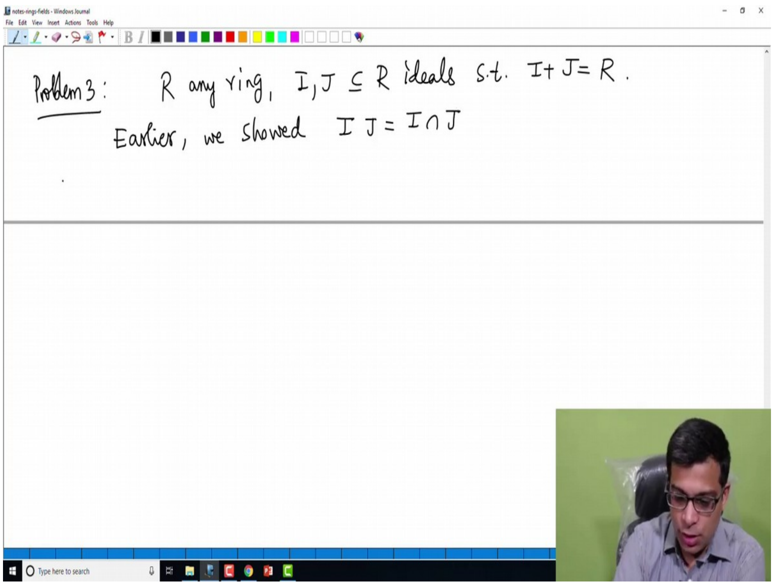
Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture – 18
Problems 5

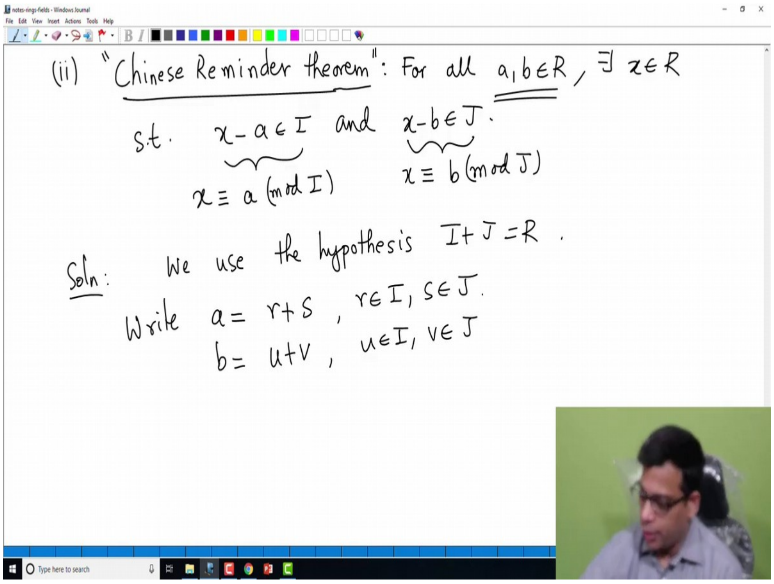
Let us continue now. In the last video, we have started doing some problems on the material that we have covered so far about rings, ideals, maximal ideals and so on. So, I ended the last video with the problem about. So, let us think, this is a 2nd problem may be or 3rd problem, 3rd problem and we have done the first part.

(Refer Slide Time: 00:37)



So, recall for problem 3, the assumption was R any ring; R any ring I J two ideals such that; such that, s.t. stands for such that, I J is equal to R. We have shown that earlier in the last video, we showed the product is equal to the intersection.

(Refer Slide Time: 01:16)



Now, the second part. So, let me write it in the different slide, second part is an important, it was a, it is a famous result in mathematics called "Chinese reminder theorem". So, it this name and what does it say. So, second part is to show that for all a comma b in R, for all elements for any pair of elements a comma b in R, there exists I will write it as a theorem, there exists x in R. The given two elements a comma b in R, there exists in element x in R such that x minus a is in I and x minus b is in J.

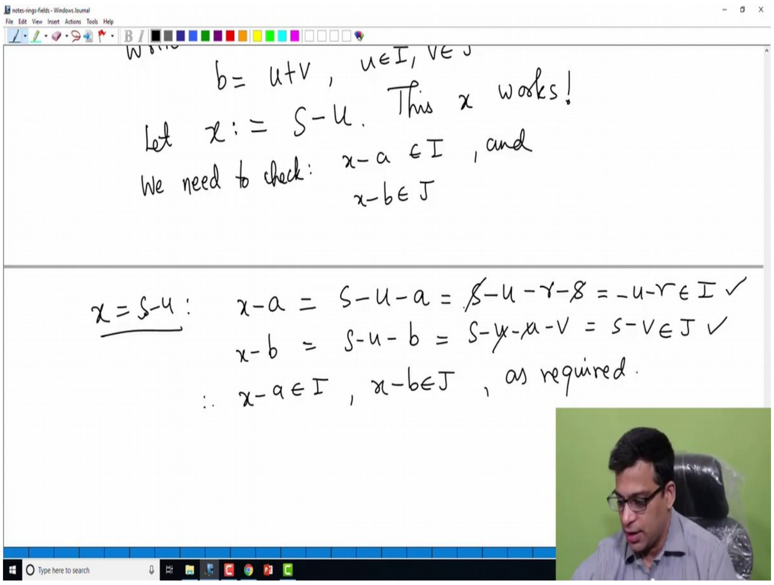
So, you understand what I am saying? Given two elements of R there is a single element R which when you subtract a, it is in I and from the same element when you subtract b it is in J. So, for those of you who know a little bit about mod language using residues and module, modulos of ideals, this is same as saying that x is a modulo I, x is congruent to a mod I. This says that x is congruent to b mod J ok.

This is just notation if you are not familiar with it, do not worry about it. All I am saying is that there is a single element x which is like a in some sense in the quotient ring R mod I because x minus a is like a x is like a, x minus a is 0 modulo I. So, x is same as a mod I, x is same as b mod J given any two elements we can do this.

The solution or the proof is the following. Again we use the hypothesis, remember the hypothesis that I plus J is equal to R was made and this is very crucial, we use that hypothesis I plus J is equal to R. So, remember I plus J is equal to R means every element of R can be written as the sum of an element of I and an element of J.

So, in particular we can apply these to r a. So, write a is equal to r plus s b is equal to u plus v. So, a is an element of R given element remember a and b are given in R. I write a as r plus s b as u plus v and what you know about r, it is in I s is in J, similarly u is in I v is in J. So, that is the point, every element of the ring R can be written as something in I plus something in J. So, I write a as r plus s, b as u plus v.

(Refer Slide Time: 04:18)



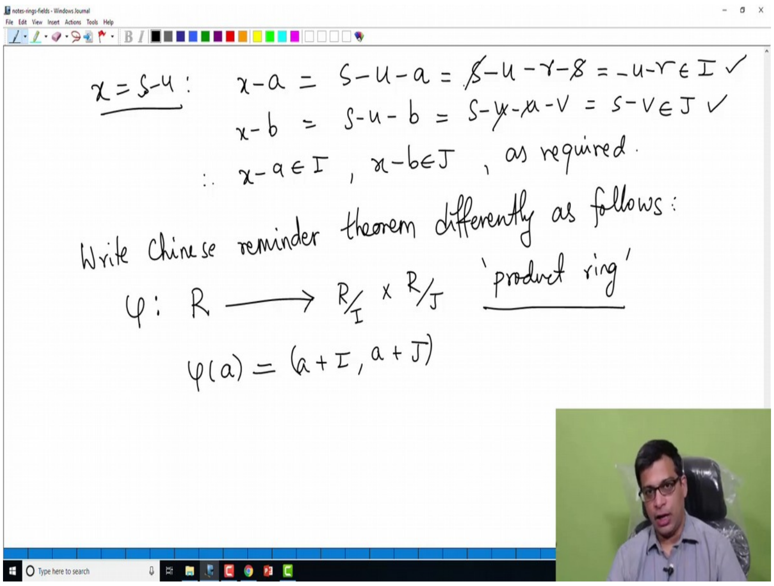
And now I claim that now I will tell you how to choose x. So, let us choose x to be let, I am defining x to be s minus u ok. So, I claim that this x works, what is it mean? Remember the theorem is asking us to show that there is an x with certain properties; I have chosen that x and I am going to show that x has the required properties, what are the required properties? We need to check that they are on the notes here. So, we need to check x minus a is in I and x minus b is in J. So, let us check these things, two things.

So, x minus a, x is s minus u; this remember that is my choice for x. So, x minus a is s minus u minus a, but what is r sorry, what is a? a is r plus s. So, s minus u minus a is s minus u minus r minus s, correct. So, s minus u minus r minus s of course, I can cancel this. So, there is minus u minus r, but u and r are both in I, r is in I u is in I. So, this is also in I if you have u and r in I minus u is in I minus r is in I there difference is in I. So, x minus a is in I as we are required to show.

Now, what is x minus b? X minus b is s minus u minus b and b is u plus v. So, s minus u minus b is s minus u minus u minus v this is now I cancel u, this is s minus v. Now, where are s and v? s and v are in J so, this is in J. So, x is in I and x is in J. So, sorry x minus I is in a and x minus b is in J sorry x minus I is in I, x minus b is in J, as required ok. So, this require these this may seem like how did I think of x to be this, but that is just by playing with the required conditions, it is not difficult to see that x minus x equal to s minus u works.

So, this is the Chinese reminder theorem. So, so solution is complete; you may have seen Chinese reminder theorem in the case of integers. So, this is the generalization of that to arbitrary rings. So, I want to now rephrase the statement of Chinese reminder theorem in a more conceptual manner.

(Refer Slide Time: 07:05)

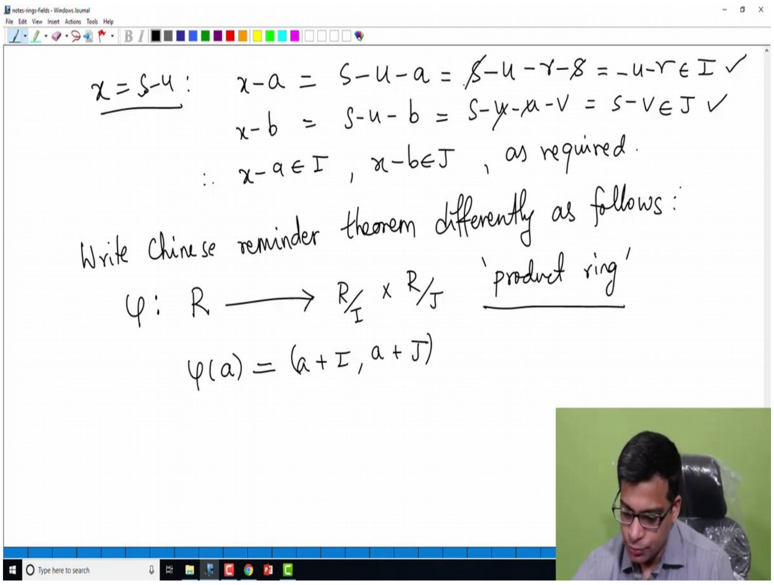


So, I want to write Chinese reminder theorem, not the proof but the statement, Chinese reminder theorem, differently as follows ok. So, now this is what I want to do. So, consider quotient ring R mod I and R mod J and the product ring, this is the product ring. I believe I mentioned product rings before, but otherwise it is not difficult to see what the operations are here, if you have two rings you take the Cartesian product.

So, elements are just pairs of elements one from the first ring, the other from second coordinate is from the second ring and multiplication and addition happen coordinate wise. So, the 0 element is (0, 0), multiplicative identity is (1,1) and if you have (a, b) times (c, d) you have (ab, ac bd) ok. So, this is easily seen to be a ring.

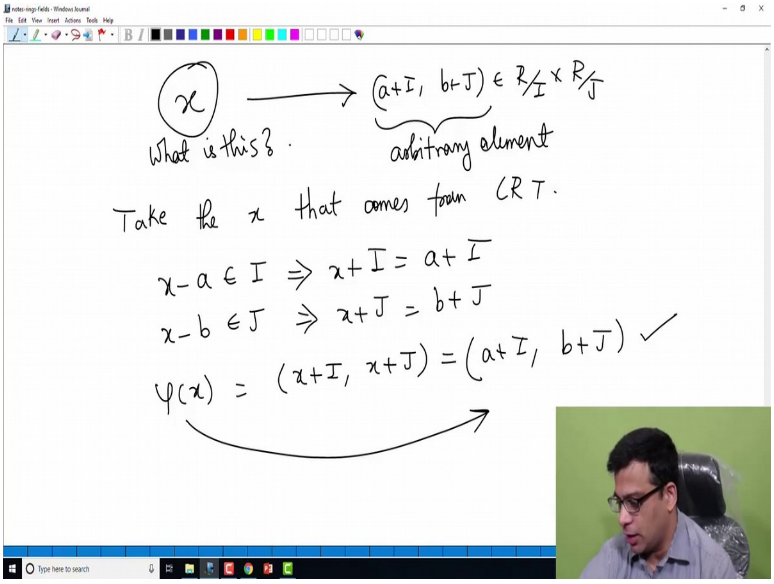
So, take the product ring and I will define a homomorphism from R to the product ring, I define phi of a to be a plus I comma b plus J sorry a plus J. So, write Chinese reminder theorem differently as follows. So, first of all, I am defining a set map R to R cross I, R mod I cross R mod J where I send a ring element to a the residues of that ring element in R mod I and R mod J.

(Refer Slide Time: 08:55)



And it is an exercise which I will not do and I will ask you to do, this is a very easy exercise, it is that phi is a ring homomorphism. Now, Chinese reminder theorem is a very nice formulation which is easy to remember in terms of this homomorphism. Chinese reminder theorem, let us call this CRT. So, CRT it is a standard abbreviation for Chinese reminder theorem, it says that the above map is surjective, the above map is surjective which is not clear a priori, because you are taking the map from R to R mod I cross R mod J with sends a to a plus I comma a plus J is the same element.

(Refer Slide Time: 09:58)



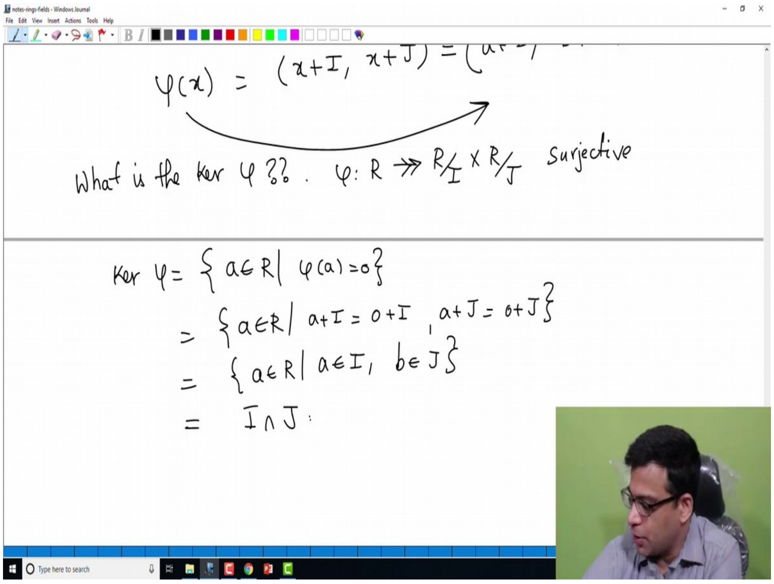
In general, to be surjective, you take an arbitrary element of the product right. So, this is an R mod I cross R mod J. In order to be surjective there must be an element x which maps to that, what is this x? Right in order for a map to be surjective take any element in the range, the co-domain ring in this case R mod I cross R mod J, every element is in the range. So, a plus I comma b plus J must be an element in the image; that means, it must come from x, some x.

And Chinese reminder is theorem is telling you that x, what that x is, take the x that comes from Chinese reminder theorem. Now, what is the property of that x? X minus a is in I, but if x minus a is in I, I claim that x plus I is equal to a plus I. If x minus a is in I in the quotient ring R mod I, x and a are basically same elements the residue of x is same as residue of I.

Similarly, x minus b is in J by the Chinese reminder theorem; that means x plus J is b plus J. Now, what is phi of x? Phi of x is x plus I comma x plus J, by definition any element was so, that element plus I, that element plus J; that means, it goes x goes to plus I, x plus J but I just proved that x plus a is a plus I and x plus J is b plus J ok. So, every element you start with an arbitrary element, this is an arbitrary element of the product ring. Take an arbitrary element and I have shown that it has a pre-image, that means it is surjective.

So, it is convenient to remember Chinese reminder theorem as saying that if you have two ideals in a ring I and J whose sum is R, that is whole point here I plus J is R then the map natural map from R to R mod I cross R mod J is a ring is a surjective ring homomorphism.

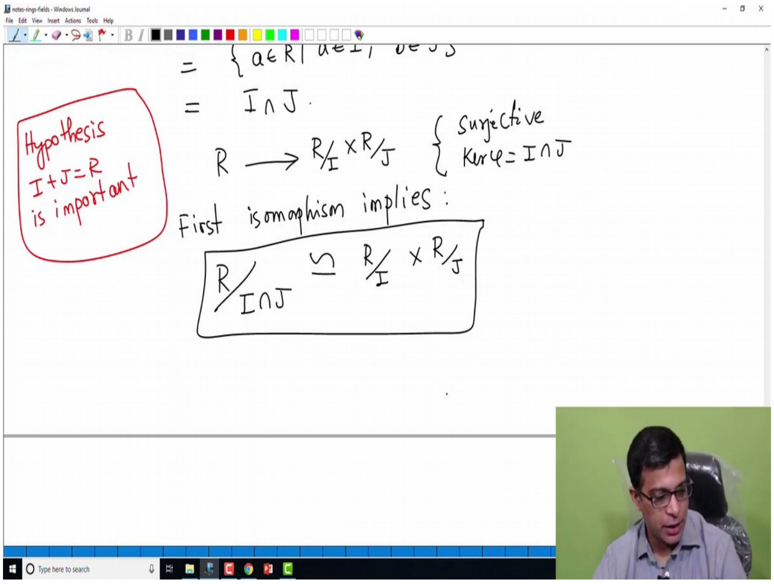
(Refer Slide Time: 12:30)



As this is a bonus question I am going to ask you, what is kernel of phi? Remember, phi is a map from R to R mod I cross R mod J; it is a surjective ring homomorphism by the previous problem.

So, what is the kernel? Remember, kernel of any ring homomorphism is all elements of the ring such that phi a is 0, but in our context; that means, it is all elements a such that a bar a plus I is 0 plus I and a plus J is 0 plus J, but; that means, elements a in R such that a is in I and b is in J because a plus I is equal to 0 plus I means a is in I, a plus J is equal to 0 plus J means b is in J. But what is, there is another name for the set of elements a such that a is in I and b is in J and what is that? That is simply the intersection. So, the kernel is intersection.

(Refer Slide Time: 13:44)

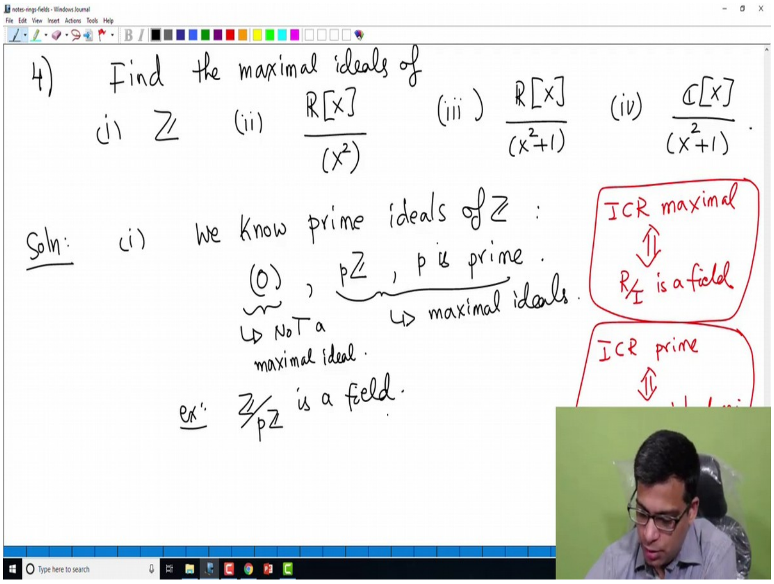


So, we understand now everything about this map R mod I to R to R mod I cross R mod J. So, this is surjective; that means, image is all of R mod I cross R mod J and kernel is I intersection J ok. So, this is a useful problem to keep in mind. And again I will reiterate the crucial hypothesis, hypothesis that I plus J is equal to R is important I and it is a good exercise for you to think of an example, where this map is not surjective and example where I plus J will not be equal to R and this map is not surjective.

Now, what does the First isomorphism theorem say? So, I want to complete the circle of ideas by stating what is the implication of first isomorphism theorem, we have a ring homomorphism which is surjective and this kernel is I intersection J.

So, R mod I intersection J is isomorphic to R mod I cross R mod J. So, this is a very important statement that we will sometimes use if I plus J is equal to R, the quotient ring R mod I intersection J is just the product ring R mod I cross R mod J. So, this is the conclusion of the Chinese reminder theorem in some sense ok. So, now I will continue with the problems.

(Refer Slide Time: 15:30)



So, the next problem I want to do may be the 4 problem is, I want to first list this is may be some of these we have done. Find the maximal ideals; find in some sense the maximal the maximal ideals of the following rings. So, one Z, two the ring R X mod the quotient ring R X mod X squared, the ring R X mod X squared plus 1 and finally, the ring C X mod X squared plus 1 ok. So, there are four rings here, I want to find the maximal ideals of this.

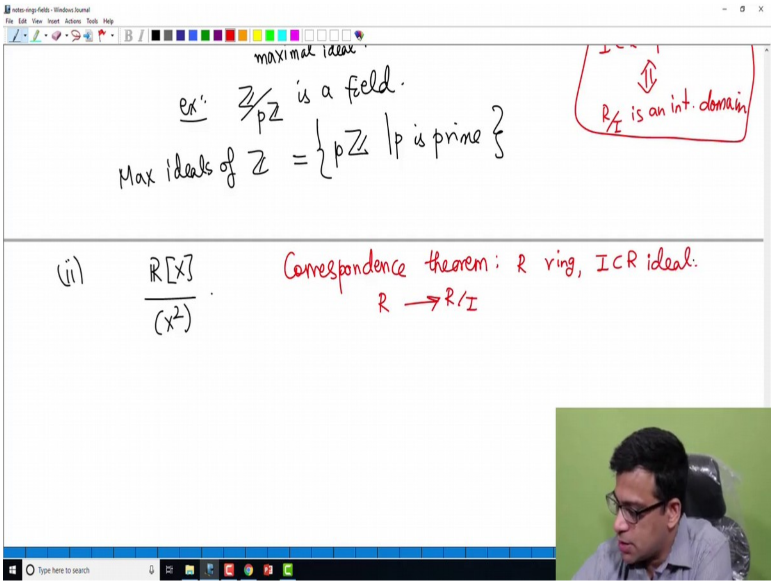
So, the first one is easy, we know prime ideals I may have done said this before, prime ideals of Z are the 0 ideal and pZ, where p is prime. Because, a maximal ideal is automatically prime, the maximal ideals will be among these right if some ideal is not prime, it cannot be maximal.

So, in order to find the maximal ideals of Z, we need to first start with prime ideals and see which of those are maximal ideals. Now, which of these are maximal ideals? Is 0 a maximal ideal? This is not a maximal ideal, why is that? By definition, a maximal ideal is an ideal which is not contained in any proper bigger ideal; 0 is certainly not like that because 0 is contained in 2Z. So, and 2Z is a proper ideal, 0 is properly contained in 2Z. So, 2Z is not the zero ideal.

So, this is not a maximal ideal, what about this? These are maximal ideals. There are several ways of doing this, pZ cannot be contained in a bigger ideal or equivalently, Z mod pZ is a field. So, we have shown that, we recall I in R is maximal if and only if the quotient ring R mod I is a field right and in this context it is also I will recall for you though we do not need this here.

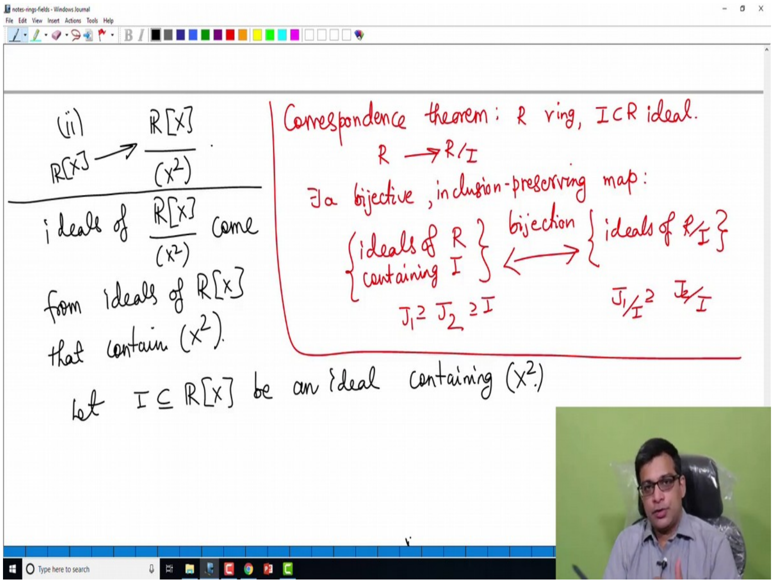
I in R is prime if and only if R mod I is an integral domain. So, to check maximality, we have want to quotient by the ideal and check if it is a field and there is an exercise I have said this a few times before Z mod pZ is a field, you take any non-zero element of Z mod pZ show that it is a multiplicative inverse. So, it is a field.

(Refer Slide Time: 18:37)



So, what are the prime ideals of maximal ideals of Z? So, max ideals of Z; max ideals of Z are pZ, where p is prime. So, any ideal generated by a prime number is a maximal ideal. So, now, let us look at the second one. So, look at R X mod X squared ok.

(Refer Slide Time: 19:44)



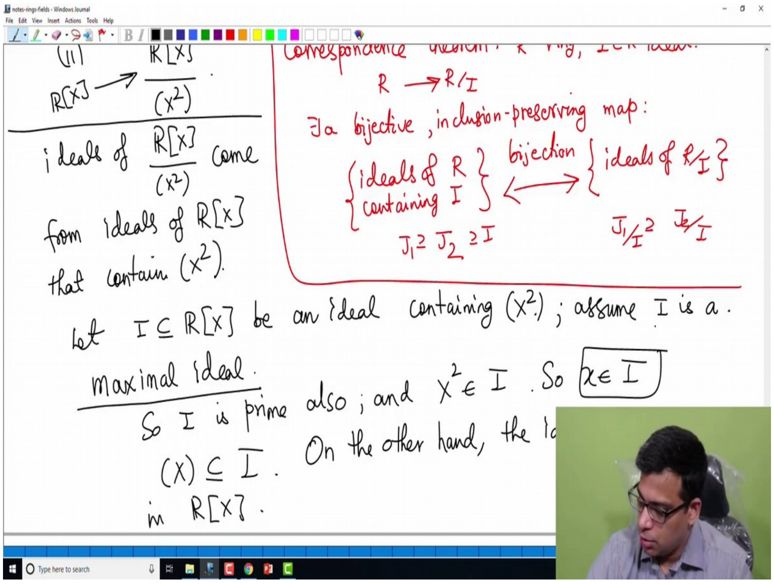
Now, in order to determine the maximal ideals of this, I am going to recall for you the correspondence theorem, what does correspondence theorem say? So, it talks about R and R mod I. So, R is a ring, I is an ideal and what is the statement of the correspondence theorem? It says that there is a bijective and inclusion preserving; you understand what I mean by that right? Map inclusion preserving map means if there is a map between ideals so ideals of R containing I. So, this is a bijection, inclusion preserving bijection from ideals of R containing I to ideals of R mod I.

So, inclusion so there is a bijection we have seen and why is it inclusion preserving? If J1 is a J1 J2 are ideals that contain I and J1 is contained in J1 J2 both contain I in the correspondence, let me write it like this ideals also have a same inclusion. In other words, the inclusion of J1 and J2 is preserved. So, I am going to use this in correspondence theorem.

So, what are ideals of this quotient rings? Are ideals are in bijective correspondence with. So, let me say ideals of this come from ideals of R X that contain X right rather I should say X squared. So, ideals of R X mod X squared come from ideals of R X. So, there is a map from R X to R X mod X squared and ideals in the ring R X mod X squared are actually images of ideals of R X which contain X squared.

So, let I be an ideal containing X squared. Remember, we are actually interested in maximal ideals of R X mod X squared, the fact that this bijection is inclusion preserving means, the bijection also gives a bijection between maximal ideals of R that contain I in the maximal ideals of R mod I. So, this bijection restricts to a bijection of the subset here in this first set of a maximal ideals containing I and it gives a bijection to the maximal ideals of R mod I.

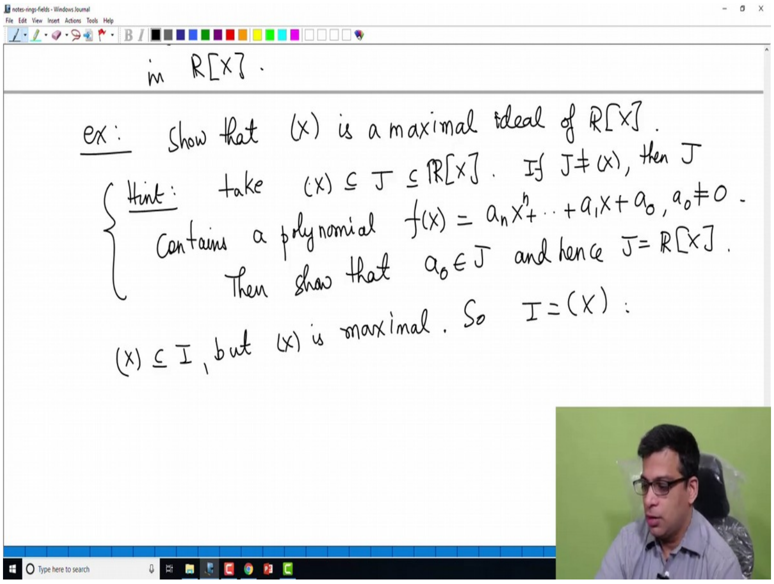
(Refer Slide Time: 22:46)



So, we can further assume that I is actually maximal ideal. So, assume that I is a maximal ideal. So, if I is a maximal ideal containing X squared. So, I is in fact, prime also right, a maximal ideal is prime this we have shown earlier and I is a prime ideal and X squared the ideal X squared is contained in the I means the element X squared is contained in I.

But prime ideals have the property that, if a product belongs to the ideal, one of the elements belongs to ideal; X squared belongs to I means X is in I; that means, the ideal generated by X is in I. Remember, I is an ideal it contains X; that means, it contains the entire ideal generated by X.

(Refer Slide Time: 23:52)

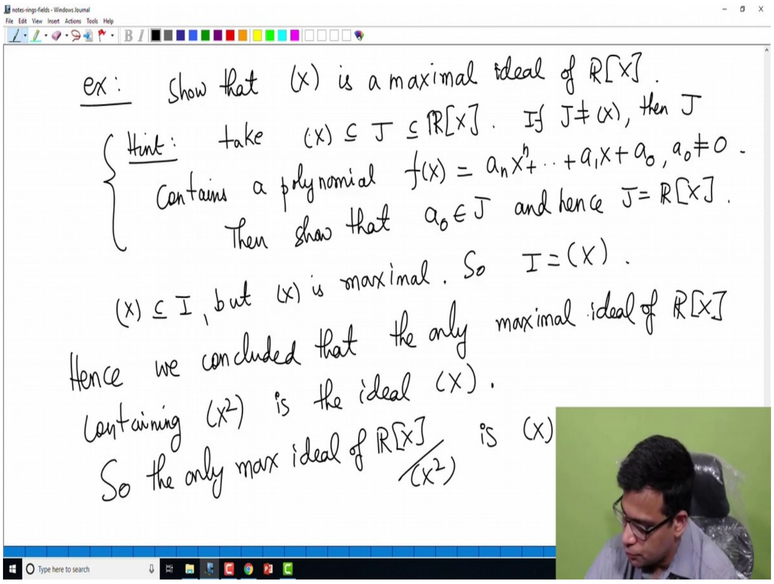


On the other hand, it is an easy exercise for you. The ideal X is maximal in R X. So, I will leave this as an exercise show that is a maximal ideal of, actually this is not quite required for us in any case, I think this is required for us. So, the idea is to show that so, the hint, take some ideal X J contained in X contained in R X ok. So, then and argue that if J is not equal to X then J contains a polynomial, let say f x remember R X is the polynomial ring. So, there is a polynomials in one variable X.

So, J I claim contains a polynomial of the form an X n, an minus 1 X n minus 1 a1 X plus a 0 and a 0 is not 0. So, if J is not equal to ideal X, argue that it must contain an element of this form because if it does not contain an element of this form, it is equal to X and once you argue this then show that a 0 is in J and hence J is equal to R X ok, this is almost a complete hint for you, using this you can show that X is a maximal ideal.

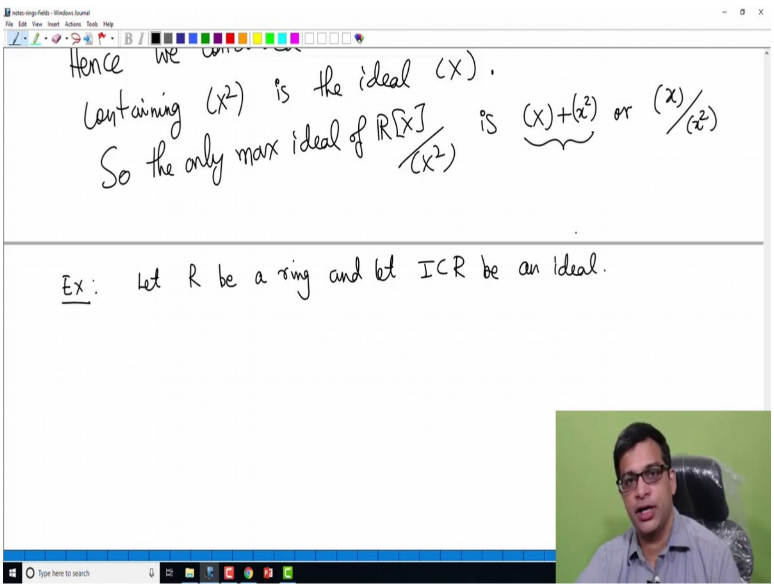
So, now let us go back here. We have shown that the ideal I contains X, but X is maximal. So, remember a maximal ideal if it and I is remember a proper ideal because I is a maximal ideal and maximal ideals are by definition, proper ideals. So, X is a maximal ideal it is contained in I, I is a proper ideal. So, the only possibility is I is equal to X.

(Refer Slide Time: 26:16)



Hence, we have concluded that, the only maximal ideal of R X containing X squared is the ideal ok. So, the only maximal ideal of X contained of R X containing X squared is X which implies by the correspondence theorem. So, the only maximal ideal of R X mod X squared is the ideal X plus I. So, this is my notation for the image under that correspondence.

(Refer Slide Time: 27:12)



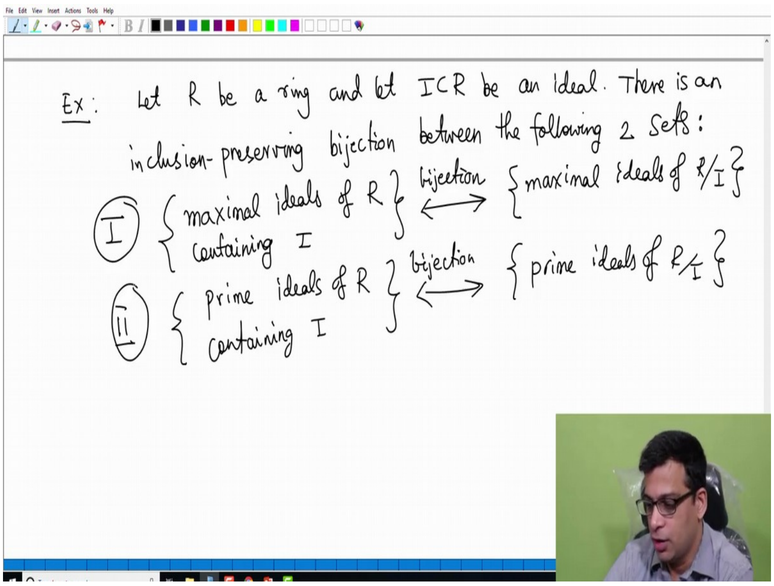
Another equivalent notation is or X mod sorry X plus X squared I should write, this is bad notation, but ok. So, in particular there is exactly one maximal ideal of R X mod X squared and it is given by the ideal X ok. So, this is a bit involved this proof it uses several facts. So, please go over this carefully, repeat this video if you want and make sure that you understand this statement. We interested in finding the maximal ideals of the quotient ring R X mod X squared and we have showed that there is exactly one such in that comes from the ideal X in R X ok.

Now, that leaves two now two more rings. So, I will stop the video now, I will continue the next video with these two examples, what I want you to do before you watch the next video is to recall the proof of R X mod X squared think about it carefully and using that try to solve these two remaining problems.

Similarly, as R X mod X squared, to determine the maximal ideals of R X mod X squared plus 1, you need to figure out the maximal ideals of R X that contain the ideal X squared plus 1. Similarly, to determine the maximal ideals of C X mod X squared plus 1, you need to determine the maximal ideals of C X that contain X squared plus 1 ok.

So, I will leave that calculation for you and I will solve it in the next video. So, I will end this video with an exercise of a statement that we have used, I have said it, but I want to emphasize it. So, I will keep this as an exercise for you to do. So, let R be a ring and let I be an ideal, this is a refined version of the correspondence theorem.

(Refer Slide Time: 29:21) (Refer Slide Time: 29:21)



So, the statement is, there is a, there is an inclusion preserving bijection between the following two sets, there is an inclusion preserving bijection between the following two sets, what are they? Maximal ideals of R containing I. So, these are maximal ideals of R that contain I and on the other side we have maximal ideals of R mod I ok.

So, if you remove the word maximum, maximal in both the sets this is exactly the correspondence theorem, ideals of R containing I are in bijective correspondence with ideals of R mod I, but now I am saying that I can add the adjective maximal and the inclusion preserving bijection still exists.

So, now I might as well write this though we do not need it in the previous problem, there is such a bijection also from prime ideals of R containing I and here also you put prime ideals of R mod I. What we have to do for the first one is easy because maximality is a statement about inclusions, all you need to do is that the original correspondence theorem is an inclusion preserving bijection. So, that gives the statement I.

For the second statement, you have to use a little more ring theory, it says that you take an ideal of R containing J, sorry an ideal of R containing I, suppose it is prime, the corresponding ideal of R mod I is also prime, you want to show and similarly if you take a prime ideal of R mod I, the corresponding of ideal of R containing I which exists by the correspondence theorem is actually prime. So, one you prove right now in order to understand the solution for the exercise here R X mod X squared and use it in the third and fourth exercises. So, which I will come back to in the next video, the statement about prime ideals also we will come back to in the next video and formally prove this statement.

So, please go over these solutions carefully, these are important and subtle statements about rings and ideals and prime ideals and maximal ideals and hopefully you will understand everything that I said after watching it if needed. So, I will stop the video here. In the next video, we will continue with more problems.

Thank you.