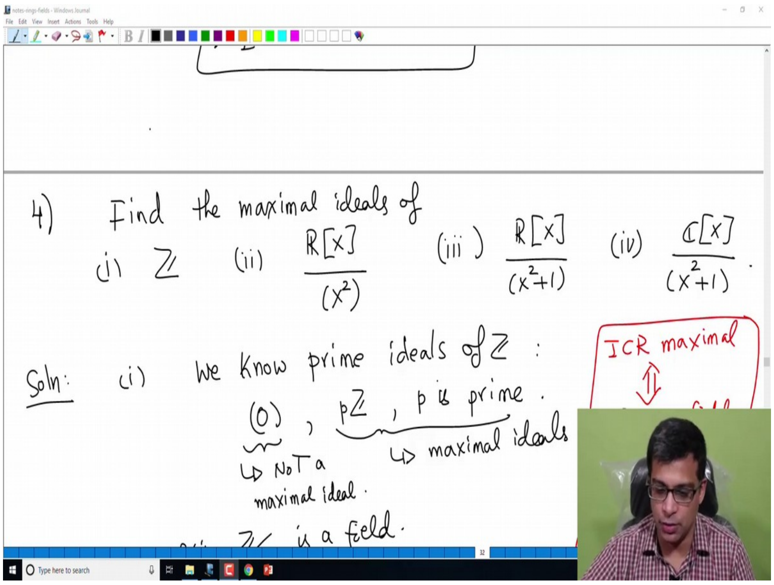
**Introduction To Rings And Fields**
**Prof. Krishna Hanumanthu**
**Department of Mathematics**
**Chennai Mathematical Institute**

**Lecture – 19**
**Problem 6**

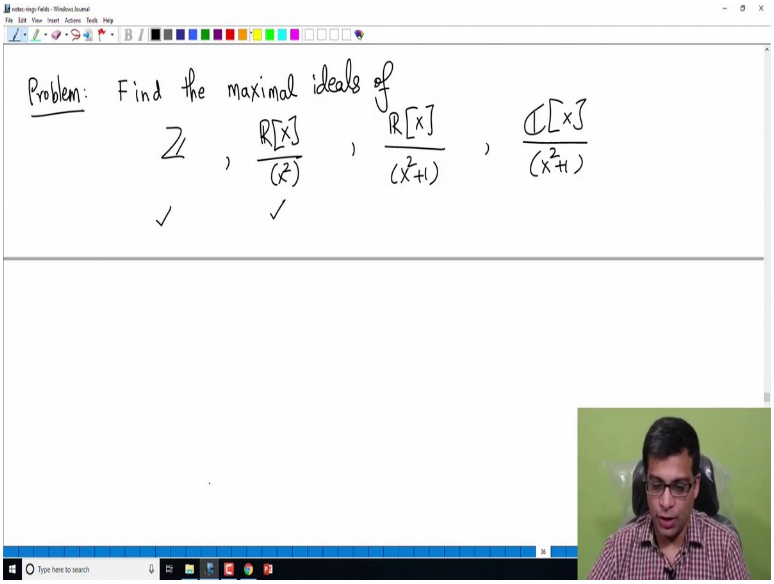
In this video we are going to continue doing problems that we started in the last video. So, if you recall in the previous video, I wanted to compute the maximal ideals of certain rings. So, I will show you the problem that we were doing and we did half of it.

(Refer Side Time: 00:32)




So, the question was to compute maximal ideals or find the maximal ideals of these four rings: Z and R X mod X squared we did the first two. So, let us do now the remaining two here and in this problem I will also recall some facts that we have learned before.

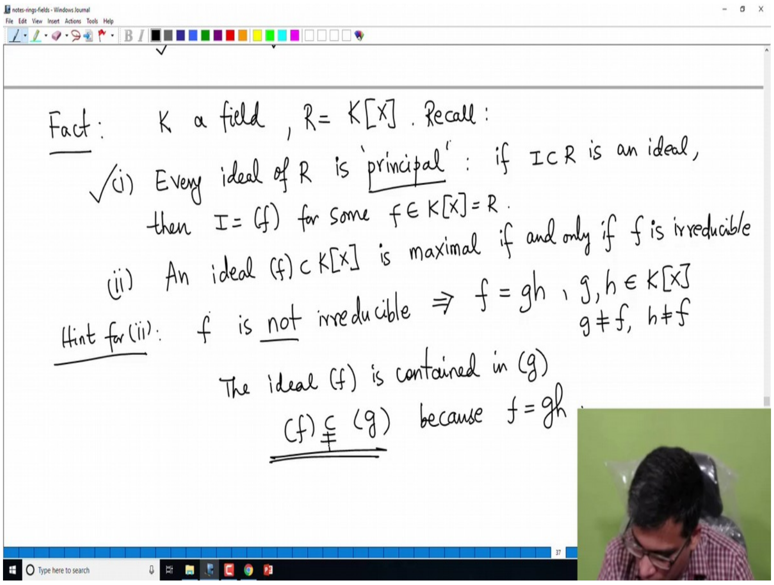
(Refer Side Time: 00:55)




So, the problem is to compute the following. So, find the maximal ideals of Z and R X mod X squared R X mod X squared plus 1 and C X mod X squared plus 1. So, we have already done this we have already done this. And for the second problem the crucial idea was that, the correspondence theorem which says that if you have a ring R ideal I in it and the ring R mod I the quotient ring there is a bijective correspondence between ideals of R that contain I and the ideals of R mod I.

And this bijection, in fact, carries over to prime ideals as well as to maximal ideals. So, using that we used that to come find out the maximal ideals of R X mod X squared. These are maximal ideals in R X that contain X squared and by a simple calculation we saw that there is only one such, namely the ideal generated by X itself.

(Refer Side Time: 02:19)




So, in order to continue this problem, let me use the following fact which I did when I first introduced polynomial rings. So, let us say K is a field and let us say R is the polynomial ring in one variable over K. So, R is K X, so then what we have is that recall. So, recall two things every ideal of R is principal remember principal means if I is an ideal, so this what I mean if I is an ideal then I is in fact, generated by a single polynomial for some f in K X which is of course, R.

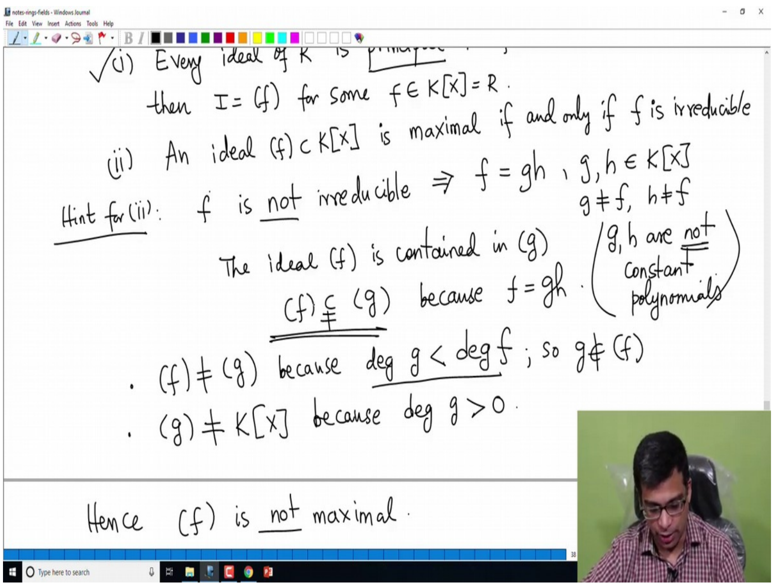
So, remember this notation here f within brackets means the ideal generated by f, this consists of all multiples of f that is one we call it a principal ideal. And recall the proof of this I did using Euclidean division algorithm, the idea is to pick the polynomial in I whose degree is smallest, positives degree polynomial whose degree is smallest. And then we use Euclidean division to show that every other polynomial that is in I is a multiple of f.

Now, second fact I will write which may be I did not mention this explicitly before, but it is an easy exercise an ideal I in K X which is again R this is a statement which is very special to polynomial rings over a field in one variable. So, an ideal is maximal if and only if f is irreducible ok. So, this is not a difficult exercise, so I will just give you a quick hint to do this. So, one is something we have done before.

Hint for two, the problem is not to do this exercise I will rather do the previous exercise that I wrote. So, I would like you to prove two for yourself, but I will give you a hint. So, suppose f is not irreducible, remember an irreducible polynomial is one, which cannot be factored into two polynomials g and h, where g and h are actually not equal to f or not equal to 1. So, f is not irreducible means f can be written as a product of two polynomials in the polynomial ring and the point of course, is that g is not f h is not f, you can always factor a polynomial as one times f. If it is not reducible it can be factored in a more interesting fashion, nontrivial fashion.

So then, the ideal by the way I should not I did not write this carefully an ideal I, so I will just I will not mention I here. The problem the exercise is to show that an ideal generated by a single polynomial is maximal if and only if f is irreducible. So, the ideal f is contained then right so what I mean is this because, f is g h. Remember the ideal generated by g is the set of all multiples of g f is one such multiple, because g times h is f.

(Refer Side Time: 06:03)

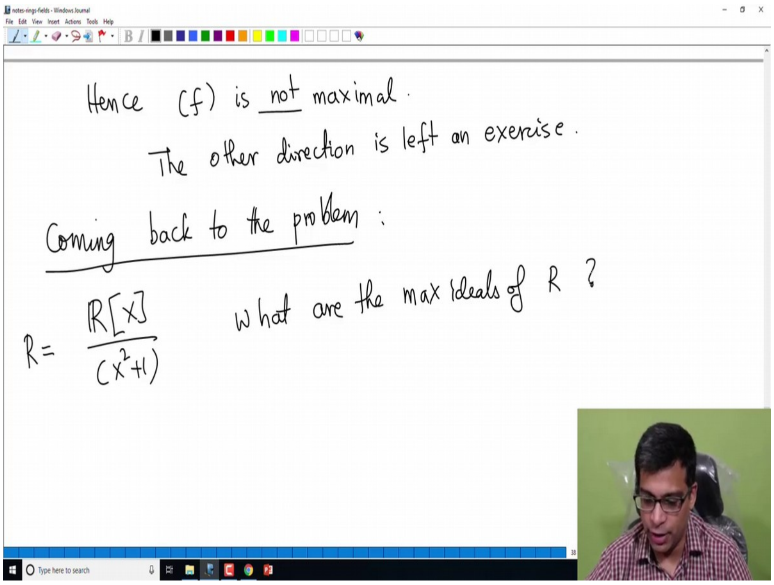



So, this belongs to this and it is not equal right its an easy exercise to show that f is not equal to g because g is a polynomial of strictly smaller degree. Otherwise, g will be equal to f when you here we need that g and h are not constant polynomials that is what it means for f to be not irreducible.

So, g and h are not constant polynomials. So, degree of g is strictly less than degree of f. So, this cannot be equal to this right because g is not in the ideal generated by f. Because if g was a multiple of f degree of g will be at least the degree of f, but degree of g is less than degree of f. At the same time the ideal generated by g cannot be all of K X because, degree of g is positive its not a constant polynomial.

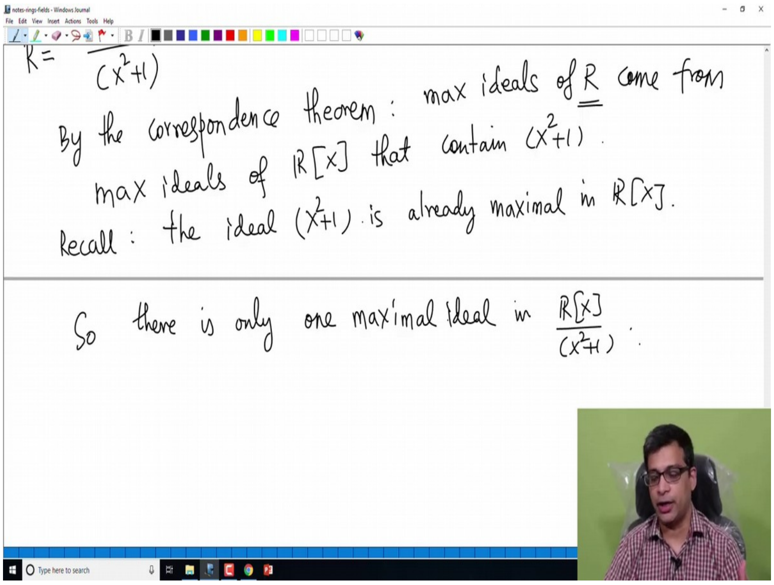
So, no polynomial no ideal generated by a non constant polynomial can be the unit ideal. So, this concludes the statement that f is not maximum. So, I have proved one direction for you: if f is not a irreducible it cannot be maximal; the other direction is f if f is actually irreducible show that the ideal generated by f is maximal. I will not do this for you, but the idea is suppose the ideal is not maximal then ideal generated by f is contained in a proper ideal which is bigger than that. But because of fact one every ideal is principal, so let us say the bigger ideal is generated by g, then you argue that g must divide f, violating the irreducibility of f.

(Refer Side Time: 07:55)




So, the other direction is left for you as an exercise ok. So, this is an easy exercise actually. So, I strongly urge you to do this carefully, so this is the fact that I am going to use. Now coming back to the problem. So, let us first consider the quotient ring R X mod X squared plus 1 what are the maximal ideals of this? Let us call this ring R what are the maximal ideals of this is remember the third part of the previous problem.

(Refer Side Time: 08:48)

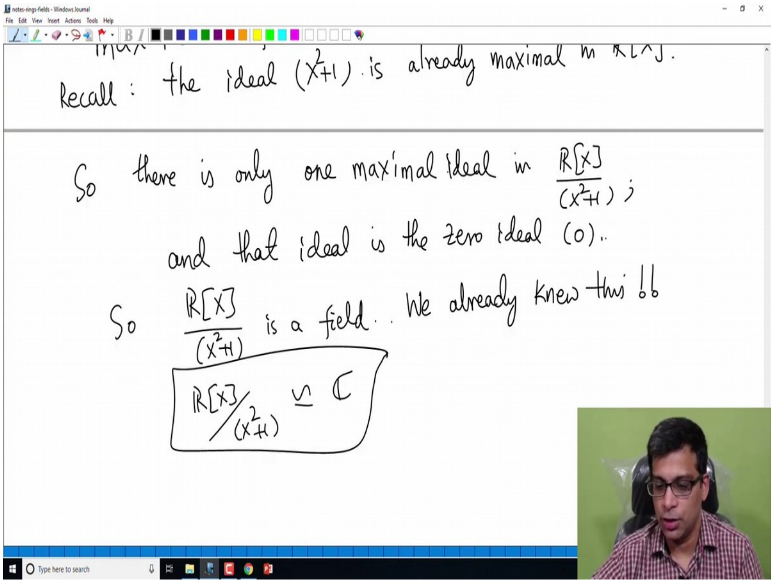



So, what are the maximal ideals of this? As we agreed by the correspondence theorem, max ideals of R come from max ideals this is the ring R; now max ideals of R come from the polynomial ring R X that contain the ideal generated by X squared plus 1.

But now recall this is something I have done at least in two different ways in previous videos, the ideal generated by X squared plus 1 is already maximal, in the polynomial ring in one variable over the real numbers. So, this I have checked in fact, for you so; that means, there is only one ideal that contains X squared plus 1 in R X namely the ideal itself. In fact, there are two ideals that contains X squared plus 1 one is X squared plus 1 the other is R X unit ideal, but there is exactly one ideal which is maximal and which contains X squared plus 1.

So, there is exactly one maximal ideal in R X that contains X squared plus 1, which I used to conclude that there is only one maximal ideal in the quotient ring right. So, I have skipped the step here, the maximal ideals of R X mod X squared plus 1 are in bijective correspondence with maximal ideals of R X that contain X squared plus 1, but there is only one maximal ideal in R X that contains X squared plus 1.

(Refer Side Time: 10:52)

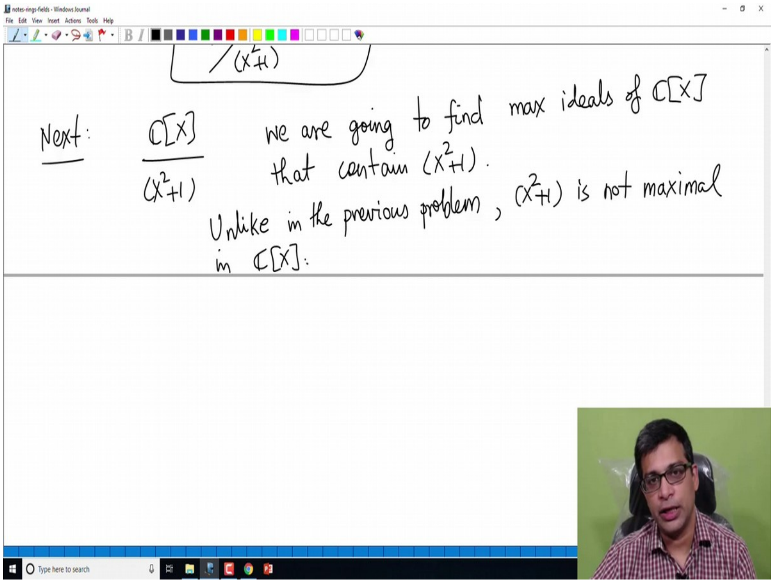



So, there is exactly one maximal ideal in R X mod X squared plus 1 and what is that and that ideal is the zero ideal because, because remember if an ideal maximal ideal of R X contains X squared plus 1, its image under the canonical map from R X to R X mod X squared plus 1 is the maximal ideal of R X mod X squared plus 1. If X squared plus 1 is that maximal ideal its image is the 0 ideal because, the ideal X squared plus 1 gets killed in the quotient ring R X mod X squared plus 1.

So, R X mod X squared plus 1 has a unique maximal ideal and that is 0 ideal, but remember there is a special name for rings that have this property that this zero ideal is a maximal ideal which is that R X mod X squared plus 1 is a field because 0 is a maximal ideal in this; that means, every non zero element is unit so, this is the field.

But in fact, we already knew this, why did we know this? Because R X mod X squared plus 1, when I showed that X plus 1 was a maximal ideal in R X. In fact, I showed that R X mod X squared plus 1 is isomorphic to C as rings or as fields, so there is only zero ideal which is maximal. So, this is easy: maximal ideals of R X mod X squared plus 1 or there is only one and that is zero ideal.

(Refer Side Time: 12:21)



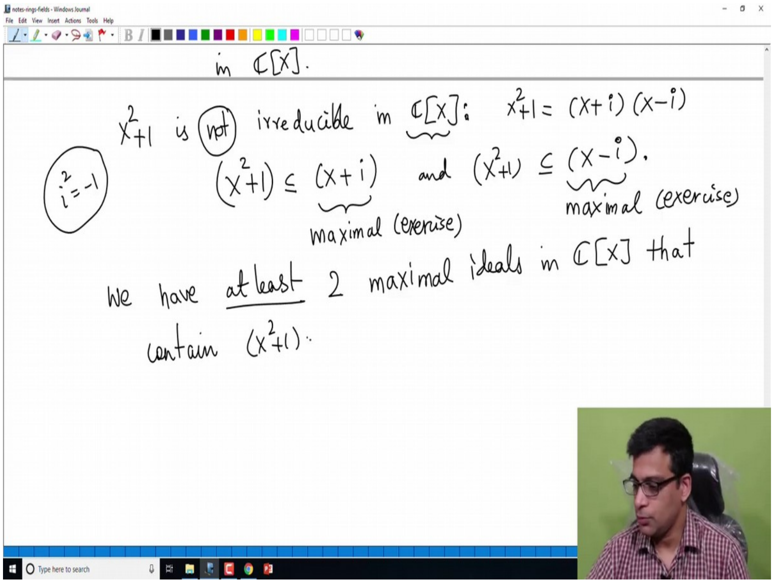

Now, let us look at CX mod X squared plus 1. So, just a final comment about the previous problem R X mod X squared plus 1, what we have concluded is that, the ideal generated by X squared plus 1 in R X is maximal remember this is the fact that I said here. So, X squared plus 1 the ideal is maximal and this is also verified by the fact that I wrote which is that an ideal is maximal if and only if its generator is irreducible.

And we do know that X squared plus 1 is an irreducible polynomial in the polynomial ring R X because a degree two polynomial is irreducible if and only if it has no roots and; the polynomial X square plus 1 has no roots in the field of real numbers. So, its ideal generated by X squared plus 1 is in fact, irreducible. So, the sorry the ideal generated by the irreducible polynomial X squared plus 1 is in fact, maximal.

Now this is no longer the case here. So, to find maximal ideals (Refer Time: 13:35) of the now let us come back to C X mod X squared plus 1 in order to find the maximal ideals of this ring we are in, we are going to find max ideals C X that contain ok. So, now, we are interested in finding ideals maximal ideals of C X that contain the polynomial X squared plus 1. So, containing the polynomial X squared plus 1 is equivalent to containing the ideal generated by the polynomial X squared plus 1. Now immediately unlike in the previous case we see that.

Unlike in the previous problem when we were dealing with the real numbers this is not maximal I claim this is not maximal in C X and the reason is every ideal in CX remember by our general fact is principal. And it is irreducible if and only if that generator is actually irreducible, it is a principle ideal generated by a polynomial is prime or maximal rather if and only if f is irreducible.

(Refer Side Time: 14:59)

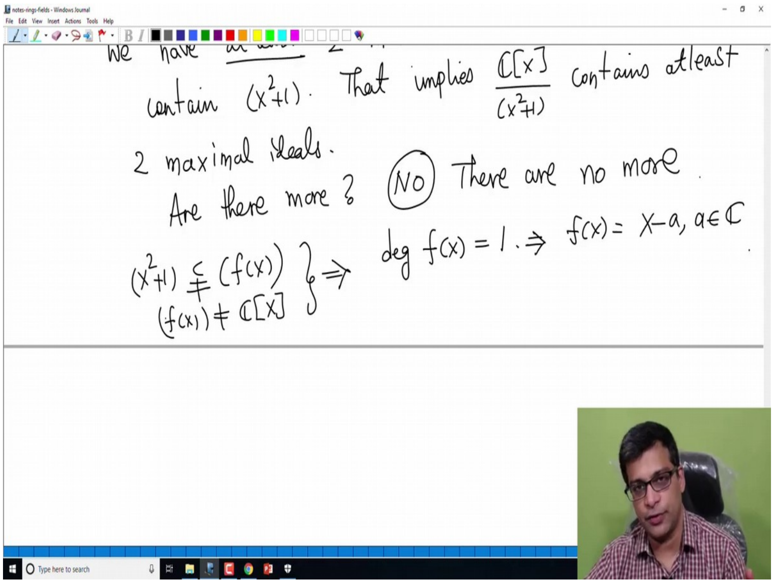



Now, the point is X squared plus 1 is not irreducible in C X; this is the difference between real numbers and complex numbers. Why is it not different; why is it not irreducible? That is because, now, it can factor as X plus i times X minus i, where of course, i is a square root of minus 1 as always. Remember i is not available in the real numbers. So, we cannot factor X squared plus 1 in R X; however, you can factor it in complex numbers. So, C X in C X, X squared plus 1 has two factors so it is not irreducible. So, immediately if you see from the previous the exercise that I left for you see that the argument that is exercise I will see that, the ideal generated by X plus X squared plus 1 is contained in X squared X plus i and also X minus i.

So, there it is you see that it is not maximal because, it is contained in a bigger ideal which is a proper ideal X plus i is strictly bigger than X squared plus the one ideals and X plus i is. In fact, not equal to the full ring CX because lots of polynomials are not there for example, the element one is not there. So, this confirms that X squared plus 1 is not irreducible. So, there are at least two maximal ideals in C X and also I should remember I should mention that, though X squared plus 1 is not maximal, this is maximal, this is also maximal. So, this I will leave for you as an exercise.

Again using the fact that I told you which was in fact, an exercise is that a principal ideal generated by a polynomial f is maximal if and only if the polynomial is irreducible. Here the ideal is generated by X plus i and X plus i is in fact, an irreducible polynomial you can clearly check that it is a degree one polynomial, you cannot possibly factor it as a product of two positive degree polynomials. So, this is irreducible X minus i is irreducible, so that ideal generated by them are maximal. So, we have at least at this point we can only say this at least two maximal ideals in C X that contain X squared plus 1.

(Refer Side Time: 17:41)

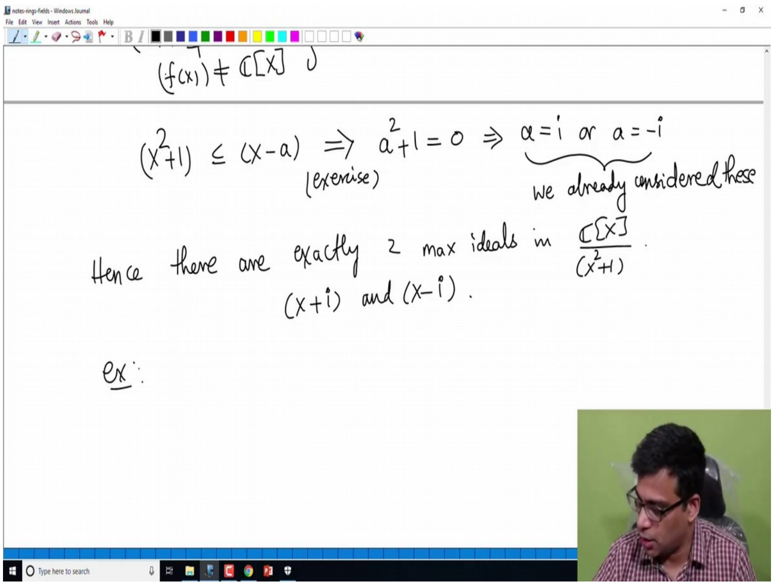



But now; that means, that implies by correspondence theorem CX mod X squared plus 1 contains at least 2 maximal ideals. Now the question is: are there any others, are there more? So, you have at least two maximal ideals unlike the ring R X mod X squared plus 1 which has a unique maximal ideal. The ring C X mod X squared plus 1 has at least 2 maximal ideals, are there more? So, if there are more, you will have you will have a maximal ideal generated by a single polynomial f X which is irreducible in CX and the ideal generated by f X contains the ideal generated by X squared plus 1.

So, now I will leave this is an exercise to show that there are no more. And the reason is if X squared plus 1 is contained in the ideal generated by f X and it is not equal to f X and let us say f X is also not equal to the full ring it is not the unit ideal; if these two facts hold; that means, that degree of f is exactly equal to 1. Because if it is two it must be equal to X squared plus 1, if it is 0 it must equal the unit ideal. So, it cannot be more than

2, it cannot be more than 2 and it cannot be 0, so it cannot it has to be 1. But if it is one then f X must be of the form X minus a belonging to C. But once that happens you can assume that f is monic because, you can always clear divide multiply by the inverse of the leading coefficient and assume that f X is monic.

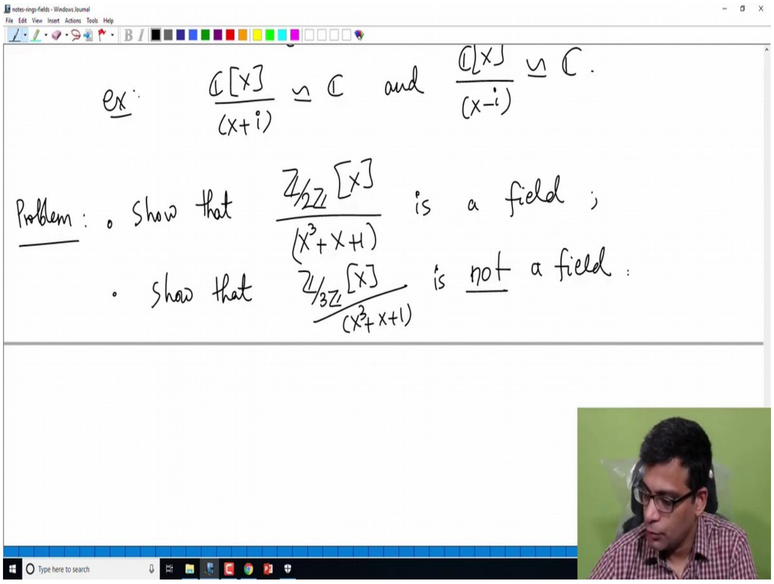
(Refer Side Time: 19:58)




So, f X is X minus a, but then if X squared plus 1 is contained in X minus a, this implies that a squared plus 1 is 0. So, this little fact is an exercise for you; because X squared plus 1 is belongs to X minus a; that means, X squared plus 1 is X minus a times something. Now you plug-in minus plug-in a in both sides, you will get that a squared plus 1 is equal to 0, but; that means, a is equal to i or a is equal to minus i. So, this is now only possibilities remember that we already considered X plus i and X minus i, this we have already considered.

So in fact, there are exactly 2 maximal ideals, in C X mod X squared plus 1. Hence there are exactly 2 ideal 2 maximal ideals, in C X mod X squared plus 1. And I will leave this there, X plus i and X minus i.

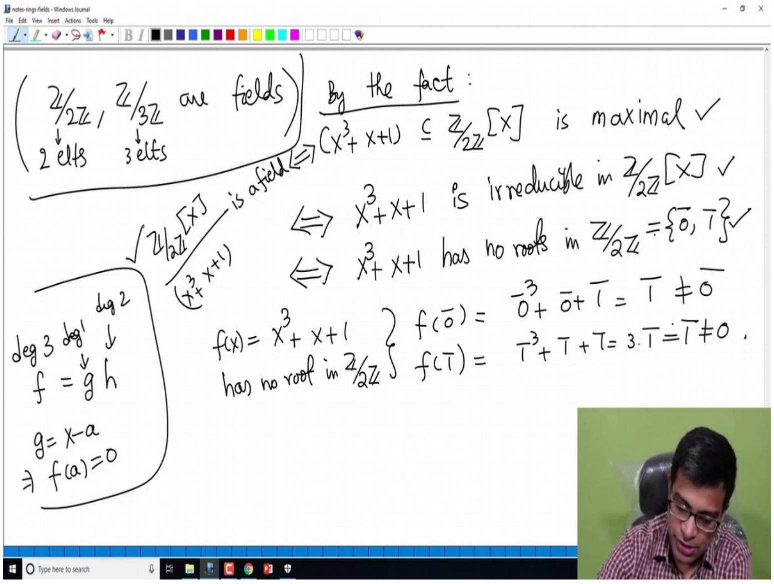
(Refer Side Time: 21:14)




And now I will leave a final exercise regarding this problem for you, we know that because X plus i is a maximal ideal CX mod X plus i is isomorphic to a field what field is that? In fact, that is just isomorphic to C and similarly C X mod X minus i is also isomorphic to C. This you can use first isomorphism theorem define a function from C X to C by evaluating a polynomial at i. So, f X goes to f of i show that its a surjective homomorphism with kernel being X minus i or X minus i. So, you have to consider two different homomorphisms. So, this is an exercise for you. So, this finishes the problem where we were computing maximal ideals of various rings ok.

So, now I will do one more problem here I have lost track of the number, but it is a different problem, similar to the previous problem which is that show that, Z mod 2Z X divided by or quotient X cubed plus X plus 1 is a field. And second part is to show that Z mod 3Z X by the same polynomial is not a field ok.

(Refer Side Time: 23:06)




So, the question is to show that, I consider two polynomial rings 1 over Z mod 2Z that is remember a ring which is. In fact, a field Z mod 2Z and Z mod 3Z are fields containing this has 2 elements this has 3 elements. The fields containing 2 and 3 elements respectively. So, I take a polynomial ring over those fields, consider the ideals to be X cubed plus X plus 1 and look at the quotient ring; in one case it happens to be a field in the other case it does not form a field. So, why is that?

By the fact that I wrote at the beginning of this video, X cubed plus X plus 1 first consider the field case Z mod 2Z X. So, X cubed plus X plus 1 in Z mod 2Z bracket X is maximal. So, I will write, so this is not by the fact so, let us leave this as side. So, what I will do is Z mod 2Z mod X cubed plus X plus 1 is a field if and only if. So, this is confusing I am not organising this properly, but hopefully its not confusing Z mod 2Z X mod X cubed plus X plus 1 is a field this is what remember we are trying to show.

This is what we want to show, it is equivalent to X cubed plus X plus 1 being a maximal ideal in Z mod 2Z X. This is an equivalent definition of a maximal ideal an ideal I in a ring R is maximal if and only if R mod I is a field. So, this is a field if and only if this is a maximal ideal in this. Now by the fact this is this implication is at by the fact X this is a maximal ideal if and only if X cubed plus X plus 1 is irreducible in Z mod 2Z X.

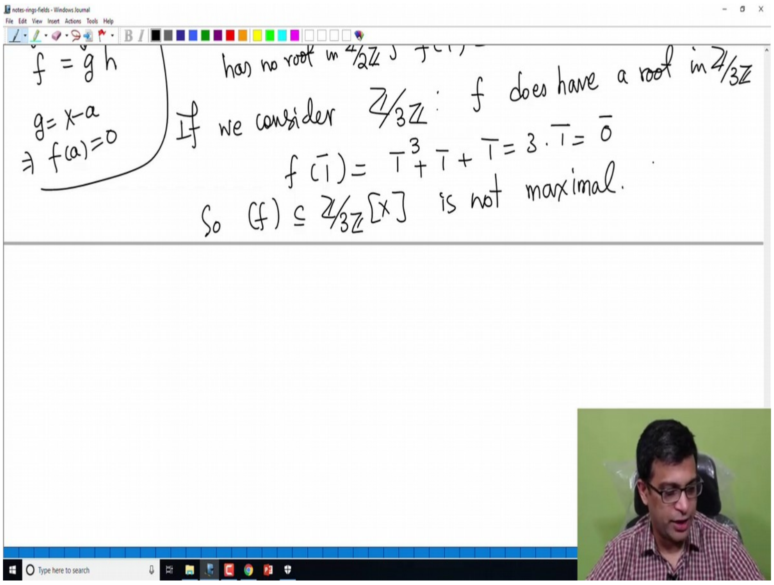
Remember an ideal generated by a polynomial f X in k X, where K is a field, that is important, is maximal if and only if that generator is irreducible. Because it is a degree 3 polynomial, a degree 3 polynomial is irreducible if and only if X cubed plus X plus 1 has no roots; this may be I mentioned before in Z mod 2Z remember you have a polynomial f which is degree 3 how can it fail to be irreducible? Remember a degree 3 polynomial in order to be not irreducible it must factor as two polynomials product of two polynomials g and h. But because degree is 3 of f degree of f is 3, the sum of degree of g plus degree of h is 3 and they are both supposed to be strictly less than 3.

That means, they have, one of them has to be degree 1, the other has to be degree 2 right. This is the only possible breakup of the degrees, because if either of them is degree 3 then it cannot be a valid factorization. For it to be valid factorization both of them have to have degree strictly smaller than degree of f which is 3. So, you have two numbers whose which are strictly less than 3 which add up to 3 positive numbers of course, they are both 1 and 2.

But a degree one polynomial is really of the form, if g is degree one then g must be of the form X minus a. But if X minus a divides f; f of a is 0; that means, f has a root, a is a root of f. So, if the polynomial in question has no roots, it cannot factor, this is only true for degree 3 or 2. So, here a degree 3, so it has no roots if and only if it is irreducible, but whether it has a root or not is easy to check because Z mod 2Z, remember has only 2 elements ok

Let us plug in; let us plug in both of them and see if they are possibly roots. So, X cubed plus X plus 1, let us call it f X for a simplicity, then what is f of 0 bar this is 0 bar cubed 0 bar plus 1 bar which is 1 bar not 0 bar. So, f of 1 bar is 1 bar cubed plus 1 bar plus 1 bar which is one 3 times, 1 bar which is actually equal to 1 bar, which is not 0. So, we conclude that neither of the 2 elements, in Z mod 2Z is a root of f x, so f has no root in Z mod 2Z; that means, this statement is true; that means, this statement is true; that means, this statement is true; that means, this statement is true which is exactly the first problem.

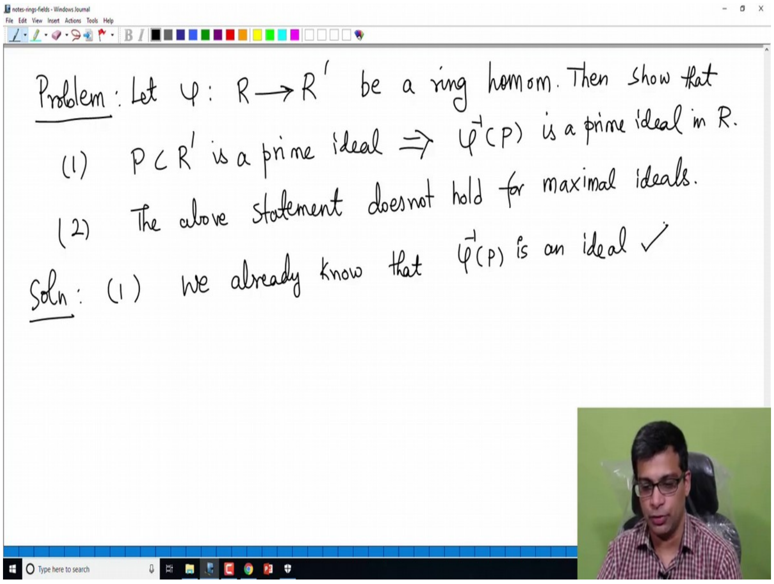
(Refer Side Time: 28:17)




Now, if we consider the other field, Z mod 3Z, we have to essentially consider the same set of equivalences. Z mod 3Z X mod X cubed plus X plus 1 remember the same polynomial is a field if and only if this is a maximal if and only if this is irreducible if and only if this has no roots. But f does have a root, in Z mod 3Z. For example, if you take f of 1 bar it will now happen to be 1 bar cubed plus 1 bar plus 1 bar which is 3 times 1 bar, but 3 times 1 bar is 0 bar in Z mod 3Z, so f has a root in Z mod 3Z.

So, the ideal generate by f in Z mod 3Z X, is not maximal hence Z mod 3Z mod X cubed plus 1 X cubed plus X plus 1 is not a field. So, we have solved both the problems. So, you can see that if you change the coefficients the field where coefficients of (Refer Time: 29:29) come from ideals behave very differently: in one it is maximal, in the other it is not maximal ok.

(Refer Side Time: 29:41)



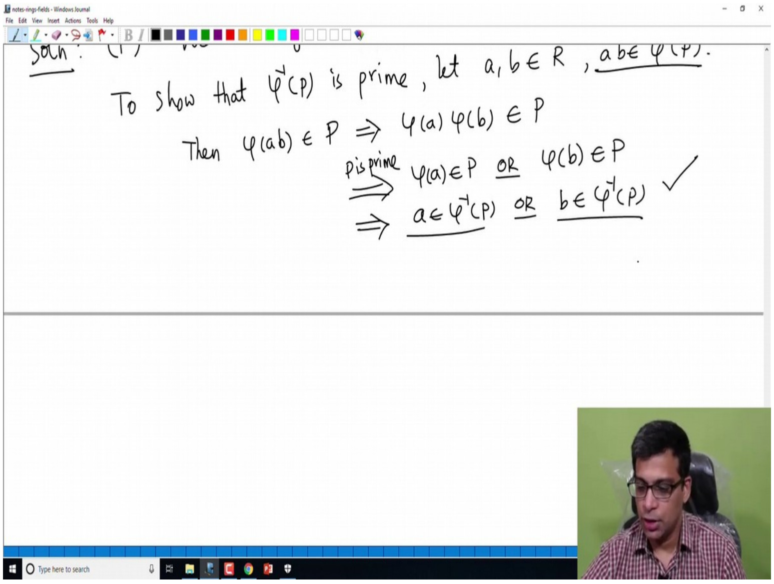

So, let me end this video now with the final problem; this is useful it is a simple problem also, but I might use this fact later. So, this is also about prime and maximal ideals. So, let me state this, I will quickly write the problem and tell you how to solve it, may be leave the details for you.

Let us say phi from R to R prime is a ring homomorphism ok, this is a ring homomorphism. So, I will write a long series of statements, then show that if P is prime in R prime is a prime ideal implies phi inverse P is a prime ideal in R this is the first problem. You take a prime ideal take its inverse image it is a prime ideal. 2 the above statement does not hold for maximal ideals.

In this problem I am only considering inverse images of primes or inverse images of maximal ideals. And I am claiming that if you take the inverse image of a prime ideal, it happens to be prime, inverse image of a maximal ideal cannot be is in general not maximal, it maybe maximal, but in general it need not be. So, let us do this first part we already know that phi inverse P is an ideal; see in order to prove that phi inverse P is a prime ideal we first need to show that it is an ideal, but that we have shown before. Inverse image of an ideal under a ring homomorphism is an ideal, this is easy to check.

Remember things are different when you are talking about the image of an ideal, in general image of an ideal is not an ideal, you need the homomorphism to be surjective. But there is no such problem for inverse image under a ring homomorphism, inverse image of an ideal is always an ideal. Now all we need to do, is so far we have only used that P is prime P is an ideal phi inverse P is an ideal.

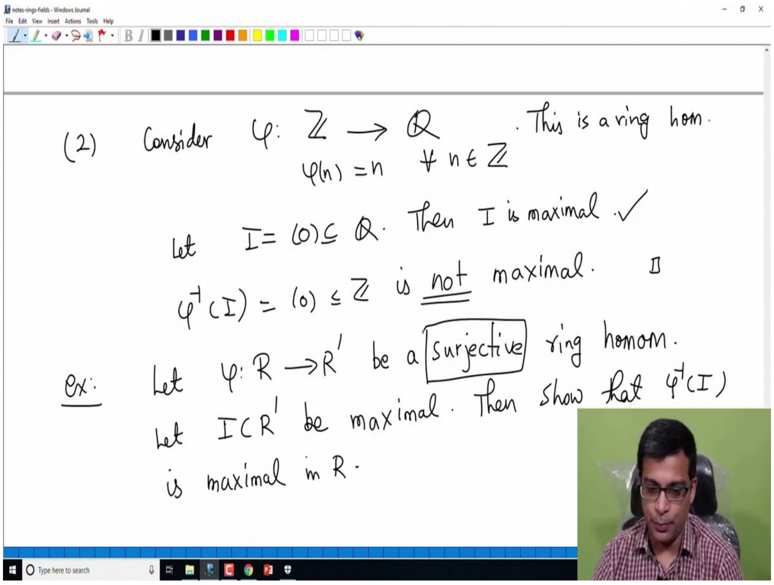
(Refer Side Time: 32:11)




Now, we need to use the fact that P is prime to show that phi inverse P is also prime. So, to show that phi inverse P is prime what do we need to show? Let a comma b be elements of R and suppose that a b is in phi inverse P; because as I said this is a fairly straightforward verification. So, what is a prime ideal? It is an ideal such that if a product belongs to the ideal one of the elements must belong to the ideal. So, let us check two ring elements whose product using phi inverse P. Then phi of a b is in P by definition a b is in the inverse image means phi of a b is in P.

Then phi of a times phi of b is in P because phi is a ring homomorphism phi of a b is equal to phi of a times phi of b. Now because P is prime phi of a is in P or phi of b is in P because, P is prime that is hypothesis. But that means, a is in phi inverse P or b is phi inverse P, as required right. I started with the product that is in phi inverse P and I have concluded that one of them must be in phi inverse P. So, this is a easy straightforward, just the definition.

(Refer Side Time: 33:34)

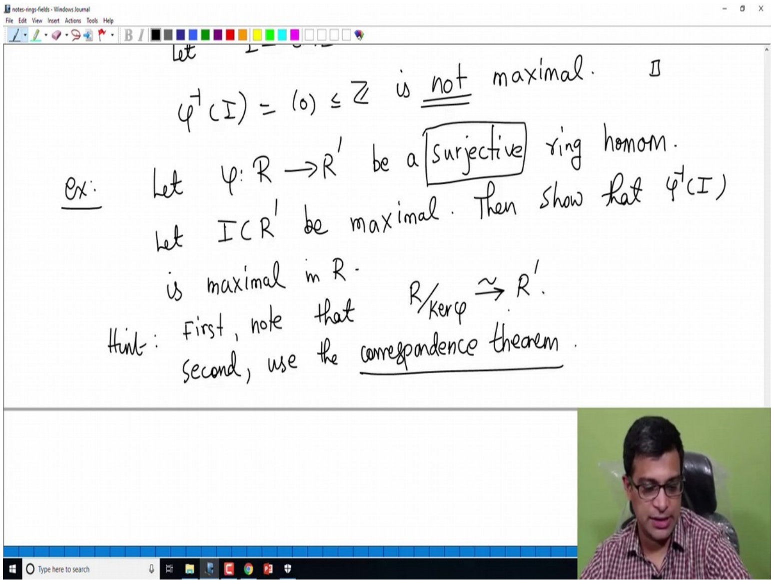



Now, why do I say that, the second statement does not hold, the same statement does not hold form maximal ideals. So, consider, phi from Z to Q; phi from Z to Q. So, this is just the inclusion map, phi of n to be n for all let us say phi of r equal to phi of r, phi of r equal to r for I should really write n sorry is n for all n in Z. So, this is just Z sitting inside Q take an integer and send it to itself; this is a ring homomorphism of course, Z and Q are rings and this is certainly a ring homomorphism.

Now, what is a maximal ideal of Q? Let I be the zero ideal in Q then, I is of course, maximal ideal of course, it is maximal. And what is phi inverse I? Because phi is an injective map, phi inverse 0 is just 0 again and of course, it is an ideal as I told you, inverse image of ideals is ideal is an ideal, but it is not maximal, ok. So, you have a maximal ideal 0 in Q, but when you pull it back to Z, you still get the zero ideal in Z now, but it is not maximal. So, in general inverse image of a maximal ideal is not maximal.

So, this completes the problem, but let me give you an exercise, suppose phi from R to R prime is a surjective ring homomorphism. Suppose this is a surjective ring homomorphism and let I be maximal in R prime then show that phi inverse I is maximal in R. So, the idea is the statement I just disproved in general that inverse image of a maximal ideal is not in general a maximal ideal. In fact, becomes true if you add a condition that the ring homomorphism is surjective ok, that is important if that happens it is true. Of course, the example from Z to Q is not surjective, there are lots of elements in rational numbers which are not in the image, any rational number that is not an integer is not in the image.

(Refer Side Time: 36:21)




So, why is this true? This exercise, the hint is actually just to use two facts; first note that, R prime is isomorphic to, in fact, I will write it like this R mod kernel phi is isomorphic to R prime right. Because it is a surjective map and first isomorphism theorem says that R mod the kernel is isomorphic to R prime. Second use the correspondence theorem or this straightly stronger correspondence theorem that I stated, at the end of the previous video. The correspondence theorem says that ideals in R mod I are in bijective to correspondence with I in ideals in R containing I.

But that you can put adjectives to these statements, prime ideals on both sides or maximal ideals also on both sides and the correspondence theorem still holds. Use that second the more stronger version of correspondence theorem for maximal ideals, to do that because if you take a maximal ideal in R prime and its inverse image will be maximal because it just corresponds to an ideal in R that contains kernel phi ok. So, this last exercise that I did today is very easy, but it is important for us we will often use in future that inverse image of a prime ideal is prime for any ring homomorphism. This statement is not true in general for maximal ideals, but if the ring homomorphism is surjective the statement is true, inverse image of a maximal ideal is maximal.

So, far in the last few videos, we learned about prime ideals and maximals ideals in rings and we did a number of exercises. So, hopefully you have got some understanding of how to work with prime and maximal ideals in rings. So, in the next video we will start talking about fields, fields of fractions of integral domains, unique factorization domains and principal ideal domains.

Thank you.