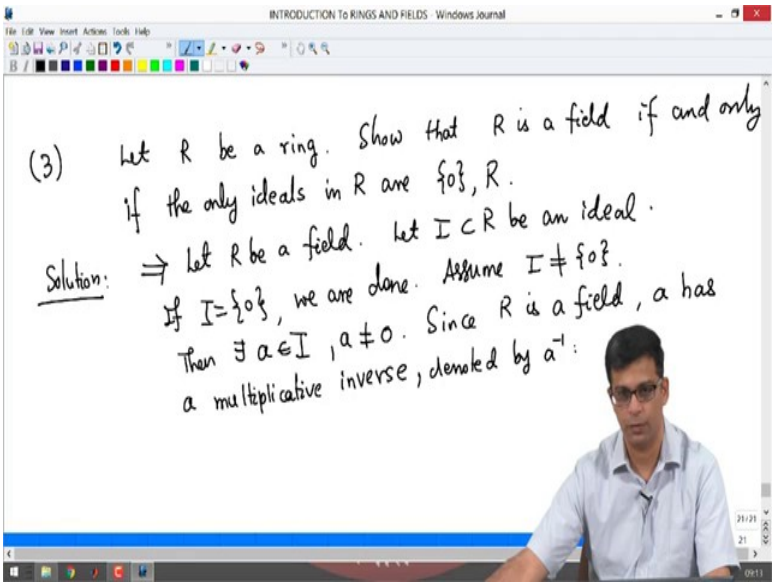
Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 09
Problems 2

So, let us continue, in the last video we did some problems. So, I want to continue and do more problems in this video. So, let us just take off, start from where we stopped in the previous video. So, we have shown that in the last video we have shown some problems we just done some problems where we have to check if some given sets rings or not ok. So, let us continue and we also check that a group ring homomorphism is injective if and only if it is kernel is 0.

(Refer Slide Time: 00:51)



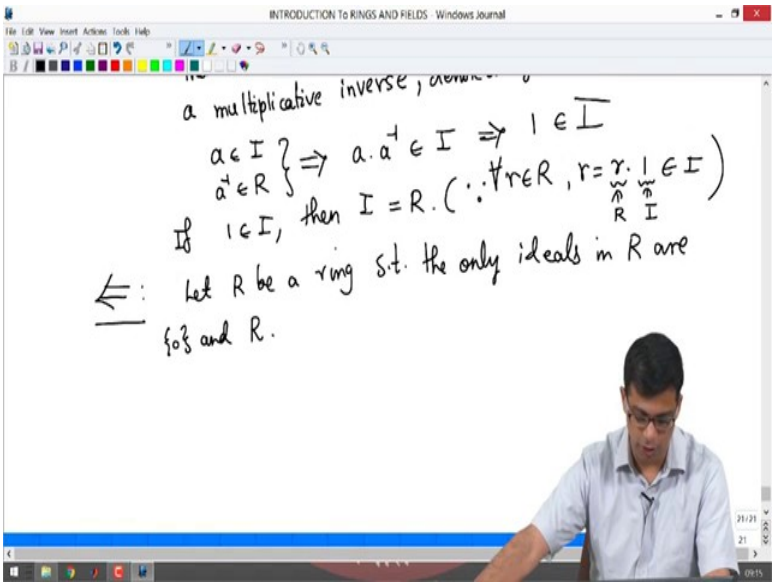
So, now the third problem; so, I will continue the counting from that is video last video. So, the third problem is the following. So, let R be a ring. So, let R be any ring, show that R is a field if and only if and only the only ideals in R are the zero ideal and the full ring, remember in any ring the zero ideal and the full ring are always ideals. So, if R happens to be a ring in which these are the only ideals then R is a field and if R is a field these are the only ideals ok.

So, let us solve this ok. So, we have to prove two implications: if R is a field we have to show that it has only two ideals and if you R is any ring which has only two ideals then R is a field. So, let us first assume this direction I will assume that ok. So, let us assume that R is a field ok. So, I want to show that the only ideals in R are the zero ideal and the full ring. So, in order to show that let us take in ideal in R let I inside R be an ideal ok. So, suppose if I is 0 we are done. I want to show that 0 and R are the only ideals.

So, assume I is not equal to 0. So, if I is not equal to 0 then there exists a in R, a in I rather which is non-zero right. This is the definition of not being equal to the zero ideal. So, there is a non-zero element in I, but since R is a field. So, recall what is the field? A field is a ring in which every non-zero element has a multiplicative inverse.

So, and a is a non-zero element, a has a multiplicative inverse right. Since R is a field and small a is a non-zero element of R it has a multiplicative inverse. So, denoted by you will simply denoted by a inverse ok. So, that is the usual notation for multiplicative inverses.

(Refer Slide Time: 03:43)



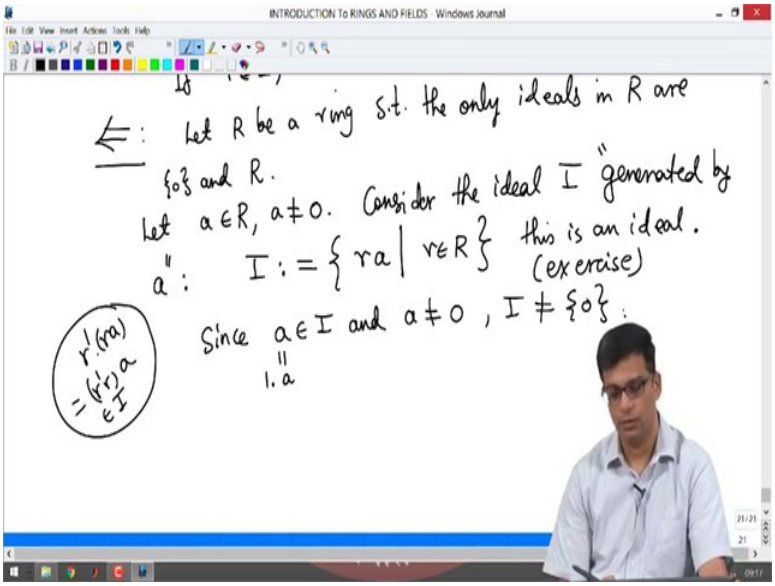
So, now let us see if a is in I and a inverse of course, is in R, it has an inverse in R we are not saying it has an inverse in I. So, we have its inverse in R, but what is the definition of an ideal? If something is in the ideal and something is in the ring their product is in the ideal, what is the product of a and a inverse that is 1. So, 1 is in I, but if 1 is in I; if 1 is in

I then I claim I is equal to R right, if 1 is in I everything is in I. This is because take any small r in R, r can be written as r times 1. So, this is in R this is in I, 1 is in I.

So, r times 1 must be in I right. So, for all r in R r can be written as r times 1 where r is an element of R, 1 is an element of the ideal. So, the product must be in the ideal. So, for all r in R r is in I. So, if 1 is in I then I is R. So, we are done in this direction right. If R is a field we have shown that any non-zero ideal must be the full ring so; that means, the only ideals are 0 and R.

Now let us take suppose that let R be a ring such that the only ideals. So, s dot t means such that the only ideals in R are 0 and R ok. So, let us now take this. So, the only ideals in R are 0 and R. If this happens we want to show R is a field and again what is the meaning of a field? A field is any ring in which every non-zero element has a multiplicative inverse.

(Refer Slide Time: 05:49)

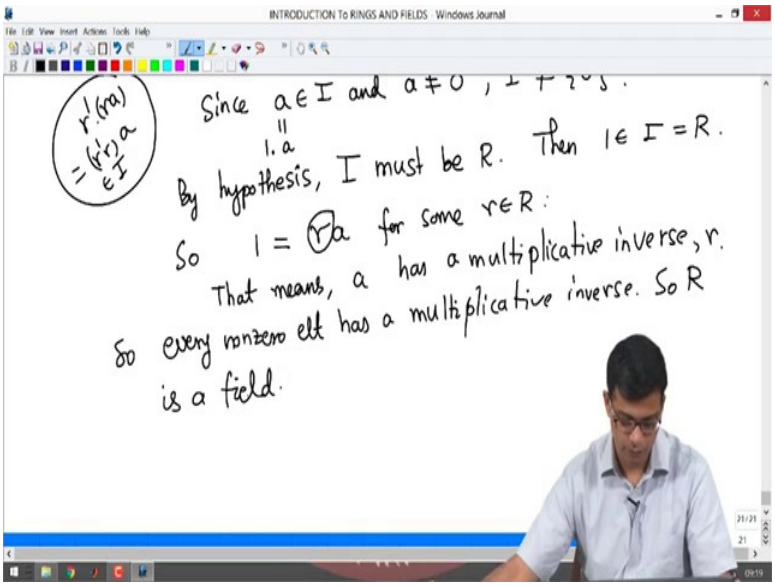


So, let us take a non-zero element. Let a be in R a non-zero. We want to show that a has a multiplicative inverse and then it will follow that R is a ring. So, to show that consider the ideal I generated by, this is new terminology. I will explain this, generated by a. So, by this I mean I is equal to all elements of the form ra where r is in R. So, I claim that this is actually an ideal and it is said to be generated by a because every element of I is a multiple of a. So, we say that it is generated by a.

So, this is an ideal is a simple exercise for you which I do not want to do and I let you do this. It is closed under addition as you want for an ideal because if you have ra plus r prime a it is r plus r prime times a. It is certainly closed under multiplication by any ring element because you take an element of this set ra multiply by r prime. So, I will write it here r prime times ra is r prime r times a because of the distributive property of multiplication and this is again in I ok. So, anywhere the remaining details I will let you check. So, consider this ideal, this is actually an ideal I.

Now, since certainly a belongs to I right and a is non-zero. Why does a belong to I? Aa-belongs to I because a is equal to 1 times a. So, I consists of all multiples of small a, small a itself is certainly a multiple of a. So, a is in I and a is non-zero, I is not equal to 0 right because it contains a non-zero element.

(Refer Slide Time: 07:59)



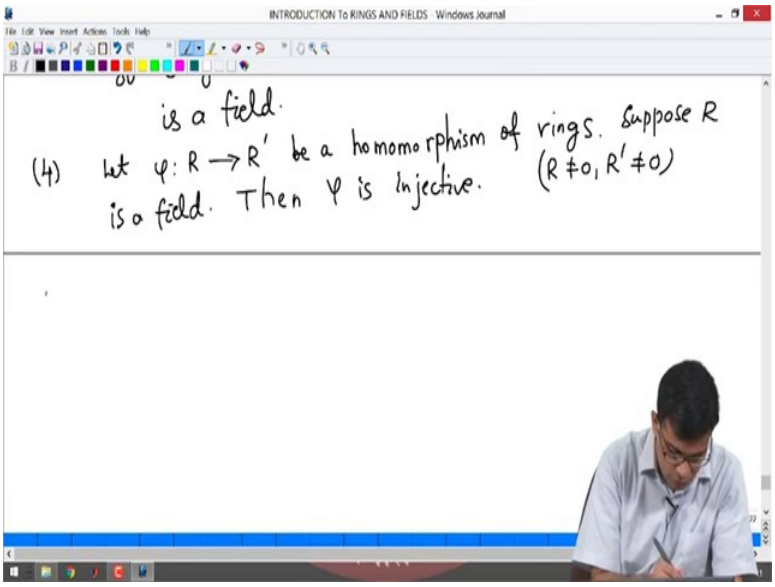
But by the hypothesis I must be R because what is the hypothesis? Hypothesis is that the only ideals in R are 0 and R and we have here an ideal I which is not 0, so it must be R, but then 1 belongs to I, 1 belongs to I because 1 is an element of R I is equal to R.

So, in other words 1 has to be of the form r a for some r right, because I only consists of elements of the form ra and 1 is one such element. So, 1 is equal to ra for some r in R; that means, a has a multiplicative inverse right. So, a has a multiplicative inverse. We have produced an element r such that r times a is 1 so; that means, r is the multiplicative

inverse of a. So, a has a multiplicative inverse. So, every non-zero element has a multiplicative inverse.

So, R is a field. So, the only rings which have exactly two ideals are fields. So, if you have any ring which has more than two ideals it must automatically be a field, sorry if you have any ring that has more than two ideals it must not be a field. So now, the next exercise or next let us see number will be 4, is a corollary of the previous two problems.

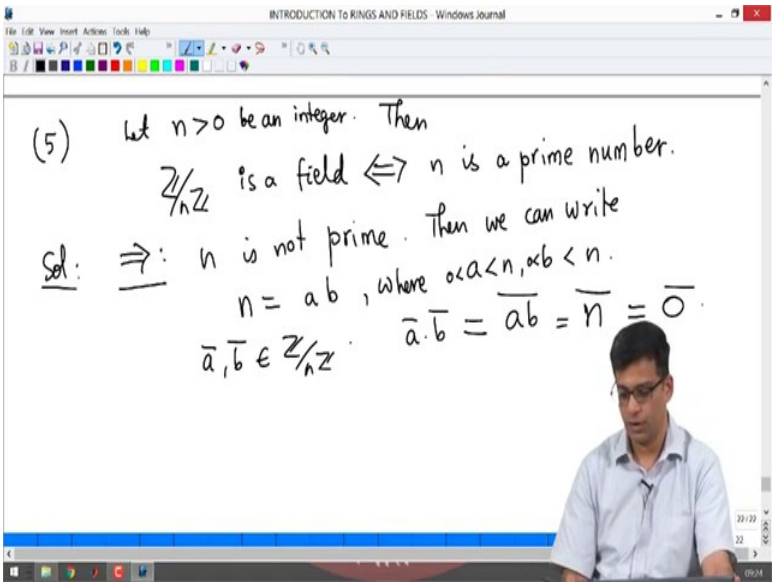
(Refer Slide Time: 10:03)



So, let us say phi is a homomorphism of rings. Suppose R is a field then phi is injective ok. It is a good time for me to remind you that all our rings are non-zero rings. R is not 0 R prime is not 0. So, the only we will never consider zero rings. So, every time I say a ring in this course I am in a non-zero ring. So, here the domain ring R is a field I claim then that the ring or ring homomorphism is automatically injective and the reason is, it is kernel is an ideal of R; R is a field.

So, the ideal is either all ideals of R are either 0 or R. So, kernel is either 0 or R, but kernel cannot be R because 1 goes to 1 for a ring homomorphism and that is not 0. So, kernel is not equal to R. So, kernel is equal to 0, which by an earlier problem means phi is injective ok. So, this is a straight forward application of the previous two problems. So, I will not say anything more about it.

(Refer Slide Time: 11:33)



But next problem this is something that I used earlier or I commented about this in an earlier video. So, let n be an integer, will be actually a natural number. So, it is a non-negative integer then we said Z mod n Z is a ring right. So, this I told you earlier there is a ring structure on this ok. So, this is a field if and only if n is a prime number ok. So, this I want to do. So, I will not recall here and the fact that Z mod nZ is actually a ring. You can multiply two residue classes modulo n or you can add two residue classes modulo n, the residue class of one is the identity element for multiplication.

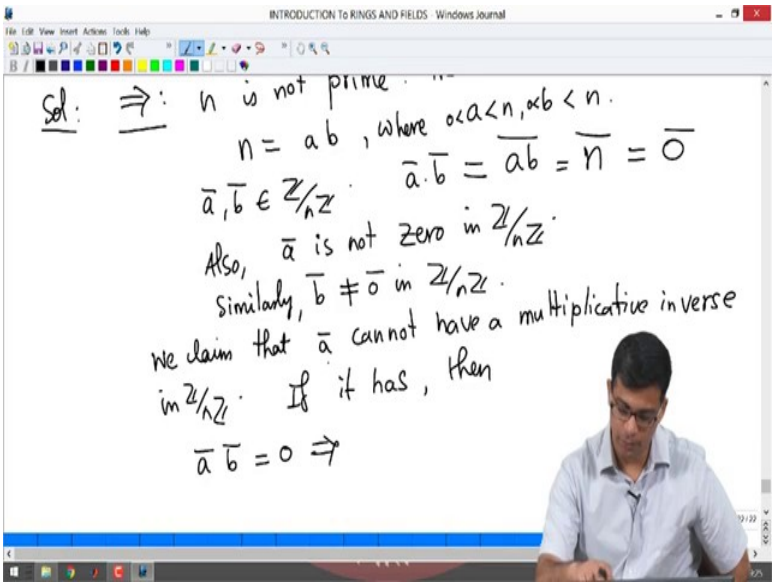
The residue class of 0 is the identity element for addition and so on. So, in the sometime in the future I am going to talk about quotient rings in more general and Z mod nZ will be an example of that. So, at that point I will remind you again how to think of this as a ring, but for now suppose that it is a ring. I claim it is a field if and only if it is a prime number n is a prime number. So, solution and the solution is something that you can construct easily.

So, I won't do all the details, but quickly tell you the basic idea. So, suppose so, in this direction or actually in this direction. So, suppose n is not prime. So, I am going to assume that Z mod nZ is a field and prove that n is a prime number suppose n is not a prime number then we can write the definition of not being prime means we can write n is equal to ab, where a and b are strictly less than n right. 4 is not a prime number be-

cause 4 can be written as 2 times 2, 6 is not a prime number because 6 can be written as 2 times 3 and 2 and 3 are.

So, actually let me take n to be a positive integer. So, 0 case I will separately consider. So, n is a positive integer. So, n is a positive integer it can be written as a product of two smaller positive integers if it is not prime. Now consider a bar and b bar in Z mod nZ. What is a bar times b bar? The definition of product in Z mod n Z means that gives me that this is a b n bar, but a b bar, but a b is equal to n right. So, a b bar is n bar, but n bar is 0 bar because n and 0 have the same residue modulo n. So; that means, a b a times b 0 in Z mod nZ.

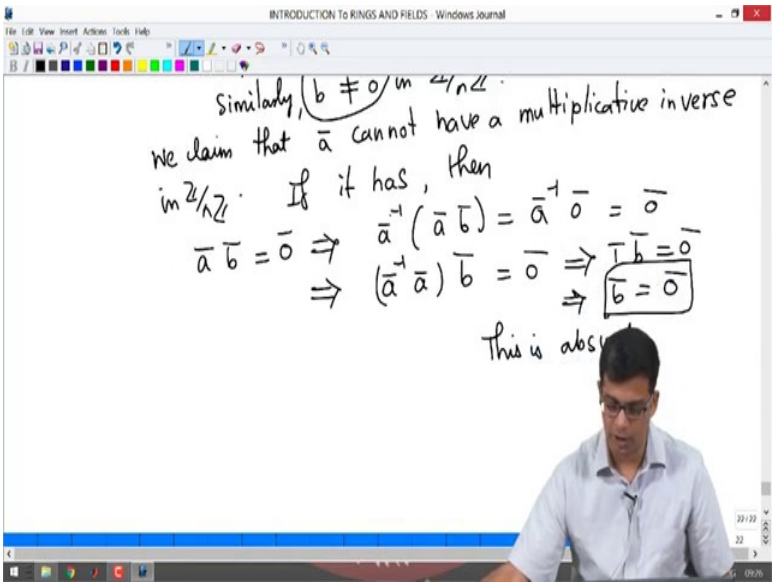
(Refer Slide Time: 14:49)



Then so, also a bar is not 0 in Z mod nZ right because a bar if a bar is a 0; that means, a is a multiple of n the only 0s, 0 element of Z mod nZ is the class of multiples of n. So, if a bar is 0, that means, a is a multiple of n, but similarly, but a is not a multiple of n because a is strictly between 0 and n similarly b bar is not equal to 0 bar in Z mod nZ.

Now, we claim that a bar cannot have a multiplicative inverse in Z mod nZ why is that? So, suppose it has if it has then let us play with it. So, a bar b bar is 0 bar right. So, that is something I commented on earlier a bar times b bar is 0 bar.

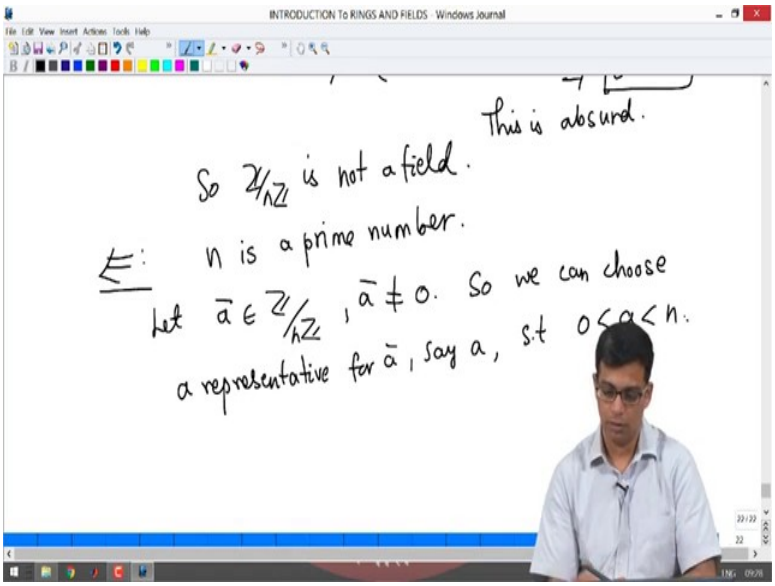
(Refer Slide Time: 16:11)



Suppose a bar has an inverse. So, let us denote that by a bar inverse as always right. So, let us multiply this equation by a bar inverse on both sides. So, you get a bar inverse times a bar b bar is equal to a bar inverse times 0 bar anything times 0 bar is 0 bar. So, this is what it is, but then associativity of multiplication says that this is equal to this a bar inverse times a bar equal times b bar, but a bar inverse a times a bar is 1 bar times b bar is 0 bar, 1 bar times b bar is 1 b bar because 1 bar is the multiplicative identity.

That means b bar is 0 bar, but this is absurd right. This is absurd because b bar also is not 0 element that I have remarked here ok. So, a bar cannot have a multiplicative inverse.

(Refer Slide Time: 17:13)

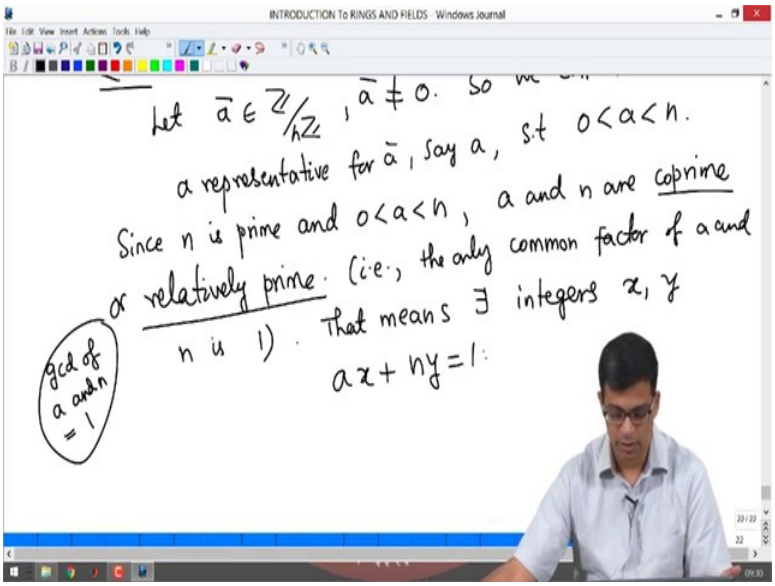


So, Z mod nZ is not a field right. So, if Z mod nZ is a field and n is not a prime number we are concluding that Z mod n bar Z mod nZ is not a field. So, that is a contradiction. So, I have proved the implication to the right hand side. Now, let us to the implication to the left hand side. So, here I am assuming n is a prime number.

So, n is a prime number I want to show that Z mod nZ bar Z mod nZ is a field. So, let a bar b in Z mod nZ which is non-zero. So, I am going to bring it back to the integers and use the properties of integers. So, we have. So, a bar is some element right. We can pick any representative we want for a bar. So, we can choose a representative remember Z mod nZ is a set of co-sets. Any co-set is a equivalence class of integers. a representative is an element of that equivalence class.

So, you can choose a representative for a bar say; obviously, it is convenient to call that representative a such that 0 is less than a less than n because any element can be any co-set in Z mod nZ has a representative in the set 0 to n minus 1, but because a bar is not 0 we can choose the representative to be actually a positive number between 0 and n ok. So now, I am going to recall for you a property of prime numbers.

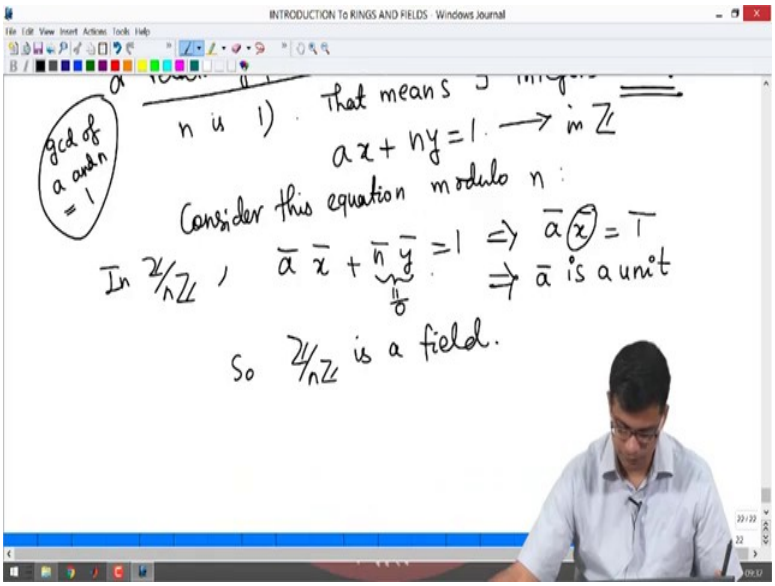
(Refer Slide Time: 19:09)



Since n is prime and a is a positive number strictly less than n, a and n are co-prime or relatively prime; a and n are relatively prime or co-prime, these are they mean the same; that means, they have no common factors because n is a prime number. The only factors of n are n and 1, a is strictly less than n. So, n cannot be a factor of 1 n cannot be a factor of a. So, the only common factors of a and n are 1. So, that is the only common factor of a and n is 1 ok, but now since they are co-prime; that means, what I am saying is that their gcd is 1.

Right the gcd: greatest common divider is 1; that means, there exist integers let us call them x and y such that ax plus ny is equal to 1. This can be done using Euclidean division algorithm. If you have a pair of integers whose gcd is 1, that means, 1 can be written as a linear combination of those two integers a in other words you can find x and y such that ax equal to ax plus ny equal to 1.

(Refer Slide Time: 21:01)

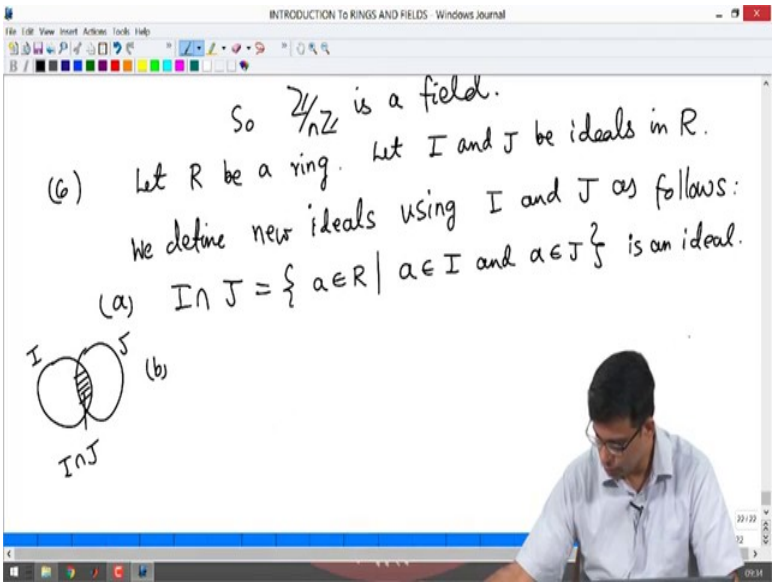


So, now consider this equation modulo n so; that means I essentially put bars. So, I have a bar x bar plus n bar y bar equals 1. But this means, so, in Z mod nZ this also. So, this is in Z going modulo Z mod nZ we get this in Z mod nZ, but n bar remember is 0 in Z mod nZ. So, we have a so, this become 0. So, a bar x bar is 1; that means, a bar is a unit it has a multiplicative inverse.

So, whatever x bar is a it is a unit it is the inverse of a bar. So, a bar is a unit and remember we have done this for any arbitrary a bar which is non-zero. So, Z mod nZ is a field ok. So, what we have done is produced an inverse and multiplicative inverse for any non-zero element of Z mod nZ when n is a prime number.

So, we have shown that Z mod nZ is a field if and only if n is a prime number ok. So, this is the solution for this problem. So, let us do next problems now. So, we have done 5 now. So, go to the 6th problem ok.

(Refer Slide Time: 22:35)

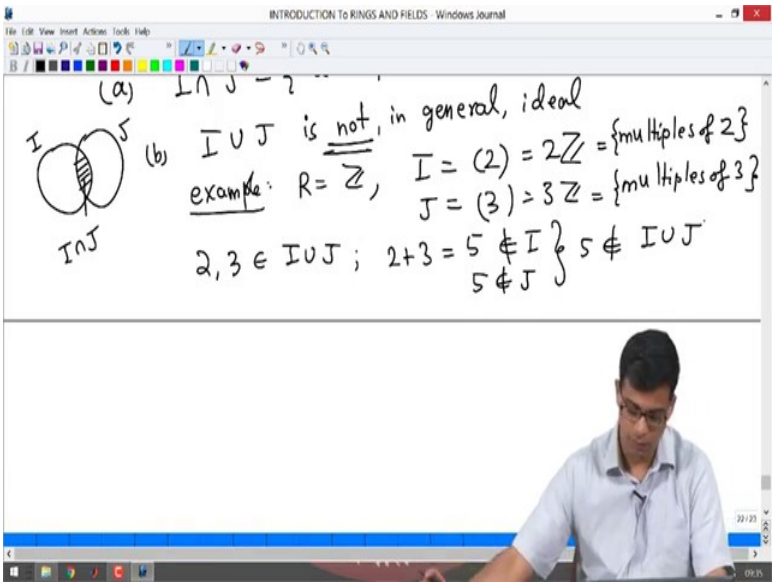


So, what is the 6th problem? So, 6th problem is about ideals ok. So, I am going to introduce, this is a fairly easy exercise. So, let R be a ring, but this is these operations I am going to define are important. So, I will write it down here and leave most of the solution to you. Let R be a ring, let I and J be ideals in R, let R be a ring and let I and J be ideals in R. So, we want to define certain operations on I and J. So, we define new ideals using I and J as follows ok. So, the first one is the, it is a very simple one it is just set-theoretic is the intersection of I and J.

So, what is this? These are elements of R which are in both I and J. So, a is in I as well as in J. So, then that is the intersection. So, this is; so, this is the I intersection J. So, this is an ideal. So, that is the first problem, this is a very easy exercise, I will not do details. If you take two things in I intersection J those two things are in I. So, their sum is in I those two things are in J their sum is in J.

So, their sum is also in the intersection. If you take something in I intersection J and take something in R the product is in I the product is also in J. So, the product is in I intersection J. So, this is the very easy exercise. So, I will not do the solution now. So, next operation so, I intersection J; so, you can check that I union J is not in general an ideal.

(Refer Slide Time: 24:41)

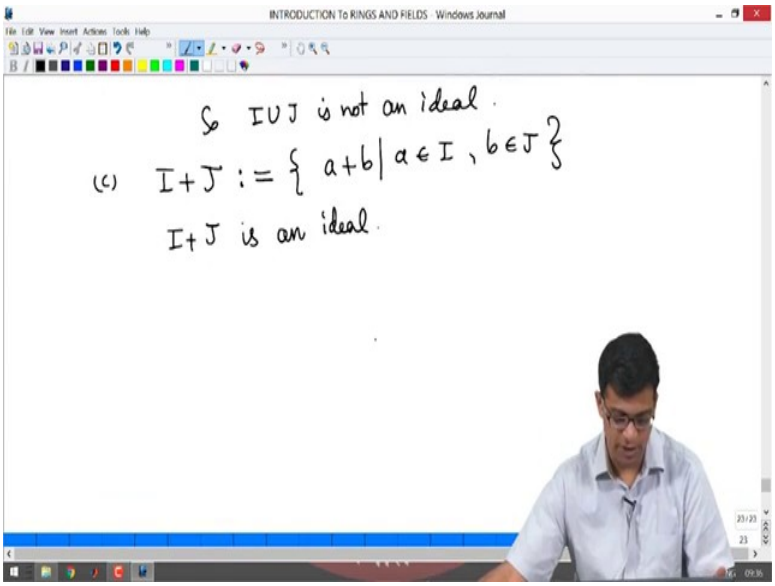


So this is not an ideal I may I have said we have define we define new ideals below, but I union J is actually not an ideal in general. So, as an example let us take R to be the set of integers and I to be the ideal generated by 2.

Remember we have shown in an earlier video that every ideal in Z is generated by a single element it is of the form 2Z or nZ for a positive integer n. Let us take 3 which is 3Z. So, these are multiples of 2 and these are multiples of and both of these are clearly ideals ok. So now, if you take I union J these are integers which are multiples of 2 or multiples of 3.

So, for example, 2, 3 are both in I union J right. So, what is 2 plus 3? 2 plus 3 is 5; 5 is not in I because 5 is not a multiple of 2, 5 is also not in J because 5 is not a multiple of 3. So, you have 2 and 3 in I union J, but their sum is not in I union J ok. So, 2 and 3 are there, but their sum is not there.

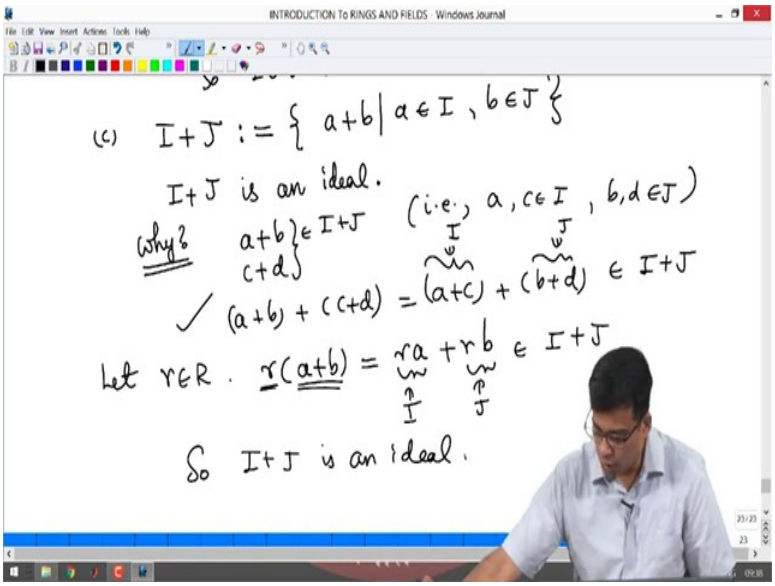
(Refer Slide Time: 26:27)



So, I union J is not an ideal ok. So, union of ideals is not an ideal, intersection of ideals is an ideal. So, let us do one operation here which is similar to union ok, but it is the ideal theoretic union if you want to call it that. So, I will define I plus J to be all elements of the form a plus b, where a is in I and b is in J, ok.

So, this I claim is an ideal. I claim that I plus J is an ideal. So, remember again what is I plus J? I plus J is sum of things one coming from I and the coming from J. So, I claim it is an ideal. So, this is actually once you have written it this way it is very easy to check that it is an ideal.

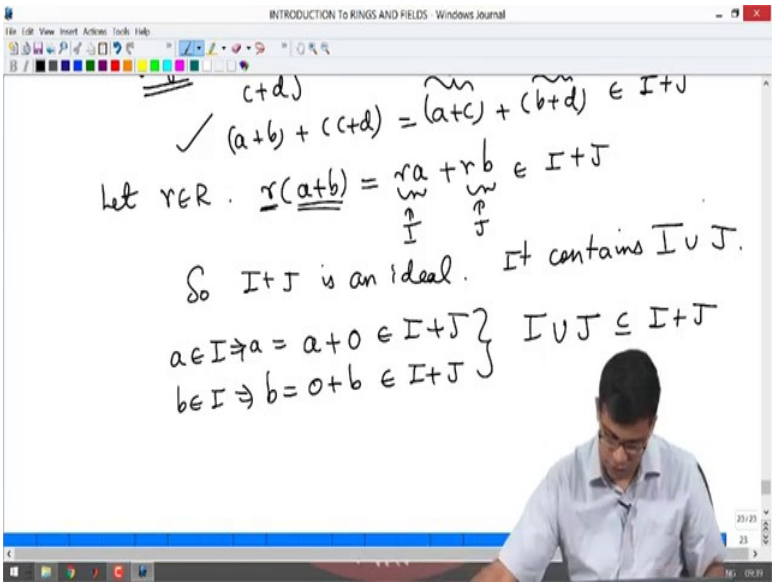
(Refer Slide Time: 27:25)



So, why? So, let us take a plus b and c plus d in I plus J ok; that means, a and c are in I, b and d are in J right, but then what is their sum? So, this can be written as a plus c plus b plus d this is in I because a and c are in I this is in J. So, this is in I plus J, no problem. What is their product? Actually I do not want to take product of anything inside I plus J. So, I will take any r; r is an element. Let us take r times a plus b. So, take a arbitrary ring element and an arbitrary set element. So, this is in R, this is in the set I. What is r times a plus b? This is r times a plus r times b.

Now, I claim this is in I because a is in I, r is in R capital I is an ideal. So, this is in I this is in J. So, this is in I plus J, ok and certainly 0 is there and so on. So, all the properties are easy to check. So, we have checked that and now if you think about it I plus J is certainly an ideal.

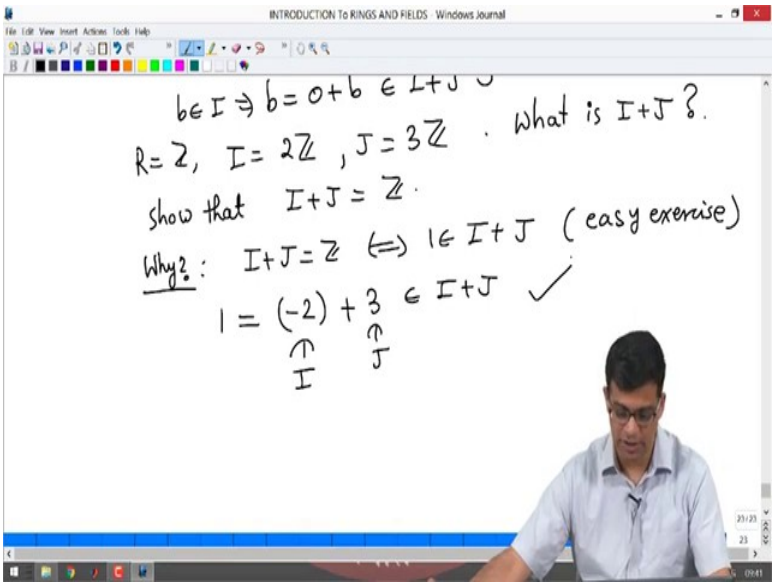
(Refer Slide Time: 29:09)



It contains the union right. Certainly it contains union because if a is in I then a plus 0 is in I plus J. So, a is equal to a plus 0 right. So, a can be written as something in I plus something in J namely 0, so, a plus 0 is in I.

Similarly, if b is in I, b can be written as 0 plus b which is certainly in I plus J. So, I is contained in I plus J, I union J is contained in I plus J. So, I union J is contained in I plus J, but I plus J can be much bigger then I union J. As this example here shows 2 and 3 are in I union J, but their sum is not in I union J. So, we have to take the sums of elements of I and J to make this union and ideal so, now, if you just to complete this circle of ideas.

(Refer Slide Time: 30:15)



So, let us take R to be Z, I to be 2Z, J to be 3Z as before. What is I plus J? Show that I claim that I plus J is in fact, all of Z. Why? So, let us see. So, I claim that to show I plus J is Z is same as saying that 1 is in I plus Z, I plus J. This is something that came up earlier. An ideal is equal to the full ring if and only if 1 is in that ideal ok. So, this is easy exercise ok. So, all we need to show we want to show I plus J is equal to Z; that means, I want to show 1 is in I plus Z, but then 1 can be written as minus 2 plus 3. This is in I because I is 2Z this is in J. So, this is in I plus J ok.

So, the sum of 2Z and 3Z is equal to the full set of integers; the union is just some collection of integers which is not an ideal, ok. So, this is another operation that you can perform for two ideals. I will now end this video here, but in the next video we will continue doing problems, and I will give you another example of operations on ideals that you can use to produce new ideals using two given ideals.

Thank you.