Galois' Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture No 11
Regression on Rings homomorphism, Algebras

(Refer Slide Time 00:25)

Let me recall that in the last lecture we have seen examples of non-algebraically closed fields and we have also stated fundamental theorem of algebra

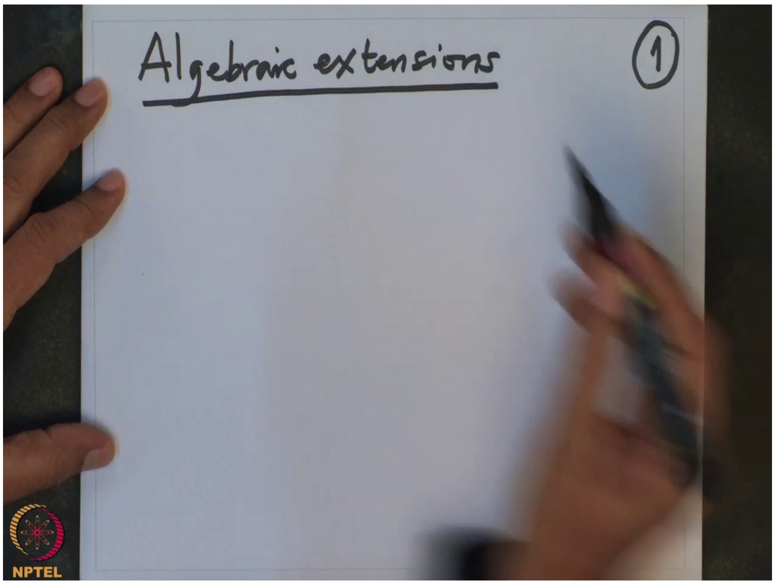
(Refer Slide Time 00:41)

which says that the field of complex numbers is algebraically closed and the proof is pending.

When I have enough prerequisites I will come back to the proof of this. That is one thing.

Next thing is today I am going to introduce what are called algebraic extensions and study their basic properties. And to

(Refer Slide Time 01:16)



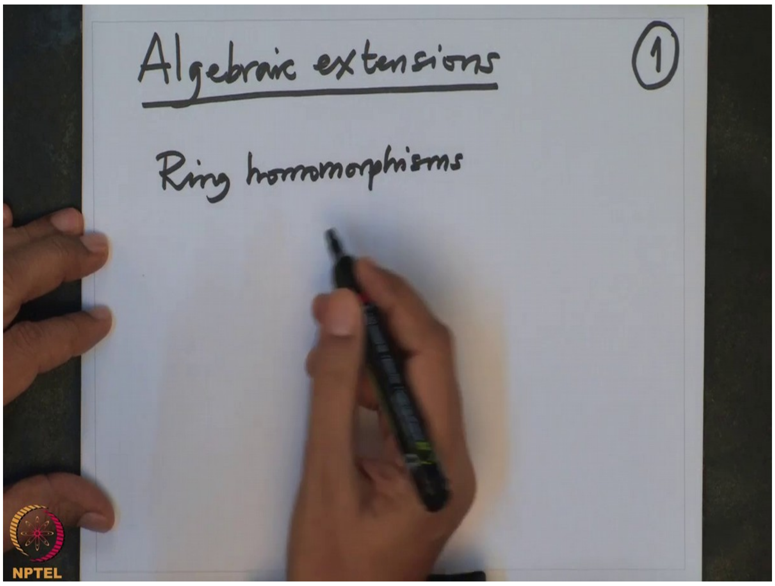
do this, also I will need some concepts from elementary abstract algebra which are concerning rings, ring homomorphisms, ideals, prime ideals etc.

So all these concepts I will briefly recall with the some guiding examples. So they should keep us going little faster in pace and also we will reach the subject with more relevant prerequisites. So as you know that we are studying polynomials over a field and especially their zeros or their roots and we have seen that the zeroes of a given polynomial with a coefficients in a given field, that may not lie in the field K.

Only some of them can lie in the field K and all of them may not lie in the field K. So we want to extend our given base field to a larger field so that the given polynomial has all zeroes in that bigger field. This is our main aim now and then we want to see how minimally we can do that and study these relationships. Those are precisely what are called Galois extensions of the polynomial F.

So let slowly start recalling. Suppose when we have a polynomial F, when we have a polynomial F...so before I go on to the polynomial I briefly recall what is ring homomorphism. Ring homomorphism is I think, I had briefly recalled earlier also. But let us do it once again.

(Refer Slide Time 03:21)



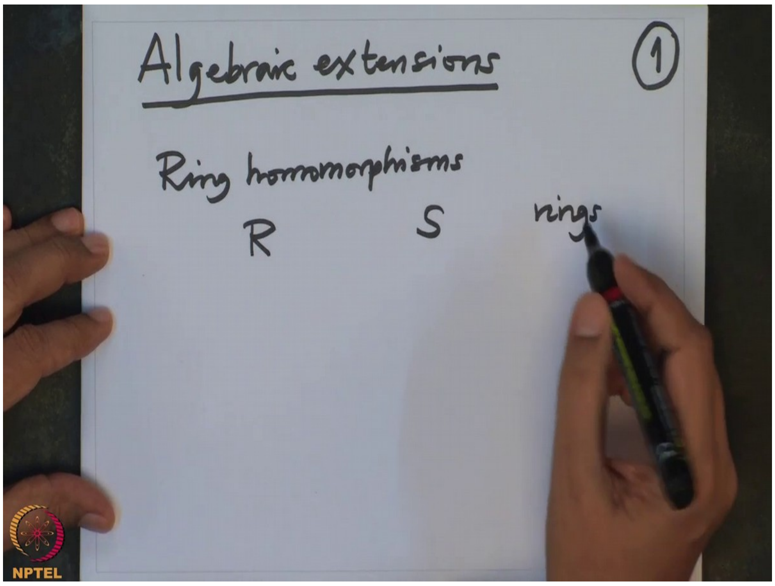
Algebraic extensions

1

Ring homomorphisms

So when we have two rings R and S, they are rings and let me remind

(Refer Slide Time 03:30)



Algebraic extensions

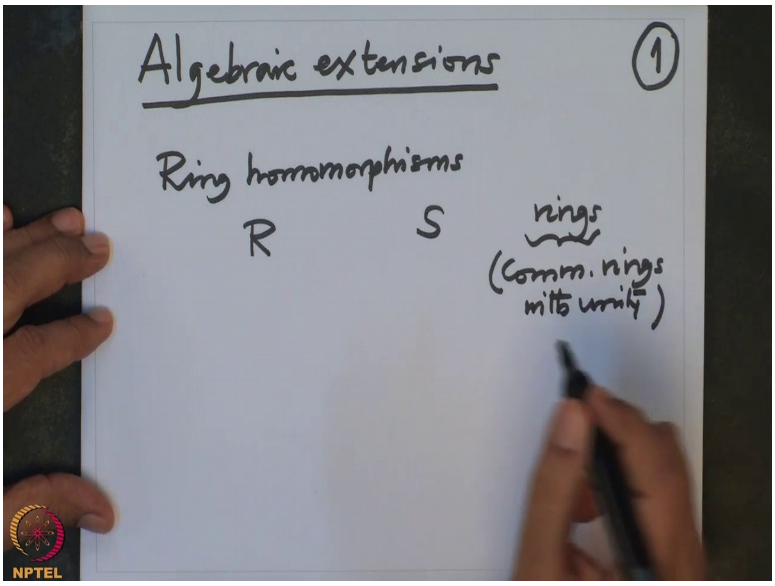
1

Ring homomorphisms

R S rings

you, when I say rings, by definition they are commutative rings with unity. Unity means multiplicative

(Refer Slide Time 03:45)



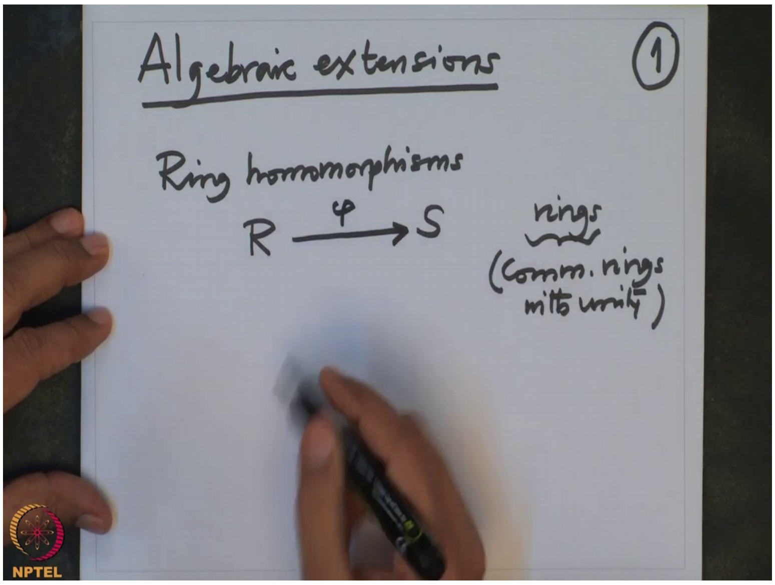
Algebraic extensions ①

Ring homomorphisms

R S $\underbrace{\text{rings}}$ (comm. rings with unity)

identity that means it is a neutral element for the multiplicative monoid made of R, multiplicative not of S. So ring homomorphism is a map ϕ from R to S

(Refer Slide Time 03:59)



Algebraic extensions ①

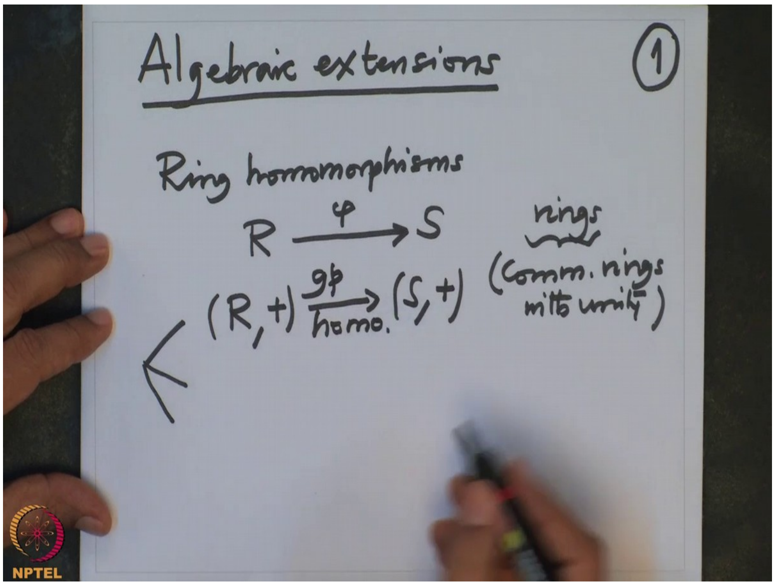
Ring homomorphisms

$R \xrightarrow{\varphi} S$ $\underbrace{\text{rings}}$ (comm. rings with unity)

such that it satisfies 3 properties.

One, it should respect the addition, that means it should be, when you think it is a map from (R ,+) to (S,+), it should be a group homomorphism. So this is a group homomorphism.

(Refer Slide Time 04:22)



Algebraic extensions

1

Ring homomorphisms

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

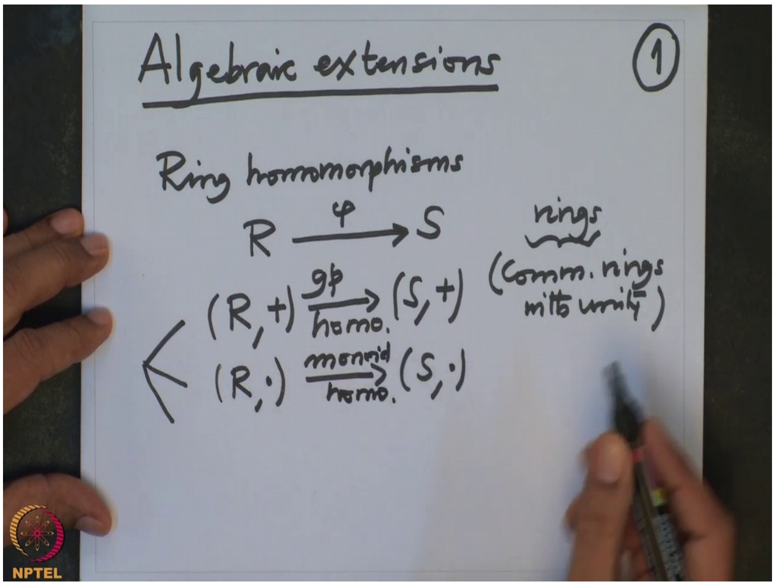
rings

(comm. rings with unity)

$$(R,+) \xrightarrow[\text{homo.}]{\text{gp}} (S,+)$$

And when you restrict, when you think it is a map from a monoid, a multiplicative monoid of R to multiplicative monoid of S this should be a monoid homomorphism.

(Refer Slide Time 04:39)



Algebraic extensions

1

Ring homomorphisms

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

rings

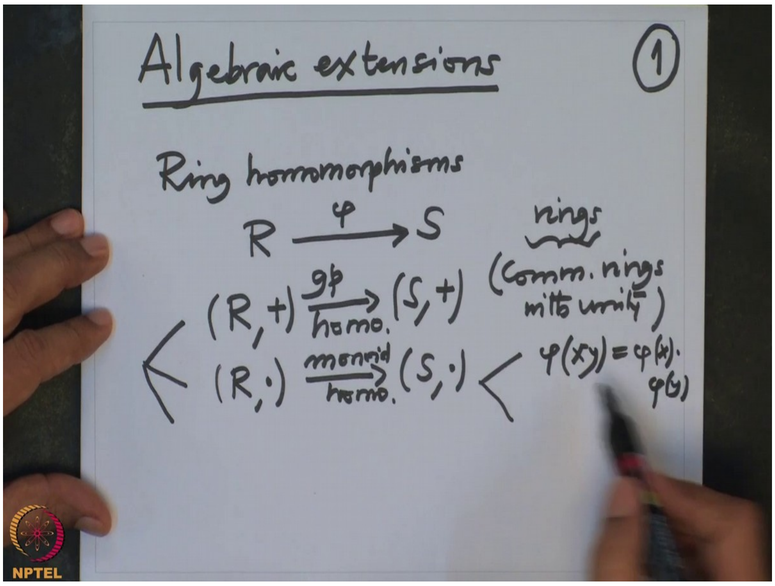
(comm. rings with unity)

$$(R,+) \xrightarrow[\text{homo.}]{\text{gp}} (S,+)$$

$$(R,\cdot) \xrightarrow[\text{homo.}]{\text{monoid}} (S,\cdot)$$

And let me stress monoid homomorphism has two, two requirements, that it respect the multiplication that is one, so this is $\phi(x \times y) = \phi(x) \times \phi(y)$ and again and again

(Refer Slide Time 05:01)



Algebraic extensions ①

Ring homomorphisms

$R \xrightarrow{\varphi} S$ $\underbrace{\text{rings}}$ (comm. rings with unity)

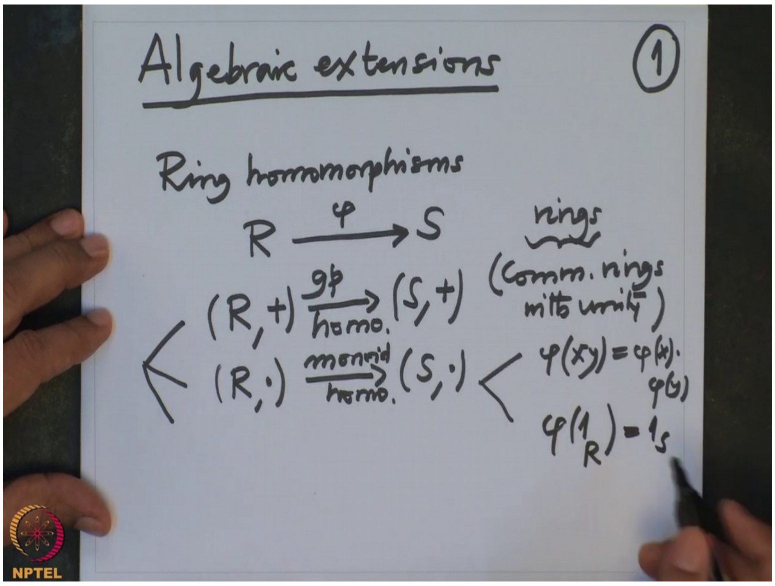
$(R,+) \xrightarrow[\text{homo.}]{\text{gp}} (S,+)$

$(R,\cdot) \xrightarrow[\text{homo.}]{\text{monoid}} (S,\cdot)$ $\varphi(xy)=\varphi(x)\cdot\varphi(y)$

I mentioned earlier also, this x y is a product in R and this $\phi(x)\phi(y)$ is a product in S. So though we are writing in the same, it is understood that when you write like this, first we are taking the product in R and then taking its image. And this means first taking the images and then multiplying in S. These two results are same.

So that is first property of the monoid homomorphism. Another one is ϕ of identity 1_R should go to 1_S . Normally

(Refer Slide Time 05:36)



Algebraic extensions ①

Ring homomorphisms

$R \xrightarrow{\varphi} S$ $\underbrace{\text{rings}}$ (comm. rings with unity)

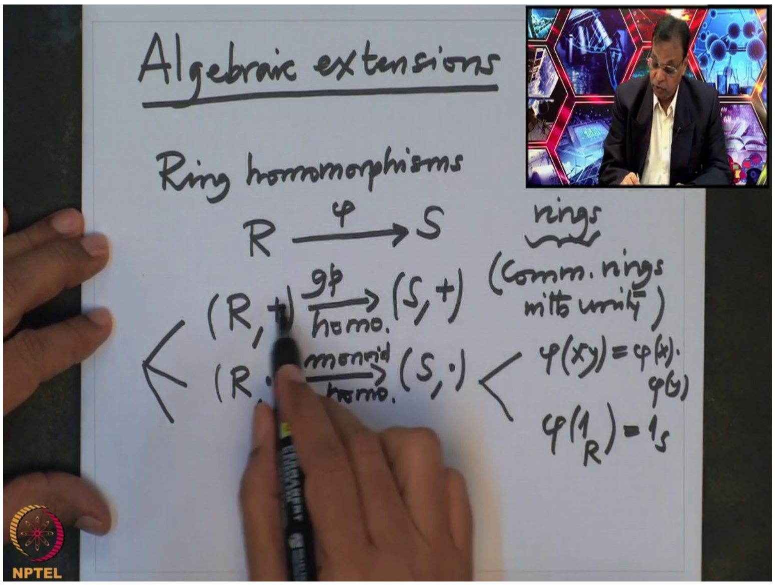
$(R,+) \xrightarrow[\text{homo.}]{\text{gp}} (S,+)$

$(R,\cdot) \xrightarrow[\text{homo.}]{\text{monoid}} (S,\cdot)$ $\varphi(xy)=\varphi(x)\cdot\varphi(y)$

$\varphi(1_R)=1_S$

many books, they do not assume this but I will assume in this course that it satisfies this property and it is very important. And I

(Refer Slide Time 05:47)



Algebraic extensions

Ring homomorphisms

$R \xrightarrow{\varphi} S$ rings (Comm. rings with unity)

$(R,+) \xrightarrow[\text{homo.}]{\text{gp}} (S,+)$

$(R,\cdot) \xrightarrow[\text{homo.}]{\text{monoid}} (S,\cdot)$

$\varphi(xy) = \varphi(x)\cdot\varphi(y)$

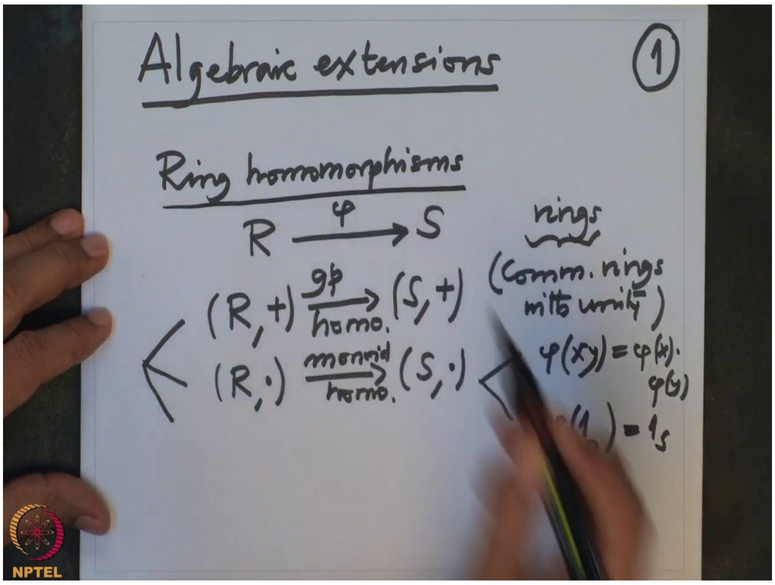
$\varphi(1_R) = 1_S$

NPTEL

do not, again the group homomorphism, just whether you add and take the image or take the images and add this result is same.

So such a map between a ring is called ring homomorphisms. And now we want to see some examples of ring

(Refer Slide Time 06:05)



Algebraic extensions ①

Ring homomorphisms

$R \xrightarrow{\varphi} S$ rings (Comm. rings with unity)

$(R,+) \xrightarrow[\text{homo.}]{\text{gp}} (S,+)$

$(R,\cdot) \xrightarrow[\text{homo.}]{\text{monoid}} (S,\cdot)$

$\varphi(xy) = \varphi(x)\cdot\varphi(y)$

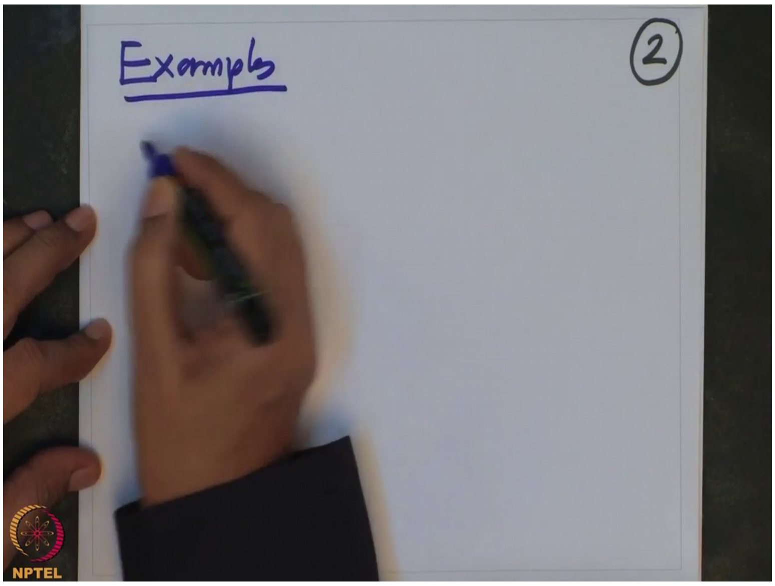
$\varphi(1_R) = 1_S$

NPTEL

homomorphisms. So some examples and usually example should consist our rings which we want to study.

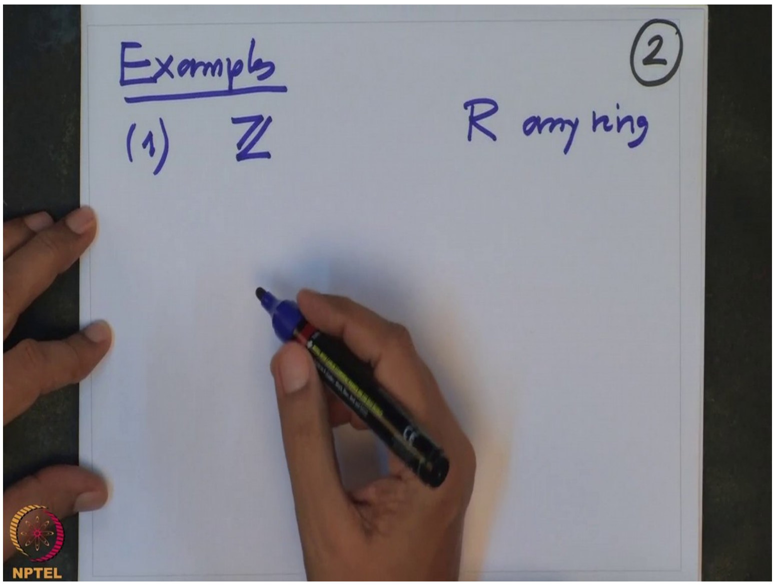
For example, so, so examples.

(Refer Slide Time 06:27)



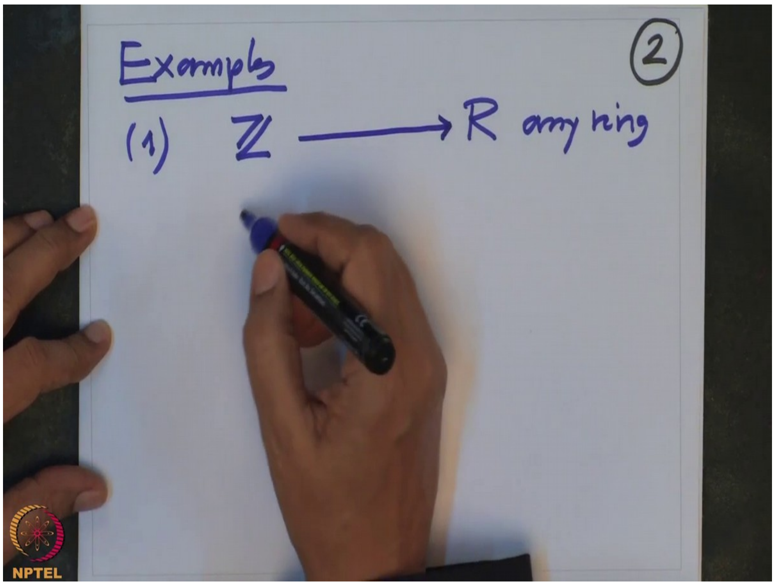
One, take the ring $\mathbb{Z}$ and take R any other ring, say this is any other ring, any ring. And $\mathbb{Z}$ is our ring of integers.

(Refer Slide Time 06:39)



And so I want to give ring homomorphism from $\mathbb{Z}$ to R. So that means

(Refer Slide Time 06:46)



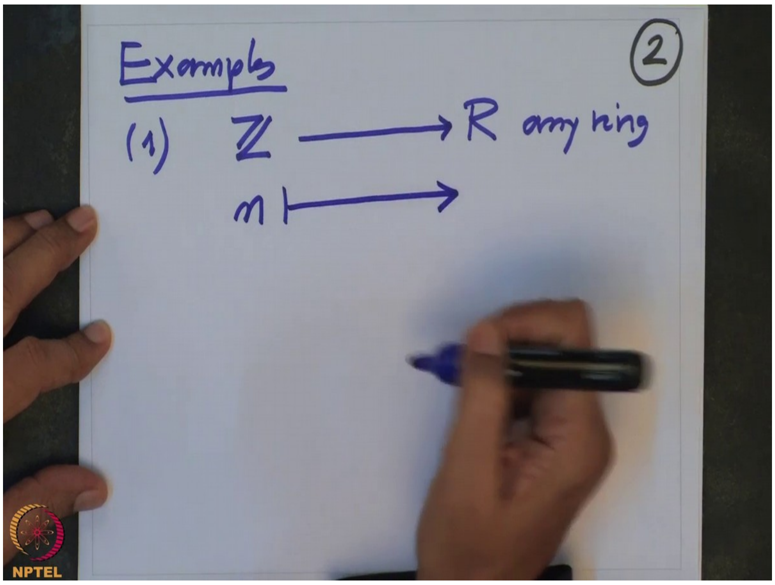
Examples

(2)

(1) $\mathbb{Z} \longrightarrow R$ any ring

I should map n to somewhere and

(Refer Slide Time 06:50)



Examples

(2)

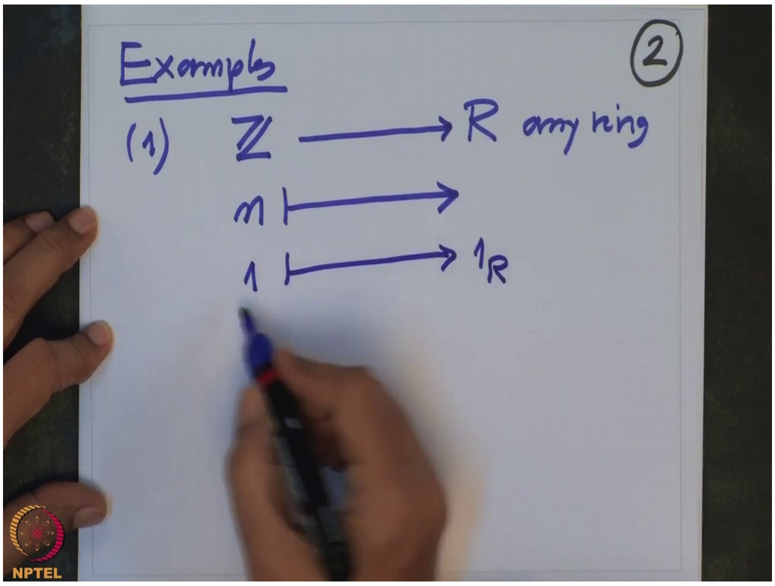
(1) $\mathbb{Z} \longrightarrow R$ any ring

$n \longmapsto$

check that it satisfies the properties of ring homomorphism.

But you see, also remember that when we want to give a ring homomorphism that we need to map one of the ring $\mathbb{Z}$ to one of the ring R. That means you have no choice. 1, usual 1, this is usual 1, it should go to 1_R .

(Refer Slide Time 07:14)



Examples

2

(1) $\mathbb{Z} \longrightarrow R$ any ring

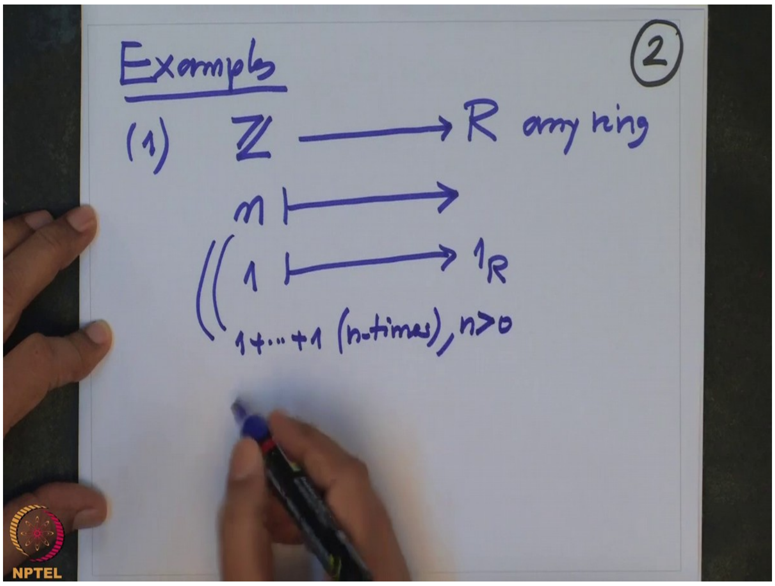
$n \longmapsto$

$1 \longmapsto 1_R$

And once it, 1 goes to 1_R , then this n has no choice. Because this n, when it is positive, you think it is $1+1+...+1$ n times, when it is negative you think it is $-1-1-\ldots-1$ n times.

So this n, you should think $1+1+...+1$ n times when n is positive and

(Refer Slide Time 07:46)



Examples

2

(1) $\mathbb{Z} \longrightarrow R$ any ring

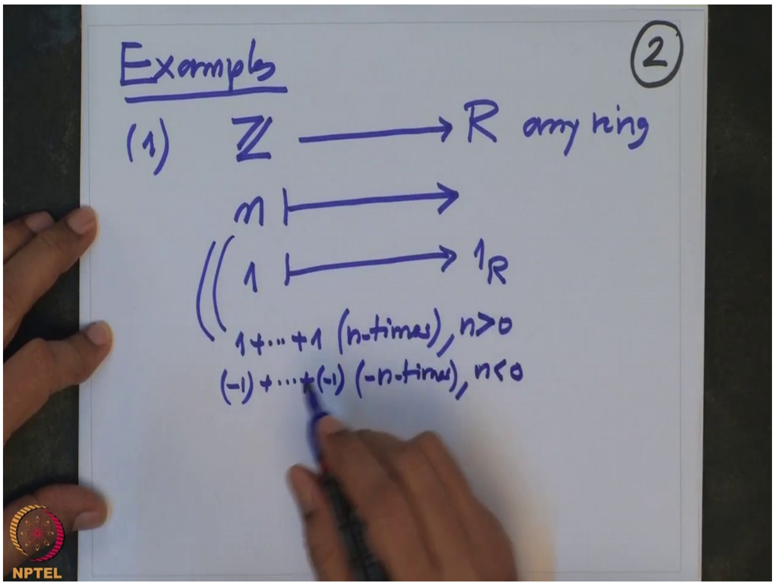
$n \longmapsto$

(($1 \longmapsto 1_R$

$1+\cdots+1$ (n-times), $n>0$

$-1-1-\ldots-1$ n times if n is negative. Of course when n is 0,

(Refer Slide Time 08:00)



Examples ②

(1) $\mathbb{Z} \longrightarrow R$ any ring

$m \longmapsto$

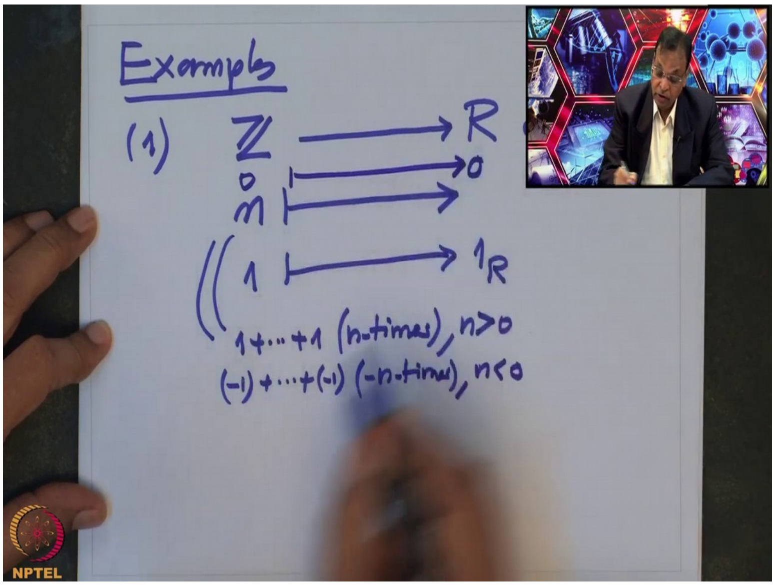
$((\ 1 \longmapsto 1_R$

$1+\cdots+1$ (n-times), $n>0$

$(-1)+\cdots+(-1)$ (-n-times), $n<0$

we know we need a group homomorphism from $\mathbb{Z}$ plus to R plus. So 0 has to go to 0. So 0 has to go to 0

(Refer Slide Time 08:09)



Examples

(1) $\mathbb{Z} \longrightarrow R$

$0 \longmapsto 0$

$m \longmapsto$

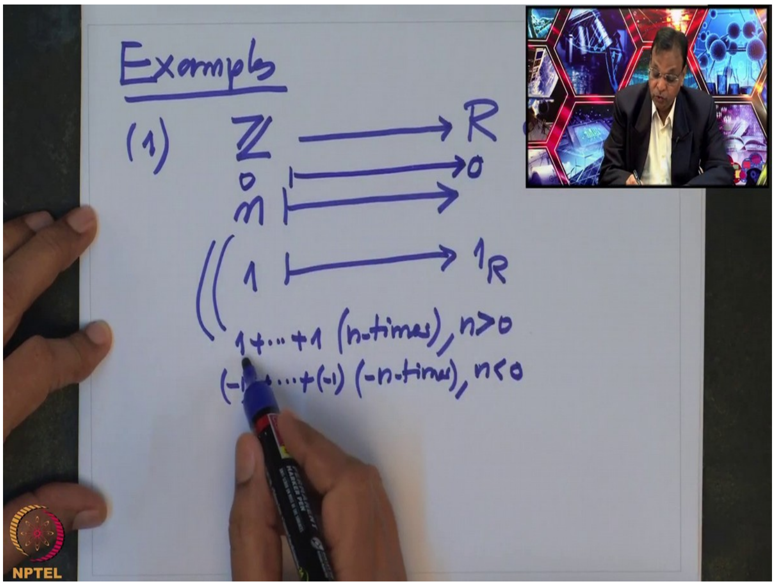
$((\ 1 \longmapsto 1_R$

$1+\cdots+1$ (n-times), $n>0$

$(-1)+\cdots+(-1)$ (-n-times), $n<0$

and then I know

(Refer Slide Time 08:11)



Examples

(1) $\mathbb{Z} \longrightarrow R$

$0 \longmapsto 0$

$m \longmapsto$

$1 \longmapsto 1_R$

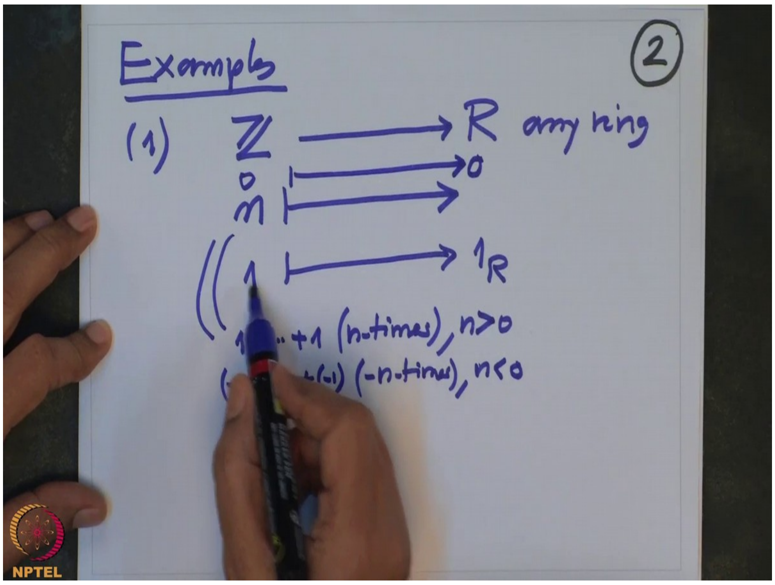
$1+\cdots+1$ (n-times), $n>0$

$(-1)+\cdots+(-1)$ (-n-times), $n<0$

it should respect the addition.

That means when I know

(Refer Slide Time 08:15)



Examples

2

(1) $\mathbb{Z} \longrightarrow R$ any ring

$0 \longmapsto 0$

$m \longmapsto$

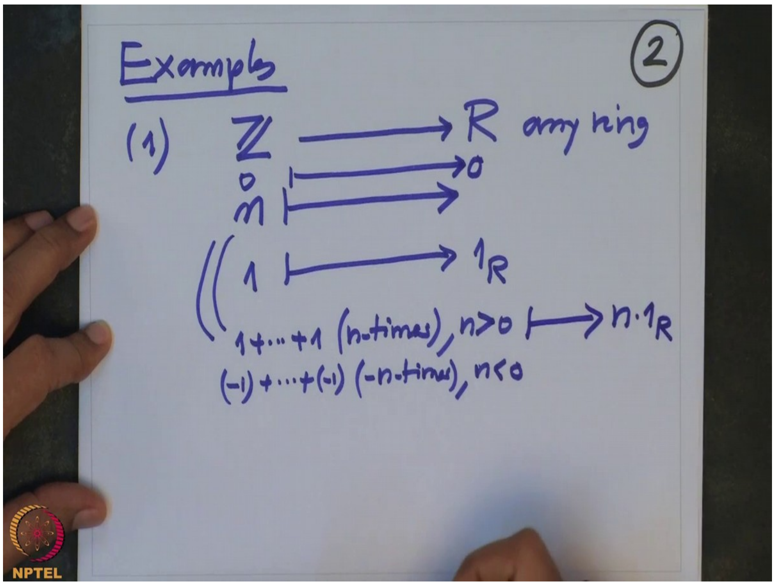
$1 \longmapsto 1_R$

$1+\cdots+1$ (n-times), $n>0$

$(-1)+\cdots+(-1)$ (-n-times), $n<0$

where 1 goes, this is clearly has to go to n times 1_R

(Refer Slide Time 08:22)



Examples

(2)

(1) $\mathbb{Z} \longrightarrow R$ any ring

$0 \longmapsto 0$

$m \longmapsto$

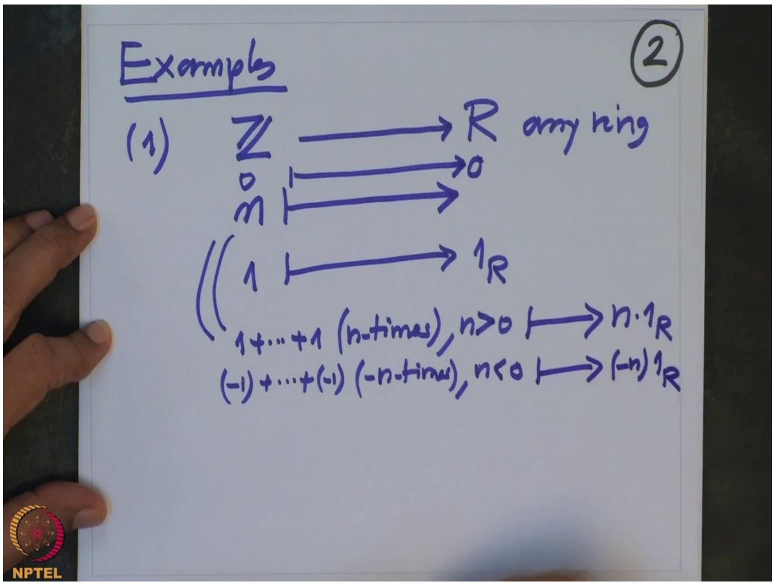
$1 \longmapsto 1_R$

$1+\cdots+1$ (n-times), $n>0 \longmapsto n\cdot 1_R$

$(-1)+\cdots+(-1)$ (-n-times), $n<0$

because it should respect the addition and this, this will automatically go to $-n \times 1_R$.

(Refer Slide Time 08:32)



Examples

(2)

(1) $\mathbb{Z} \longrightarrow R$ any ring

$0 \longmapsto 0$

$m \longmapsto$

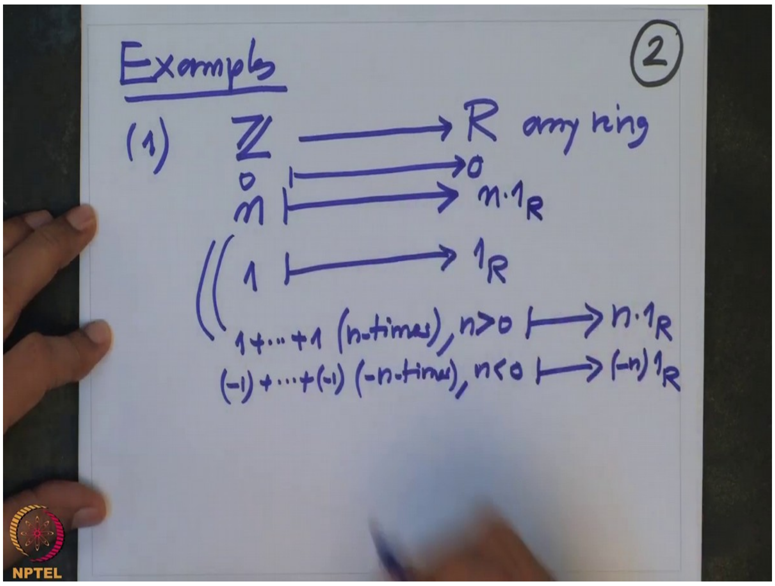
$1 \longmapsto 1_R$

$1+\cdots+1$ (n-times), $n>0 \longmapsto n\cdot 1_R$

$(-1)+\cdots+(-1)$ (-n-times), $n<0 \longmapsto (-n)1_R$

So every time n has to go to $n \times 1_R$. That is what we conclude.

(Refer Slide Time 08:39)



Examples (2)

(1) $\mathbb{Z} \longrightarrow R$ any ring

$0 \longmapsto 0$

$m \longmapsto m \cdot 1_R$

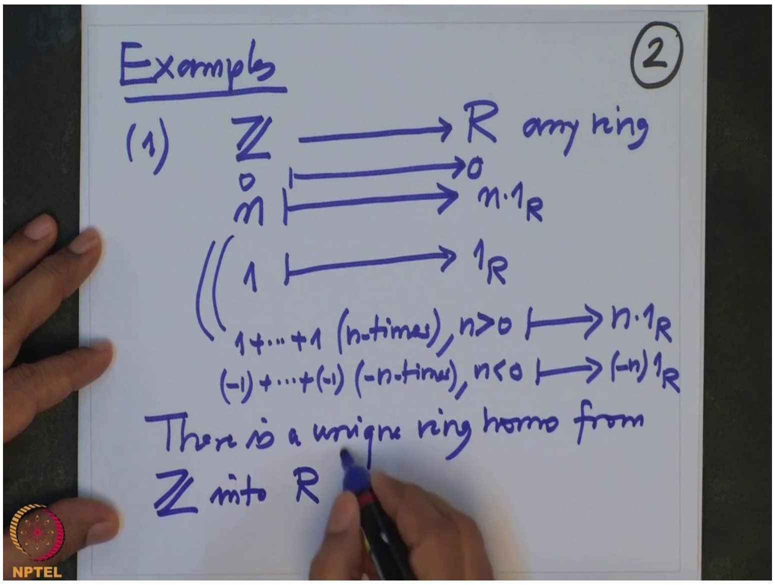
$1 \longmapsto 1_R$

$1+\cdots+1$ (n-times), $n>0 \longmapsto n \cdot 1_R$

$(-1)+\cdots+(-1)$ (-n-times), $n<0 \longmapsto (-n) 1_R$

So that means there is exactly one ring homomorphism from $\mathbb{Z}$ to R. There is a unique, so I will write the result; there is a unique ring homomorphism from $\mathbb{Z}$ into any other ring R. And this unique homomorphism

(Refer Slide Time 09:08)



Examples (2)

(1) $\mathbb{Z} \longrightarrow R$ any ring

$0 \longmapsto 0$

$m \longmapsto m \cdot 1_R$

$1 \longmapsto 1_R$

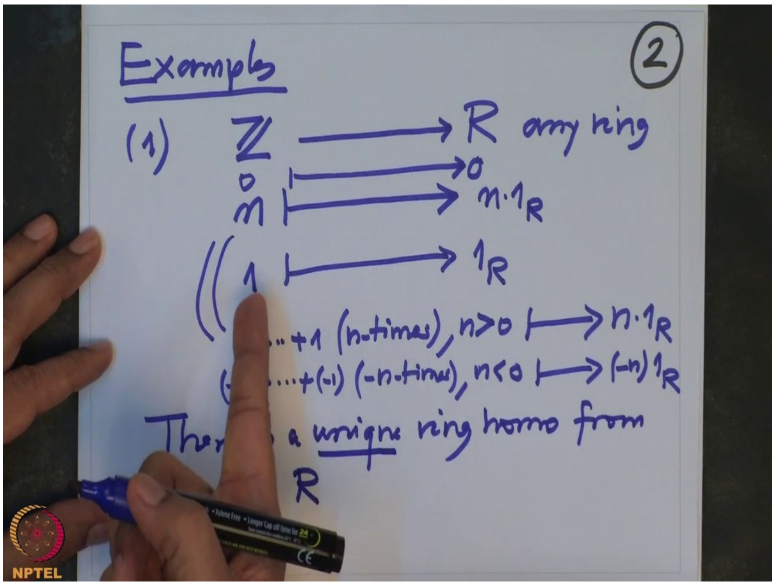
$1+\cdots+1$ (n-times), $n>0 \longmapsto n \cdot 1_R$

$(-1)+\cdots+(-1)$ (-n-times), $n<0 \longmapsto (-n) 1_R$

There is a unique ring homo from $\mathbb{Z}$ into R

I am, it depends on R because it tells

(Refer Slide Time 09:12)



Examples 2

(1) $\mathbb{Z} \longrightarrow R$ any ring

$0 \longmapsto 0$

$m \longmapsto n\cdot 1_R$

$1 \longmapsto 1_R$

$\dots+1$ (n-times), $n>0 \longmapsto n\cdot 1_R$

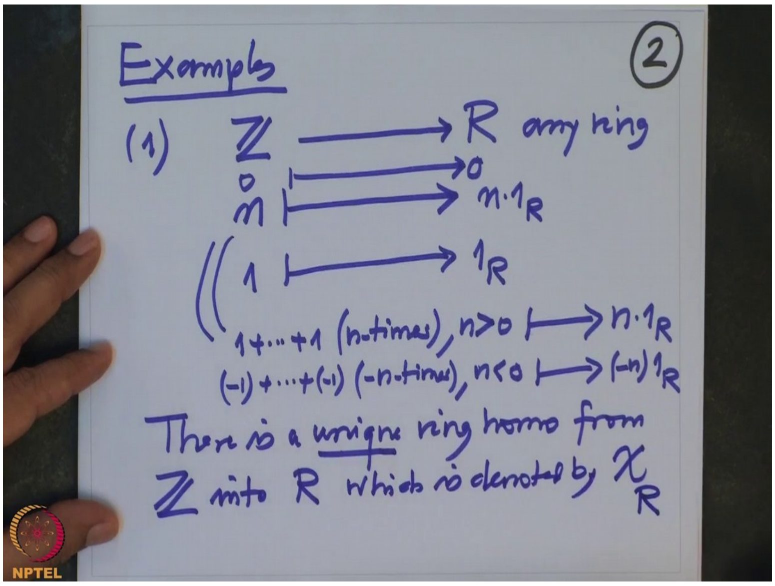
$(\dots+(-1)$ (-n-times), $n<0 \longmapsto (-n)1_R$

Ther a unique ring homo from

R

where 1 goes to R, so which is denoted by χ_R .

(Refer Slide Time 09:25)



Examples 2

(1) $\mathbb{Z} \longrightarrow R$ any ring

$0 \longmapsto 0$

$m \longmapsto n\cdot 1_R$

$1 \longmapsto 1_R$

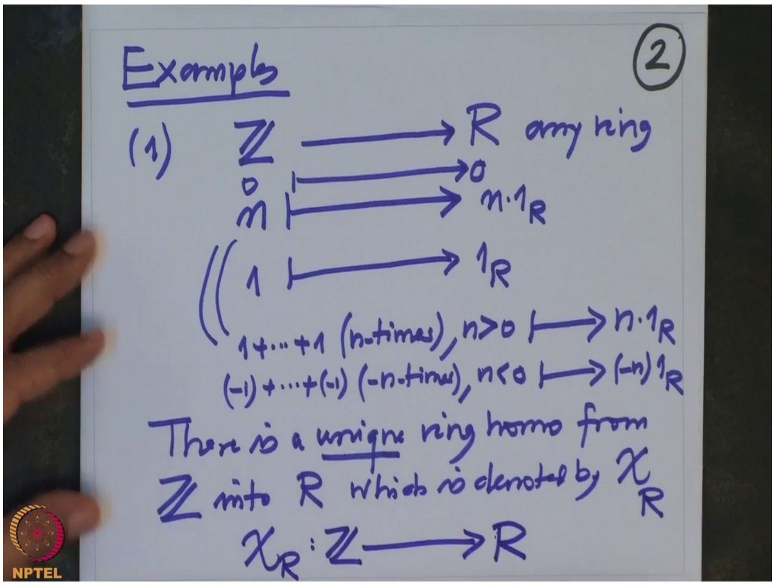
$1+\dots+1$ (n-times), $n>0 \longmapsto n\cdot 1_R$

$(-1)+\dots+(-1)$ (-n-times), $n<0 \longmapsto (-n)1_R$

There is a unique ring homo from $\mathbb{Z}$ into R which is denoted by χ_R

So chi of R is a ring homomorphism, the unique one from $\mathbb{Z}$ to R. This is very important fact

(Refer Slide Time 09:34)



Examples ②

(1) $\mathbb{Z} \longrightarrow R$ any ring

$0 \longmapsto 0$

$n \longmapsto n\cdot 1_R$

$((1 \longmapsto 1_R$

$1+\cdots+1$ (n-times), $n>0 \longmapsto n\cdot 1_R$

$(-1)+\cdots+(-1)$ (-n-times), $n<0 \longmapsto (-n)1_R$

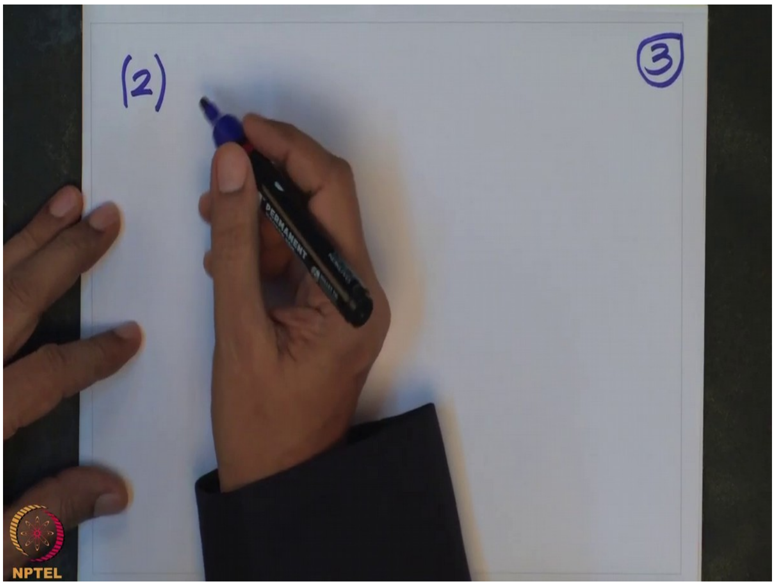
There is a unique ring homo from $\mathbb{Z}$ into R which is denoted by χ_R

$\chi_R : \mathbb{Z} \longrightarrow R$

and I will keep on using this again and again. So this is one prime example what we will keep looking and the next example is then, many, many other examples I want to give together.

So second examples, second example, let us

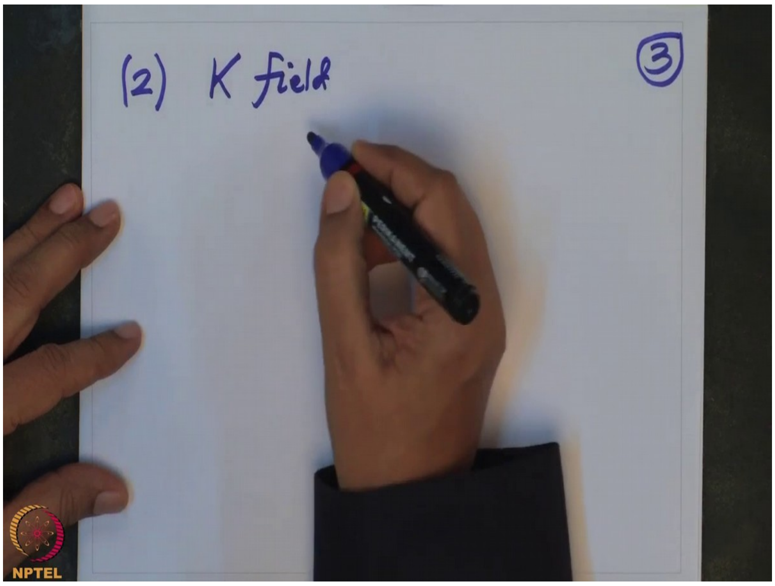
(Refer Slide Time 09:55)



(2) ③

take K to be any field.

(Refer Slide Time 10:01)

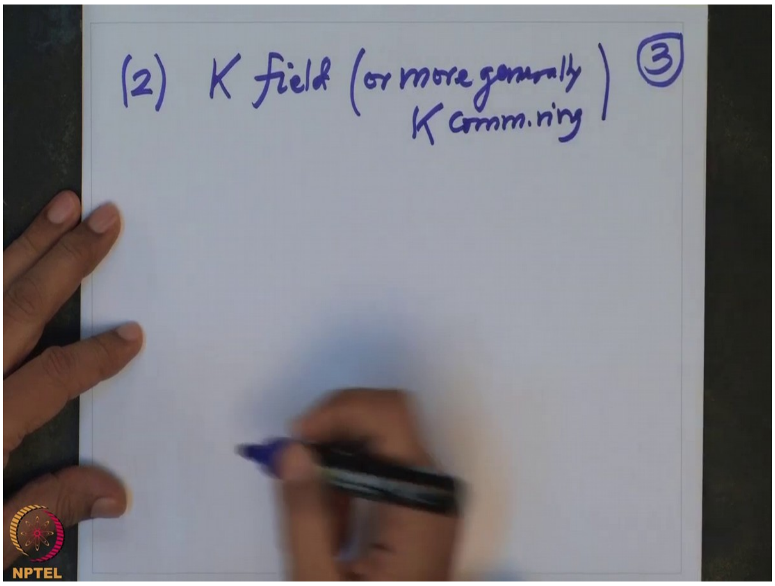


(2) K field

3

Actually assuming field is not really necessary. We could do, or more generally K to be any commutative ring.

(Refer Slide Time 10:20)



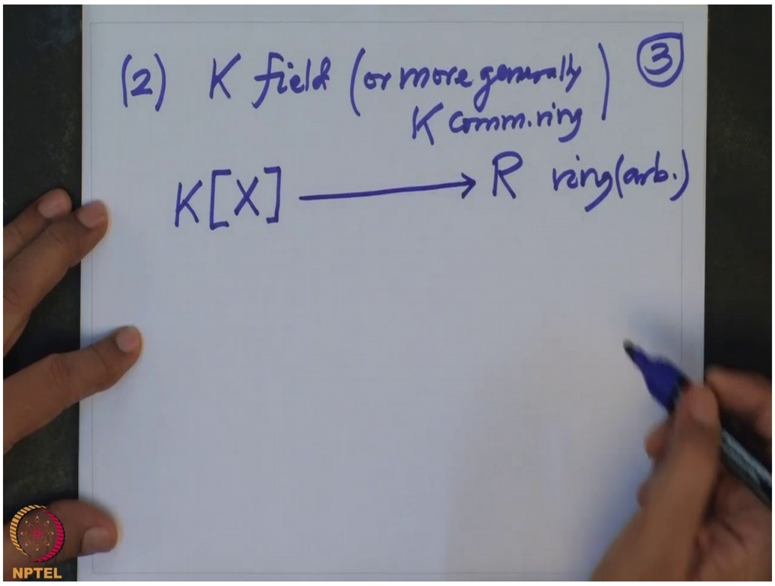
(2) K field (or more generally K comm. ring)

3

But when, when we apply, we usually, we are going to apply many things to the fields only. But there is no harm in knowing the general definition.

So then you consider a polynomial ring, from this field K we have constructed the polynomial ring whose elements are precisely the polynomials. And I want to give, R is any ring, R is any arbitrary ring, arbitrary and I want to give ring homomorphism from here to here.

(Refer Slide Time 10:57)

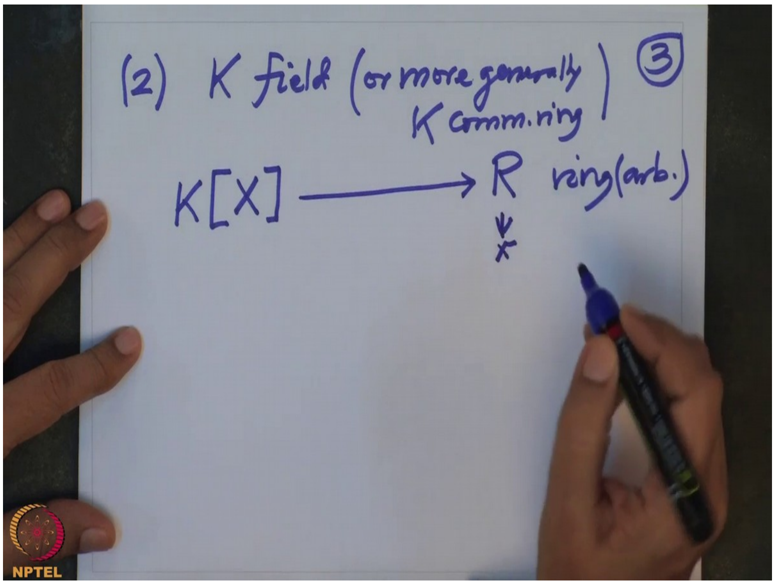


(2) K field (or more generally K comm. ring) ③

$K[X] \longrightarrow R$ ring(arb.)

So whenever I have an element small $x \in R$, I am going to give

(Refer Slide Time 11:07)



(2) K field (or more generally K comm. ring) ③

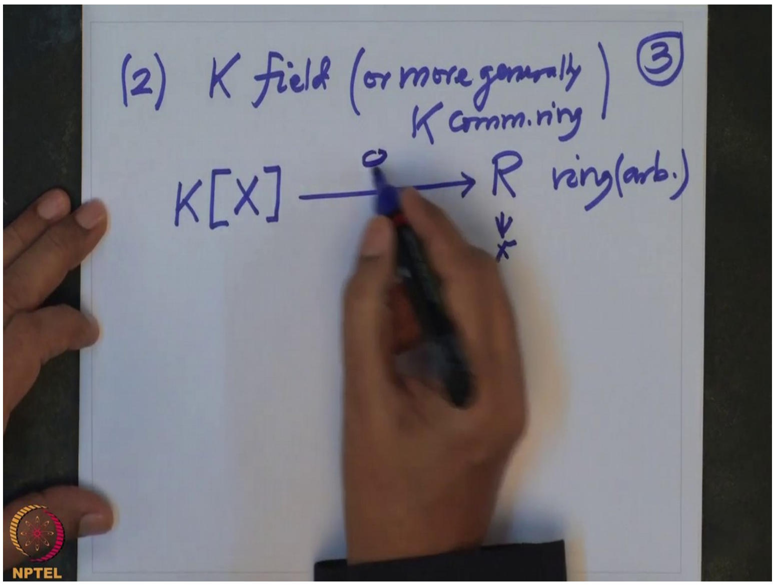
$$\begin{tikzcd} K[X] \arrow[r] & R \arrow[d, phantom, "\ni" rotate] \\ & x \end{tikzcd}$$

ring(arb.)

a ring homomorphism corresponding to this small x.

So therefore I am going to denote it by phi of small x, not phi, sorry,

(Refer Slide Time 11:16)



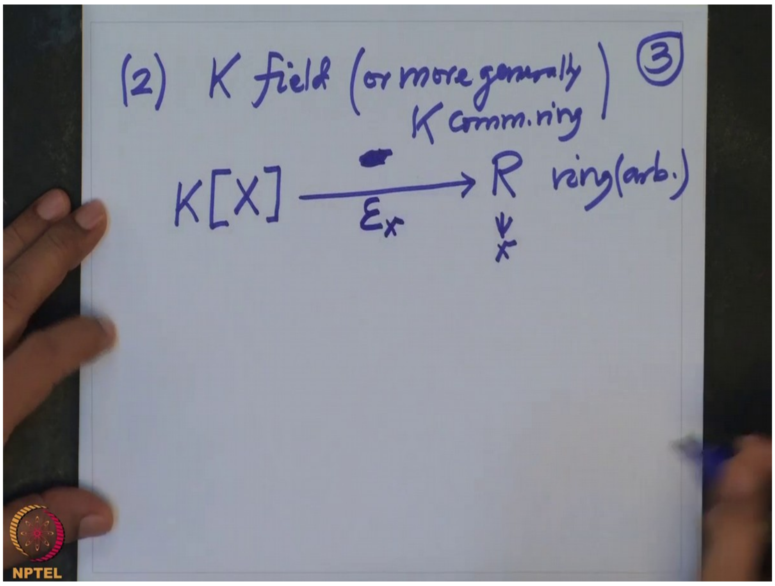
(2) K field (or more generally K comm. ring) ③

$$\begin{tikzcd} K[X] \arrow[r] & R \arrow[d, phantom, "\rotatebox{-90}{$\in$}"] \\ & x \end{tikzcd}$$

ring (arb.)

ϵ_x . I am going to define a map ϵ_x ,

(Refer Slide Time 11:22)



(2) K field (or more generally K comm. ring) ③

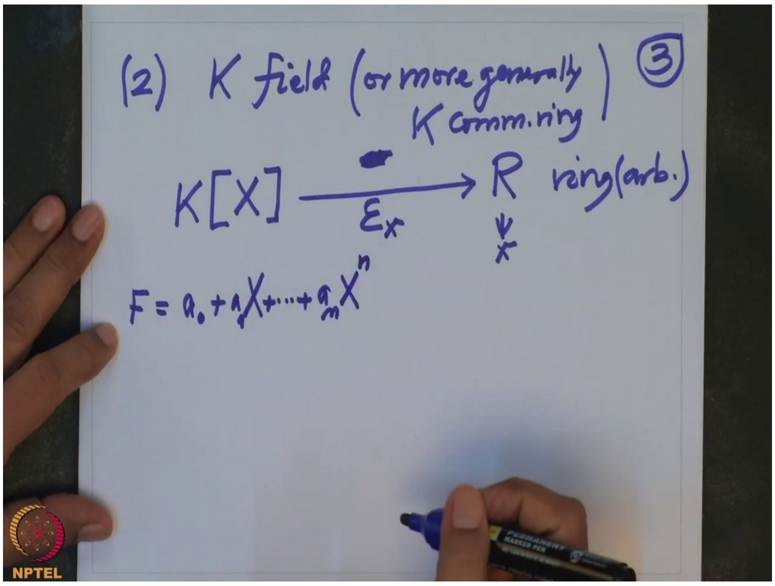
$$\begin{tikzcd} K[X] \arrow[r, "\varepsilon_x"'] & R \arrow[d, phantom, "\rotatebox{-90}{$\in$}"] \\ & x \end{tikzcd}$$

ring (arb.)

so how do I define it?

Take any polynomial F, this is $a_0 + a_1 X + ... + a_n X^n$. Any polynomial looks like this.

(Refer Slide Time 11:40)



(2) K field (or more generally K comm. ring) ③

$$\begin{tikzcd} K[X] \arrow[r, "E_x"'] & R \end{tikzcd}$$ ring (arb.)

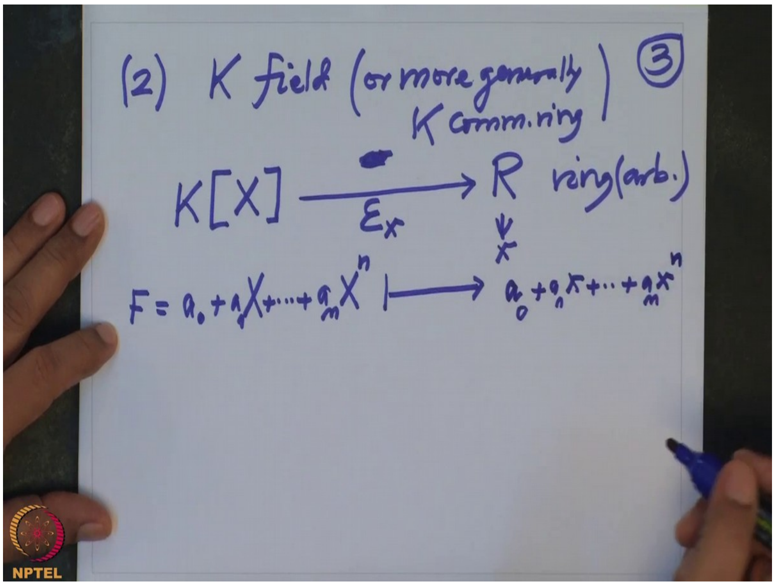
$x \in R$

$F = a_0 + a_1 X + \dots + a_m X^n$

And these I want to map it to somebody in R and I know only X in R. And I know these a is. They are fixed when I fix F, and I want to map this somewhere.

So I want to try whether this makes sense, $a_0+a_1x+...+a_nx^n$.

(Refer Slide Time 12:09)



(2) K field (or more generally K comm. ring) ③

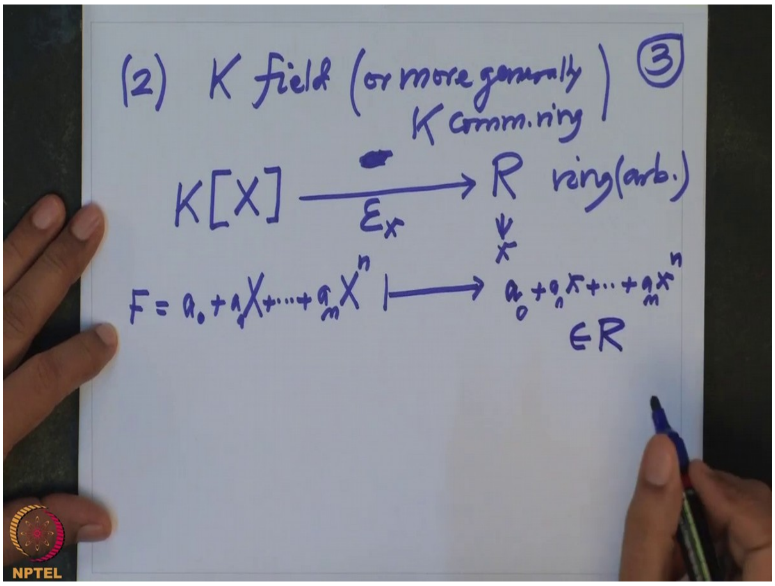
$$\begin{tikzcd} K[X] \arrow[r, "E_x"'] & R \end{tikzcd}$$ ring (arb.)

$x \in R$

$F = a_0 + a_1 X + \dots + a_m X^n \longmapsto a_0 + a_1 x + \dots + a_m x^n$

And this should again be an element in R. So naturally we should

(Refer Slide Time 12:14)



(2) K field (or more generally K comm. ring) ③

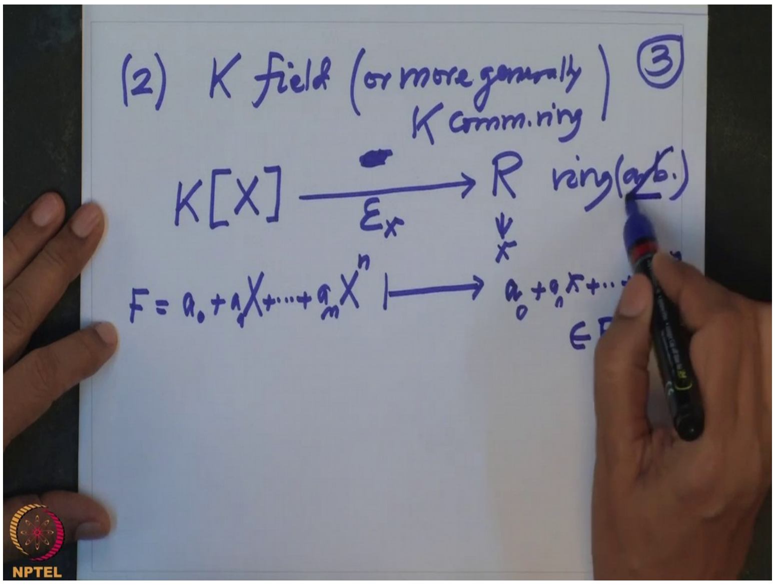
$$\begin{tikzcd} K[X] \arrow[r, "\mathcal{E}_x"'] & R \end{tikzcd}$$ ring (arb.)

$X \mapsto x$

$F = a_0 + a_1 X + \cdots + a_m X^n \longmapsto a_0 + a_n x + \cdots + a_m x^n \in R$

put a condition on R, not arbitrary

(Refer Slide Time 12:17)



(2) K field (or more generally K comm. ring) ③

$$\begin{tikzcd} K[X] \arrow[r, "\mathcal{E}_x"'] & R \end{tikzcd}$$ ring (~~arb.~~)

$X \mapsto x$

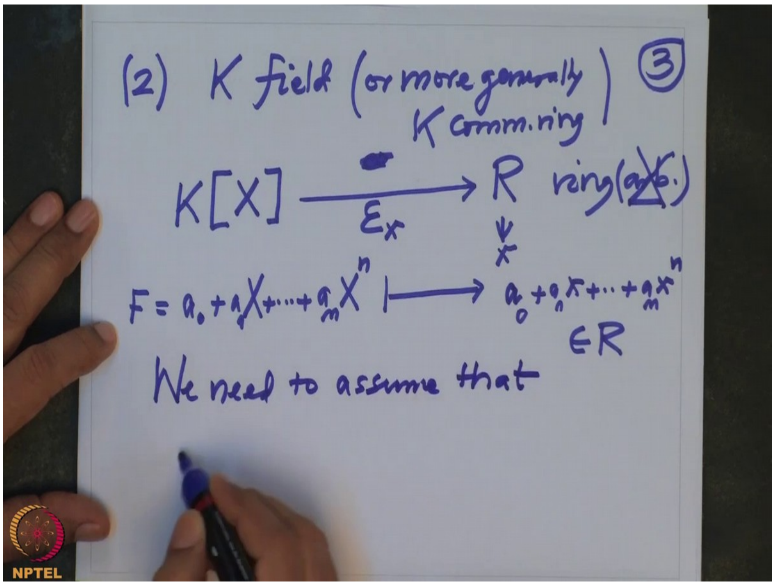
$F = a_0 + a_1 X + \cdots + a_m X^n \longmapsto a_0 + a_n x + \cdots$

$\in$

but it should be, it should have multiplication of K inside that, there should be a scalar multiplication of K on R.

So we need to assume, in order to make sense, we need to assume that

(Refer Slide Time 12:39)



(2) K field (or more generally K comm. ring) ③

$K[X] \xrightarrow[\varepsilon_x]{} R$ ring(~~comm.~~)

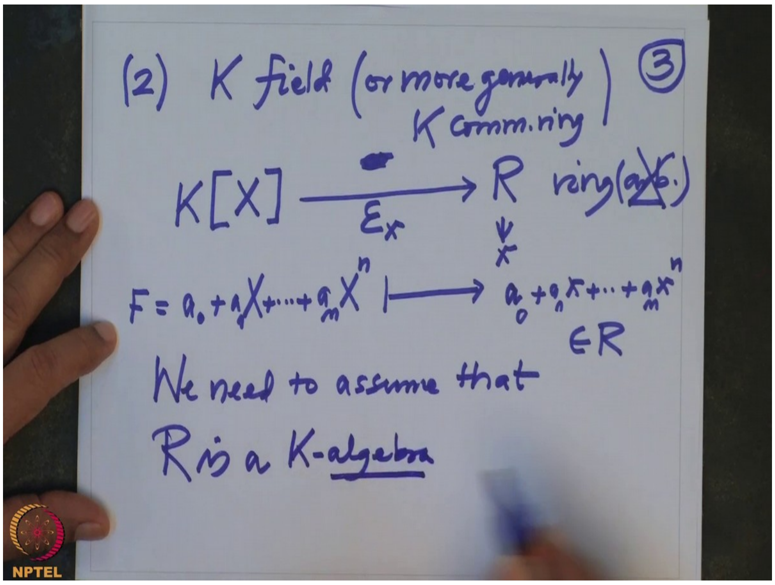
$\rotatebox{90}{$\in$}$ x

$F = a_0 + a_1X + \cdots + a_mX^n \longmapsto a_0 + a_1x + \cdots + a_mx^n \in R$

We need to assume that

R is what is called a K-algebra. What is K-algebra?

(Refer Slide Time 12:50)



(2) K field (or more generally K comm. ring) ③

$K[X] \xrightarrow[\varepsilon_x]{} R$ ring(~~comm.~~)

$\rotatebox{90}{$\in$}$ x

$F = a_0 + a_1X + \cdots + a_mX^n \longmapsto a_0 + a_1x + \cdots + a_mx^n \in R$

We need to assume that

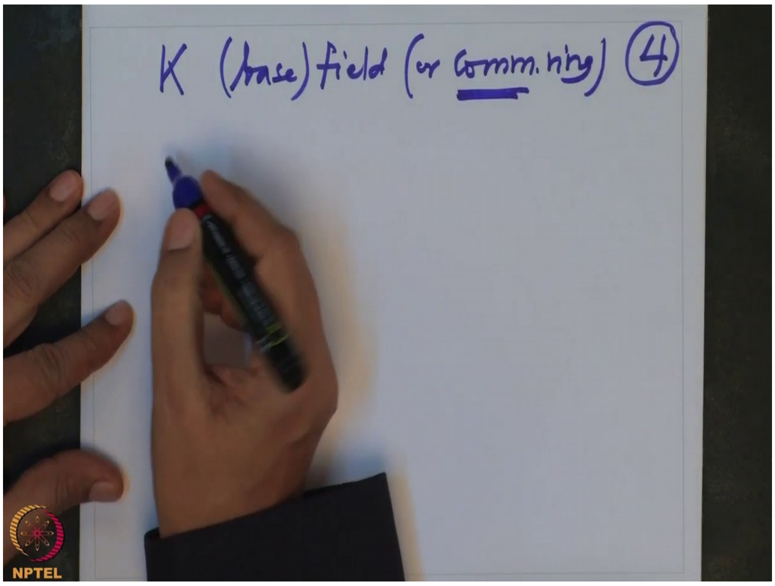
R is a K-algebra

K-algebra is where there is a multiplication also and there is a scalar multiplication also.

So I want to elaborate this and come back to this example. And then we will have many more examples of this kind. This is very important. So let us now recall what is a K-algebra. So, so now we have base ring K. K is, I will call it base field. One could take also ring, commutative ring or commutative ring. But commutative is very important.

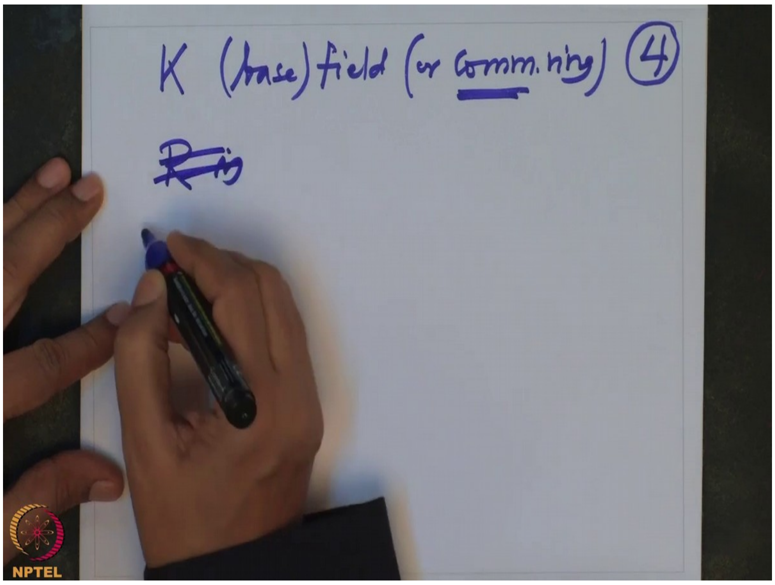
And

(Refer Slide Time 13:31)



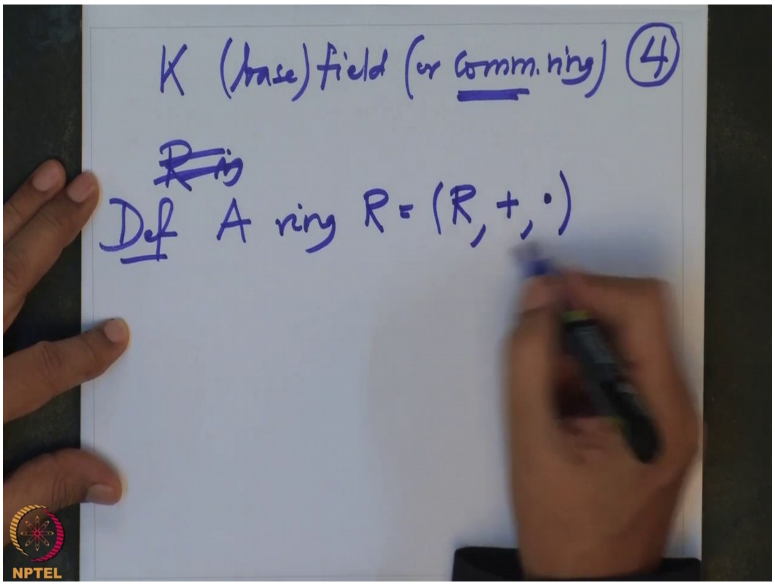
we have a ring R, R is a ring. Or better to write it

(Refer Slide Time 13:39)



a definition, a ring R which, just to remember R has a two binary operation, addition and multiplication

(Refer Slide Time 13:55)



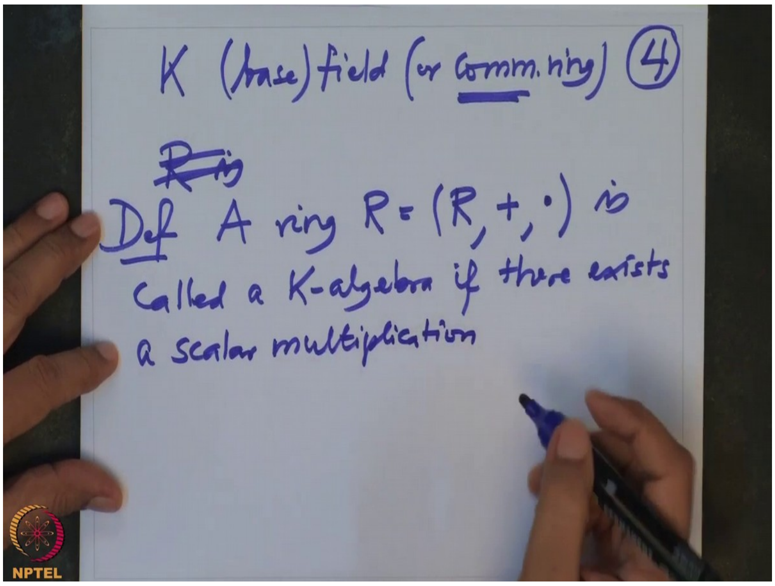
K (base) field (or comm. ring) 4

~~Ring~~

Def A ring $R=(R,+,\cdot)$

and they satisfy the usual properties of the ring, both these binary operations, ring R is called a K-algebra if there exists a scalar multiplication, scalar multiplication one

(Refer Slide Time 14:27)



K (base) field (or comm. ring) 4

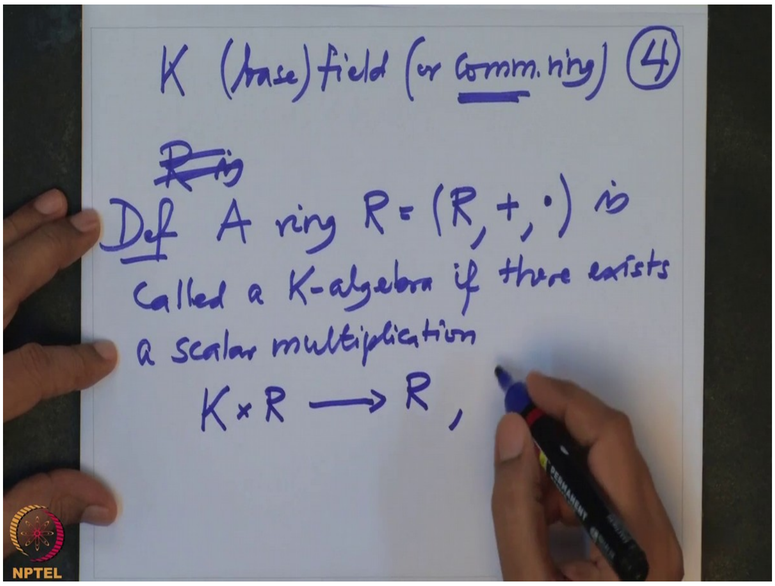
~~Ring~~

Def A ring $R=(R,+,\cdot)$ is called a K-algebra if there exists a scalar multiplication

should think a map from $K\times R\to R$.

This is usually denoted

(Refer Slide Time 14:36)



K (base) field (or comm. ring) 4

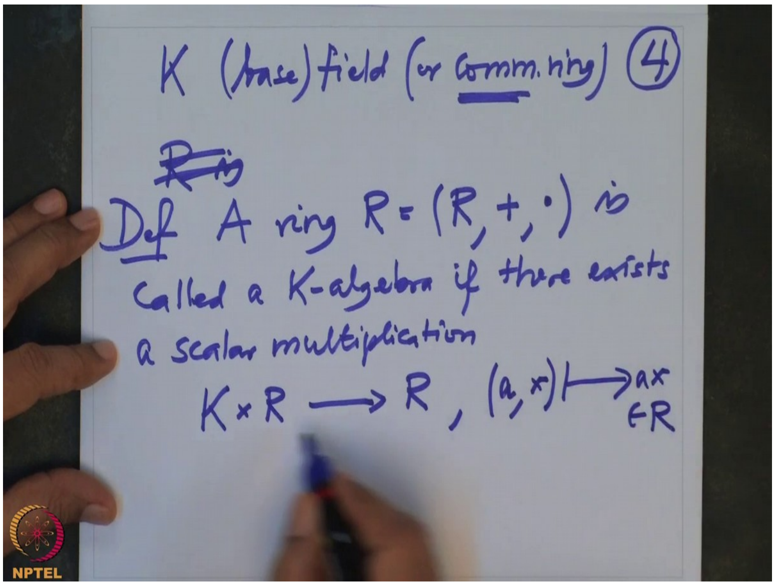
~~Ring~~

Def A ring $R = (R, +, \cdot)$ is called a K-algebra if there exists a scalar multiplication

$$K \times R \longrightarrow R,$$

by, scalars are the elements of K and these elements of R are denoted by small x, they should go somewhere which is an element of R again and that is denoted by ax. This is a

(Refer Slide Time 14:53)



K (base) field (or comm. ring) 4

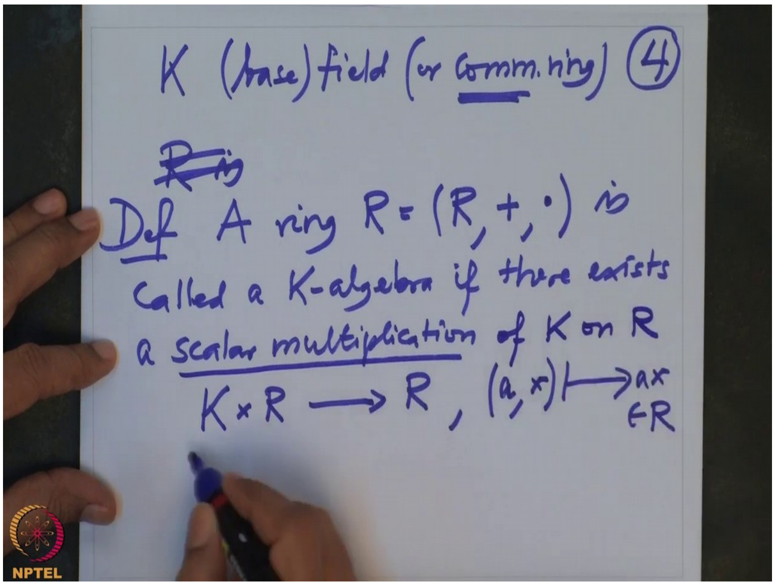
~~Ring~~

Def A ring $R = (R, +, \cdot)$ is called a K-algebra if there exists a scalar multiplication

$$K \times R \longrightarrow R, \quad (a, x) \longmapsto ax \in R$$

scalar multiplication. This is called a scalar multiplication of K on R which is a map

(Refer Slide Time 15:01)



K (base) field (or comm. ring) ④

~~Ring~~

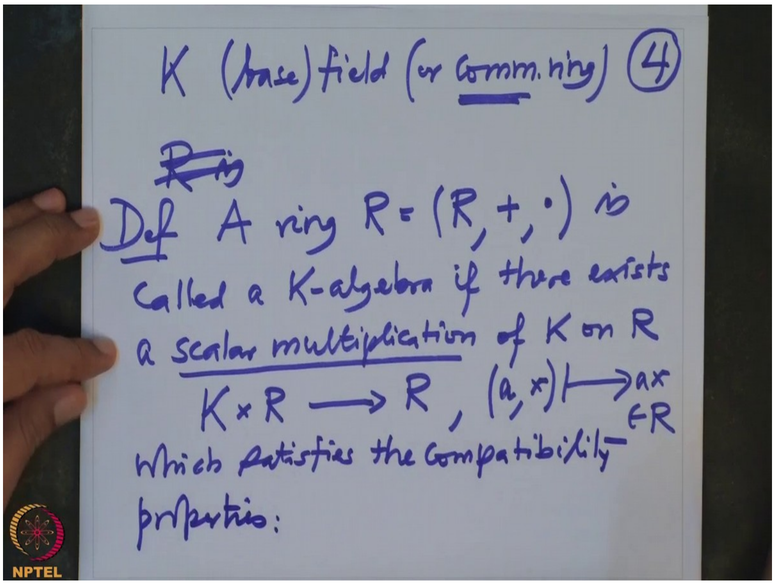
Def A ring $R = (R, +, \cdot)$ is called a K-algebra if there exists a scalar multiplication of K on R

$$K \times R \longrightarrow R \,, \quad (a, x) \longmapsto ax \in R$$

like this, which satisfies the compatibility properties, compatibility properties.

What are they? They are the following properties. That simply means

(Refer Slide Time 15:23)



K (base) field (or comm. ring) ④

~~Ring~~

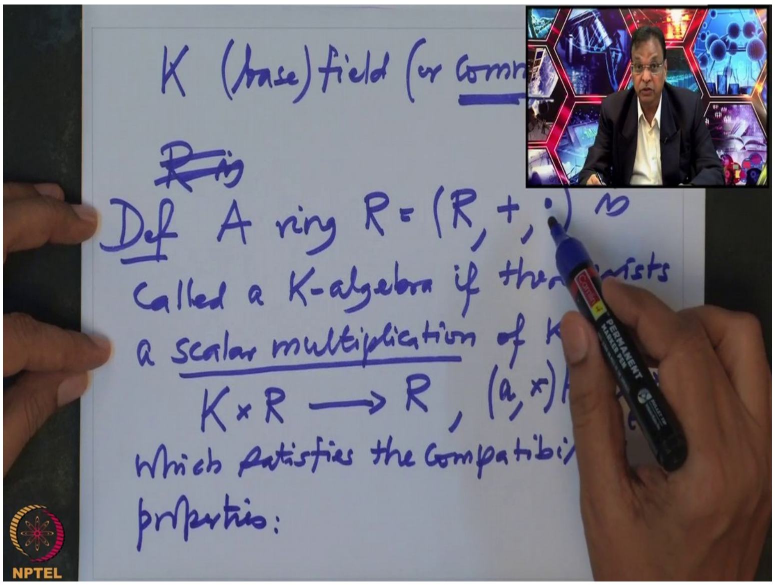
Def A ring $R = (R, +, \cdot)$ is called a K-algebra if there exists a scalar multiplication of K on R

$$K \times R \longrightarrow R \,, \quad (a, x) \longmapsto ax \in R$$

which satisfies the compatibility properties:

that this scalar multiplication should not meddle, should be compatible

(Refer Slide Time 15:28)



K (base) field (or comm

~~Ring~~

Def A ring $R = (R, +, \cdot)$ is

Called a K-algebra if there exists

a scalar multiplication of K

$K \times R \longrightarrow R \,,\ (a, x) \mapsto$

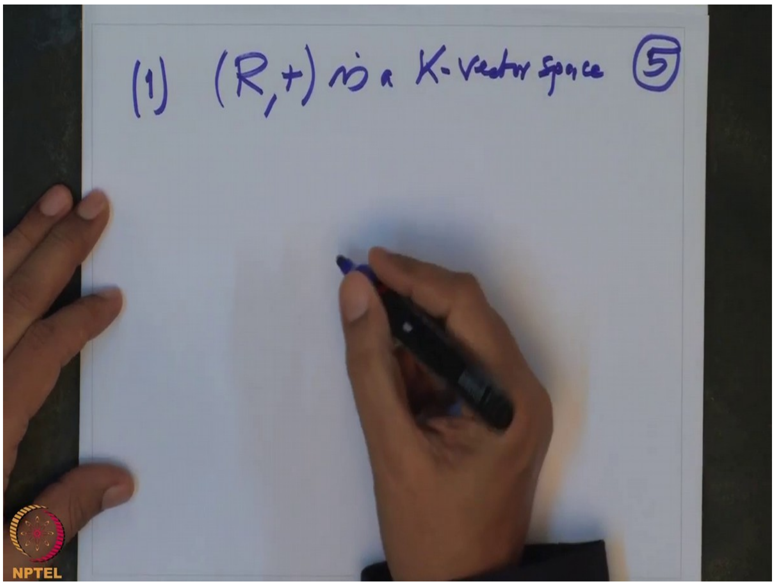
Which satisfies the Compatibi

properties:

with this given multiplication of the ring R. This is the given multiplication of the ring R. So multiplication, one should again think it is a map from $R \times R \to R$ which is associative etc etc.

So what are the compatibility properties of the, of the scalar multiplication of K? So, so first of all with the plus, so first one is with the addition of the ring it should be compatible. That means if I take this R with plus, this abelian group, this is a K-vector space.

(Refer Slide Time 16:12)

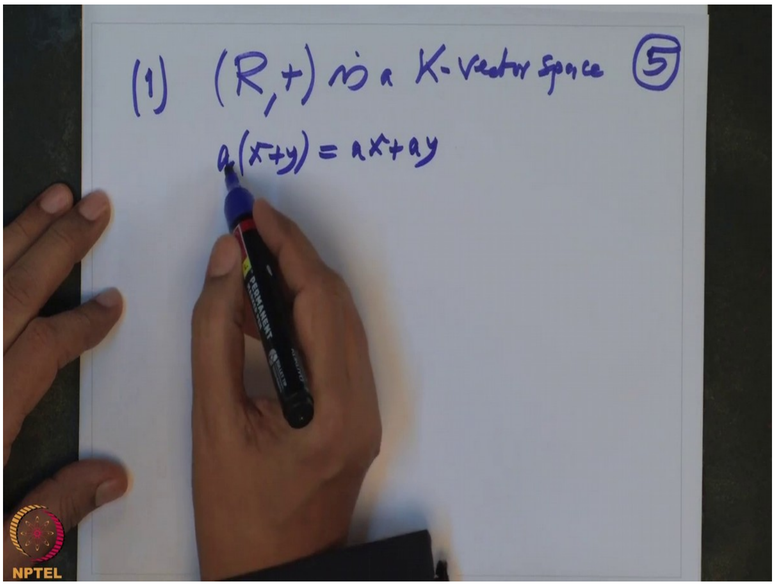


(1) $(R, +)$ is a K-vector space 5

That means whether you add first and multiply by a scalar or you multiply by scalars and add this result is same.

So that, I will just simply write it $a(x+y)=ax+ay$. Also the, if I add in the field K, so that is $(a+b)x=ax+bx$. This is for all a b in K and for all x , y in R.

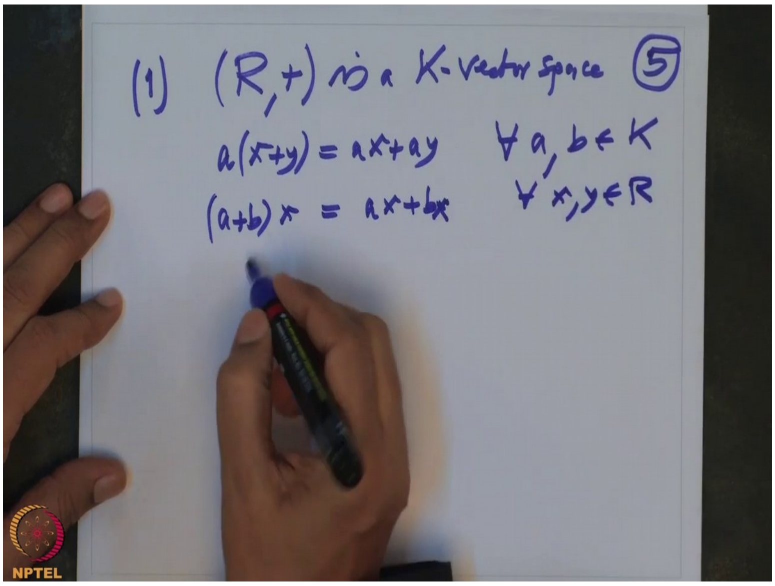
(Refer Slide Time 16:34)



(1) $(R,+)$ is a K-vector space ⑤

$a(x+y) = ax+ay$

(Refer Slide Time 16:56)



(1) $(R,+)$ is a K-vector space ⑤

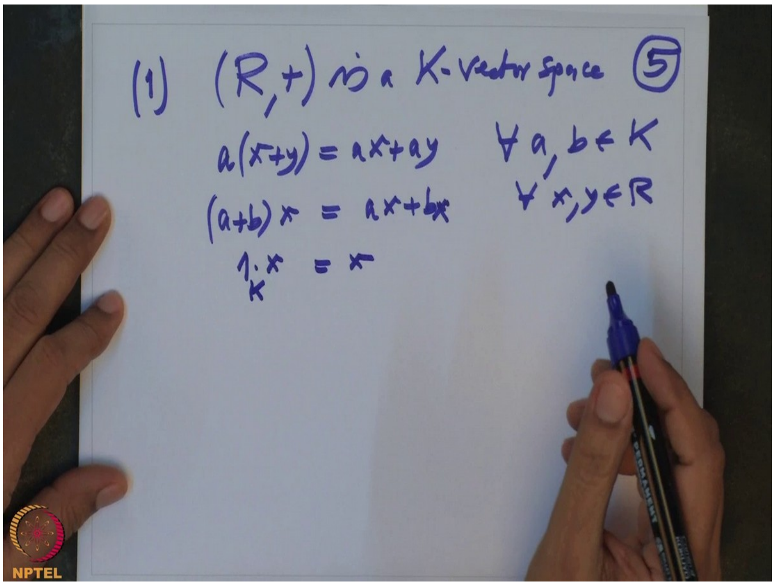
$a(x+y) = ax+ay \quad \forall a,b \in K$

$(a+b)x = ax+bx \quad \forall x,y \in R$

And moreover $1\times x=x$. This 1 is now $1\in K$.

So these

(Refer Slide Time 17:04)



(1) $(R,+)$ is a K-vector space 5

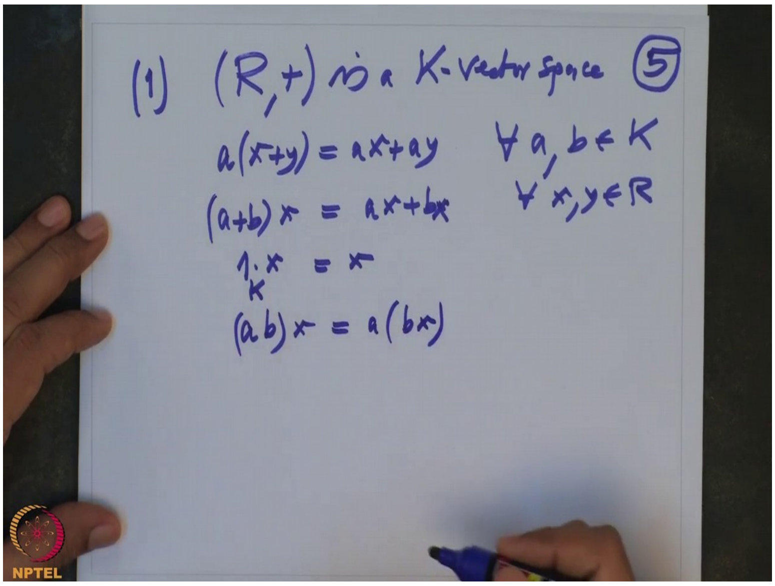
$a(x+y) = ax+ay \quad \forall\, a,b \in K$

$(a+b)x = ax+bx \quad \forall\, x,y \in R$

$1_K \cdot x = x$

are the compatibility properties so that it becomes the vector space. One more thing I should write it really, that is multiplication in K, that is $(a \times b) \times x = a \times (b \times x)$.

(Refer Slide Time 17:23)



(1) $(R,+)$ is a K-vector space 5

$a(x+y) = ax+ay \quad \forall\, a,b \in K$

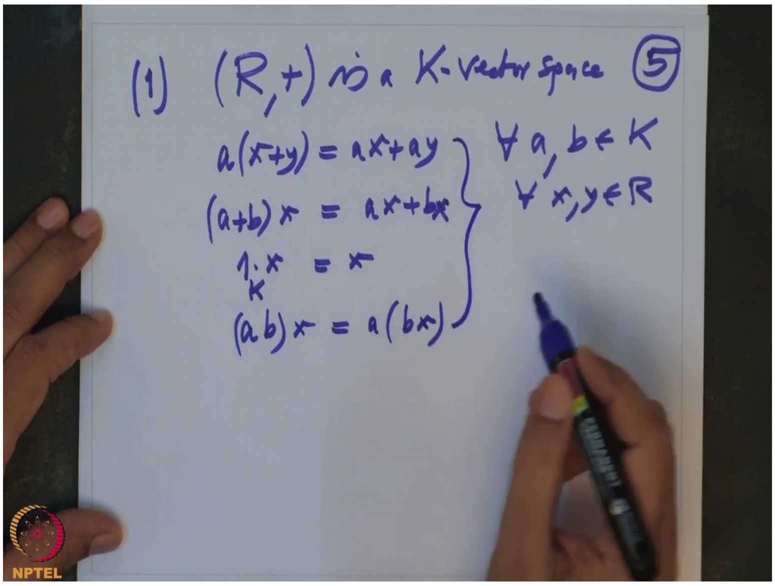
$(a+b)x = ax+bx \quad \forall\, x,y \in R$

$1_K \cdot x = x$

$(a.b)x = a(bx)$

So these four properties

(Refer Slide Time 17:26)



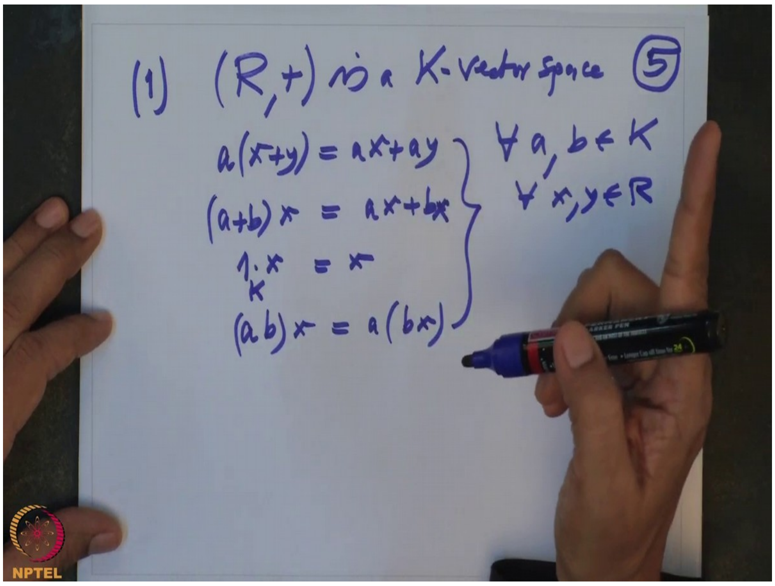
(1) $(R,+)$ is a K-vector space 5

$$\left.\begin{aligned} a(x+y) &= ax+ay \\ (a+b)x &= ax+bx \\ 1_K \cdot x &= x \\ (ab)x &= a(bx) \end{aligned}\right\} \begin{aligned} &\forall\, a,b \in K \\ &\forall\, x,y \in R \end{aligned}$$

which satisfies, the scalar multiplication which satisfies these four properties; that will make this abelian group R plus as a K-vector space.

And when you are dealing

(Refer Slide Time 17:38)

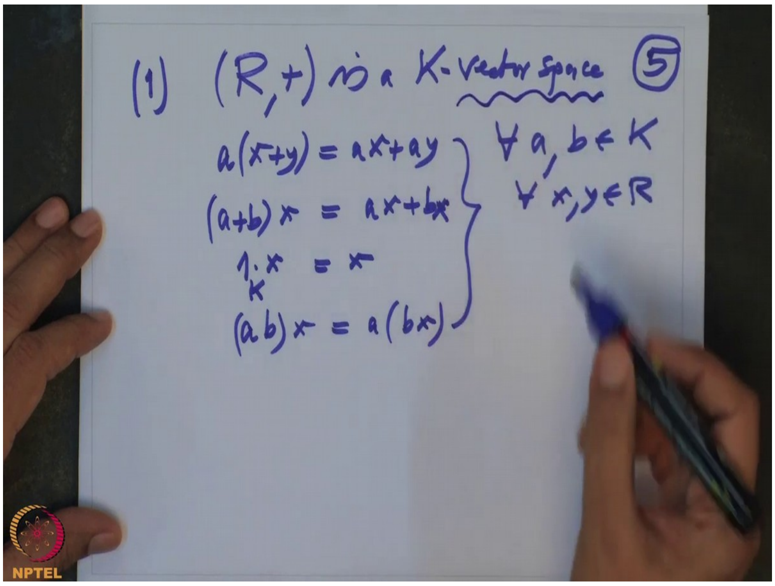


(1) $(R,+)$ is a K-vector space 5

$$\left.\begin{aligned} a(x+y) &= ax+ay \\ (a+b)x &= ax+bx \\ 1_K \cdot x &= x \\ (ab)x &= a(bx) \end{aligned}\right\} \begin{aligned} &\forall\, a,b \in K \\ &\forall\, x,y \in R \end{aligned}$$

with, not with the field case but with the commutative ring case, then one, instead of vector space, one

(Refer Slide Time 17:47)

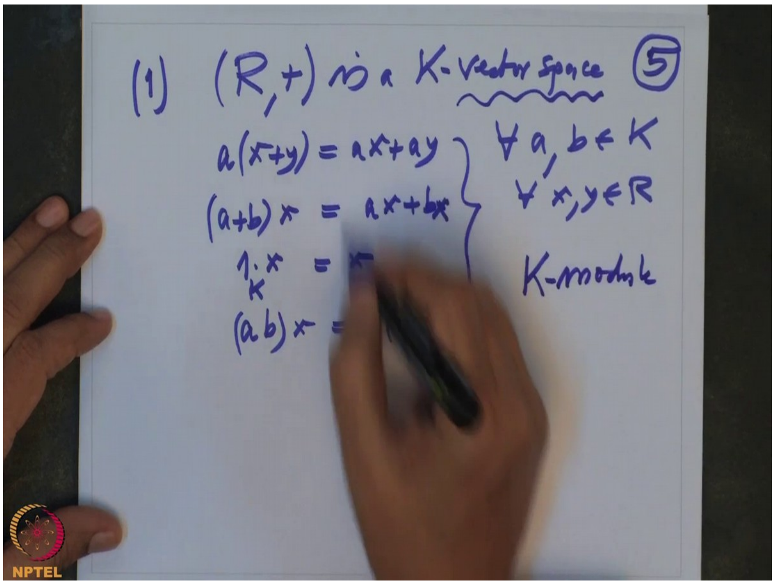


(1) $(R,+)$ is a K-vector space ⑤

$$\left.\begin{aligned} a(x+y) &= ax+ay \\ (a+b)x &= ax+bx \\ 1_K \cdot x &= x \\ (a\,b)x &= a(bx) \end{aligned}\right\} \begin{aligned} &\forall\, a, b \in K \\ &\forall\, x, y \in R \end{aligned}$$

uses the word K-module. Properties

(Refer Slide Time 17:52)

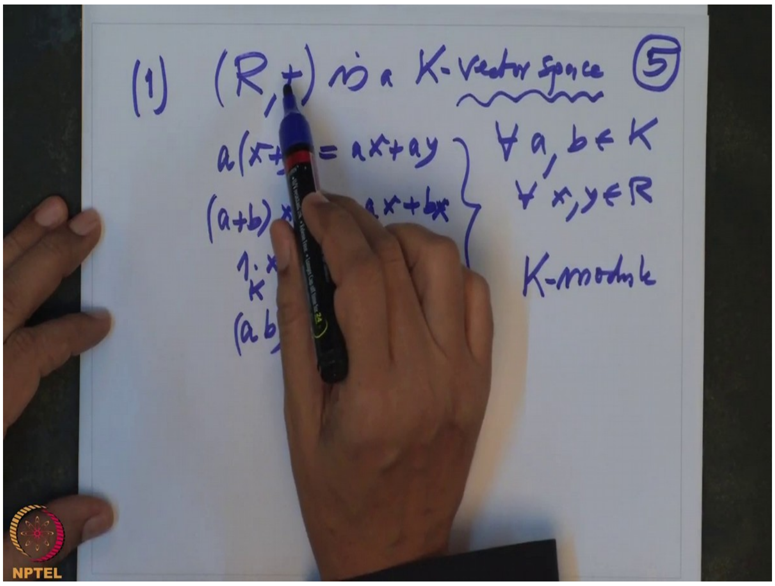


(1) $(R,+)$ is a K-vector space ⑤

$$\left.\begin{aligned} a(x+y) &= ax+ay \\ (a+b)x &= ax+bx \\ 1_K \cdot x &= x \\ (a\,b)x &= \end{aligned}\right\} \begin{aligned} &\forall\, a, b \in K \\ &\forall\, x, y \in R \\ &K\text{-module} \end{aligned}$$

are the same, so when one says the K-vector space, that indicates the base ring you are assuming is the field. Otherwise it may not be a field, it is a commutative ring. So this is the compatibility of the scalar multiplication with

(Refer Slide Time 18:09)



(1) $(R,+)$ is a K-vector space 5

$a(x+$ … $= ax+ay$ $\forall\, a,b\in K$

$(a+b)x$ … $ax+bx$ $\forall\, x,y\in R$

$\underset{K}{1}\cdot x$ … K-module

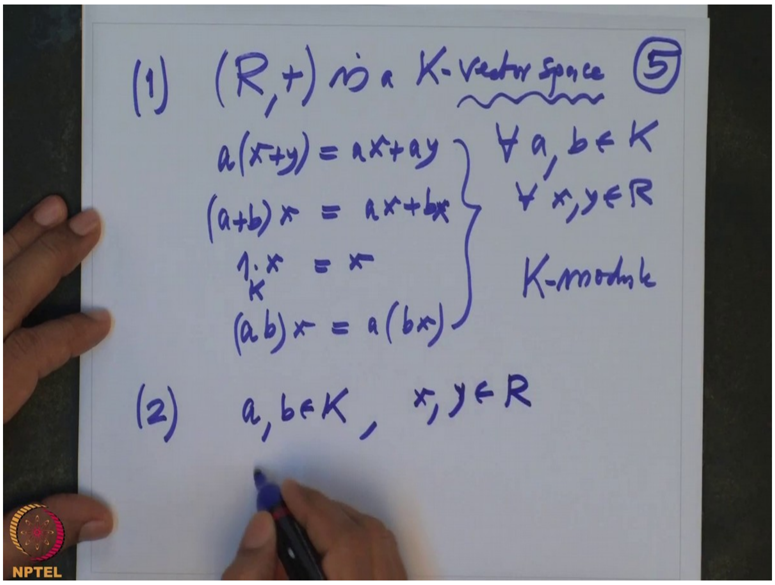
$(a\, b$ …

this plus, and obviously the, the addition and multiplication of the given field.

Second one, now with the multiplication of the ring. These are the compatibility with the multiplication of the ring. Now I will write the multiplication in the ring by just dot.

So that means what, whether I multiply first in the scalar, so that means if I have a, b are in the scalars and x, y are elements in the ring R,

(Refer Slide Time 18:48)



(1) $(R,+)$ is a K-vector space 5

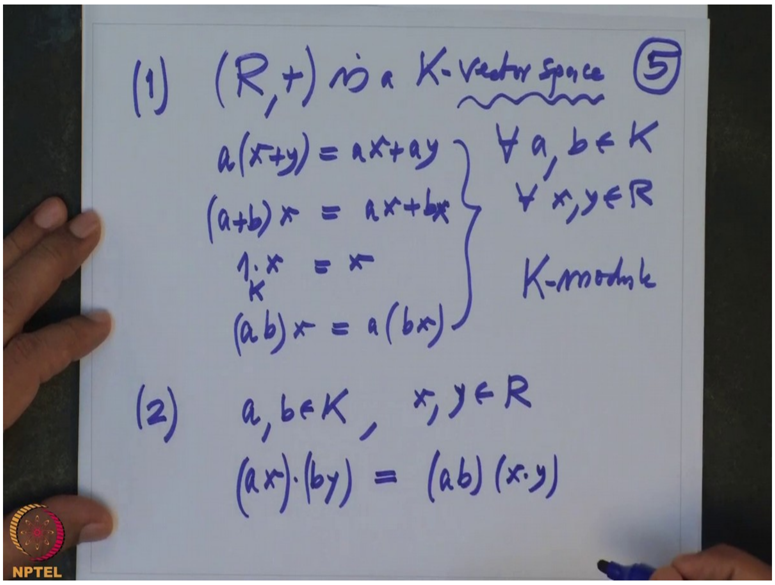
$$\left.\begin{aligned} a(x+y) &= ax+ay \\ (a+b)x &= ax+bx \\ \underset{K}{1}\cdot x &= x \\ (a\, b)x &= a(bx) \end{aligned}\right\}\quad \begin{aligned} &\forall\, a,b\in K \\ &\forall\, x,y\in R \\ &K\text{-module} \end{aligned}$$

(2) $a,b\in K$, $x,y\in R$

whether I multiply this scalar with this x, the resulting element is in R and this scalar with this element b y, I get 2 elements in R and I multiply these elements in the ring.

This result should be, first I multiply these a and b in the field K and then multiply these elements in the ring x and y. And then multiply

(Refer Slide Time 19:12)



(1) $(R,+)$ is a K-vector space ⑤

$$\left.\begin{array}{l} a(x+y) = ax+ay \\ (a+b)x = ax+bx \\ 1_K\cdot x = x \\ (a b)x = a(bx) \end{array}\right\} \begin{array}{l} \forall\, a,b\in K \\ \forall\, x,y\in R \\ K\text{-module} \end{array}$$

(2) $a,b\in K,\quad x,y\in R$

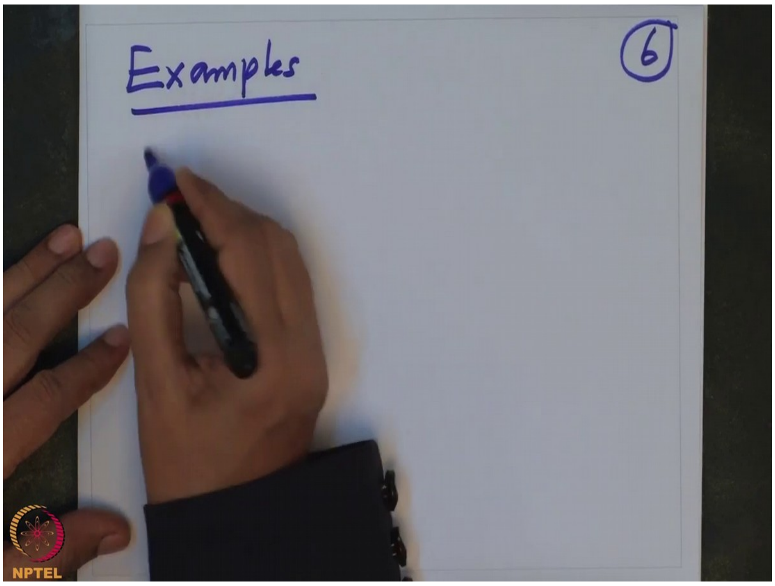
$$(ax)\cdot(by) = (ab)(x\cdot y)$$

this as a scalar multiplication.

So this result should be same. Then one says that this scalar multiplication of K on R is compatible with the ring multiplication of the ring. So typical example is the polynomial algebra. So this is called an algebra. So let us see some examples.

6, examples.

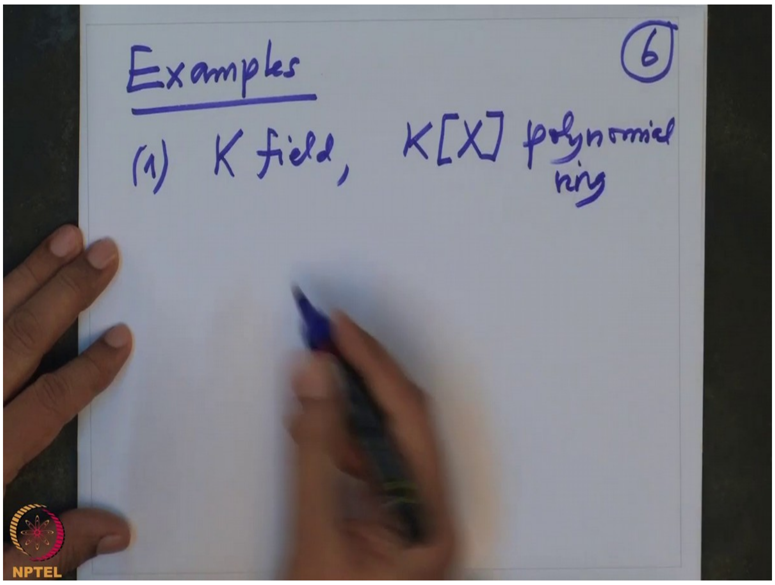
(Refer Slide Time 19:44)



Examples ⑥

One, K field and then this $K[X]$ is a polynomial ring.

(Refer Slide Time 20:01)



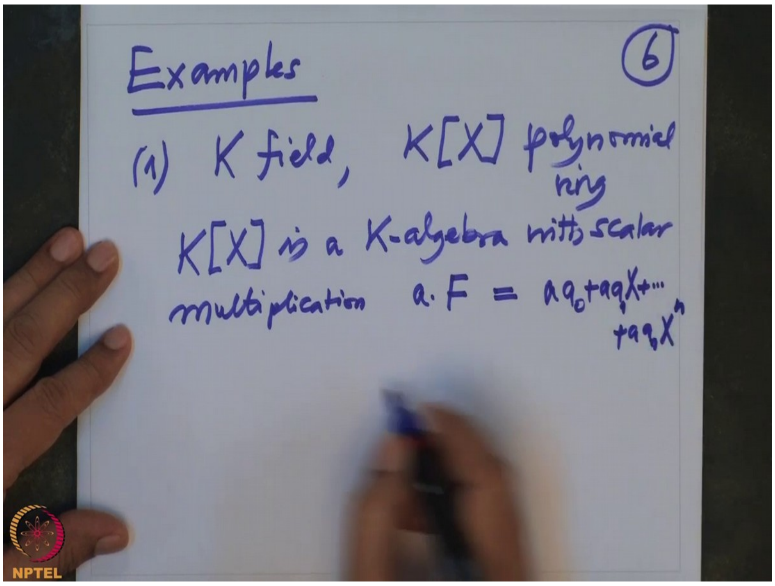
Examples

6

(1) K field, $K[X]$ polynomial ring

Then $K[X]$ is a K algebra with scalar multiplication a times any F to be, you multiply all coefficients of a by, F by a. So this is $aa_0+aa_1X+...+aa_nX^n$

(Refer Slide Time 20:42)



Examples

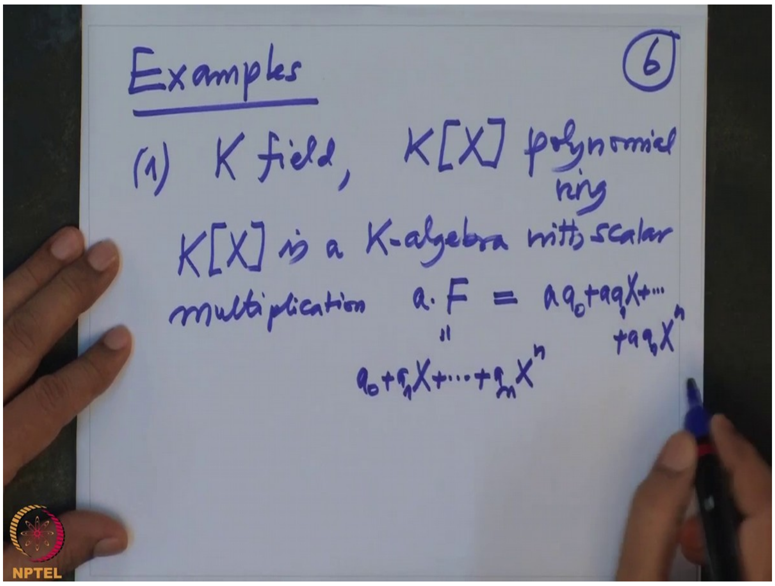
6

(1) K field, $K[X]$ polynomial ring

$K[X]$ is a K-algebra with scalar multiplication $a.F = aa_0+aa_1X+\cdots+aa_nX^n$

where F is $a_0+a_1X+...+a_nX^n$.

(Refer Slide Time 20:52)



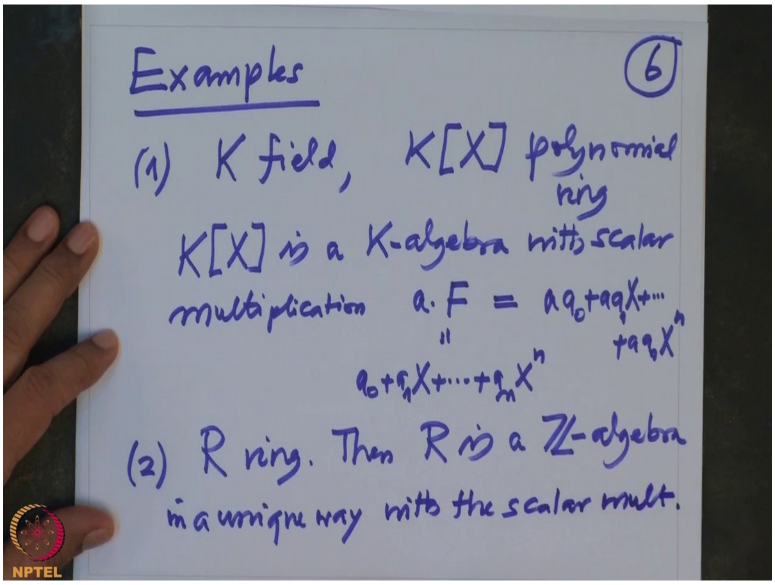
Examples 6

(1) K field, K[X] polynomial ring

K[X] is a K-algebra with scalar multiplication $a\cdot \underset{\overset{\|}{a_0+a_1X+\cdots+a_nX^n}}{F} = aa_0+aa_1X+\cdots+aa_nX^n$

This is how the scalar multiplication of K on $K[X]$ is given. So I should have said this example before, but does not matter. If R is any ring then R is $\mathbb{Z}$ algebra in a unique way. There is only one scalar multiplication, with the scalar multiplication.

(Refer Slide Time 21:31)



Examples 6

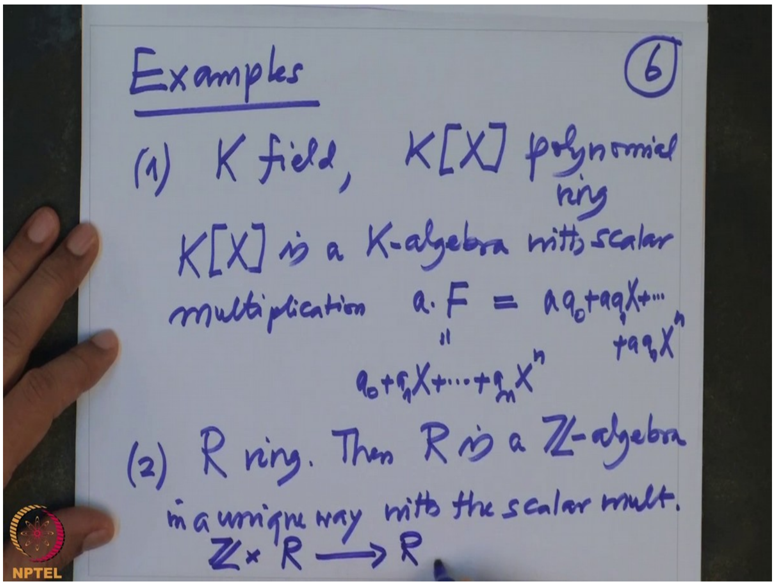
(1) K field, K[X] polynomial ring

K[X] is a K-algebra with scalar multiplication $a\cdot \underset{\overset{\|}{a_0+a_1X+\cdots+a_nX^n}}{F} = aa_0+aa_1X+\cdots+aa_nX^n$

(2) R ring. Then R is a $\mathbb{Z}$-algebra in a unique way with the scalar mult.

So we need a map from $\mathbb{Z}\times R\to R$.

(Refer Slide Time 21:39)



Examples ⑥

(1) K field, K[X] polynomial ring

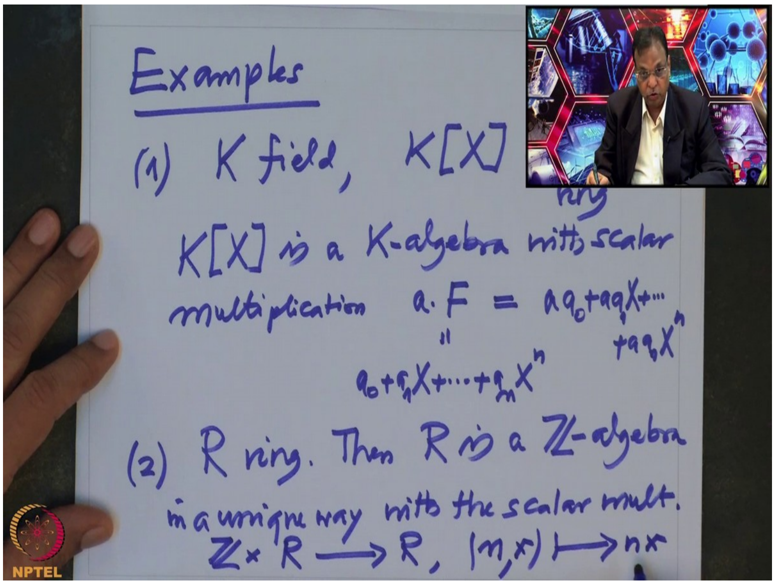
K[X] is a K-algebra with scalar multiplication $a\cdot \underset{\overset{\|}{a_0+a_1X+\cdots+a_nX^n}}{F} = aa_0+aa_1X+\cdots+aa_nX^n$

(2) R ring. Then R is a $\mathbb{Z}$-algebra in a unique way with the scalar mult. $\mathbb{Z}\times R \longrightarrow R$

So this is obviously, if you take any n, take any x and map it to n x.

n x is clear. nx is $x+x+\ldots+x$, n times

(Refer Slide Time 21:52)



Examples

(1) K field, K[X]

ring

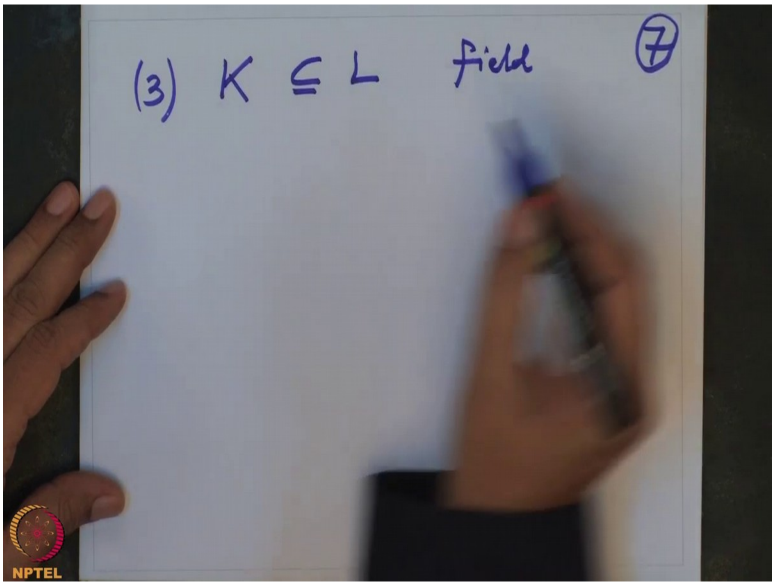
K[X] is a K-algebra with scalar multiplication $a\cdot \underset{\overset{\|}{a_0+a_1X+\cdots+a_nX^n}}{F} = aa_0+aa_1X+\cdots+aa_nX^n$

(2) R ring. Then R is a $\mathbb{Z}$-algebra in a unique way with the scalar mult. $\mathbb{Z}\times R \longrightarrow R,\ (n,x)\longmapsto nx$

when n is positive and otherwise it is $-x-x-\ldots$ n times when n is negative. So this is, this is the only one scalar multiplication which makes R as a $\mathbb{Z}$ module.

Ok, one more, this is what we will use it more often, 7, third one, if I have, K is a field contained in a bigger field L. So these are fields,

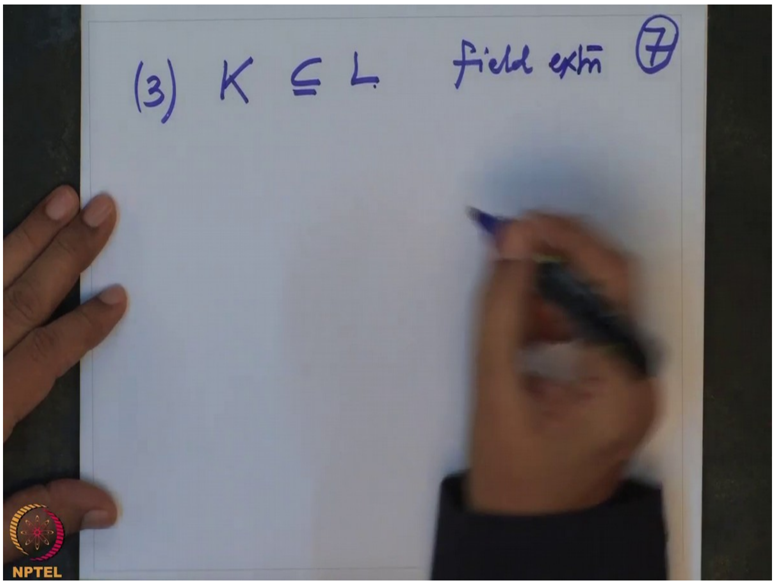
(Refer Slide Time 22:30)



so this is a bigger field and when I say K is a subfield of L or L is a bigger field than K that means we assume that the operations of K are induced from the operations of L, or one says operations in L are extended from the operations of K.

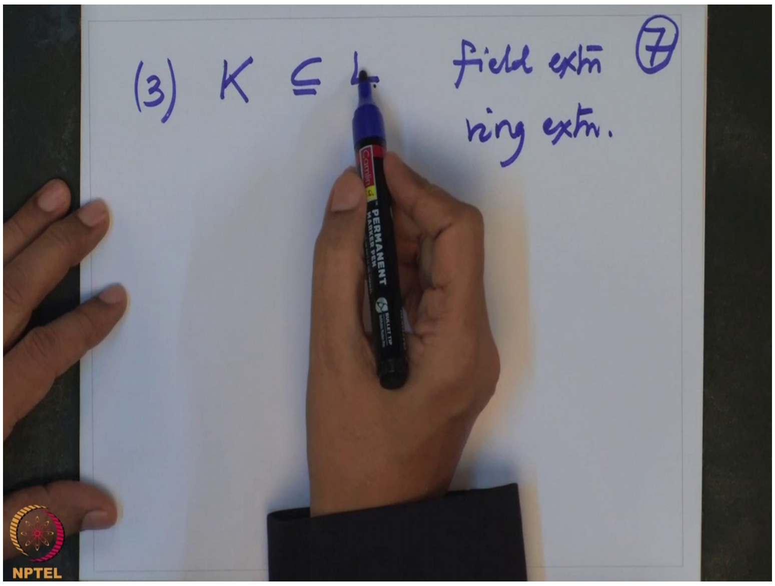
So such a thing is called a field extension.

(Refer Slide Time 22:55)



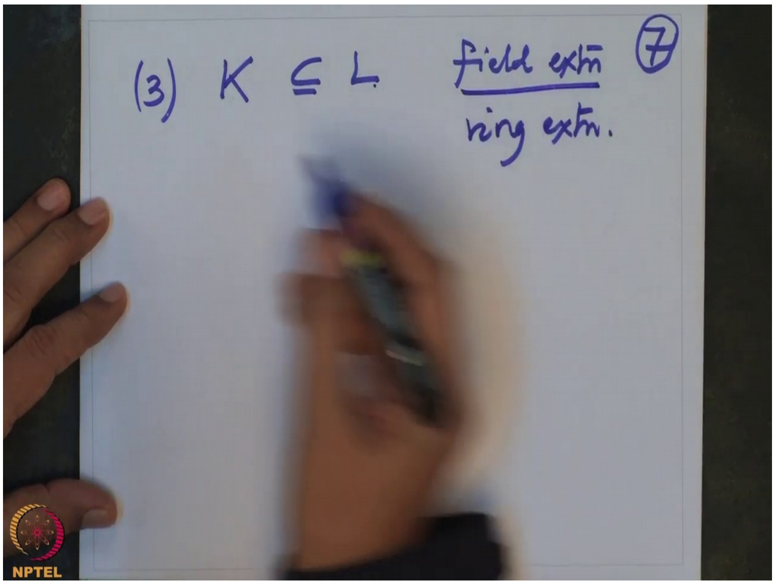
They need not be field also. If K is a ring and L is a ring, then we say, if K is a sub-ring of L, then we will say ring extension. Then the bigger one,

(Refer Slide Time 23:12)


(3) $K \subseteq L$ field extn ring extn. ⑦

let us stick to the field

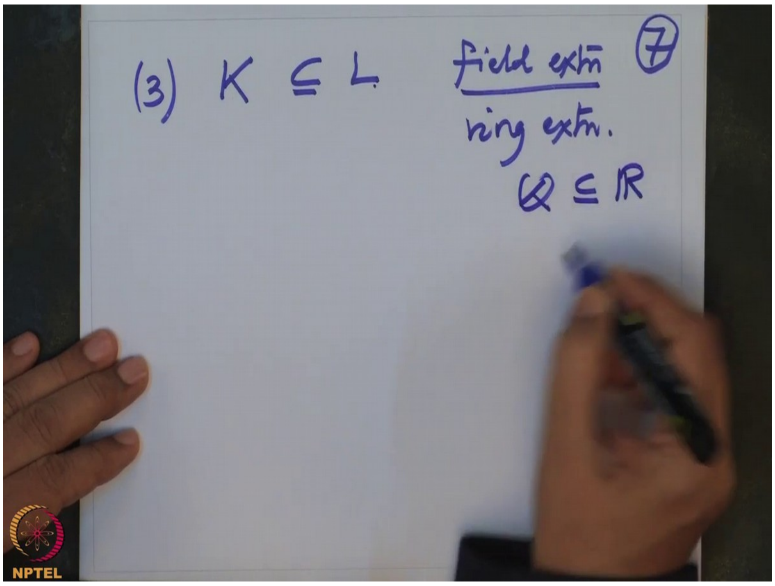
(Refer Slide Time 23:14)


(3) $K \subseteq L$ $\underline{\text{field extn}}$ ring extn. ⑦

extension here because that is what we are going to use more often,

L is a bigger field than L, so typical example of this kind are $\mathbb{Q}$ contained in $\mathbb{R}$

(Refer Slide Time 23:25)


(3) $K \subseteq L$ field extn

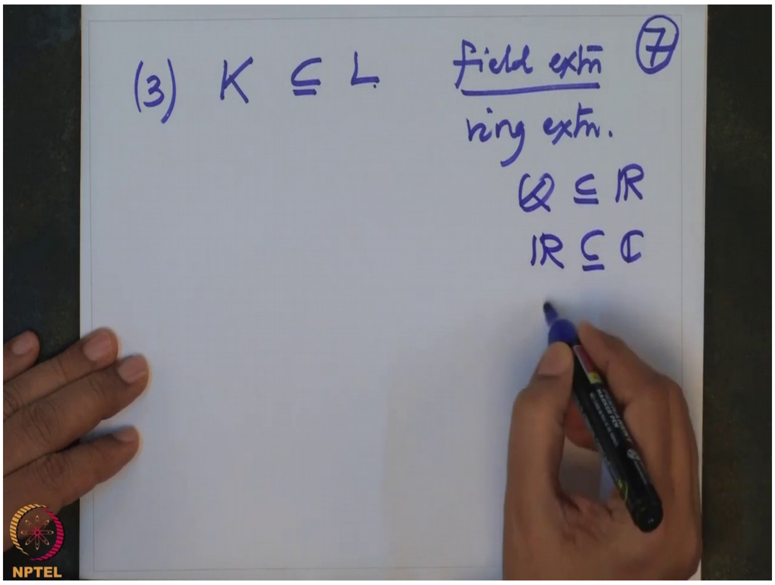
ring extn.

$\mathbb{Q} \subseteq \mathbb{R}$

7

or $\mathbb{R}$ contained in $\mathbb{C}$

(Refer Slide Time 23:29)


(3) $K \subseteq L$ field extn

ring extn.

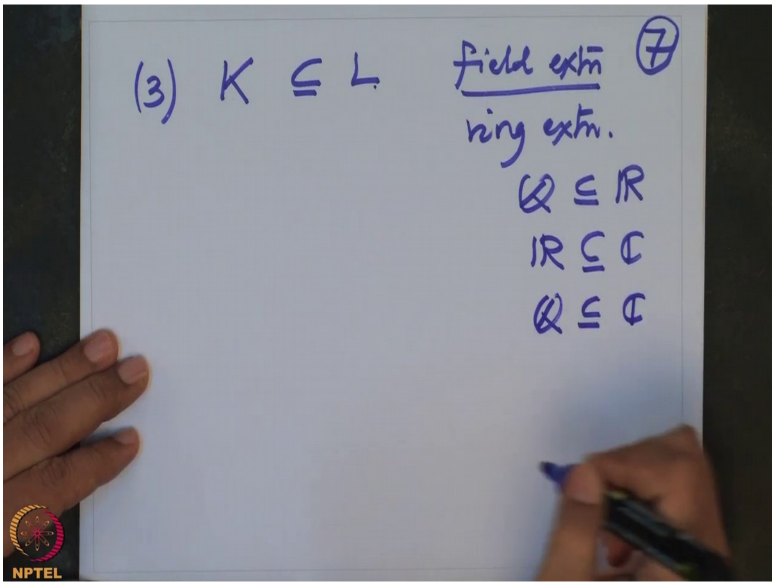
$\mathbb{Q} \subseteq \mathbb{R}$

$\mathbb{R} \subseteq \mathbb{C}$

7

or $\mathbb{Q}$ contained in $\mathbb{C}$; these are the typical examples

(Refer Slide Time 23:34)



7

(3) $K \subseteq L$ field extn

ring extn.

$\mathbb{Q} \subseteq \mathbb{R}$

$\mathbb{R} \subseteq \mathbb{C}$

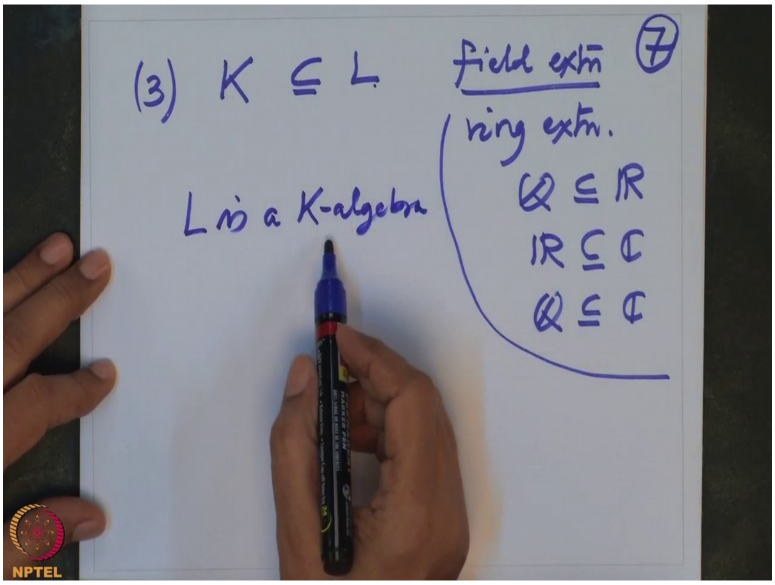
$\mathbb{Q} \subseteq \mathbb{C}$

of this kind.

And that is what one of our requirements today that I want to extend the field so that the given polynomial has zeroes in the bigger field, all zeroes in fact. I want to extend the field in such a way that a given polynomial in K X has a all-zeroes in the bigger field. It may not have zeroes in L.

So in any case when you have such a field extension, then the upper one L is a K-algebra. So remember to give a K-algebra

(Refer Slide Time 24:18)



7

(3) $K \subseteq L$ field extn

ring extn.

$\mathbb{Q} \subseteq \mathbb{R}$

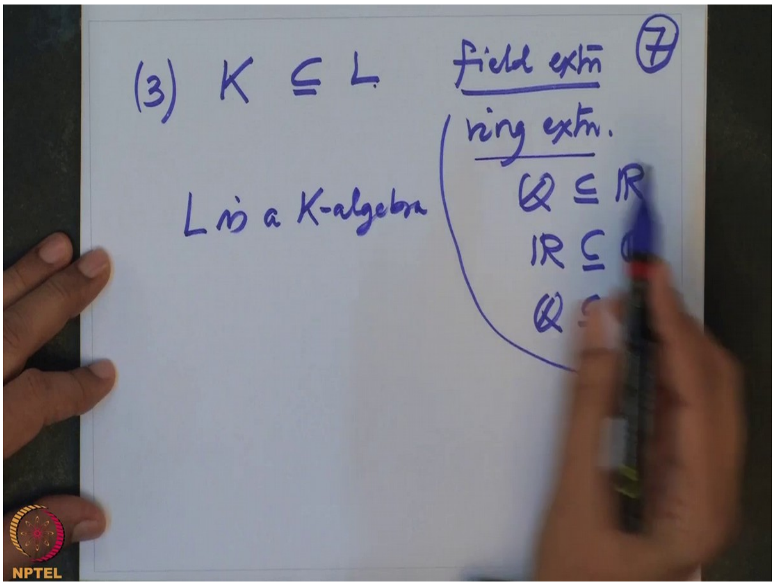
$\mathbb{R} \subseteq \mathbb{C}$

$\mathbb{Q} \subseteq \mathbb{C}$

L is a K-algebra

you need a ring which already, L is a ring, in fact L is a field. So in this case also it is fine.

(Refer Slide Time 24:24)



(3) $K \subseteq L$ field extn 7

ring extn.

$\mathbb{Q} \subseteq \mathbb{R}$

$\mathbb{R} \subseteq$

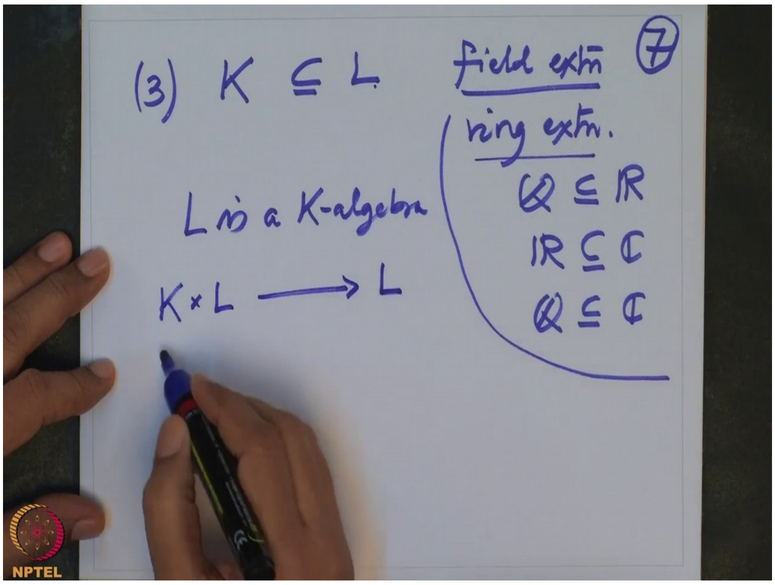
$\mathbb{Q}$

L is a K-algebra

So L is a ring and you need a scalar multiplication of K on L, but then you can just restrict that multiplication of L.

So take

(Refer Slide Time 24:35)



(3) $K \subseteq L$ field extn 7

ring extn.

$\mathbb{Q} \subseteq \mathbb{R}$

$\mathbb{R} \subseteq \mathbb{C}$

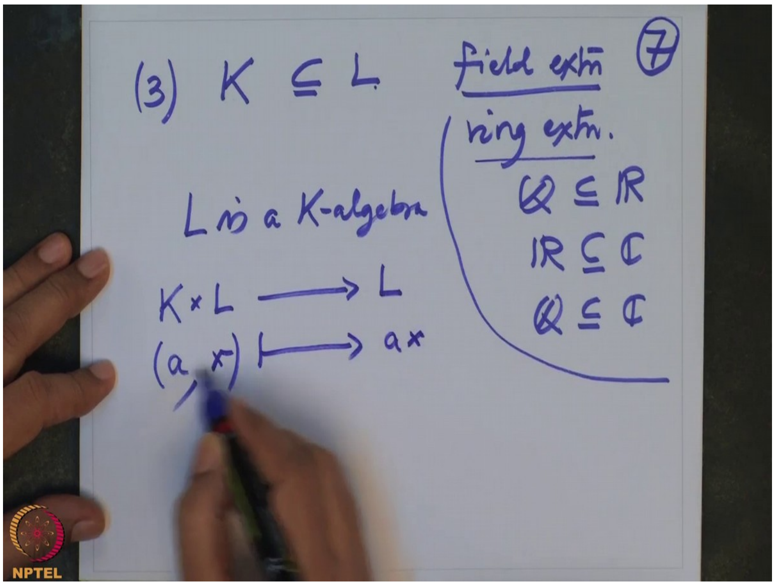
$\mathbb{Q} \subseteq \mathbb{C}$

L is a K-algebra

$K \times L \longrightarrow L$

any a in K and take any x in L and map it to a x if you are multiplying these elements

(Refer Slide Time 24:41)



(3) $K \subseteq L$ field extn ring extn. 7

$\mathbb{Q} \subseteq \mathbb{R}$

$\mathbb{R} \subseteq \mathbb{C}$

$\mathbb{Q} \subseteq \mathbb{C}$

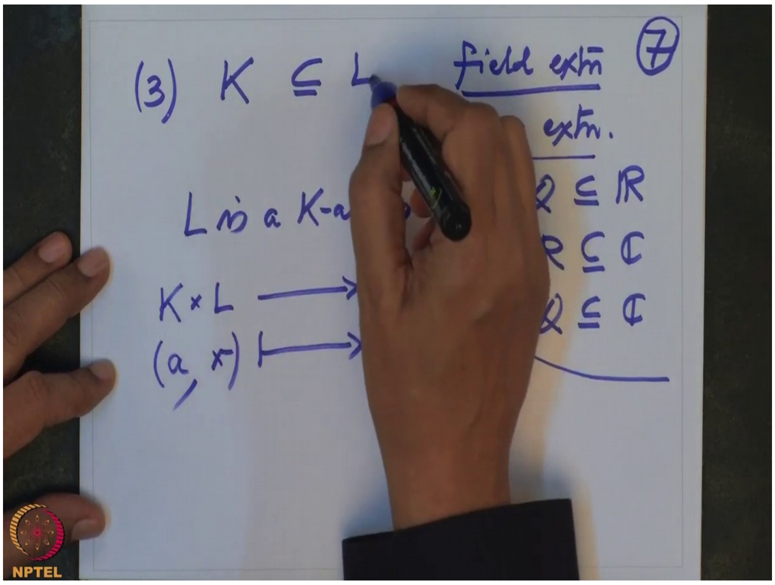
L is a K-algebra

$K \times L \longrightarrow L$

$(a, x) \longmapsto ax$

are in L because the multiplication in

(Refer Slide Time 24:45)



(3) $K \subseteq L$ field extn extn. 7

$\mathbb{Q} \subseteq \mathbb{R}$

$\mathbb{R} \subseteq \mathbb{C}$

$\mathbb{Q} \subseteq \mathbb{C}$

L is a K-a

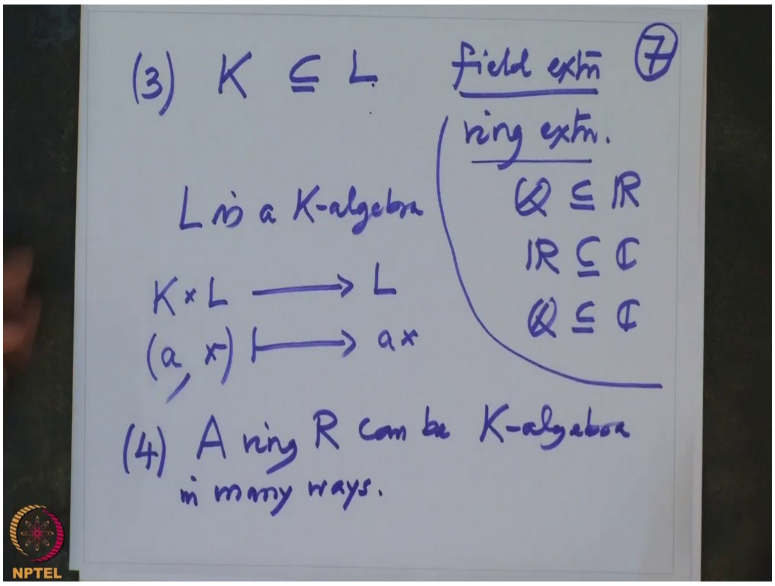
$K \times L \longrightarrow$

$(a, x) \longmapsto$

the ring here is same as whether you take, and consider them as elements here or, or elements of K. So this is a scalar multiplication and with this scalar multiplication, this L becomes K-algebra.

Ok, now one more example, we will just say it. So a ring can be, a ring R can be K-algebra in many ways. We will see these

(Refer Slide Time 25:31)



(3) $K \subseteq L$ field extn 7

ring extn.

$\mathbb{Q} \subseteq \mathbb{R}$

$\mathbb{R} \subseteq \mathbb{C}$

$\mathbb{Q} \subseteq \mathbb{C}$

L is a K-algebra

$K \times L \longrightarrow L$

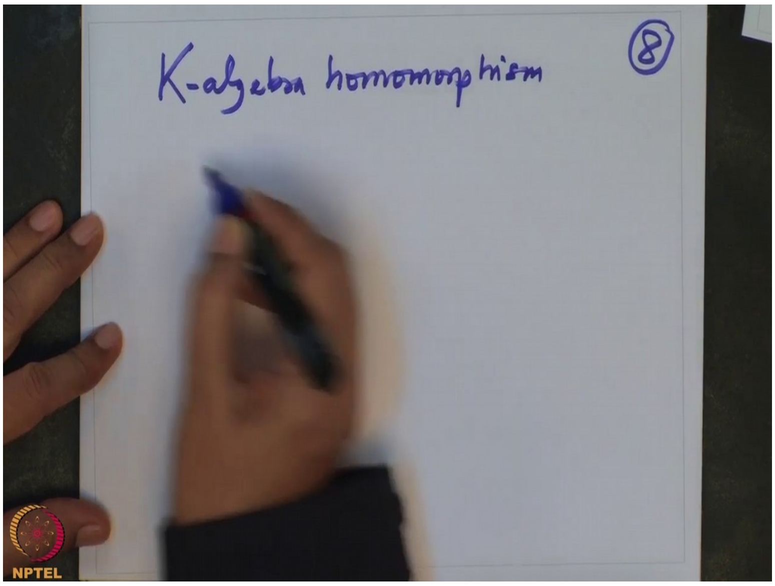
$(a, x) \longmapsto ax$

(4) A ring R can be K-algebra in many ways.

kind of examples when, in the assignments. So the, this means the scalar multiplication of the ring, of K on the ring R are, may be different, Ok.

So we have seen now ring homomorphism. We have seen K-algebras. One more important class of K-algebra I want to give is, Oh before I go on to that I also want to recall what should be K-algebra homomorphism. K-algebra homomorphism, it should mean

(Refer Slide Time 26:13)

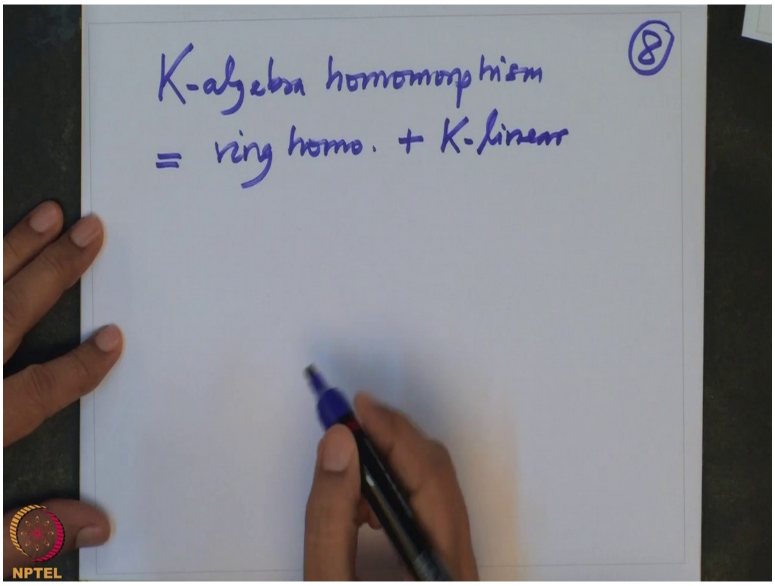


K-algebra homomorphism 8

ring homomorphism and K-vector space homomorphism, K-linear.

So what

(Refer Slide Time 26:27)



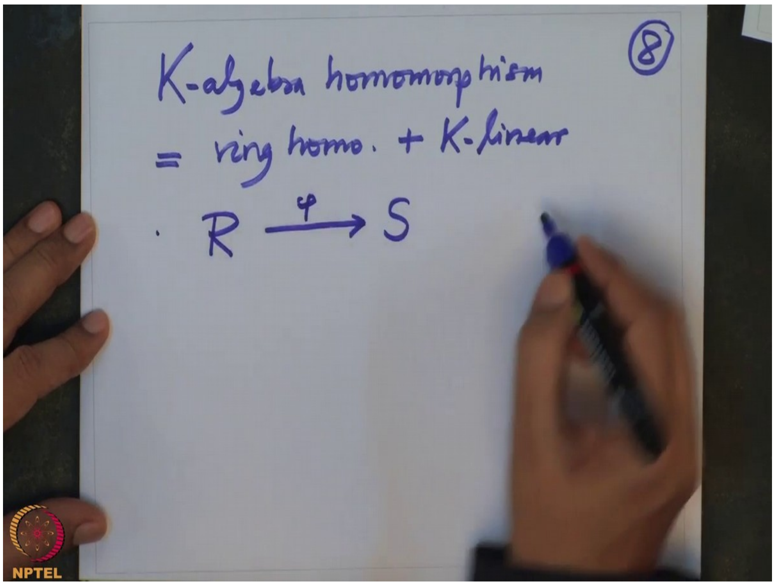
K-algebra homomorphism

= ring homo. + K-linear

⑧

does that mean? Let me write in the notation now. Now you have 2 K-algebras R and S and a map between them, ϕ . So

(Refer Slide Time 26:37)



K-algebra homomorphism

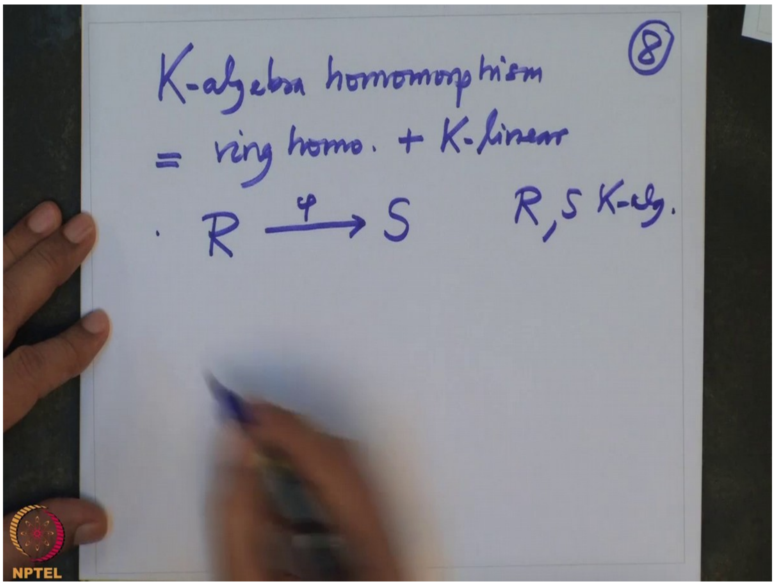
= ring homo. + K-linear

. $R \xrightarrow{\varphi} S$

⑧

R and S are K-algebras

(Refer Slide Time 26:42)



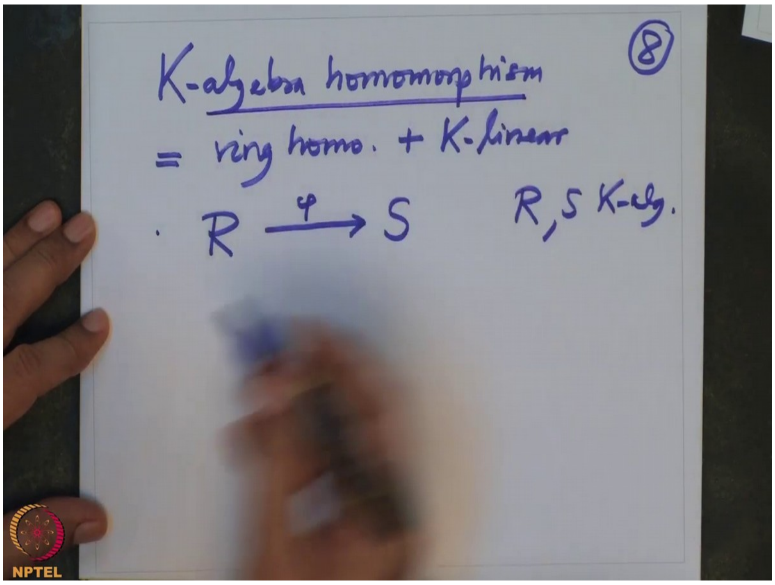
K-algebra homomorphism ⑧

= ring homo. + K-linear

· $R \xrightarrow{\varphi} S$ R, S K-alg.

and ϕ is a map between them. It is called K-algebra homomorphism

(Refer Slide Time 26:46)



K-algebra homomorphism ⑧

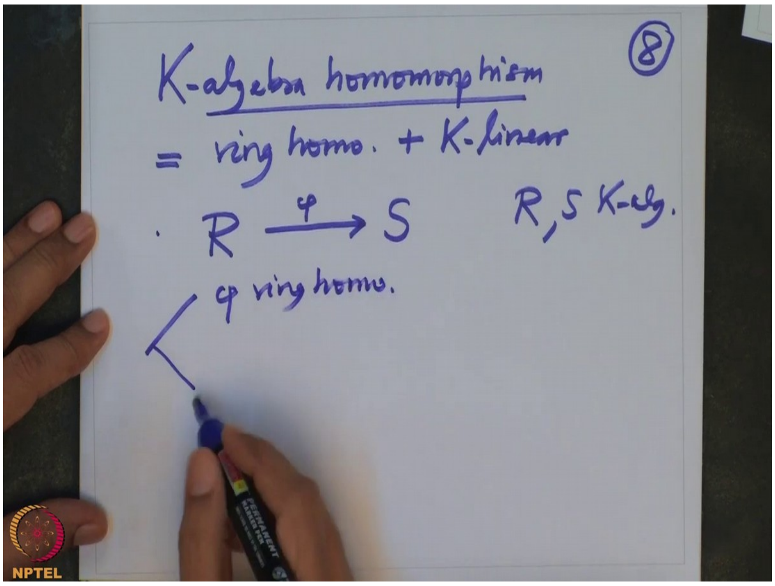
= ring homo. + K-linear

· $R \xrightarrow{\varphi} S$ R, S K-alg.

if it satisfies, first of all phi should be ring homomorphism.

And

(Refer Slide Time 26:54)



K-algebra homomorphism 8

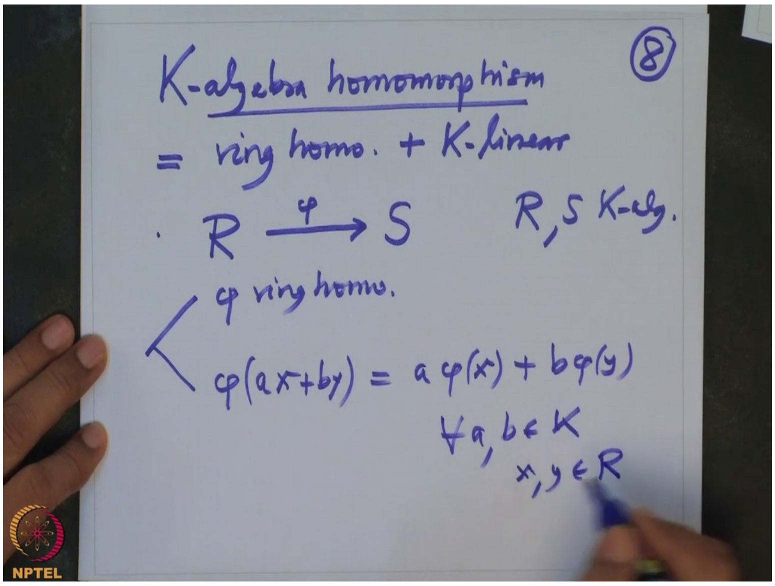
= ring homo. + K-linear

· $R \xrightarrow{\varphi} S$ R, S K-alg.

φ ring homo.

now we know that, because they are K-algebras they are K-vector spaces. And therefore it makes sense to talk about K-vector space homomorphism or K-linear map. That means phi should satisfy this property, $\phi(ax+by)=a\phi(x)+b\phi(y)$ for all $a,b\in K$ and $x,y\in R$.

(Refer Slide Time 27:24)



K-algebra homomorphism 8

= ring homo. + K-linear

· $R \xrightarrow{\varphi} S$ R, S K-alg.

φ ring homo.

$\varphi(ax+by) = a\varphi(x) + b\varphi(y)$

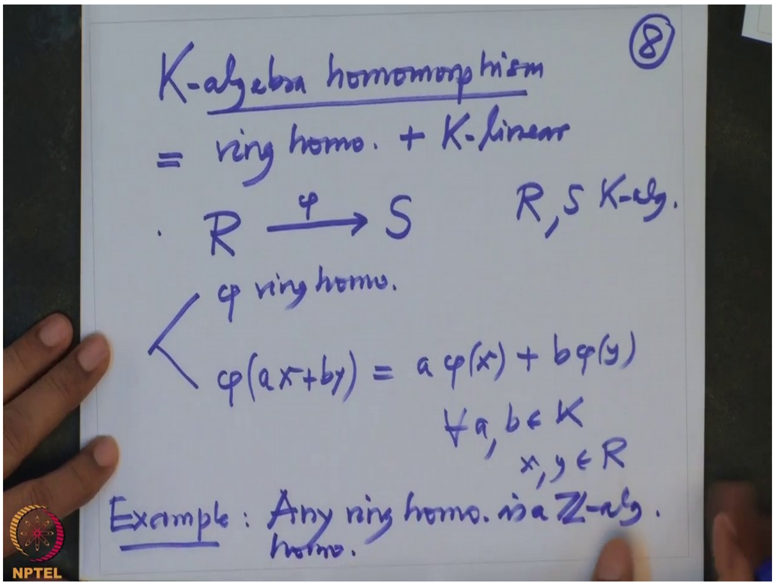
$\forall a, b \in K$

$x, y \in R$

Such a thing is called a K-algebra homomorphism.

So any ring homomorphism is a $\mathbb{Z}$ -algebra homomorphism. So example, because there we do not have to check nothing, it is only one. So any ring homomorphism is a $\mathbb{Z}$ -algebra homomorphism. This is immediate from the

(Refer Slide Time 27:52)



K-algebra homomorphism (8)

= ring homo. + K-linear

$R \xrightarrow{\varphi} S$ $\quad R, S$ K-alg.

φ ring homo.

$\varphi(ax+by) = a\varphi(x) + b\varphi(y)$ $\forall\, a, b \in K$, $x, y \in R$

Example: Any ring homo. is a $\mathbb{Z}$-alg. homo.

definitions. So recall that what we have done in these few minutes is that we have recalled the definition of ring homomorphism.

(Refer Slide Time 28:04)

We have also defined what are K-algebras and we have also defined what is a K-algebra homomorphisms and in the next, after the break I will continue with more examples which would lead to the concept of algebraic elements. We will continue after break. Thank you.