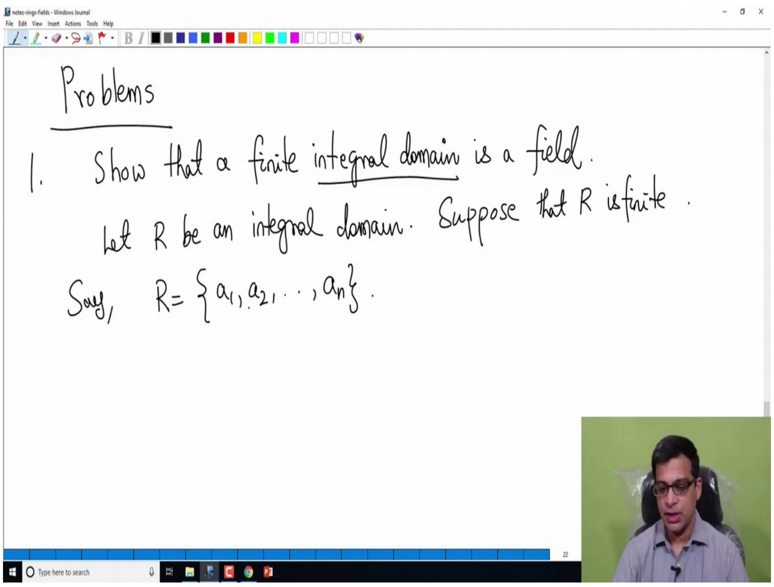
Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture – 17
Problems 4

In the last video, I talked about maximal ideals in a ring. I showed in particular that every commutative ring with unity has a maximal ideal. We used what was called Zorn's lemma for this and as I told you in that video this is an important fact, the proof is not that important. So, if you are unfamiliar with Zorn's lemma, you do not need to worry about it. It is the statement of the theorem which is that every ring contains maximal ideals that we will use in this course.

So, we also talked in the previous video or last two videos about prime ideals. Prime ideals and maximal ideals are important classes of ideals in a ring and we also talked about integral domains; integral domain is a ring where the zero ideal is a prime ideal. So, in this video I am going to do some problems to get familiarized with all these concepts that we are doing in the last few videos. So, this is a video containing problems.

(Refer Slide Time: 01:10)

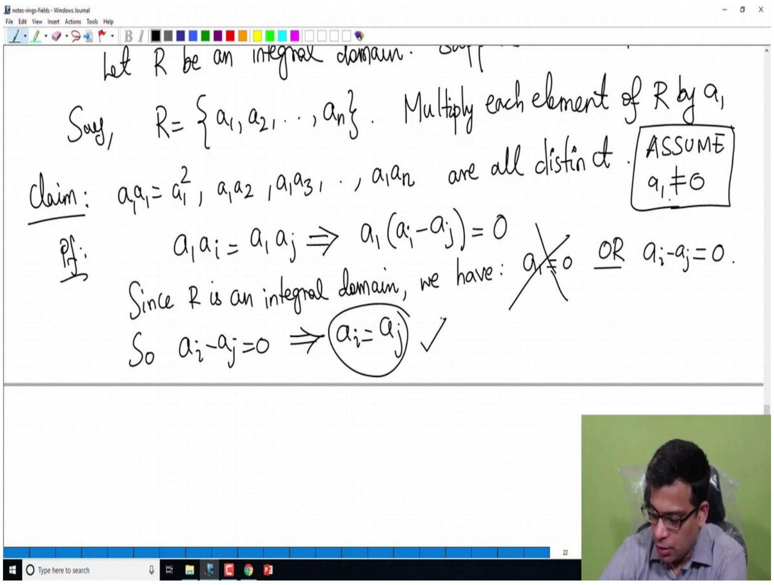


So, the first problem is the following. So, show that a finite integral domain is a field. So, remember that, what is a finite integral domain? You know what integral domain is, it is a ring where the zero ideal is a prime ideal, finite simply means this has only finitely many elements

So, let us do this so let R be an integral domain and suppose that R is finite, so this is the hypothesis. So, in other words R has only finitely many elements. So, let us list these elements, so there let us a call a 1, a 2, a n. So, say R is like this. So, remember this is where the finiteness assumption is critically used, R has only finitely many elements say n of them. So, I will call them a 1, a 2, a n like this.

Now, I will consider the following. So, of course, remember that 1 is an element of R. I am not specifying what 1 is, one could be a 1, 1 could be a 2 and so on. I do not need to know what one is, I am just listening all the elements they are all same to me.

(Refer Slide Time: 02:51)



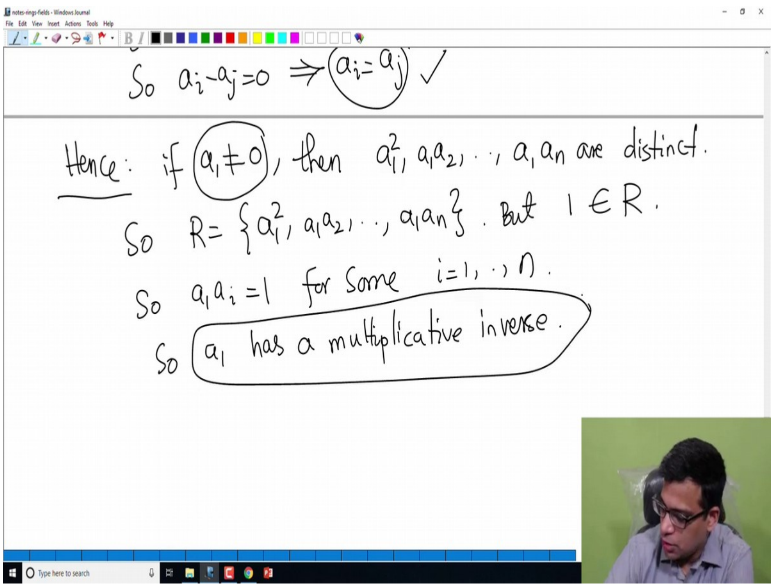
Now, consider, multiply each element of R, let say by a 1. So, what I am doing is, consider a a 1, a 1 a 1 which is a1 squared, a 1 a 2, a 1 a 3, a 1 a n right. So, let us consider these n these elements, I now claim that these are all distinct this is my claim.

So, you choose a 1 multiply a 1 with every element of the ring. I claim they are distinct, why is this? So, let us prove this; this is because suppose they are not distinct may be when you multiply two different elements a i and a j when you multiply with a 1 may become equal that is a possibility. I am saying that it does not happen in integral domain.

So, suppose a 1 a i is equal to a1 a j for suppose this happens, if a1 a i is equal to a1 a j. I claim that this implies by usual ring theory ring properties this is a1 times a1 minus a j right, I am taking a 1 a j to the one side. Factoring a 1 from each term and writing a 1 equals a a i minus a 1 times a i minus a j is equal to 0. But now since R is an integral domain. Remember, R is an integral domain we know that one of the equivalent properties of an integral domain is that if you have two ring elements whose product is 0 one of them is 0. So, a 1 is 0 or a i minus a j is 0

So, now suppose a 1 is not 0. So, I am going to assume that assume a 1 is not 0, you will see why I will assume that in a minute. So, I am assuming a 1 is not 0, remember I am choosing a 1 to begin with. So, I will only deal with non-zero elements, so a 1 is non-zero. So, this is not possible; that means, a i minus a j is 0, but; that means, a i is equal to a j ok. So, in other words what we are saying is that, if a 1 multiplies a i and a j to the same element, in other words a 1 a i is equal to a i a j then a i is equal to a j.

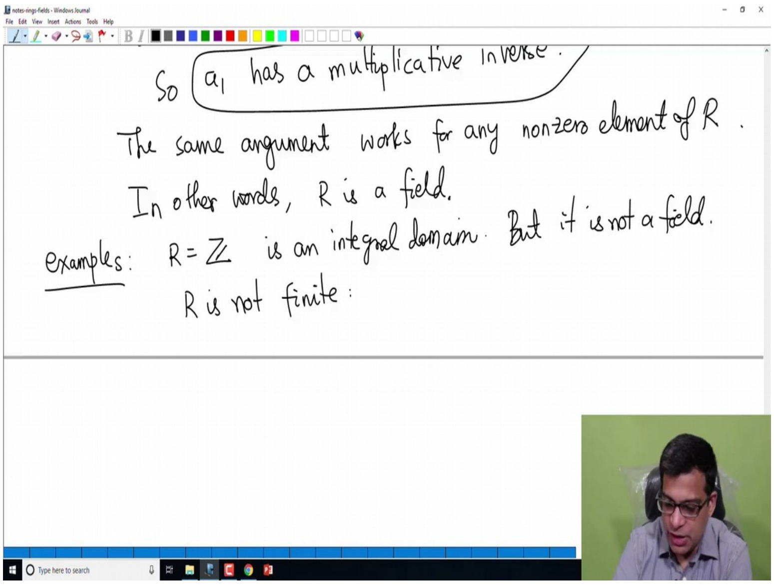
(Refer Slide Time: 05:59)



So, what did we conclude? Hence, if a 1 is not 0 then a 1 squared, a 1 a 2, a 1 a n are distinct elements. In other words so R is equal to a 1 a squared, a 1 a2, a 1 an. Remember, because R is a ring when you multiply elements of R you again get elements of R. So, the set a 1 squared, a 1 a 2, a 1 a n is certainly a subset of R, but because R has n elements and these are n distinct elements it must equal R, so R is equal to this set.

But 1 is contained in R; so 1 is contained in this set a 1 squared, a 2, a 1 a 2, a 1 a n. So, a 1 a i is equal to 1 for some i from 1 to n, we do not know what it is, we do not need to know what it is, but for some i, a 1 a i is equal to 1. So, a 1 has an inverse has a multiplicative inverse, I should write. So, a 1 has a multiplicative inverse. So, as soon as a 1 is non-zero, we are concluding that a 1 has a multiplicative inverse.

(Refer Slide Time: 07:31)

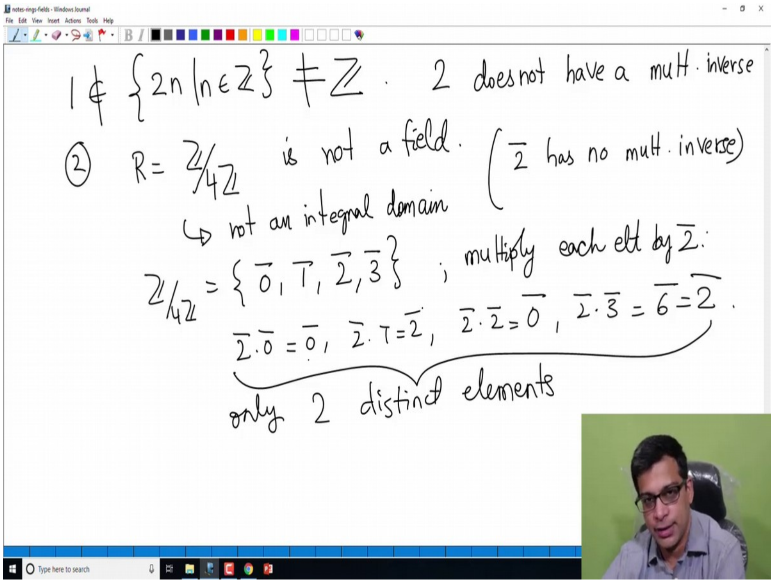


The same argument works for any non-zero element of R right. We started with a1, but I instead of a1, we can choose any non-zero element of R and multiply by that, argue that there are n distinct elements. So, one of them must be 1, so that element has an inverse.

Hence, in other words R is a field. So, as soon as you have a ring where every non-zero element has a multiplicative inverse, it is a field by definition right. A field is a ring where every non-zero element has a multiplicative inverse. So, I have assumed that R is a finite integral domain and showed that R is a field. So, this is exactly the problem. Now, before continuing to the next problem, I am going to give two examples to illustrate the fact that both statements that we have finite and that it is an integral domain or crucial, without that you cannot conclude that R is a field.

So, let us consider R to be Z, the ring of integers. So, this is an integral domain, but not a field right that we know it is not a field because for example, the integer 2 which is a non-zero integer has no multiplicative inverse. So, it is an integral domain, it is not a field and the reason that the previous problem does not apply here is R is not finite.

(Refer Slide Time: 09:31)



So, the previous argument will not work here because for example, if you multiply every element of integers by 2 you get 2 n where, n is in Z, this is not equal to Z. When you multiply all elements by 2, you get also an infinite set using the previous problems argument, but it is not equal to Z, so 1 is not in this. So, in other words 2 does not have a multiplicative inverse. So, the previous argument is critically dependent on the fact that R is finite. So, if you have an infinite integral domain it need not be a field.

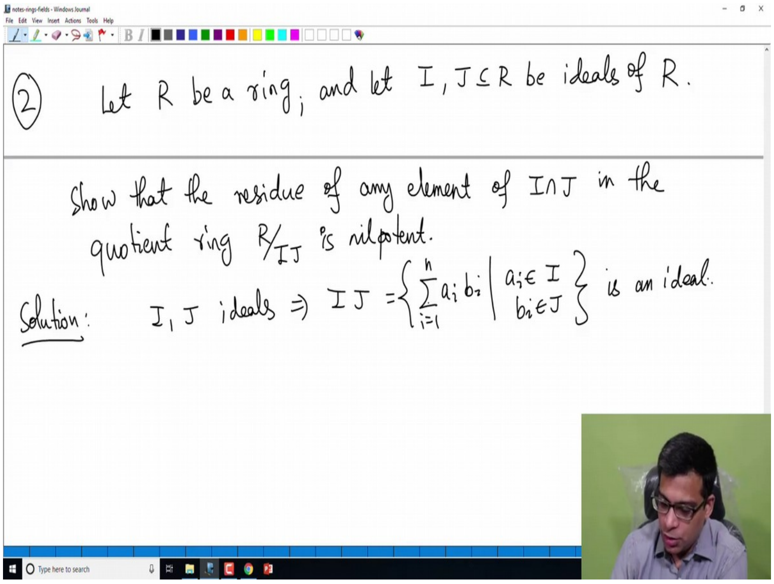
On the other hand, if you have a finite ring, but it is not an integral domain again it need not be a field, so this is not a field. So, this is an obvious statement because a field is by definition in integral domain. So, this is not an integral domain and I will quickly tell you why the previous argument fails here.

So, for example, if you take remember 2 bar has no multiplicative inverse in this ring. So, if you Z mod 4 Z remember is the set of residues modulo 4. So, the elements can be written as 0 bar, 1 bar, 2 bar, 3 bar; if you multiply each element by 2 bar, what you get? So, you get 2 bar times 0 bar which is 0 bar, 2 bar times 1 bar which is 1 bar, 2 bar times 2 bar which is 0 bar, 2 bar times 3 bar which is 6 bar which is 2 bar ok.

So, after multiplying by 2, we have only 2 distinct elements not 4 distinct elements. Earlier, in the case of finite integral domains, when you multiply by non-zero element you get all the ring elements, here you do not get all the ring elements you get only 0 bar and 1 bar sorry 0 bar and 2 bar, I should write 2 bar times 1 bar is 2 bar.

So, 1 bar is not one of this products, so 2 bar has no multiplicative inverse. So, these examples show that if you have an integral domain, but it is not finite it is not a field. If you have a finite ring that is not an integral domain also it is not a field ok. So, let us continue now. So, I will do one more problem now next problem.

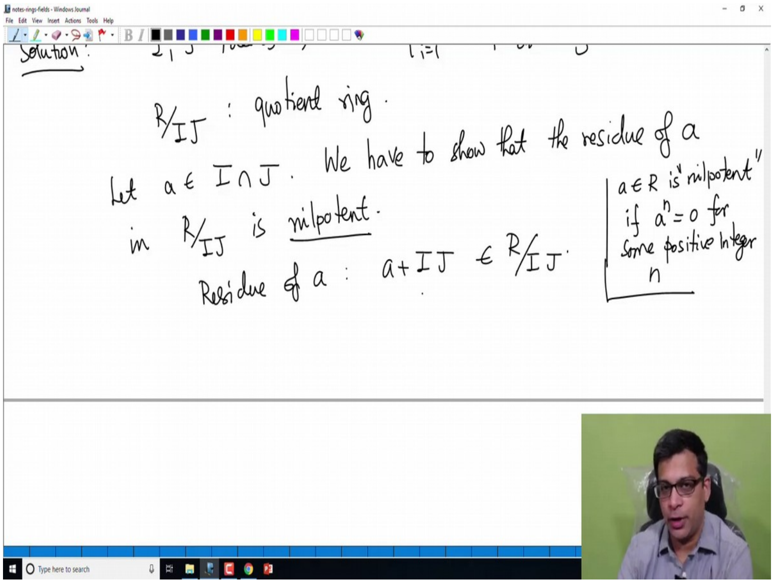
(Refer Slide Time: 12:05)



Problem number 2 is the following, let us consider any ring R without any further assumption it is R is a ring and let I and J be ideals of R, let I and J be ideals of R. So, I want to show that, any element in I intersection J ok. So, actually I should not write it like this, so I will write it like the following. Show that the residue I will explain this, residue of any element of I intersection J in the quotient ring R mod I J is nilpotent ok. So, this requires a bit of an explanation. So, let me carefully explain what do I need to do here, so before I do the solution.

So, remember if I, J are ideals implies I the product is also an ideal. So, this is in one of the earlier videos I defined the product of two ideals. So, these are elements which are obtained by taking products of elements of I and J adding any finite number of them ok. So, the way to remember this is, I J consists of finite sums of products of elements of I and J. So, this is an ideal which is an easy verification.

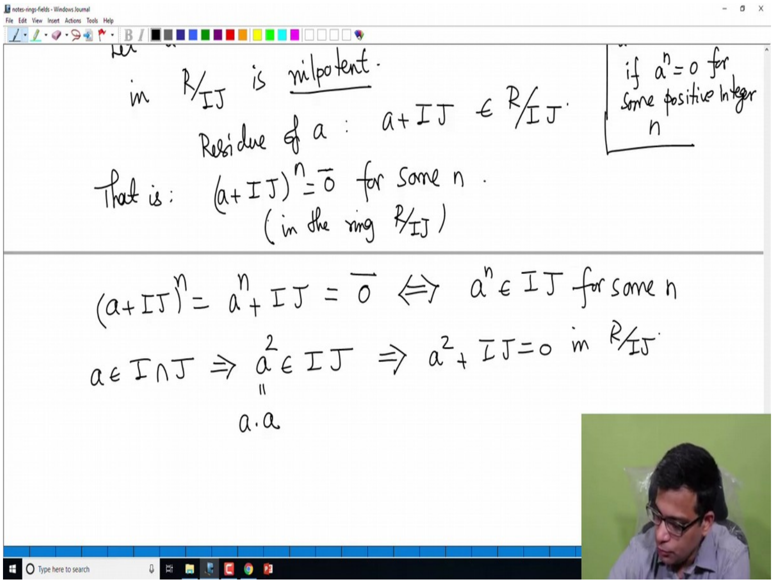
(Refer Slide Time: 14:08)



So, we can consider R mod I J, so the quotient ring. Remember, every time you have a ring and an ideal in that ring you can consider the quotient ring. Now, the problem is saying that if so let a be an element of I intersection J, residue of any element of I intersection J. So, let a be an element of I intersection J. In other words, a is in both I and J, we want to show that we have to show that the residue of a in R mod I J is nilpotent. Residue is denoted by a bar, but remember it is the coset of a. So, residue of a is a plus I J and there is an element of R mod I J. Remember, the quotient ring as a set consists of all left cosets under the operation of addition, so residue of a is this.

Finally, what is nilpotent? This is something I defined in previous video; an element of a ring is called nilpotent, if a power n is 0 for some positive integer n right, a is called nilpotent if some power of a when you multiply a with itself certain number of times you get 0. We want to show that a plus I J is a nilpotent element of the quotient ring R mod I J.

(Refer Slide Time: 16:01)



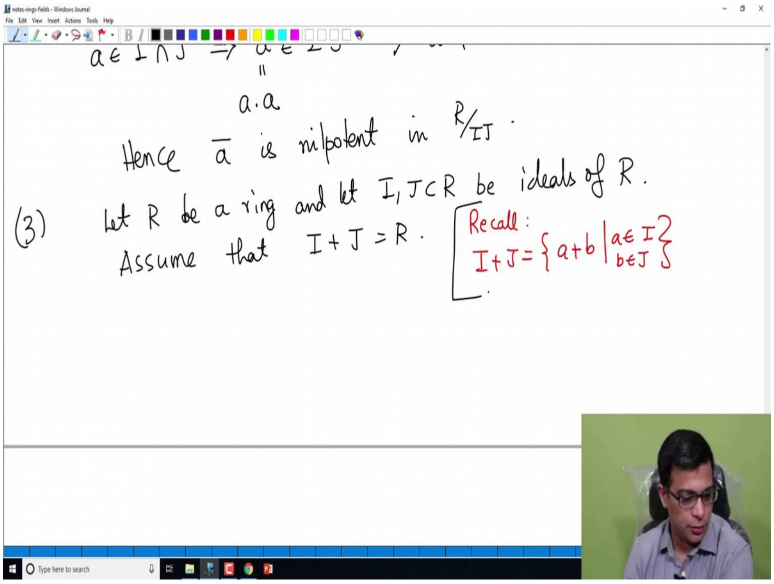
In other words, that is, we want to show a plus I J power n is equal to 0 for some n right, this equality must happen in the ring R mod I J right because residue of a in R mod I J is nilpotent. So, a plus I J power n is equal to 0 for some n.

But remember, what is a plus I J plus power n under the ring under the definition of multiplication in the quotient ring; this is simply a power n plus I J, but let me actually write 0 bar here because 0 means you might be confused with the 0 element of the ring. So, 0 bar is the 0 element of the ring R mod I J.

So, a plus I J power n is a n plus I J. Remember, this in order for this to be equal to 0 bar, we want a power n is I J for some n, this is now after translating everything in the problem this is not we are reduced to if a belongs to I intersection J, a power n belongs to I J for some n.

Now, once you identify that this is what you need to do, its clear what n you need to take. Remember, what is known about a and I, a it is in I intersection J; that means, it is in I as well as it is in J. Once that happens, a squared remember is an I J because a squared is a times a, a is in I a is in J, if you recall the product of two ideals is sums of products, one from the ideal I, the other from the ideal J. Here I am just taking a single product a times a; a is in I, a is in J. So, a times a is an I J; that means, a squared plus I J is 0 in R mod I J.

(Refer Slide Time: 18:11)



So; that means, hence the conclusion is a bar is nilpotent in R mod I J. So, the question was show that any element of I intersection J, the residue of any element of I intersection J is nilpotent in R mod I J, we have shown that. In fact, we have shown that a square of any element of I intersection J is 0 in R mod I J it is not just nilpotent, but the power you need to take is just 2.

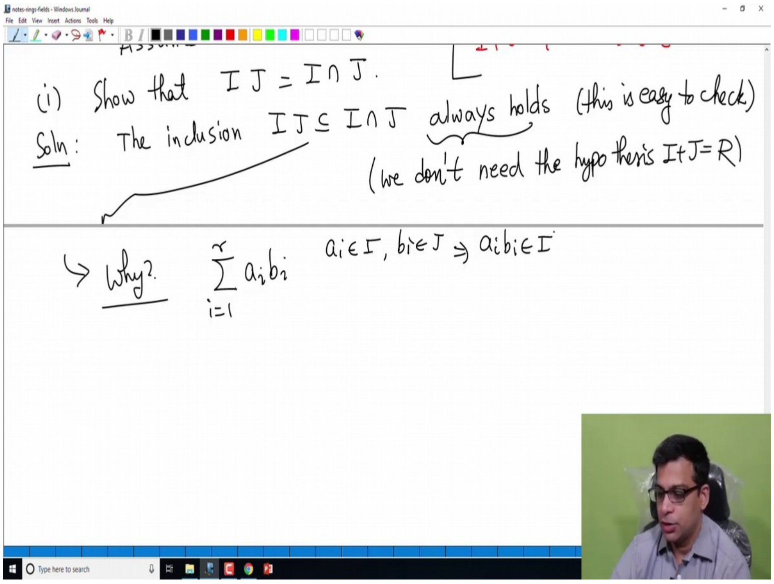
So, the next problem I want to do is building on this notion of I J and the quotient ring R mod I J ok. So, let me now do the following, let R be an arbitrary ring this is as before in the previous problem also we started with in the ring and let I and J be two ideals, let I and J be two ideals of R. So, I have a ring and two ideals of R.

Now, I am assuming something about these two ideals. Assume that I plus J is R and again just like the product of two ideals, we have also learned about the sum of two ideals and what is the sum? So, recall. So, I will use the colour red for recalling, I plus J unlike the product I plus J is simpler actually all you need to do is a plus b, where a is in I and b is in J.

So, you can take two elements one from I one from J and you take their sum. If you take this and you take the collection of those elements it is actually an ideal, that is an exercise from a previous video and it is what we call the ideal I plus J. So, I plus J is this ok.

So, now I am telling you that that is equal to R, that is not in general true, but in this problem I am assuming that I and J have this property that I plus J is equal to R.

(Refer Slide Time: 20:26)

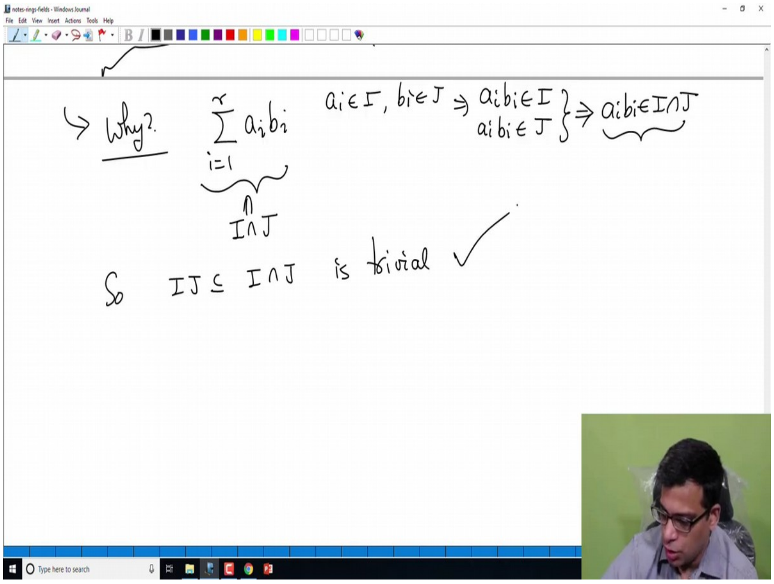


I need to now prove the following statement. So, there are two parts to this problem we will first state one and solve it and then we will state two and then solve two. Show that the first problem is I J is equal to I intersection J, so the solution of this we will do first. So, under the assumption that I plus J is equal to R, show that the product is equal to the intersection. So, there is one obvious in inclusion, so in order to show equality, we will show that I J is contained in I intersection J and we also show that I intersection J is contained in I J.

Note that, the inclusion I J is contained in I intersection J always holds and this is an easy check. What I mean always holds is, do not need we do not need the hypothesis that I plus J equal to R right. So, this is in general true not just for ideals whose sum is R, why is this? I will show you quickly why is this.

So, why is this? Take an element of I J. What is an element of I J? Arbitrary element is of this form right a i is in I, bi is in J so take an arbitrary element. Now, a i is in I. So, and bi is in J; that means, bi is a ring element a i is a ideal element; that means, a i b i is in I because remember an ideal has a property that anything in the ring times anything in the ideal is in the ideal.

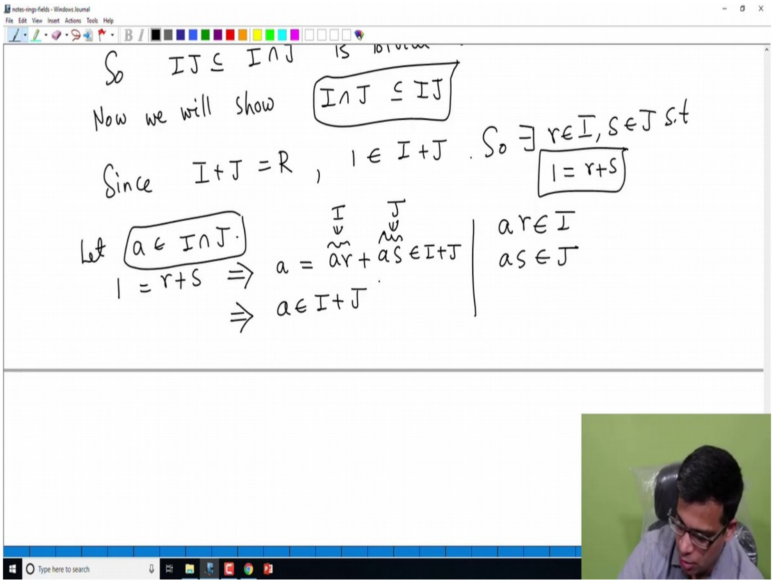
(Refer Slide Time: 22:39)



So, a i is in I bi is in the ring; that means, a i b i is in I, but similarly for the same reason bi is in J a i is in I; that means, a i is a ring element bi is the ideal element the product is in J; that means, a i b i is in I intersection J. Once a i bi is in I in I intersection J, this whole thing is in I intersection J, because I intersection J is an ideal this is something we proved earlier or I have asked you to prove.

So, if you have a bunch of elements inside I intersection J their sum is in I intersection J. So, all these elements are in I intersection J, so their sum is in I intersection J. So, the inclusion I J contained in I intersection J is trivial, it is very easy ok.

(Refer Slide Time: 23:29)



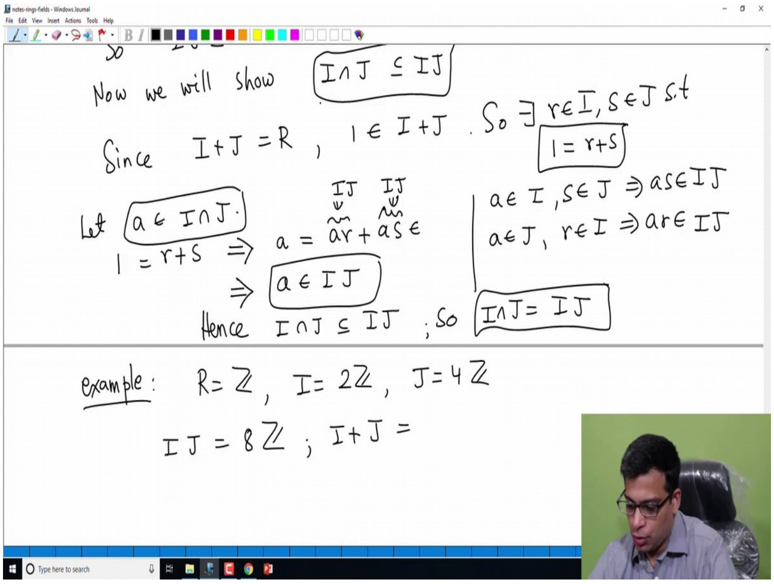
So, now we will prove that the opposite inclusion holds. Now, we will show I intersection J is contained in I J and this is the crucial inclusion that is not in general true; after solving this I will give you an example, this requires the hypothesis that I plus J is equal to R.

So, now since I plus J is equal to R, the element 1 belongs to I plus J right because the element the identity element 1 is a ring element it is in R, but I plus J is equal to R, so 1 is in I plus J. So, there exist elements r in I and s in J such that 1 is equal to r plus s right. So, 1 is an element of I plus J and I recalled for you what is I plus J, I plus J is simply the collection of sums one from I one from J, so 1 is equal to r plus s ok.

So, now I am trying to show that I intersection J is contained in I J. So, let us choose an element a in I intersection J, we will eventually show that a is in I J ok. So, now, 1 is equal to r plus s that we know. So, we can write ar; a is equal to ar plus as right. I am multiplying both sides by a, 1 is equal to r plus s means a times a is equal to a times r plus a times s. This I claim will give me what I want because let us look at a r, what is r? r is an I, a is an arbitrary ring element.

So, ar is in I fine, a is an arbitrary ring element r is an element of I, so this is in I similarly, s is in J a is an arbitrary ring element, so a s is in J. So, ar is in I as in J so; that means, there is an I plus J right. So, we have written a as something in I plus something in J ; that means, and that is all we have started with an arbitrary element of I intersection J and we have concluded that it is in I plus J.

(Refer Slide Time: 26:07)



Hence, I intersection J is I plus J. So, we have the other inclusion always holds. So, I plus J is equal to I intersection J. So, and then the second inclusion we needed crucially the fact that I plus J is R. So, now, in general as I told you earlier this is not true. So, let us take R to be Z and I to be 2Z and J to be 4Z. So, the ideal I is all even integers, the ideal J is all multiples of 4. What is I J? In this case you can check that, it is simply 8Z.

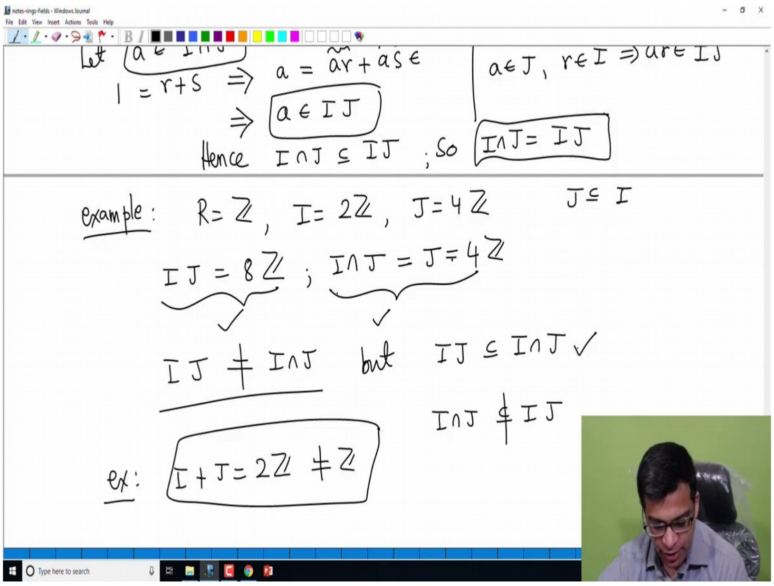
So, you take products of I elements of I with elements of J and you add them, everything happens to be a multiple of 8 because 2 times 4, that is a crucial idea. And what is I plus J? If you think about this, sorry, so sorry actually I made a mistake. So, I am not interested in showing that sorry I have to go back here I am not interested in showing that I intersection J is contained in I plus J, I plus J is R. So, of course, I intersection J is contained in I plus J, what I want is a is contained in I J; so now, yeah sorry.

So, what I want is a is contained in I intersection J. So, let me go back here a is contained in I and r is and s is contained in J, so as is contained in I J. So, I this is something I missed here. Similarly, a is contained in J and r is contained in I. So, this implies ar is contained in I J ok. So, I should have written here a is remember I have never use that a is actually both I intersection J both I and J that is crucial a.

So, a is contained in I a is contained in J whereas, r is contained in I. So, ar is contained in I J it is a product of something in I something in J. Similarly, a s is also product of something in I something in, so ar as is contained in I J. So, a is equal to ar plus as, it is something in I J plus something in I J; that means, a is in I J.

So, what we have shown is that, in I intersection J is contained in I J and hence I intersection J is equal to I J, here I showed that I intersection J is already contained in I J. Sorry, here we showed that I J is contained in I intersection I J a I J is contained in I intersection J this we have showed. Now, we are trying to show that I intersection J is contained in I J. So, I intersection J is equal to I J.

(Refer Slide Time: 29:36)



And now this example shows that, I intersection J is in general not equal to I J. So, I J in this example when I is 2Z and J is 4Z, I J is 8Z; this is easy to check and what is I intersection J? Remember in this case, J is actually contained in I because every multiple of 4 is definitely even. So, if you take intersection of I and J, you will get J.

So, and of course, J is 4Z, so the intersection of the two ideals is 4Z, the product of two ideals is 8Z. So, I J is not equal to I intersection J, but one inclusion always holds I J which is 8Z is contained in I intersection J. In the solution if you see what always holds is that the product is in the intersection that we have, what we do not have here is I intersection J is contained in I J. So, this does not happen, but this inclusion always holds.

And the problem here is why does the argument in the problem does not work, why does it not work? It is because the sum of these two ideals and there is an exercise for you, I will leave it for you to check. The sum of these ideals is actually 2Z and it is not Z. If you take the sum of elements of I and J you get actually 2Z which is not equal to the full ring. So, the sum is only a proper ideal and hence the argument in the problem does not work and we do not have the equality of the product and intersection.

So, just remember that product is always contained in the intersection, but for intersection to be contained in the product you need to assume that the sum of the ideals is the full ring. So, sorry about the confusion in this problem, but I hope it is clear now. So, I will stop this video here. In the next video, we will continue solving more problems.

Thank you.