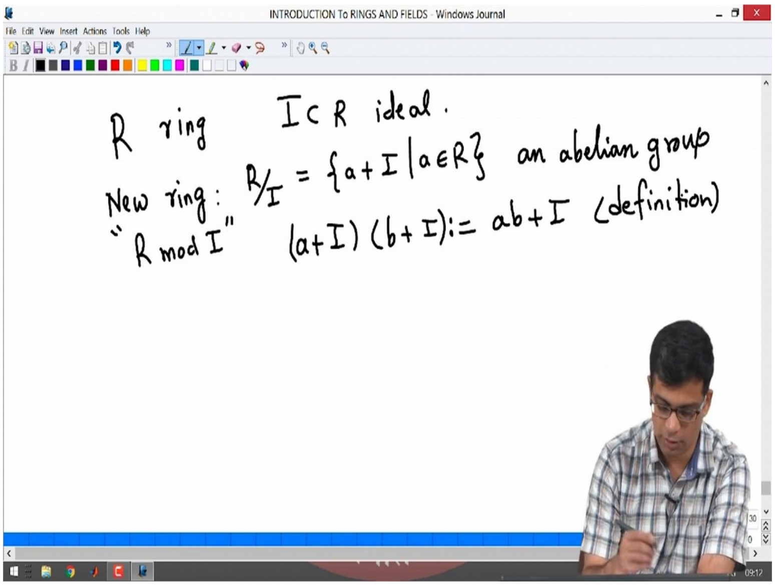
Introduction To Rings And Fields

Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 12
First isomorphism and correspondence theorems

(Refer Slide Time: 00:19)



INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

R ring $\quad I \subset R$ ideal.

New ring: $R/I = \{a+I \mid a \in R\}$ an abelian group

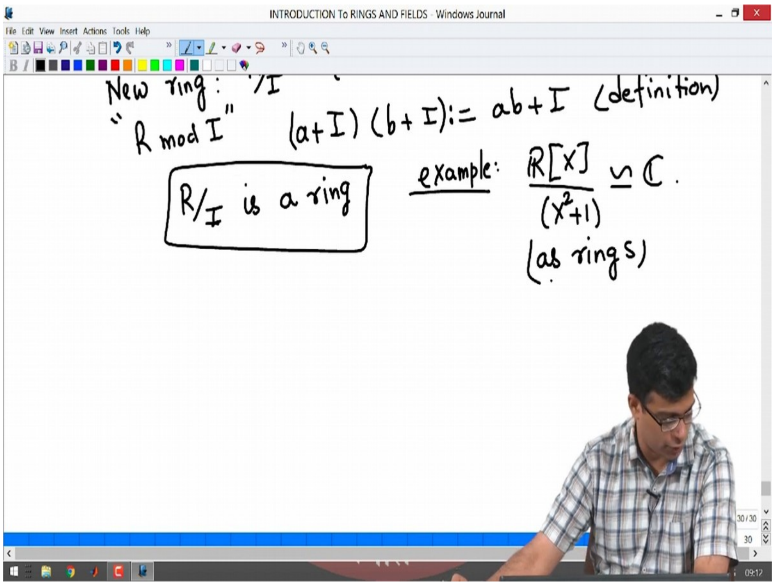
"R mod I" $\quad (a+I)(b+I) := ab+I$ (definition)

Let us continue. In the last video I discussed the important operation of quotient rings. So, recall the operation quickly, so, R is any ring, I is an ideal in R, we defined a new ring right a new ring called quotient ring which is denoted by R mod I. So, this is actually read as R mod I.

So, remember as I said, this is simply the left cosets of I for the operation of addition that is defined on R. So, it is really for the definition all you need to consider is the fact that R is an abelian group under addition. And I is a subgroup of R under addition. So, this is an abelian group automatically. So, as such it is a quotient of an abelian group by sub groups, it is an abelian group and multiplication is defined by this operation: a plus I times b plus I is a b plus I. So, this is the definition and we saw in last video that, we saw in the last video that this is a well defined multiplication that is because of the fact that I is an ideal, it is not merely a subgroup, if you multiply an element of I with an element of the ring you the result is still in the ideal.

So, using that, we were able to show that this is a well defined operation and that I did not prove this I asked you to check these details.

(Refer Slide Time: 01:53)



INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

New ring: /I

"R mod I" $(a+I)(b+I) := ab+I$ (definition)

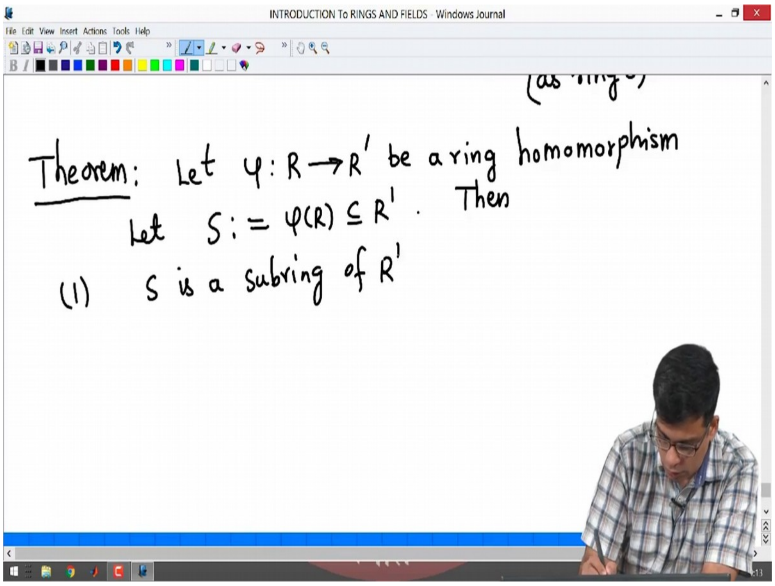
$\boxed{R/I \text{ is a ring}}$

example: $\frac{\mathbb{R}[X]}{(X^2+1)} \cong \mathbb{C}$.

(as rings)

With this operation R is R mod I is in fact a ring ok. So, this is an important construction for us. And I gave you a few examples, the most important example was this. I may have gone fast doing this, but the point was if you take the polynomial ring over the real numbers and go modulo the ideal generated by X squared plus 1 what you get is the complex numbers as rings. So, this is an isomorphism of rings ok. So, I will come back to this, this is an important isomorphism to understanding ring theory. So, we will see this in many situations ok. So, you we will come back to this later.

(Refer Slide Time: 02:40)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

(as rings)

Theorem: Let $\varphi : R \to R'$ be a ring homomorphism

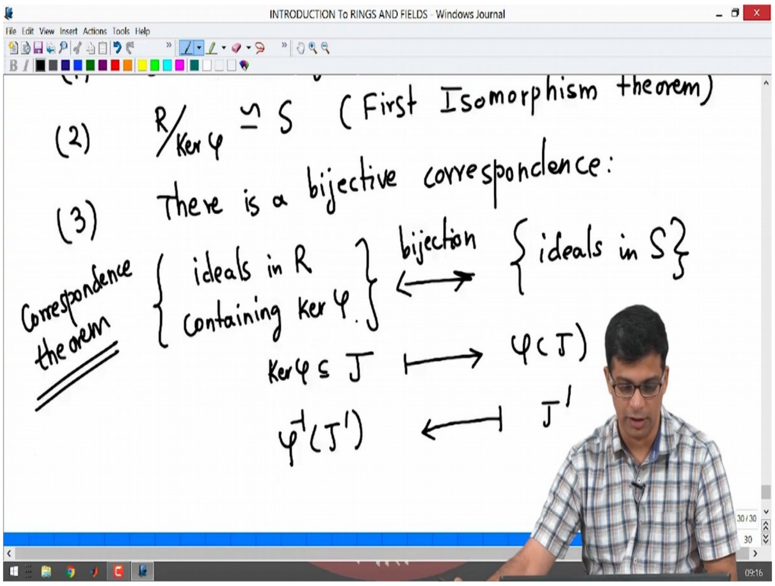
Let $S := \varphi(R) \subseteq R'$. Then

(1) S is a subring of R'

So, what I want to do today is to continue my study of quotient rings and do this very important theorem. So, I am going to club various properties of quotient rings and ring homomorphisms here. So, I am going to make three statements. So, let us say phi from R to R prime is a ring homomorphism. So, let phi be a ring homomorphism. So, R and R prime are two rings and phi is a ring homomorphism. Then and define S to be the image of R. So, S is actually a subset of R prime.

So, we have three statements now. So, then 1: S is a subring of R prime ok.

(Refer Slide Time: 03:34)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help
30 / 30
09:16

(2) $R/\text{Ker}\,\varphi \simeq S$ (First Isomorphism theorem)

(3) There is a bijective correspondence:

Correspondence theorem

$$\left\{\begin{array}{c}\text{ideals in } R\\ \text{containing Ker}\,\varphi.\end{array}\right\} \xleftrightarrow{\text{bijection}} \{\text{ideals in } S\}$$

$$\text{Ker}\,\varphi \subseteq J \longmapsto \varphi(J)$$

$$\varphi^{-1}(J') \longleftarrow\!\shortmid \; J'$$

So, this is a statement about ring homomorphism. First is that S is a subring of R prime. Second is that R mod kernel of phi is isomorphic to S ok. So, this is isomorphism as rings and this is called the “first isomorphism theorem”. You may have learned and in group theory, there are isomorphism theorems; first and second and third isomorphism theorems. Similarly in ring theory also we have them and this is the first isomorphism theorem. If you have a ring homomorphism, the image is isomorphic as a ring to R mod kernel of that homomorphism.

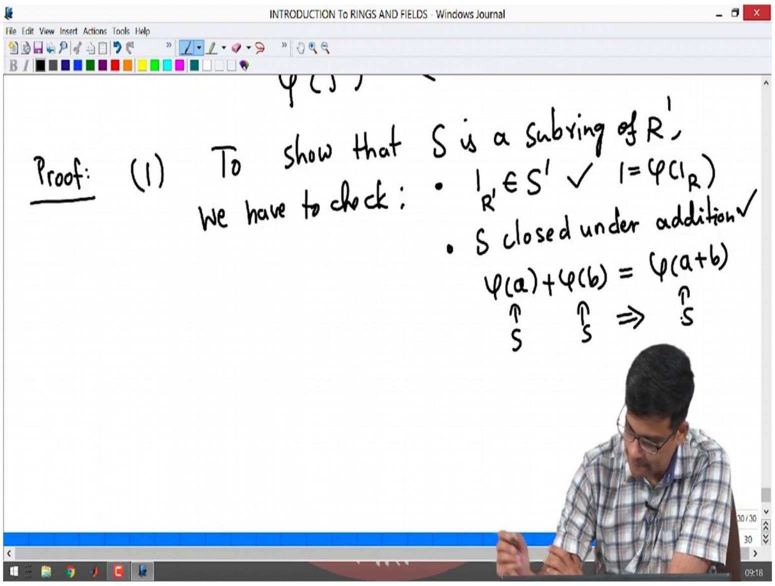
We already know by 1 that S is a ring. So, we can ask for this isomorphism. We can make this statement. And third one is: there is a bijective correspondence; there is a bijective correspondence between the following two sets, the first set being ideals in R containing kernel phi. So, this is the bijection ok. So, there is a bijection between on the one hand you have ideals in R that contain the kernel and on the other hand you have ideals of S.

So, you have the bijective correspondence, this is called “correspondence theorem”. And this is called correspondence theorem. So, I am putting these things together, because it is good to have one theorem which mentions the important facts about quotient rings. This is called the correspondence theorem and the bijection is in fact, given by: you take an ideal J. So, you take an element in this set in other words, you take an ideal J that by definition contains kernel phi, because it is in this set you map it to phi of J ok.

So, we have seen in an earlier video that image of an ideal under a ring homomorphism is an ideal. On other hand we take an ideal J prime of S; J prime is an ideal of S and you simply take phi inverse of J prime ok. And we have also seen in that problem set that, if you have a ring homomorphism which is onto, in other words it is a surjective, inverse image of an ideal is an ideal. Here the map from R to S is surjective by definition because S is defined to be the image right. S is defined to be the image. So, R to S is a surjective ring homomorphism. So, inverse image is an ideal, we have to show; however, that it contains kernel phi in order to land in the set ok. So, this we will do in the proof.

So, theorem has three parts, let us prove them one by one.

(Refer Slide Time: 06:25)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help
30/30
30
09:18

$\varphi(S)$

Proof: (1) To show that S is a subring of R',
we have to check:

- $1_{R'} \in S'$ ✓ $1=\varphi(1_R)$
- S closed under addition ✓

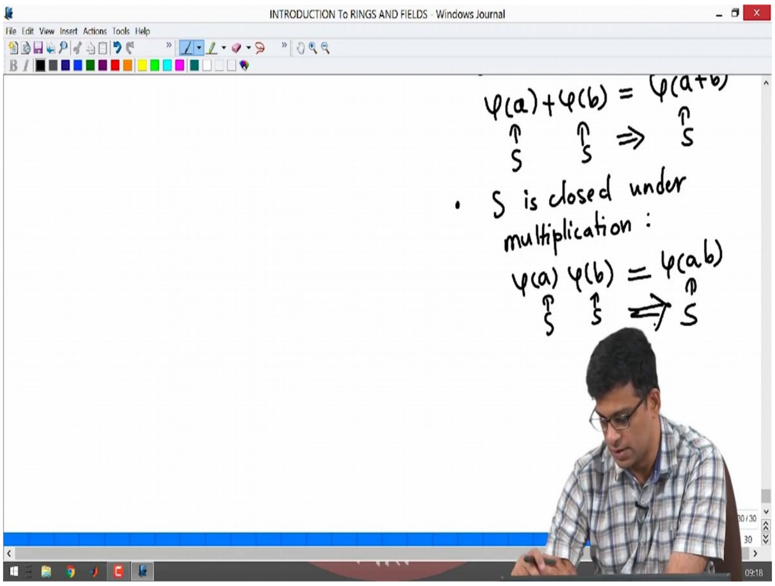
$$\underset{\substack{\uparrow\\ S}}{\varphi(a)}+\underset{\substack{\uparrow\\ S}}{\varphi(b)} = \underset{\substack{\uparrow\\ S}}{\varphi(a+b)}$$

$$\Rightarrow$$

So, proof theorem: the first part is fairly easy. So, let us quickly prove this. What is the meaning of a subring? To show S is a subring, to show that S is a subring of R prime, we have to check various things right. We have to check for example, so, I will list some of these properties now. We have to check that 1 is in S prime is 1in S prime S, because 1 is remember this is because 1 is phi of 1.

So, here of course, I mean 1 of R prime and here I mean 1 of R. So, I am writing this just for clarity, if you take the multiplicative identity element of R, its image under a ring homomorphism by definition is the multiplicative identity of R prime. So, 1 is in S prime. So, is S closed under addition this is also right. If you take phi of a plus phi of b so, two elements of S are of the form phi of a and phi of b, their sum is simply phi of a plus b right. So, that is also in S.

(Refer Slide Time: 07:46)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

$$\underset{S}{\underset{\uparrow}{\varphi(a)}}+\underset{S}{\underset{\uparrow}{\varphi(b)}} = \underset{S}{\underset{\uparrow}{\varphi(a+b)}} \quad \Rightarrow$$

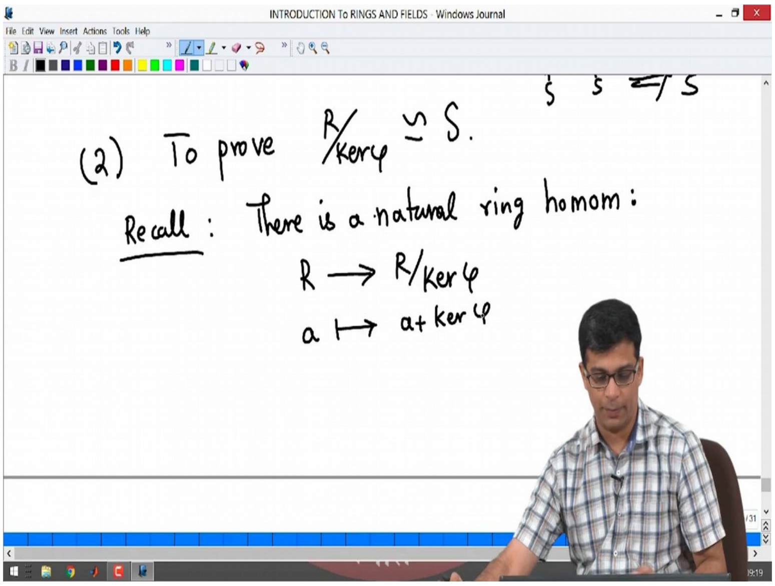
- S is closed under multiplication :

$$\underset{S}{\underset{\uparrow}{\varphi(a)}}\,\underset{S}{\underset{\uparrow}{\varphi(b)}} = \underset{S}{\underset{\uparrow}{\varphi(ab)}} \quad \Rightarrow$$

So, this is in S, this is in S, this implies this is in S and third property is S is closed under multiplication. This is also trivial right.

So, this is exactly the same calculation. This is because if you take two elements of S they are by definition of the form phi a and phi b, their product is, because phi is a group homomorphism is, phi a b which is again by definition in S. Because it is the image of a b. So, S is a subring ok. So, this is easy to check and I will not do this I will not do this more details of this, but. So, this proves that S is the subring ok.

(Refer Slide Time: 08:37)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

$S \quad S \Rightarrow S$

(2) To prove $R/\ker\varphi \cong S$.

Recall : There is a natural ring homom :

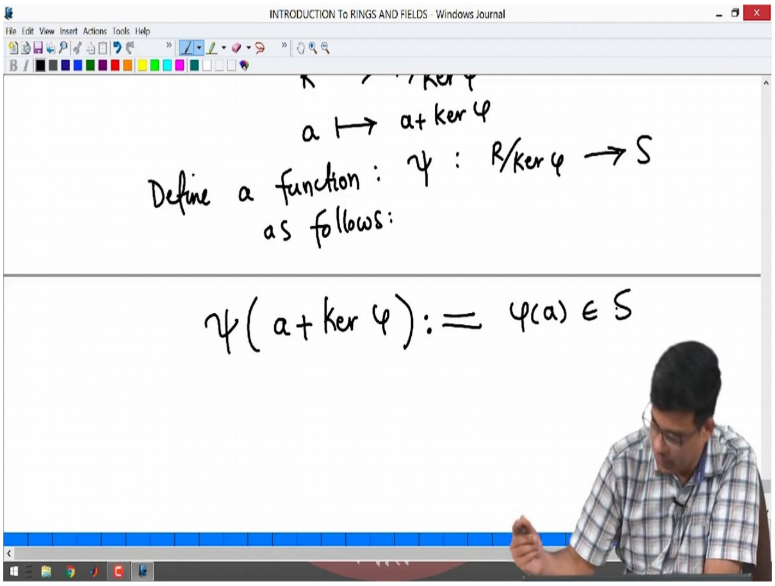
$$R \longrightarrow R/\ker\varphi$$
$$a \longmapsto a+\ker\varphi$$

So, second property says that remember, what is the second statement that S mod R mod kernel phi. So, we want to prove here is s. So, this is what we want to show.

So, we now use the notion of ring, quotient rings. So, recall from last video so recall, we have a natural homomorphism, natural ring homomorphism from R to R mod kernel phi ok. And what is this? This simply sends an element a to a plus kernel phi. So, remember this is exactly the map that we have in the group theory, when you have a group homomorphism you have this map.

Now, using this I can define the function first of all from R mod kernel phi to S.

(Refer Slide Time: 09:50)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

$R \to R/\ker\varphi$

$a \mapsto a + \ker\varphi$

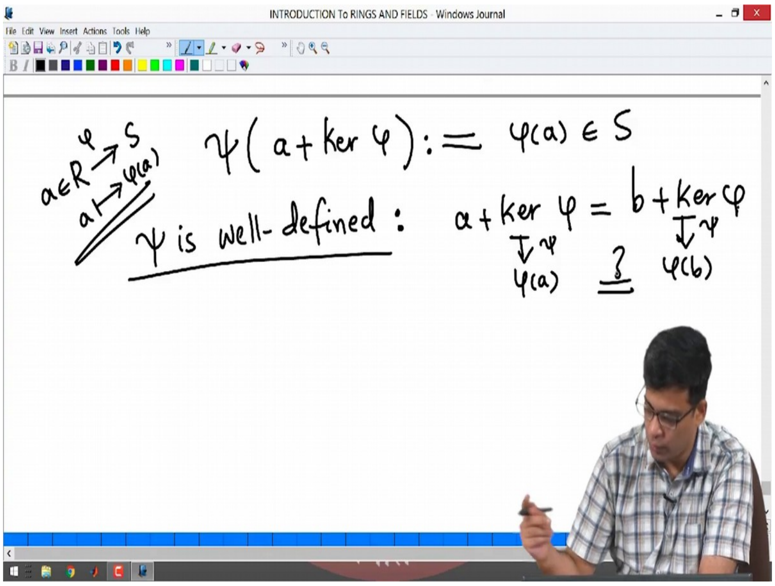
Define a function : $\psi : R/\ker\varphi \to S$
as follows:

$\psi(a + \ker\varphi) := \varphi(a) \in S$

So, define a function, let us call that may be psi from R mod kernel phi to S as follows. So, remember I am trying to show that R mod kernel of phi is isomorphic to S. In order to do that, I will first define a function, I will show that it is a homomorphism then I will show that it is bijective.

So, the first step is to define the function. So, what is an arbitrary element of R mod kernel phi, it is of the form a plus kernel phi. And I define this to be simply phi of a of course, phi of a is in S right.

(Refer Slide Time: 10:46)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

$a \in R \xrightarrow{\varphi} S$

$a \mapsto \varphi(a)$

$\psi(a + \ker \varphi) := \varphi(a) \in S$

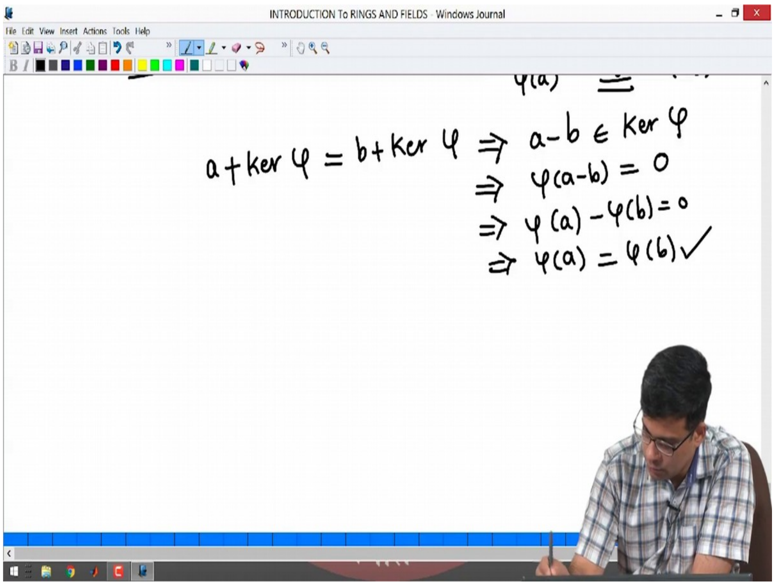
$\underline{\psi \text{ is well-defined}}:$

$$\begin{tikzcd} a + \ker \varphi \arrow[d, "\psi"] \arrow[r, phantom, "="] & b + \ker \varphi \arrow[d, "\psi"] \\ \varphi(a) \arrow[r, phantom, "\overset{?}{=}"] & \varphi(b) \end{tikzcd}$$

So, here remember a plus kernel phi means a is in R. We have a function from R to S, namely phi a goes to phi of a.

So, now we have to check that, this is well defined, this is fine to define it like this, but phi psi is well defined. Why do we need to show it is well defined? Because it seems to depend on the representative for a coset in the quotient ring because a plus kernel phi perhaps is equal to b plus kernel phi, remember a coset of the form a plus kernel phi often is also equal to some other element plus kernel phi, b and a could be different. So, a plus kernel phi could be same as b plus kernel phi as elements of R mod kernel phi. In order for psi to be well defined, I need the image of psi for these two elements should be the same, but I am sending this to phi of a under psi I am sending this to phi of a I am sending this under psi to phi of b, are these two equal is what I have to check.

(Refer Slide Time: 11:58)

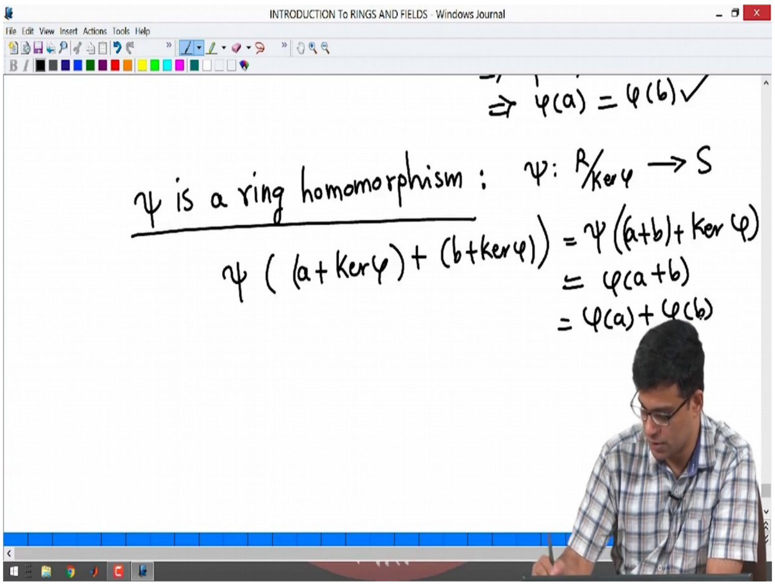


$$a + \ker\varphi = b + \ker\varphi \Rightarrow a - b \in \ker\varphi$$
$$\Rightarrow \varphi(a-b) = 0$$
$$\Rightarrow \varphi(a) - \varphi(b) = 0$$
$$\Rightarrow \varphi(a) = \varphi(b) ✓$$

But then that once you identify what needs to be showed, it is easy to show this. So, suppose a plus b a plus kernel phi is equal to b plus kernel phi. This by definition means a minus b is in the kernel right. If two additive cosets are equal the differences of these two elements is in the subgroup, but if a minus b is in the kernel, phi of a minus b is by definition 0, kernel consists of those elements which map to 0; that means, because phi is a homomorphism of rings, phi of a minus phi of b is 0; that means, phi of a is equal to phi of b right.

So, we have if a plus kernel phi is equal to be plus kernel phi, we have verified that phi of a is equal to phi of b. So, psi is well defined. So, that is good.

(Refer Slide Time: 12:48)



$$\Rightarrow \varphi(a) = \varphi(b) ✓$$

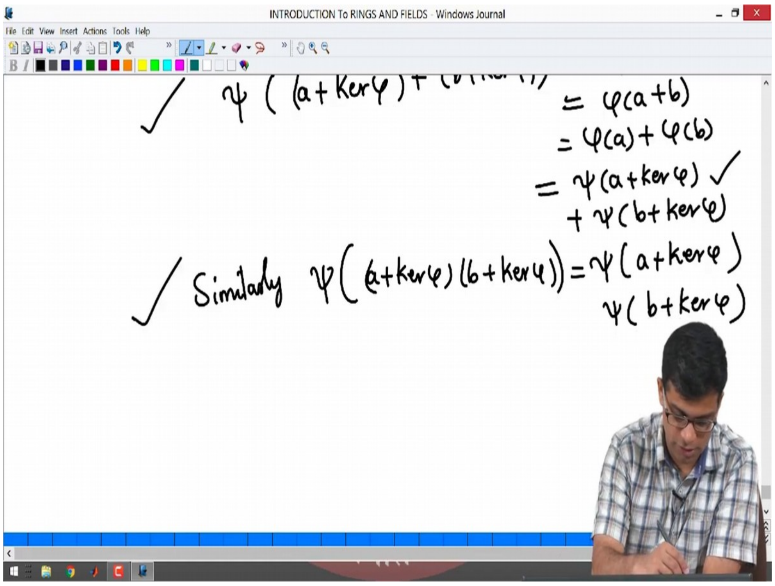
$\underline{\psi \text{ is a ring homomorphism}}$: $\psi : R/\ker\varphi \to S$

$$\psi\big((a + \ker\varphi) + (b + \ker\varphi)\big) = \psi\big((a+b) + \ker\varphi\big)$$
$$= \varphi(a+b)$$
$$= \varphi(a) + \varphi(b)$$

Next, we will show that psi is a ring homomorphism. So, remember our strategy, I want to show two rings are isomorphic, namely R mod kernel phi is isomorphic to S. What is our strategy? We will start with defining a function from one ring to the other, then we want to check the, we will check that it is a ring homomorphism, then we will check that it is 1-1 and then we will check that its onto. We have already checked that we have a well defined function.

Now, let us take that, it is a ring homomorphism. So, what I have to check is. So, remember psi is a function from R mod kernel phi to S. So, we want to check that psi of a plus kernel phi plus psi of b plus sorry a plus kernel phi plus b plus kernel phi. So, take two arbitrary elements of the quotient ring, take the sum and apply psi, but this is equal to psi of because the addition in the quotient ring is simply a plus b plus kernel psi phi. And by definition psi of a plus b plus kernel phi is a plus b phi of a plus b which is by definition of ring homomorphism is equal to phi of a plus phi of b which is equal to.

(Refer Slide Time: 14:14)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

✓ $\psi\big((a+\operatorname{Ker}\varphi)+$

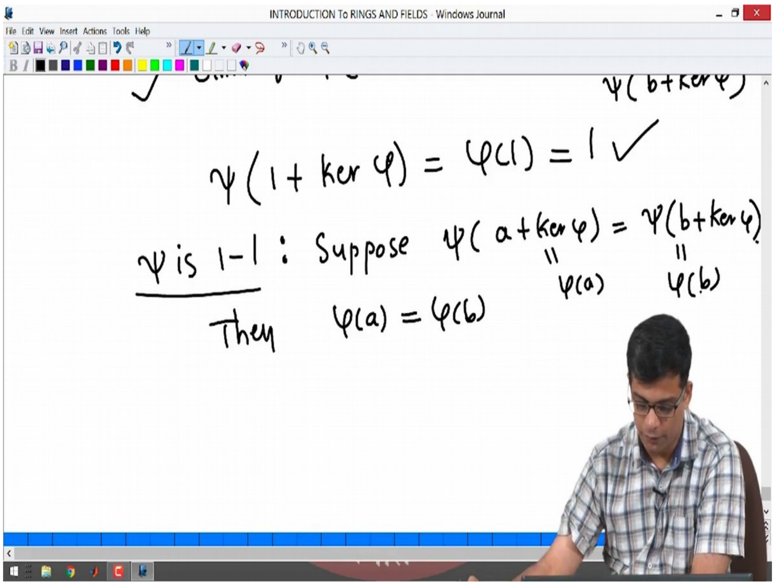
$$= \varphi(a+b)$$
$$= \varphi(a)+\varphi(b)$$
$$= \psi(a+\ker\varphi) \checkmark$$
$$+ \psi(b+\ker\varphi)$$

✓ Similarly $\psi\big((a+\ker\varphi)(b+\ker\varphi)\big) = \psi(a+\ker\varphi)\,\psi(b+\ker\varphi)$

So, this we will write is psi of a plus kernel phi plus psi of b plus kernel phi ok. So, this is right. So, each step I hope is clear.

So, we have checked that psi is psi of sum of two elements is sum of psi of those elements, similarly exactly the same calculation, we can show that psi of a plus kernel phi and times b plus kernel phi. So, there is nothing really to do here is psi of a plus kernel phi times psi of b plus kernel phi ok. So, this is also this is.

(Refer Slide Time: 15:02)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

✓ $\psi(b+\ker\varphi)$

$$\psi(1+\ker\varphi) = \varphi(1) = 1 \checkmark$$

$\underline{\psi \text{ is } 1\text{-}1}$: Suppose $\underset{\substack{\| \\ \varphi(a)}}{\psi(a+\ker\varphi)} = \underset{\substack{\| \\ \varphi(b)}}{\psi(b+\ker\varphi)}$

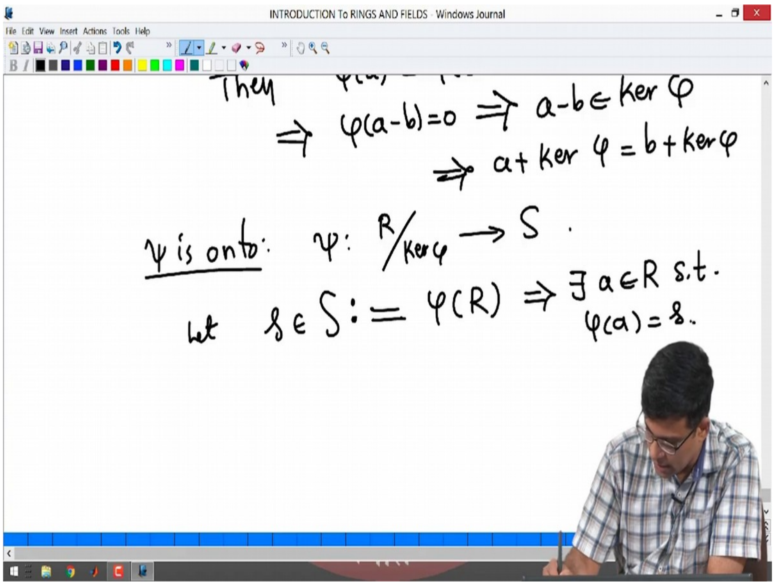
Then $\varphi(a) = \varphi(b)$

What is the third property of a ring homomorphism, we want to check that psi of the identity element is the identity element. What is the multiplicative identity element of R mod kernel phi? It is by definition 1 plus kernel phi, but this is by definition phi of 1, but phi of 1 is 1. So, this is also ok. So, in other words psi is a ring homomorphism. So, we have shown that psi is a ring homomorphism. So, far we have a ring homomorphism.

Next step is to show psi is 1-1 or psi is injective ok. So, how do we show this, what is injectivity mean, if image of two elements is equal those two elements are equal. So, suppose psi of a plus kernel phi is equal to psi of b plus kernel phi ok. What am I interested in showing? I am interested in showing that a plus kernel phi is equal to b plus kernel phi.

So, let us see how do we show that, this is also simple. So, if this happens by definition phi of a is equal to phi of b because this is phi of a by definition of psi and this is phi of b.

(Refer Slide Time: 16:16)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

They

$\Rightarrow \varphi(a-b)=0 \Rightarrow a-b\in \ker\varphi$

$\Rightarrow a+\ker\varphi = b+\ker\varphi$

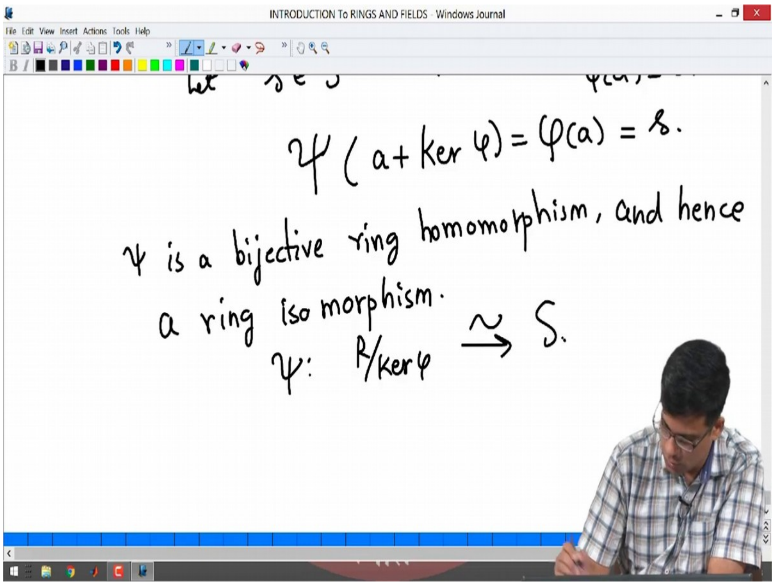
ψ is onto: $\psi: R/_{\ker\varphi} \longrightarrow S$.

Let $s \in S := \varphi(R) \Rightarrow \exists\, a\in R$ s.t. $\varphi(a)=s$.

So, now phi of a is equal to phi of b; that means, phi of a minus b is 0 right. Because phi is a group ring homomorphism; that means, a minus b is in kernel phi and; that means, a plus kernel phi is equal to b plus kernel phi ok. So, this is and finally, psi is onto why is this? So, this is remember psi a function from R mod kernel phi S, we have we have. so, far showed that psi is a ring homomorphism. We have also showed that psi is a 1-1 function, last step is to show psi is onto.

So, pick any element of. So, let us say small s is an element of capital S, but what is capital S remember capital S is by definition phi of R right so; that means, there exists a in R such that phi of a equals S right; that means, small s is an image of something.

(Refer Slide Time: 17:29)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

Let

$\psi(a+\ker\varphi)=\varphi(a)=s$.

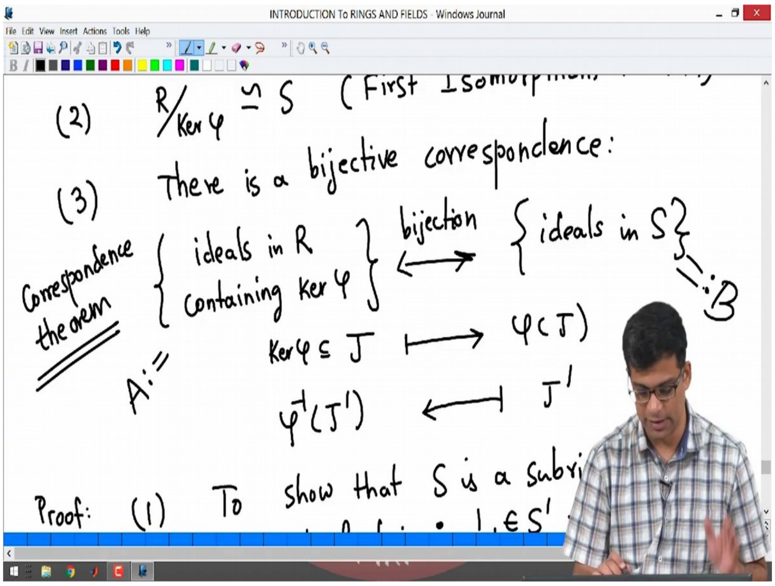
ψ is a bijective ring homomorphism, and hence a ring isomorphism.

$\psi: R/_{\ker\varphi} \xrightarrow{\sim} S$.

But; that means, psi of a plus kernel phi is by definition phi of a which is s ok. So, everything in S is in the image of psi. So, psi is onto.

So, in other words, psi is a bijective; bijective remember means its 1-1 and onto, bijective ring homomorphism, and hence a ring isomorphism ok. So, you have a bijective ring homomorphism, which is then automatically a ring isomorphism. So, in other words, we have showed that. So, psi is an isomorphism from R mod kernel phi to S. So, this is exactly the second part of the theorem. So, second part of the theorem said that R mod kernel phi. So, let us try to recall the statement of the theorem we have made three statements here.

(Refer Slide Time: 18:36)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

(2) $R/_{\mathrm{Ker}\,\varphi} \cong S$ (First Isomorphism

(3) There is a bijective correspondence:

Correspondence theorem

$A := \left\{ \begin{matrix} \text{ideals in } R \\ \text{Containing Ker } \varphi \end{matrix} \right\} \xleftrightarrow{\text{bijection}} \{\text{ideals in } S\} =: B$

$\mathrm{Ker}\,\varphi \subseteq J \longmapsto \varphi(J)$

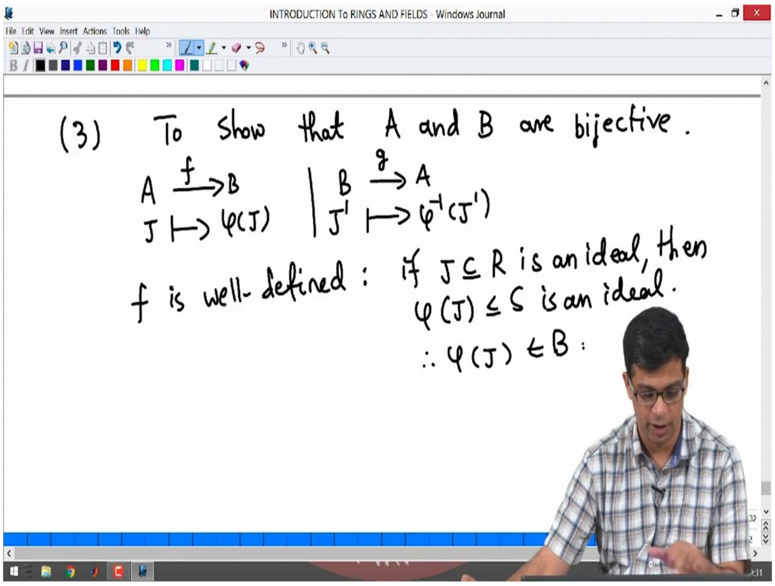
$\varphi^{-1}(J') \longleftarrow J'$

Proof: (1) To show that S is a subri

$1_{\ldots} \in S'$

First statement was that image of a ring homomorphism is a subring of the ring codomain, which we have proved. Second is R mod kernel phi is isomorphic to the image subring. So, that we just proved, the next step is to show: There is a bijective correspondence between the two sets. So, let us maybe call the sets A is a set of ideals in R containing kernel phi. And let say B is just all ideals of S. So, we are supposed to show that there is a bijection between A and B. A is the ideals in R containing kernel phi, B is ideals in R and we are also told what are the functions. From A to B the function say takes an ideal in R and simply maps it to its image, from B to A, the function takes an ideal in S maps it to its inverse image. Which we know is an ideal, but we have to show that it is. In fact, in B ok.

(Refer Slide Time: 19:34)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

(3) To show that A and B are bijective.

$A \xrightarrow{f} B$ | $B \xrightarrow{g} A$

$J \mapsto \varphi(J)$ | $J' \mapsto \varphi^{-1}(J')$

f is well-defined : if $J \subseteq R$ is an ideal, then $\varphi(J) \leq S$ is an ideal.

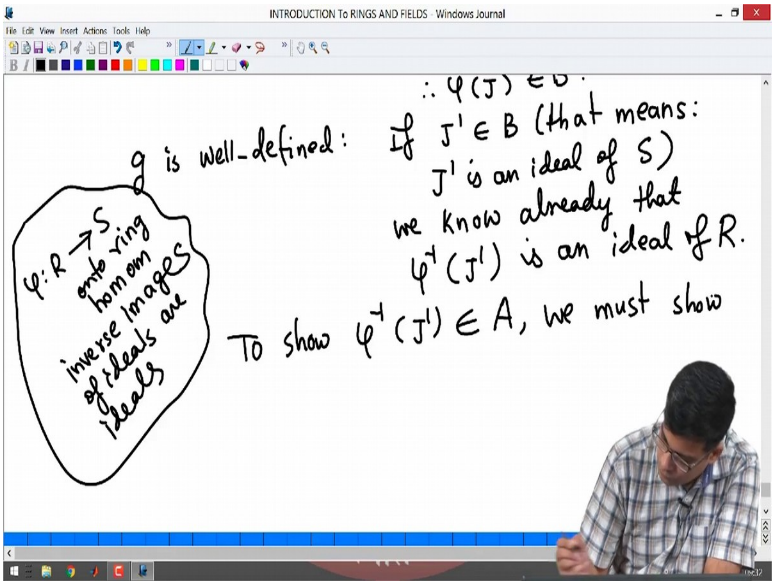
$\therefore \varphi(J) \in B$:

So, the third part, which I will prove now. So, to show that A and B with A and B just defined I defined in the statement are bijective. Remember A and B are just sets. So, there is no additional structure here, they are just sets. I want to show that they are bijective and the function is A to B J goes to phi of J and B to A J prime goes to phi inverse J ok. So, J prime phi inverse J prime ok.

So, the first statement is, this is a function. So, let us call this f let us call this J see, f is well defined f is well defined, because if J is an ideal in R, then we know always that phi of J is an ideal of S right. So, in other words phi of J is in B. So, there is nothing else to show all we have to show is that, you start with something in A here its image must be in B. So, that is what I have shown.

So, if you take an element in A its image is in J is in B.

(Refer Slide Time: 21:00)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

$\therefore \varphi(J) \in B.$

g is well-defined: If $J' \in B$ (that means: J' is an ideal of S)

we know already that $\varphi^{-1}(J')$ is an ideal of R.

$\varphi: R \to S$ onto ring homom inverse images of ideals are ideals

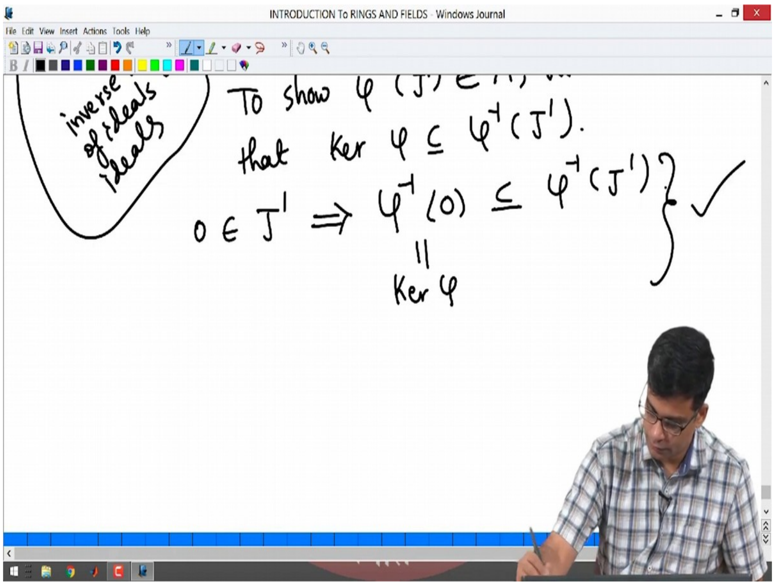
To show $\varphi^{-1}(J') \in A$, we must show

To show g is well defined, what we have to show is, if J prime is an ideal. So, J prime is in B let say; that means,; that means, what is B? Remember B is the set of ideals of S. That means, J prime is an ideal of B sorry J prime is an ideal of S, we have to show. So,

We I will first write this, we all we know already that phi inverse J prime is an ideal of R right. This we know because, if you have a onto ring map; onto ring homomorphism inverse image of ideals inverse images of ideals are ideals. This I proved in a problem session few videos ago, but it does not yet prove that it is in A. What is A? A is not set of all ideals in R right, A is not the set of all ideals in R. A is a set of ideals in R that contain kernel phi.

So, to show phi inverse J prime is in A, we must show that it is an ideal is that we have showed already.

(Refer Slide Time: 22:47)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

inverse of ideals ideals

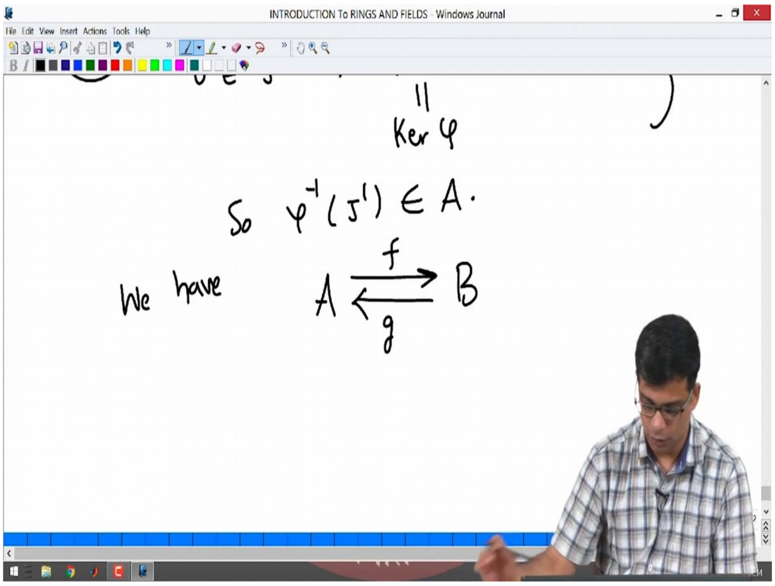
To show $\varphi\,(J') \in A,$

that $\operatorname{Ker}\varphi \subseteq \varphi^{-1}(J')$.

$$0 \in J' \Rightarrow \underset{\substack{\| \\ \operatorname{Ker}\varphi}}{\varphi^{-1}(0)} \subseteq \varphi^{-1}(J') \Big\} \checkmark$$

We must show in addition that, kernel phi is contained in J prime sorry contained in phi inverse J prime. Remember A capital A consists of all ideals of R that contain the kernel. So, in order for us to show that phi inverse J prime is in A, we need to show that kernel phi is in phi inverse J prime. And this is not difficult because remember J prime is an ideal. So, J prime contains 0, the 0 element of the ring S, but this means just a set theoretic statements, phi inverse 0 is contained in phi inverse J prime right. If you have two one set contained in another, inverse images have the same inclusion anything that maps to 0 is in the inverse image of J prime. So, this is ok, but what is phi inverse 0 this is by definition kernel phi. This is just a different way of writing kernel phi. Because kernel phi is the set of elements which map to 0; that means, kernel phi is phi inverse 0. So, this is.

(Refer Slide Time: 23:53)



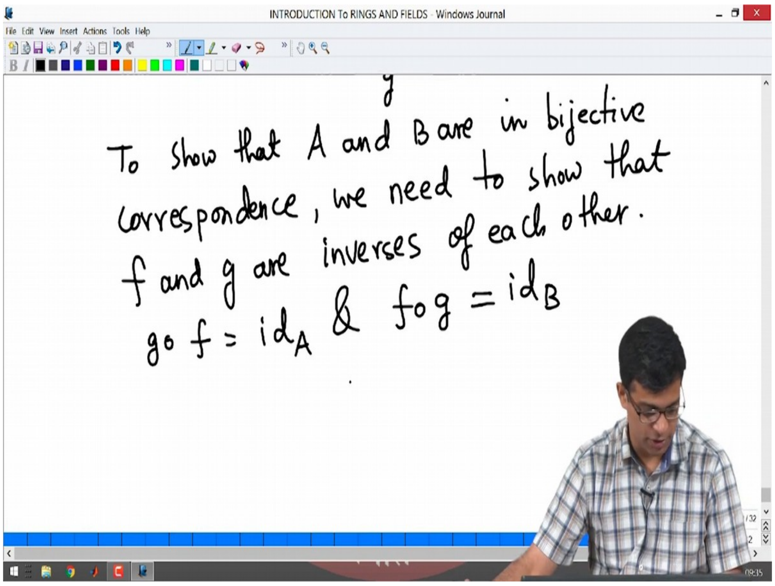
$$\begin{tikzcd} {} \arrow[d, phantom, "\parallel"] \\ \operatorname{Ker}\varphi \end{tikzcd}$$

So $\varphi^{-1}(J') \in A$.

We have $$\begin{tikzcd} A \arrow[r, shift left, "f"] & B \arrow[l, shift left, "g"] \end{tikzcd}$$

So, in other words phi inverse J prime does belong to A. So, now, we have functions. So, I will write it like this we have functions from A f goes to B and g goes to. So, f goes from A to B, g goes from B to A.

(Refer Slide Time: 24:19)



To show that A and B are in bijective correspondence, we need to show that f and g are inverses of each other.

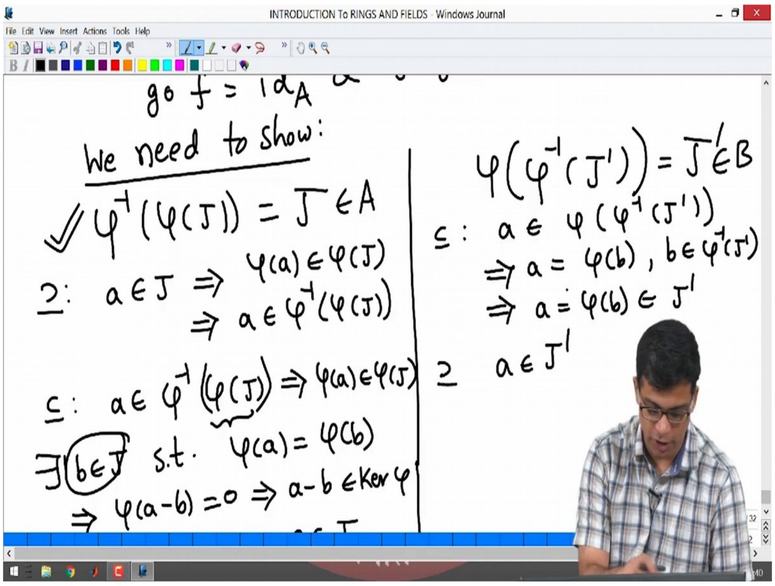
$g \circ f = id_A$ & $f \circ g = id_B$

Now, how do we show, that they are bijective. To show that A and B are in bijective correspondence to show that they are in bijective correspondents, it is of course, not enough to produce two functions right. We need to produce that they are inverses of each other, we need to show that f and g are inverses of each other. This is the usual way of showing two sets are bijective.

So, in other words, what we have to show is that if you first travel via f then travel via g. So, you start with A go to B via f then come back to A, it must be the identity function on A and similarly if you first do g and then f this must be identity function on B. So, we need to check these two, in terms of the definition of f and g that we had earlier.

What we have to show in other words?

(Refer Slide Time: 25:27)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

$g \circ f = id_A$

We need to show:

✓ $\varphi^{-1}(\varphi(J)) = J \in A$

$\supseteq$: $a \in J \Rightarrow \varphi(a) \in \varphi(J)$
$\Rightarrow a \in \varphi^{-1}(\varphi(J))$

$\subseteq$: $a \in \varphi^{-1}(\varphi(J)) \Rightarrow \varphi(a) \in \varphi(J)$
$\exists\, \boxed{b \in J}$ s.t. $\varphi(a) = \varphi(b)$
$\Rightarrow \varphi(a-b) = 0 \Rightarrow a-b \in \mathrm{Ker}\,\varphi$

$\varphi(\varphi^{-1}(J')) = J' \in B$

$\subseteq$: $a \in \varphi(\varphi^{-1}(J'))$
$\Rightarrow a = \varphi(b),\ b \in \varphi^{-1}(J')$
$\Rightarrow a = \varphi(b) \in J'$

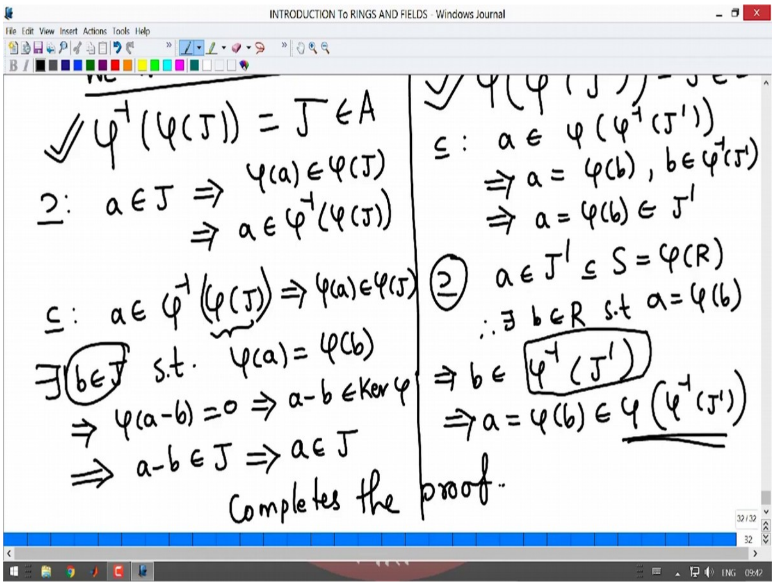
$\supseteq$ $a \in J'$

So, we need to show two things, I will write them here and check them. We need to show. So, I will write two things here. So, first is phi inverse of phi of J is J ok, this is one of these things. So, first take f and then take g. So, this is the first one you start with an ideal in R that contains kernel phi take, its image then take the inverse image you get J and what is the correspondence for f circle g is identity B.

You first take phi inverse J prime then take phi, you need to get J. So, this J is in A, J prime is in B. So, let us check these things now. So, these are once you identify them they are not difficult. Almost all of these are just set theoretic properties and in one place you want to use that J contains kernel phi.

So, this let me show it like this. So, the this is an equality of two sets in A. So, to check that they are equal I need to show that one each contains the other. So, to show that J is contained in phi inverse phi J is clear. Because, so, suppose a is in J; that means, by definition phi of a is in phi of J right. If a is in J phi of a is in phi of j, but that means, a must be in phi inverse of phi J right. Because a maps to phi J. So, inverse image of phi J must contain a. What is inverse image of phi J? These are all elements that map to phi J. So, a is one such. So, a is in phi inverse phi J. So, we started with something in J and we showed that its in phi inverse phi J.

(Refer Slide Time: 27:14)



INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help
32 / 32
32
ENG 09:42

✓ $\varphi^{-1}(\varphi(J)) = J \in A$

$\supseteq$: $a \in J \Rightarrow \varphi(a) \in \varphi(J)$

$\Rightarrow a \in \varphi^{-1}(\varphi(J))$

$\subseteq$: $a \in \varphi^{-1}(\underset{\sim}{\varphi(J)}) \Rightarrow \varphi(a) \in \varphi(J)$

$\exists \boxed{b \in J}$ s.t. $\varphi(a) = \varphi(b)$

$\Rightarrow \varphi(a-b) = 0 \Rightarrow a-b \in \operatorname{Ker}\varphi$

$\Rightarrow a-b \in J \Rightarrow a \in J$

Completes the proof.

✓ $\varphi(\varphi^{-1}(J')) = J' \in$

$\subseteq$: $a \in \varphi(\varphi^{-1}(J'))$

$\Rightarrow a = \varphi(b)$, $b \in \varphi^{-1}(J')$

$\Rightarrow a = \varphi(b) \in J'$

$\boxed{2}$ $a \in J' \subseteq S = \varphi(R)$

$\therefore \exists\, b \in R$ s.t $a = \varphi(b)$

$\Rightarrow b \in \boxed{\varphi^{-1}(J')}$

$\Rightarrow a = \varphi(b) \in \underline{\varphi(\varphi^{-1}(J'))}$

To prove the opposite inclusion, let us start with an element of phi inverse phi J. So, I am now starting with an element of phi inverse phi J and I want to show its image is in it is in J. So, this implies first of all that phi of a; obviously, is in phi J. This is the definition of being in the inverse image of phi J. Something is in the inverse image of phi J. So, something is in the inverse image of phi J; that means, its image is in phi J, but then we can not immediately conclude a is in B a is in J, because phi of a is in phi of J does not in general mean a is in J.

However what it means is that there exists a b in J such that phi of a equals phi of b, right. Because what is phi of J? Phi of J is by definition all elements phi of all elements of J. So, phi of a is in; that means, its equal to phi of b for some b in J, but this means phi of a minus b is 0 because phi of a is equal to phi of b, but this means a minus b is in the kernel right. a minus b is in the kernel, but now remember that J is in A; that means, J contains kernel phi capital A consists of all ideals that contain kernel phi. So, a minus b is in the kernel means, a minus b is in J, but b is already in J right. So, b is in J means, and a minus b is in J means a sum is in j; that means, a is in J. Which is what we want to show, we started with something in phi inverse phi J and we have showed that it is in J. So, this is.

Now, to come to this, this is even more easy to phi of phi inverse J prime is J prime. So, again let us prove these two inequalities. So, to prove the inclusion of the left hand side into in the right hand side, let us take a in phi of phi inverse J prime. So, a is in phi inverse phi of phi inverse J prime; that means, a is equal to phi of b for some b in phi inverse J prime right. That is the definition of being in the image of this; a is equal to phi of this means there is something inside phi inverse J prime, such that a is equal to phi of b, but b is in phi inverse J prime; that means, a is equal to phi b is in J prime. Because if b is in phi inverse J prime phi of b is in J prime; that means, a is in J prime. So, that is exactly the inclusion of this in J prime.

Now, the opposite inclusion is also easy, let us pick something in J prime. So, this is actually completely set-theoretic. This equality always holds in the left hand side here one of the equalities always holds.

So, a is in J prime; that means, remember J prime is in S and S is the image of it S is the image of R. So, there exists b in R such that a equals phi of b right. By definition a is in the image means, a is equal to phi of some element, but that means, a is in J prime. So, b is in phi inverse J prime right, because phi of b is J prime b is in phi inverse J prime, but; that means, so, b is in phi inverse J prime; that means, a which is phi of b is in phi of see, b is inside phi inverse J prime. So, its image is phi of phi inverse J prime. So, b is in this. So, phi of b is phi of, is in phi of this. So, its in phi of phi inverse J prime, which is exactly the ideal here. So, a is inside this. So, we have proved this.

So, we started with something in J prime, we have showed it is here ok. So, these are both showed so; that means, the functions f and g that I have defined here are inverse of each other. So, I may have gone a little bit fast for the last part, but in that case please pause the video, think about this, if you have any doubts listen to the video again and hopefully this will become clear to you.

So, what I have done is. So, this completes the proof. I have proved that correspondence theorem between ideals of R that contain kernel phi and ideals of S. And I have also proved in this theorem that R mod kernel phi is isomorphic to S, which is called the first isomorphism theorem ok. And this is an important theorem. So, I am going to stop the video here; in the next video, we will do some examples to understand all the results that we have done in this theorem.

Thank you.