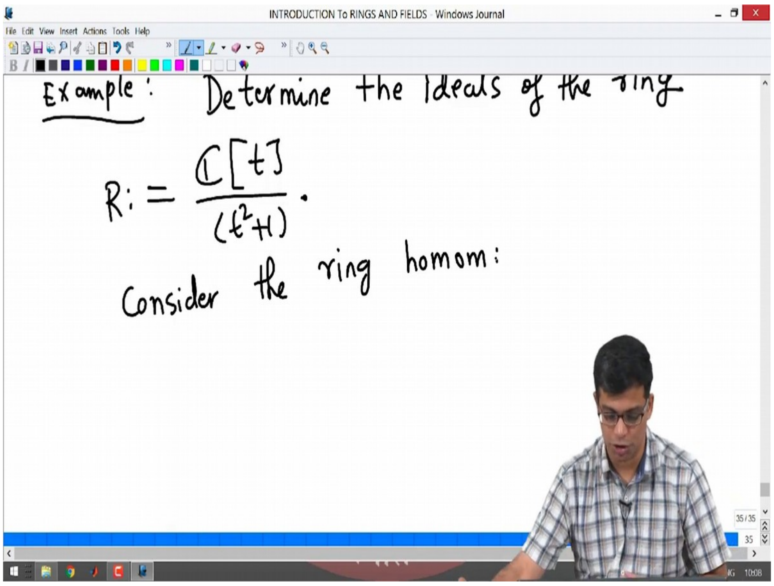
(Refer Slide Time: 19:48)



So, in other words if you have an ideal x squared plus, I, x squared plus 1 contained in an ideal I which is an ideal of R x; that means, I is x squared plus 1 or I is R x there are no ideals between x squared plus 1 and R x that are different from a both of them. So, such ideals are called maximal ideals. So, x squared plus 1 is a maximal idea.

So, I will define this formally later, but this is just to give you a preview of this is called a maximal ideal where maximal ideals are ideas which have these this property that there are no ideals that contain that ideal other than that ideal that ideal itself and the full ring ok. So, now, this is a useful result using the correspondence theorem. So, now, I want to do some more examples, these examples also are suppose to help you with understanding ring homomorphism and kernels of ring homomorphism ok.

(Refer Slide Time: 20:57)

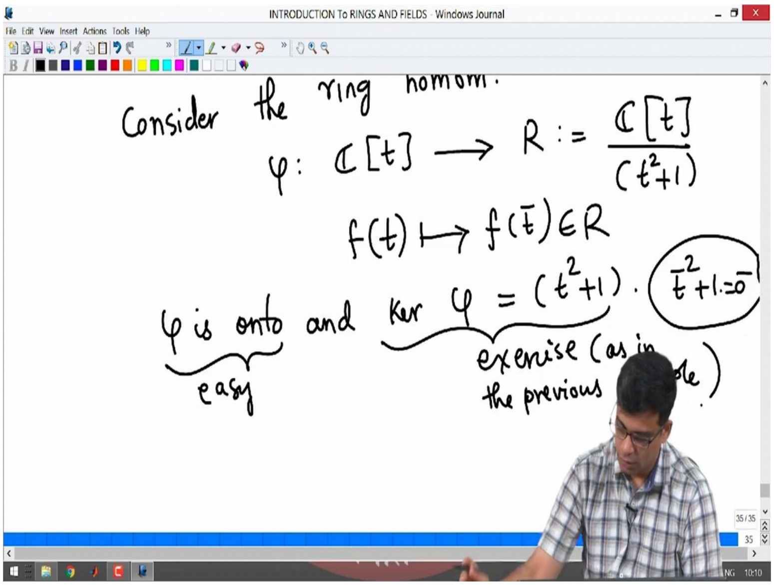


So, let us do the following. So, this is another example. So, actually let us just do one example which talks about correspondence theorem.

So, the question is determine the ideals of the ring C t by t squared plus 1, C t divided by t squared plus 1 ok. So, now, this is sort of application of the bijective correspondence theorem, but I want to set it up properly. So, I let us call this ring R, we do not know what this ring is I am not interested in knowing what this ring is. In fact, I do not even know what it means to know this ring, the question is only to determine the ideals of the ring ok. So, remember correspondence theorem says that if you have a ring homomorphism this already leads to an isomorphism of rings, quotient ring and the co-domain ring and then there is a correspondence of ideals in these two rings.

So, here consider the ring homomorphism here R is already given as a quotient ring.

(Refer Slide Time: 22:22)



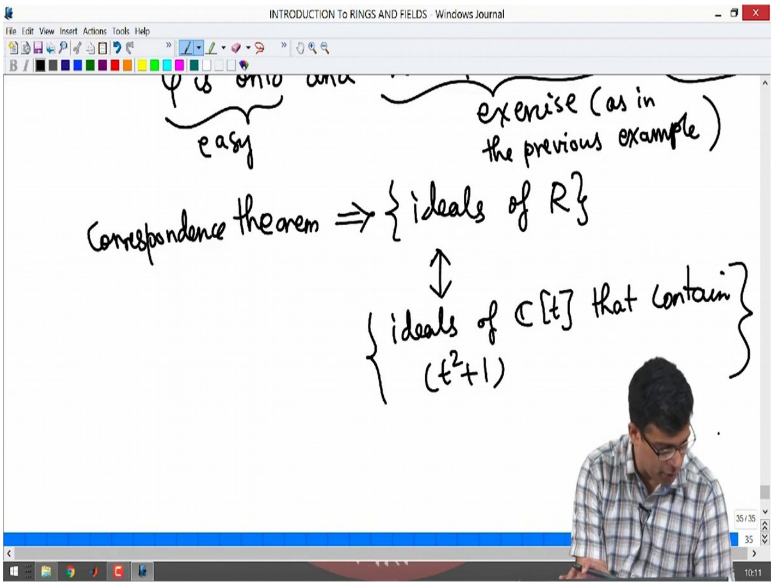
So, I can define the following ring homomorphism from C t to R what is R? R is C t modulo t squared plus 1 and what is this function? I will simply send it to f of t to I will send it to f of t bar. Remember t bar is the t bar always represents the coset corresponding to t, in general bar is a convenient notation to denote cosets in a quotient ring.

So, I will take an element, polynomial in t I will simply replace t by t bar, all the other things are left as they are. So, this is an element of R by definition ok. So, this an exercise, phi is onto, this is clear because t bar is in image because t goes to t bar anything here is a polynomial in t bar. So, its in image and kernel phi is precisely t square plus 1.

So, this is exactly how we make R isomorphic to Ct mod t squared plus 1. So, this I will leave for you to check. So, this is easy, this an exercise this also an exercise, but it is an easy exercise this is slightly more work. But again use the fact that every element every ideals in C t is generated by single element because C is a field t squared plus 1 is in the kernel of this because t squared plus 1 goes to t bar squared plus 1, but t bar squared plus 1 is 0 ok. So, t squared plus 1 is in the kernel and you argue that there is no linear polynomial in the kernel. So, this is as in the last example ok.

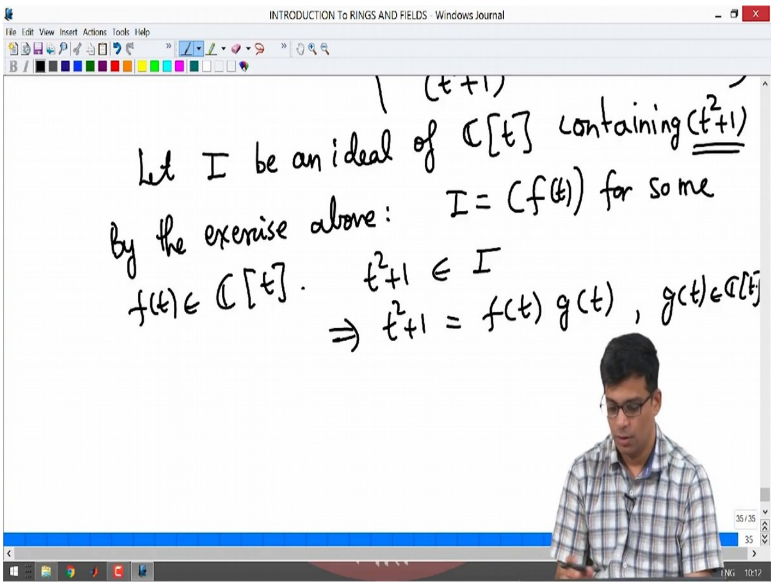
So, these I will leave for you to do.

(Refer Slide Time: 24:47)



So, now the conclusion of the correspondence theorem says that, correspondence theorem gives ideals of R which is what we are interested in finding are in bijective correspondence with ideals of C t that contain t squared plus 1 right. The correspondence theorem because C t t square plus 1 is the ideals of C t mod t squared plus 1 are ideals of C t that correspond that contain t square plus 1. So, in order to determine ideals of R, I need to determine what are the ideals of C t that contain t square plus 1. So, let us do that now.

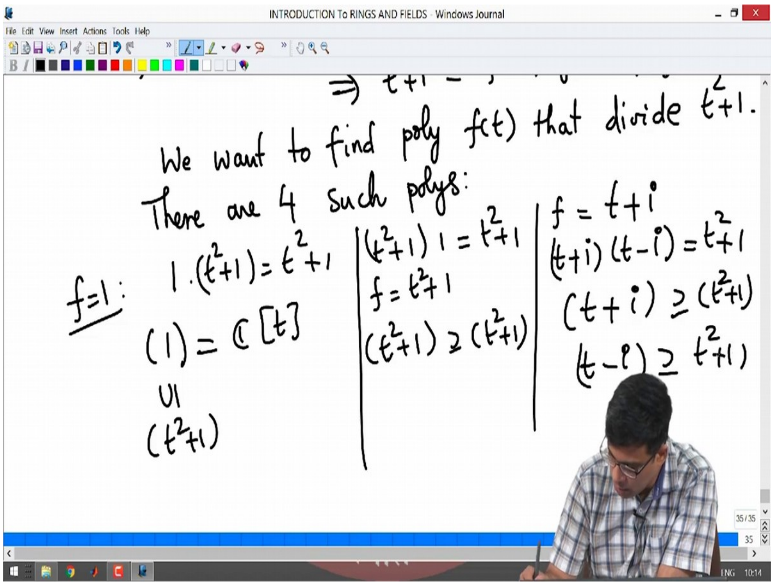
(Refer Slide Time: 25:33)



So, let I be an ideal of R, C t containing t squared plus 1. See first of all note that there are two obvious ideals that contains t squared plus 1: t squared plus 1 itself and C t itself.

So, these are two ideals, are there any more? By the exercise above because C is a field, I is actually an ideal generated by f t for some t some f t rather some ft in C t. But t squared plus 1 is contained in I this means t squared plus 1 can be written as f of t times g of t for some g of t in C t ok. Now f t divides t squared plus 1 what are the polynomials that divide t square plus 1?

(Refer Slide Time: 26:50)

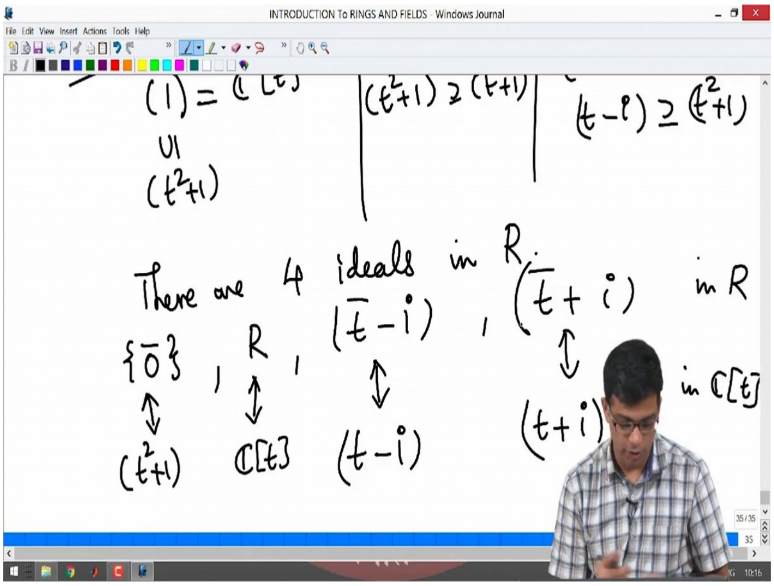


So, we want to find polynomials f t that divide t squared plus 1 ok.

So, now if you think about this, there are four such polynomials. So, certainly 1 divides it right? 1 times t squared plus 1 is t squared plus 1. So, that one possibility for f is all the polynomials here; the second possibility is of course, t squared plus 1 t squared plus 1 itself divide t squared plus 1 these corresponds to here the ideal generated by 1, in other words is C t.

So, here f is equal 1, here f equals t squared plus 1. So, the ideal generated by t squared plus 1 is of course, ideal the generated by t squared plus 1 this contains t squared plus 1 this of course, contain t squared plus 1. So, these are the obvious two ideals contains t squared plus 1. Now are there any other fs that divide it? Of course, there are for example, t plus i. So, here t plus i times t minus i is t squared plus 1. So, then other words the ideal generated by t plus i contains t squared plus 1, similarly the ideal generated by t minus i contains t squared plus 1.

(Refer Slide Time: 28:36)



So, there are four ideals that contains t squared plus 1 and hence there are four ideals in R and what are they? They are 0 ideal this corresponds to.

So, I will write down these and then I will tell you how to what are the corresponding ideals in C t. Of course, there is R and there is t bar minus i and t bar plus i. So, these are ideals in R what are the corresponding ideals in C t? This corresponds to 0, this corresponds to the ideal t squared plus 1 sorry this is not bracket, this is the ideal generated by t squared plus 1. So, this corresponds to the ideal generated by t squared plus 1. This is the smallest ideal corresponds to that contains t squared plus 1 which is the kernel of the map phi.

So, the smallest ideal in this set of ideals of that contains t squared plus 1 is t squared plus 1 and it corresponds to the smallest ideal of R which is the 0 ideal. And the largest ideal that contains t squared plus 1 C t itself and that corresponds to the largest ideal of R. The ideal in C t that is generated by t minus i corresponds to t bar minus i the ideal t plus i corresponds to t bar plus i. So, R has four ideals. So, R is an infinite ring of course, R has infinitely many elements, but it has four ideals.

So, this is again an application of bijective correspondence result, in order to understand ideals in that ring R; namely C t mod t squared plus 1 we have used bijective correspondence and then our knowledge about ideals in C t to conclude that R has exactly four ideals. So, hopefully these examples and problems gave you some idea how to work with rings and quotient rings and ideals. So, I going a stop the video here, in the next video we will continue our study of quotient rings and I will give you a few more examples.

Thank you.