Galois' Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture No 13
Algebraic elements

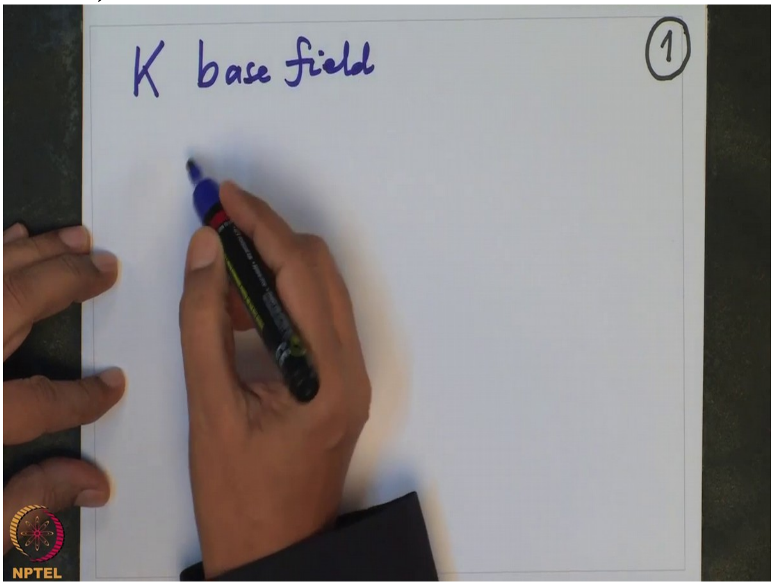
(Refer Slide Time 00:25)

Good afternoon. In the last couple of lectures, we have been preparing for the basic concepts for the course which I will be using throughout this course and let me just summarize briefly last time I have

(Refer Slide Time 00:49)

introduced concepts of given a field K, K is a given field which, I will call it a base field then

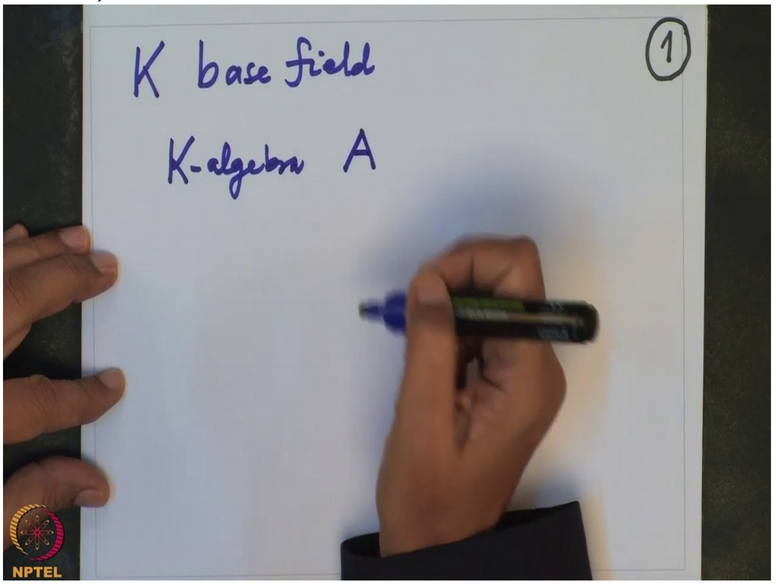
(Refer Slide Time 01:02)



we have defined what is a K-algebra.

Usually we use the standard notation for that is the capital alphabets A, B, C etc. So let me use it A here,

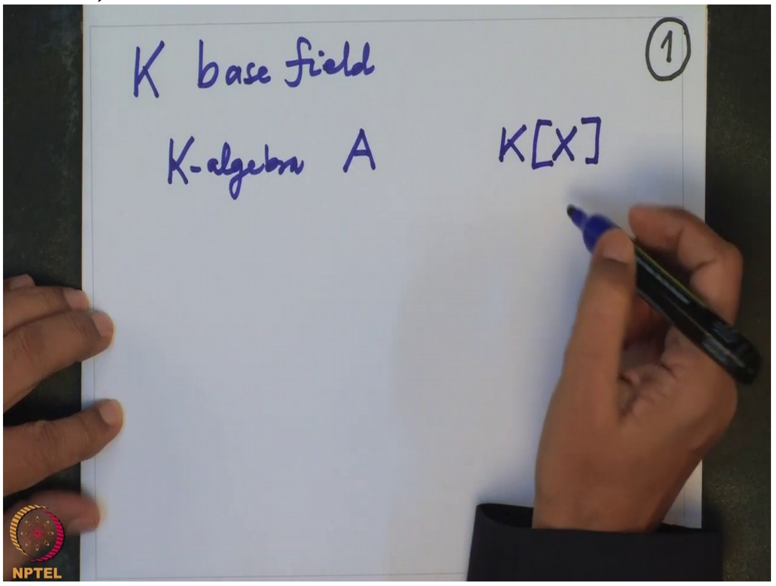
(Refer Slide Time 01:21)



so it is a K vector space as well as ring and this vector space and ring structures are compatible with each other.

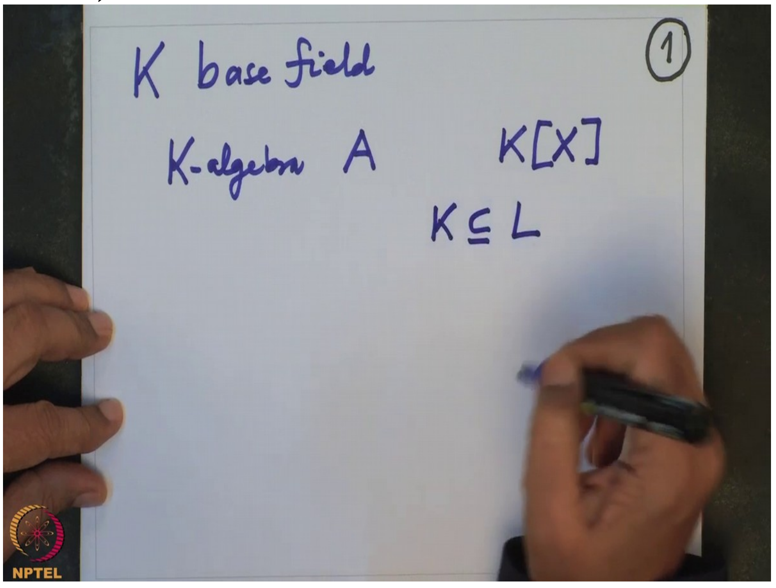
Then particular examples of K-algebra, we will use are polynomial ring in one variable, over a field

(Refer Slide Time 01:42)



and may be more variables, also field extension L. L is a bigger field containing K

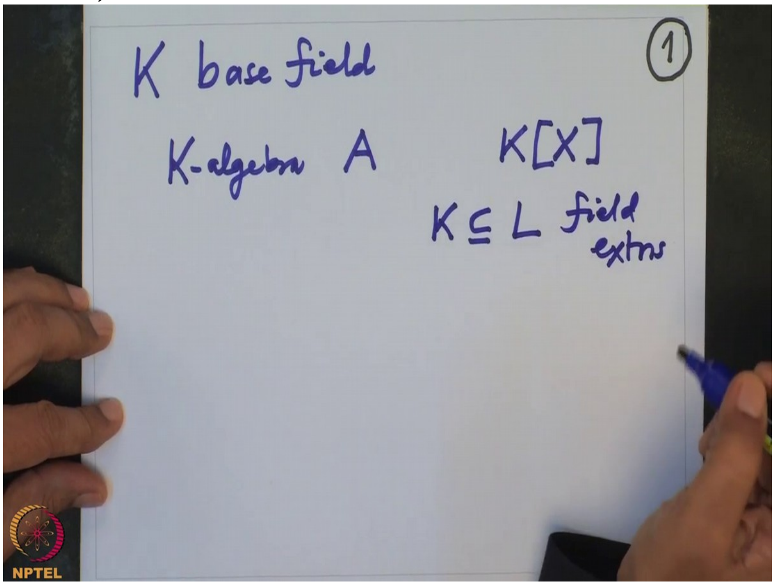
(Refer Slide Time 01:53)



so that is K, there is a field associating is called field extension.

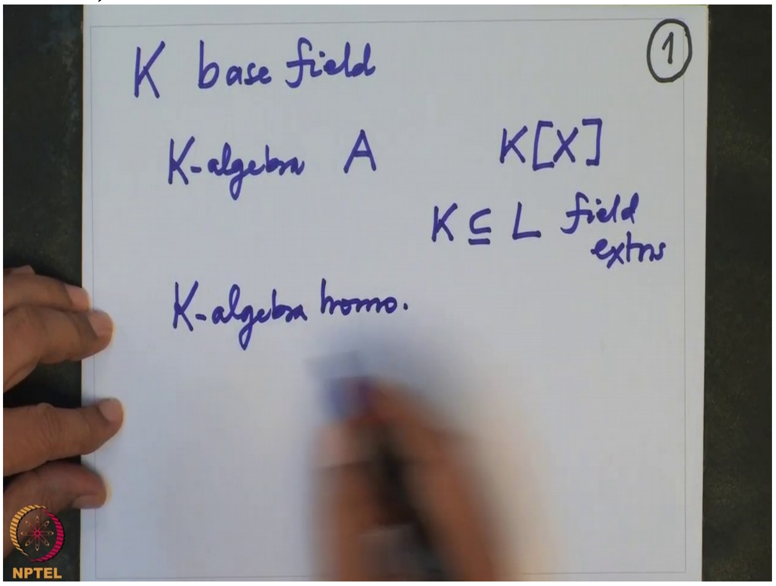
So these are the examples of K-algebra that we will

(Refer Slide Time 02:01)



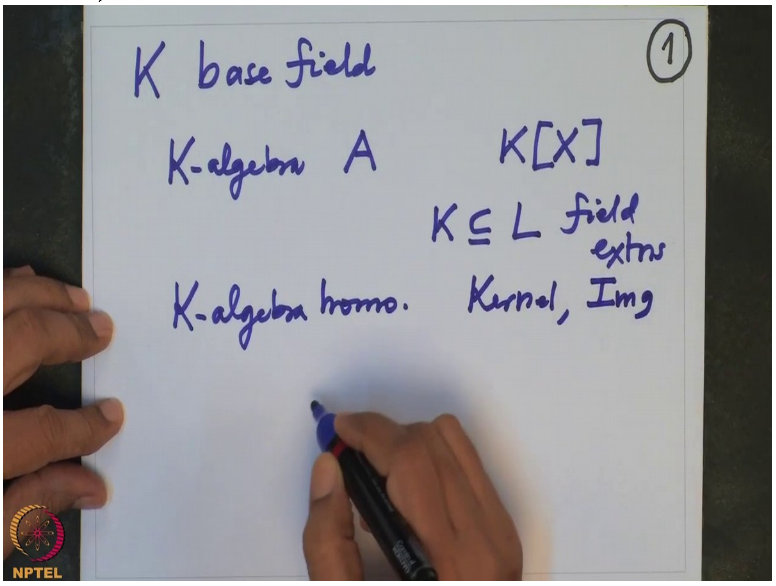
use and also we have defined a concept of K-algebra homomorphisms, homomorphisms,

(Refer Slide Time 02:17)



also kernels of a homomorphism, image of homomorphisms all these

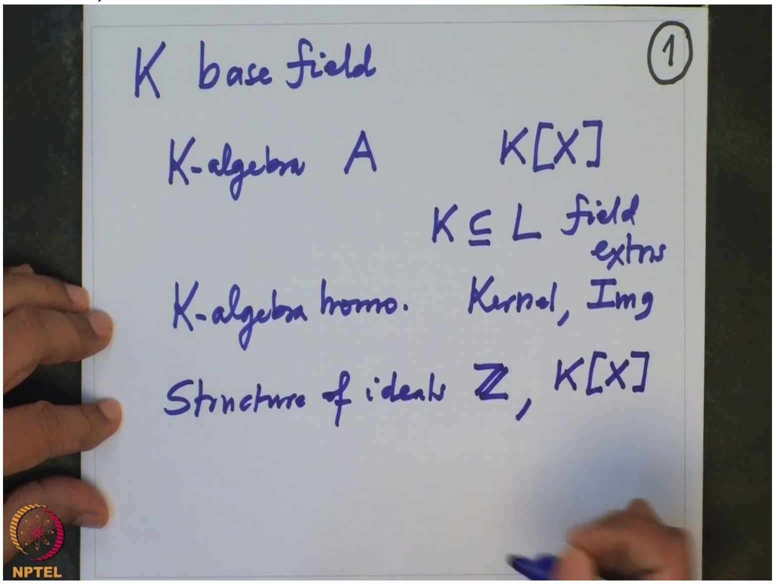
(Refer Slide Time 02:26)



you must have studied in the basic course on algebra and also linear algebra.

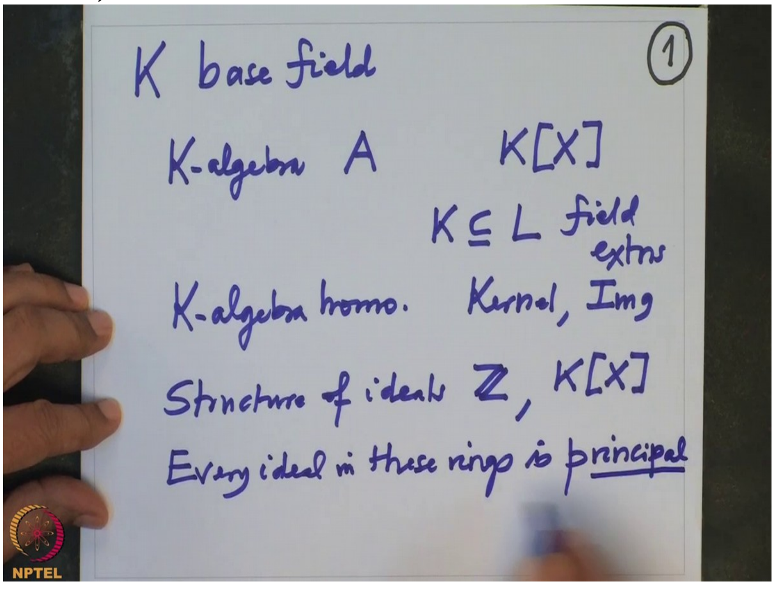
And the most important thing I want to recall is what we have proved is structure of ideals, ideals in the ring, ring of integers and also a polynomial ring in one variable over the field

(Refer Slide Time 02:58)



K. And we have proved that every ideal in these rings, in these rings is principal. Principal means

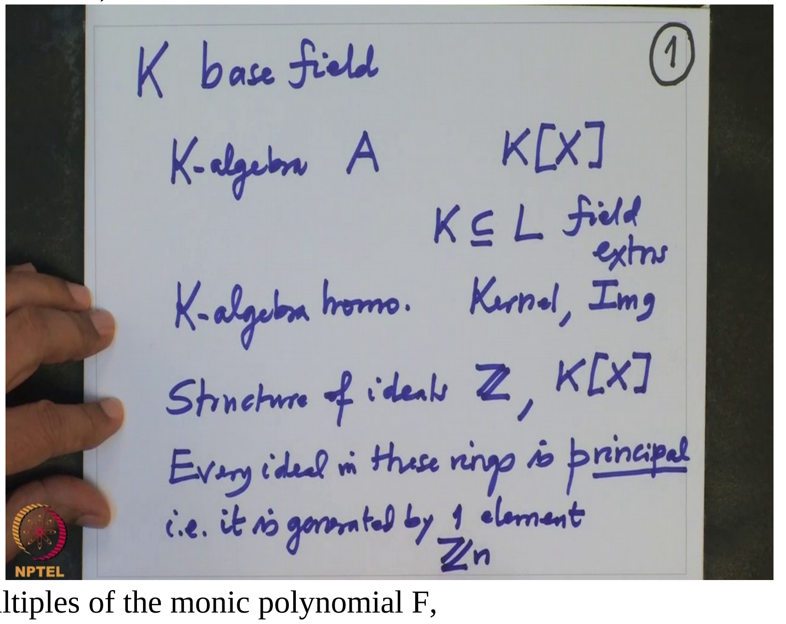
(Refer Slide Time 03:22)



it is generated by 1 element; that is it is generated by 1 element.

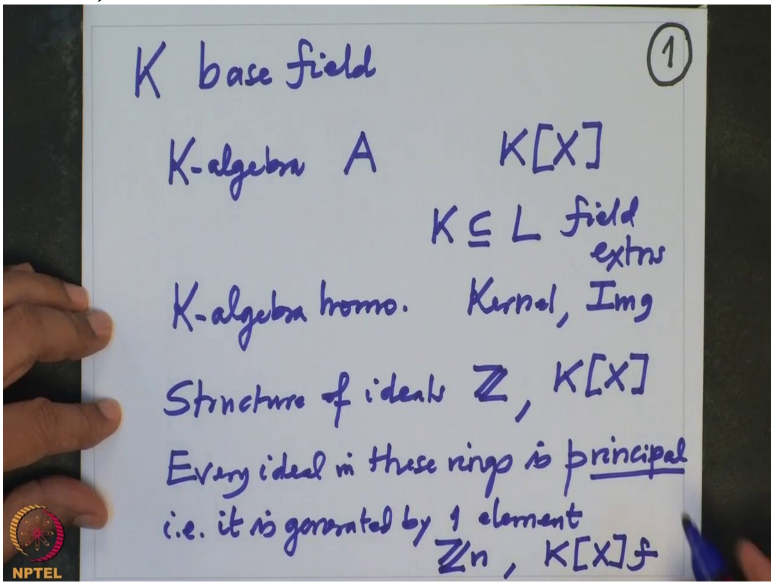
That means for example in $\mathbb{Z}$ they are of the form multiples of a fixed natural number n

(Refer Slide Time 03:42)



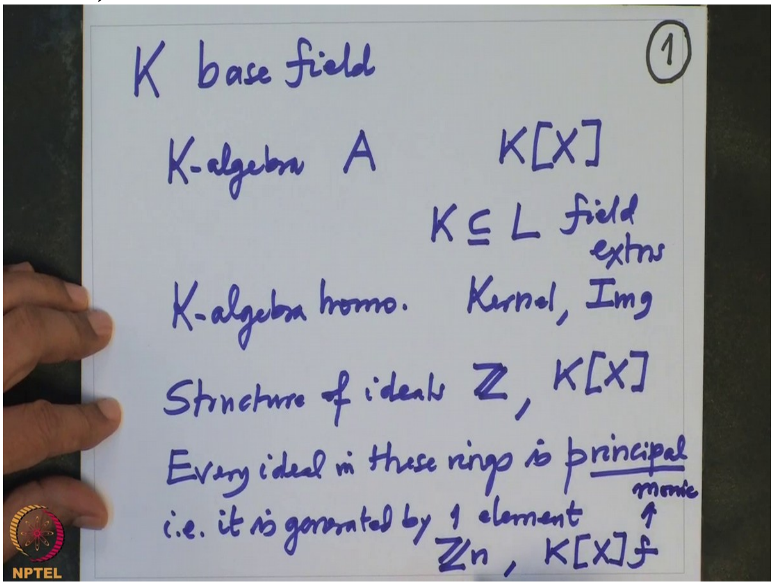
and in K it is multiples of the monic polynomial F,

(Refer Slide Time 03:53)



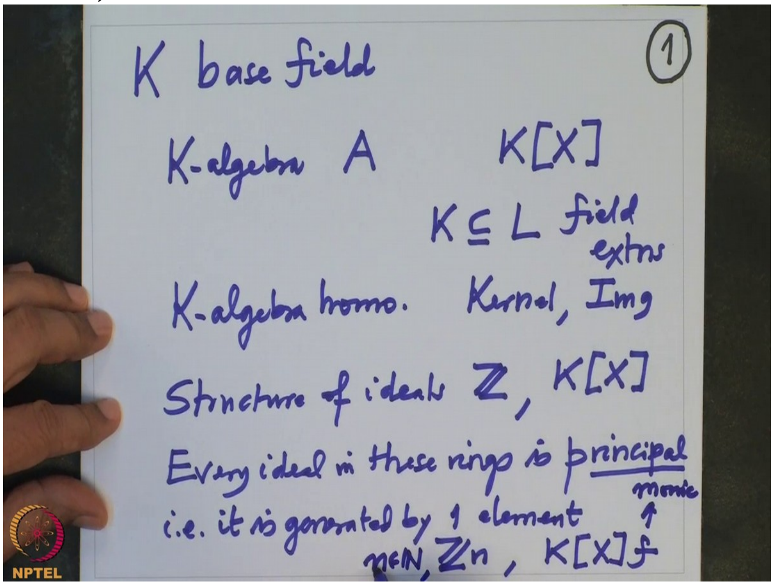
F monic.

(Refer Slide Time 03:58)



It is monic means the leading coefficient is 1 and this n is a natural number. And this, the natural number n and

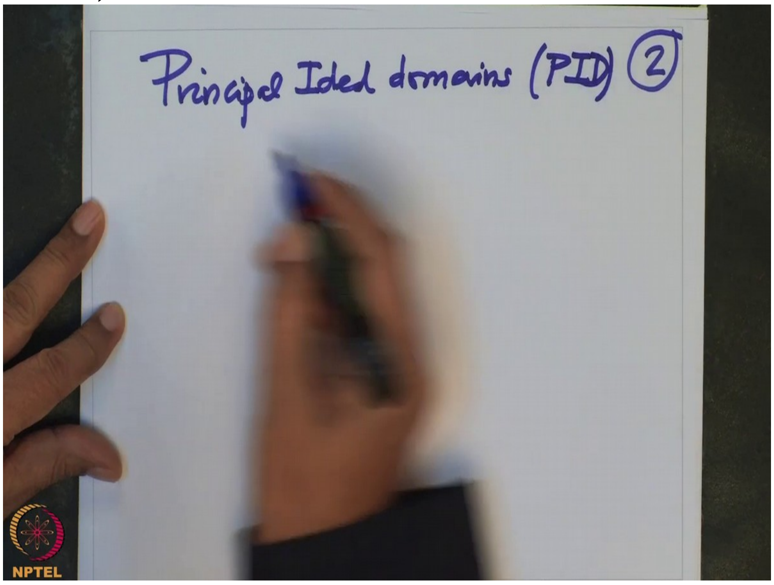
(Refer Slide Time 04:05)



the monic generators are uniquely determined.

This, this fact we will keep using, again and again using and because every ideal is of this form these rings are usually called as, we have already noted that they are integral domains and because ideals are principal, these rings are called principal ideal domains, ideal domains and this is usually abbreviated as P I D.

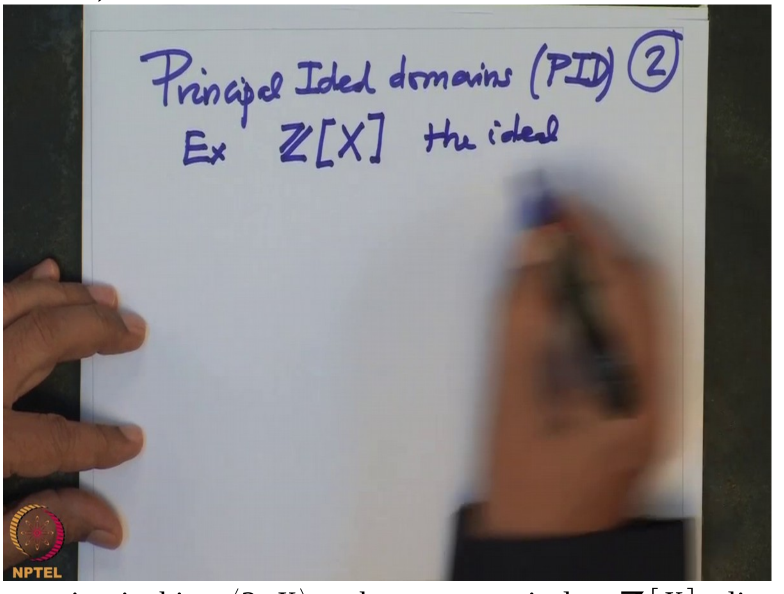
(Refer Slide Time 04:46)



And we have seen example that not every ring is a, not every integer domain is a P I D.

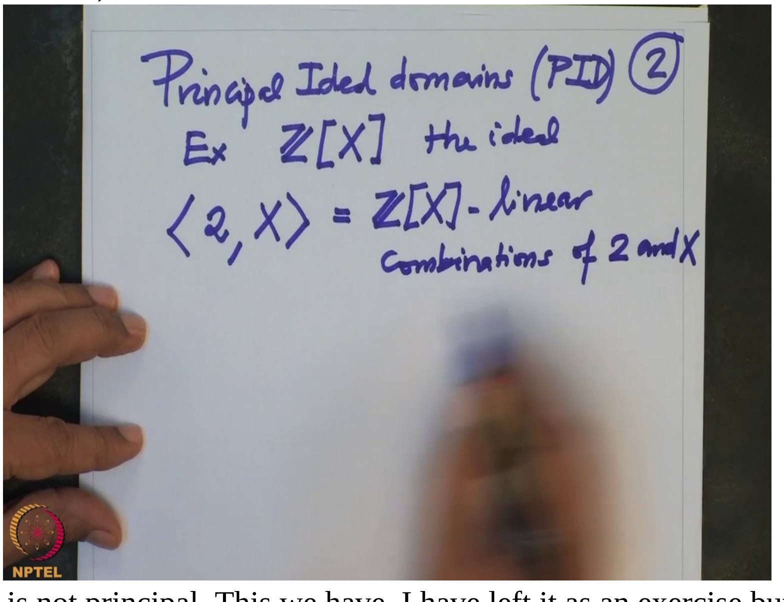
For example we have seen that the ideal, in the polynomial ring over integers, in this ring the ideal

(Refer Slide Time 05:04)



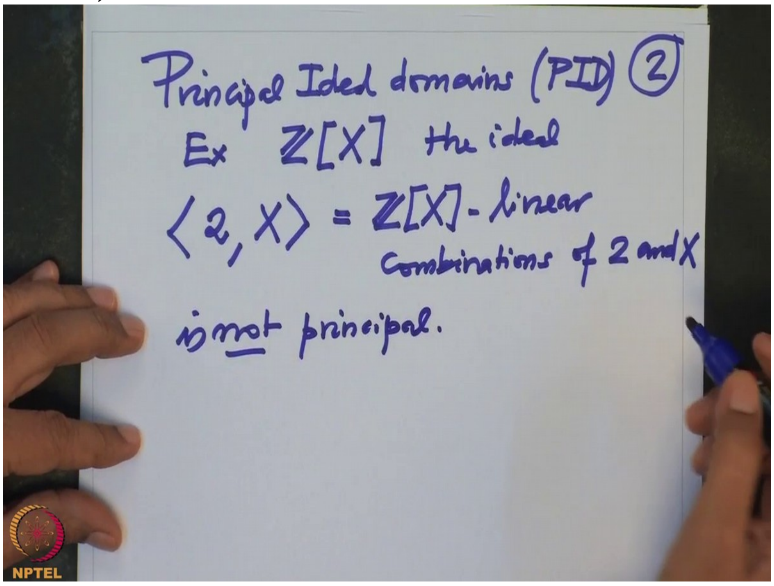
generated by the notation is this $\langle 2, X \rangle$, these are precisely $\mathbb{Z}[X]$ linear combinations, combinations of 2 and X.

(Refer Slide Time 05:27)



This ideal is not, is not principal. This we have, I have left it as an exercise but

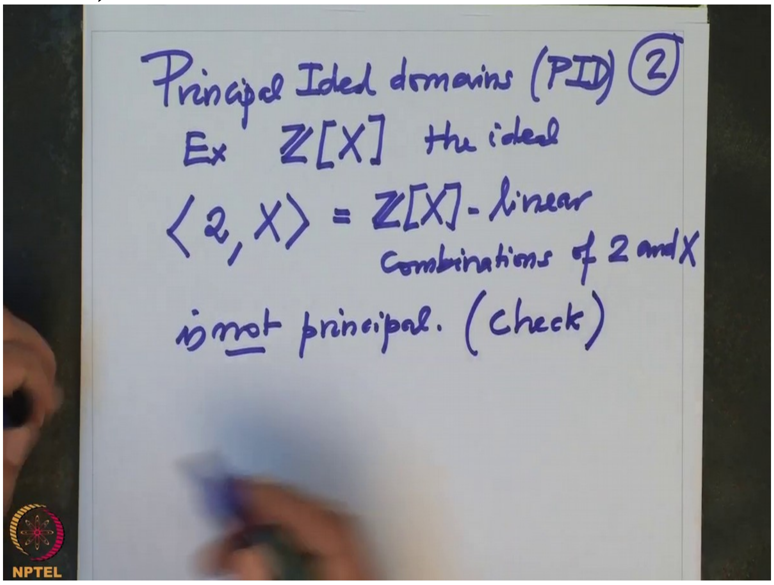
(Refer Slide Time 05:37)



this is very easy to check that there is no polynomial, no single polynomial F so that this ideal is generated by F.

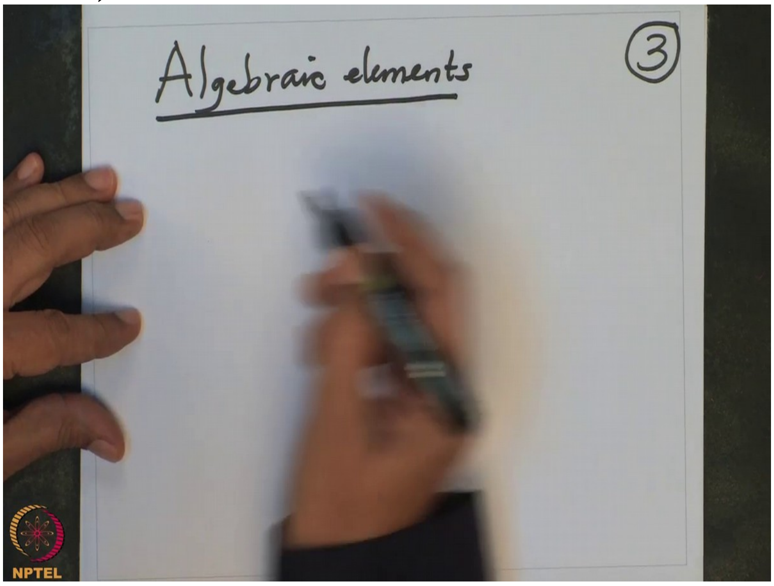
So this we remind you to check in the exercises,

(Refer Slide Time 05:52)



alright. With this I want to now define what is an algebraic elements or what is an algebraic extension. So definition, so this is algebraic elements.

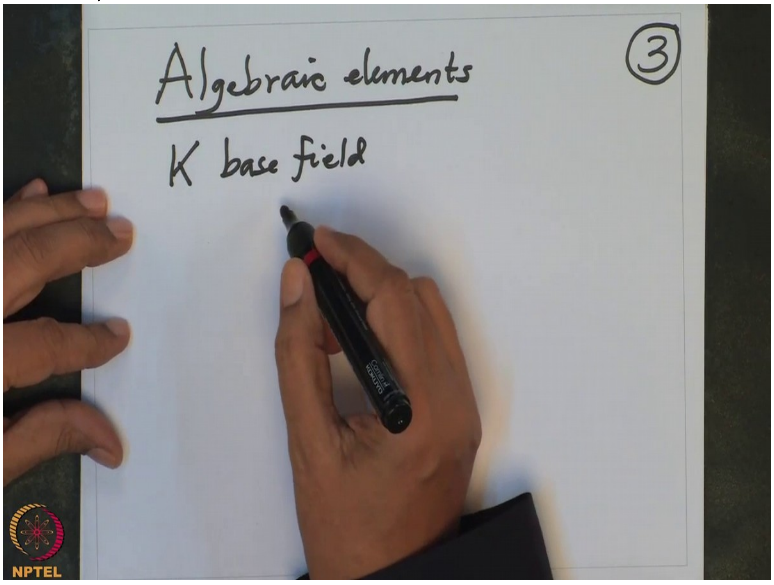
(Refer Slide Time 06:16)



Ok, so let K be our base field.

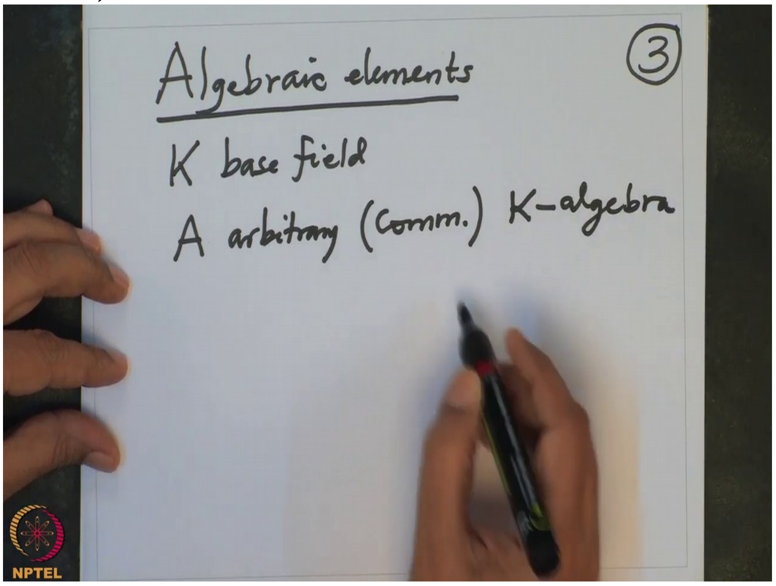
Many of these concepts can be done

(Refer Slide Time 06:26)



for arbitrary commutative in K but I am not going to do this. In this whole course, we are going to concentrate on the base field and then develop concepts with respect to this field K. But instead of a field extension I am going to consider A to be K-algebra, A to be arbitrary K-algebra, arbitrary. I would also assume it is commutative, K-algebra.

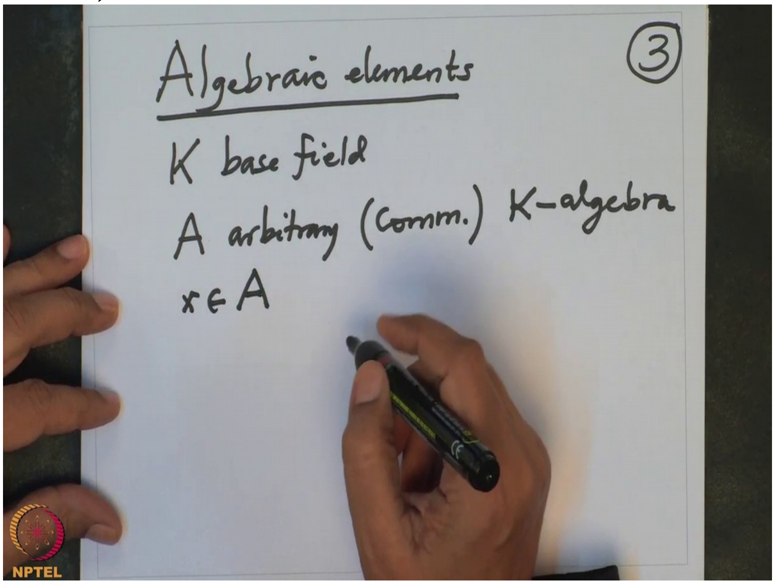
(Refer Slide Time 07:02)



Actually this also I do not want to assume but to begin with we assume. When the example comes I will indicate that time.

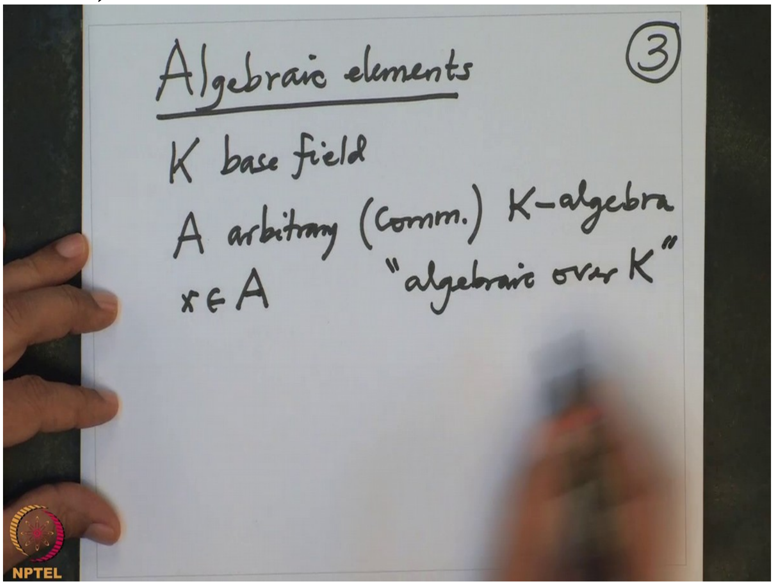
And we have an element, so x in, small x in the algebra, K-algebra here.

(Refer Slide Time 07:19)



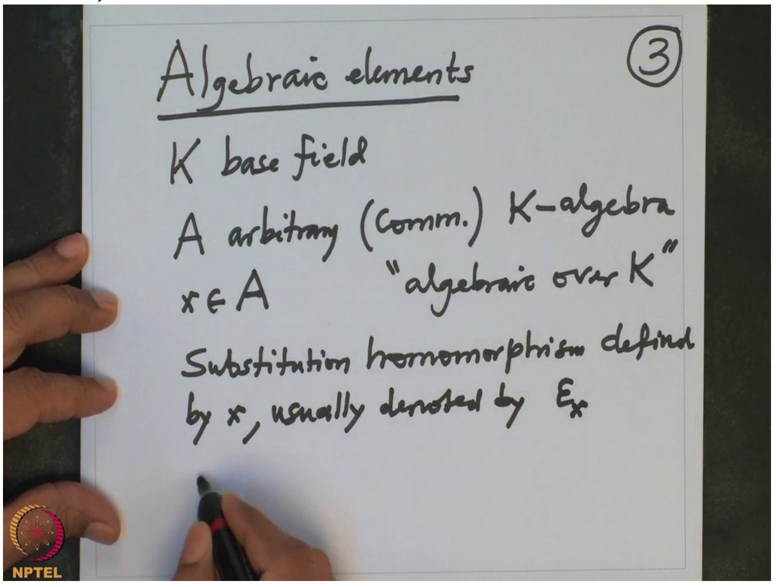
And I want to define when is x algebraic over K. I want to define this concept, algebraic over K. This concept.

(Refer Slide Time 07:35)



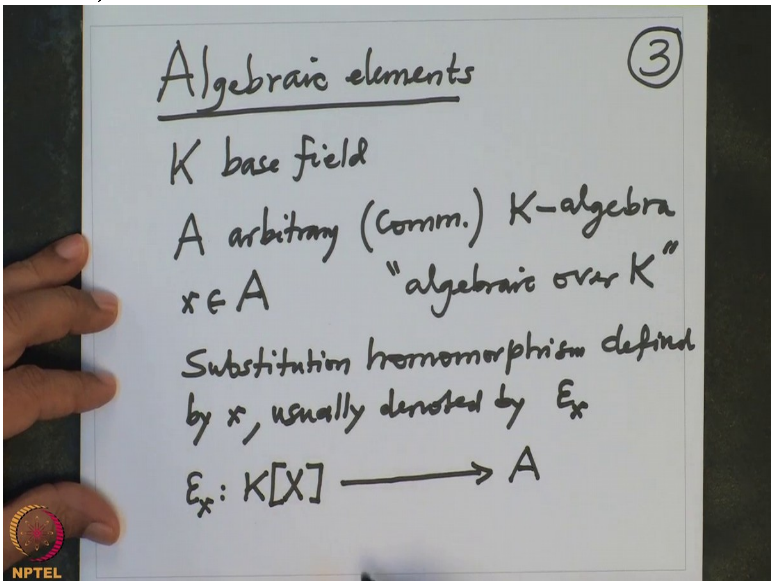
So note that given any x in A, I have this evaluation map or substitution map. So substitution homomorphism, defined by F, defined by x, this usually denoted by ϵ_x or E_x .

(Refer Slide Time 08:14)



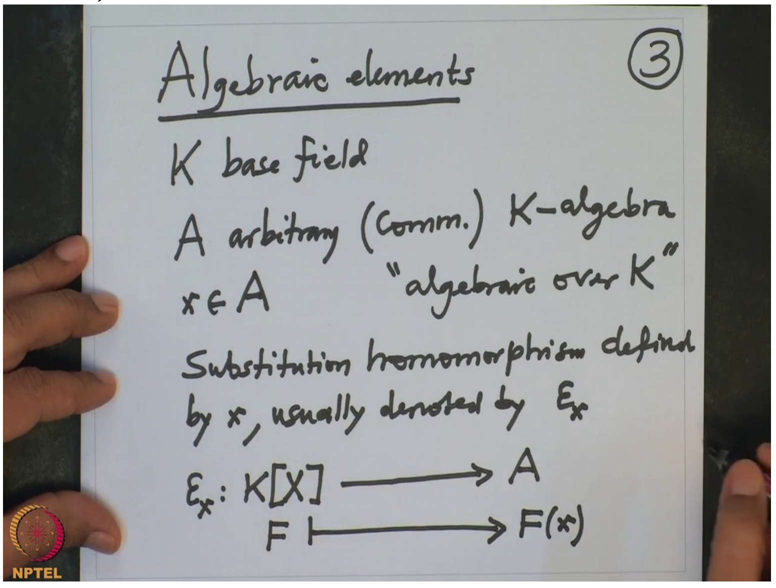
So this is a map from the polynomial ring in n variable over K to algebra A,

(Refer Slide Time 08:26)



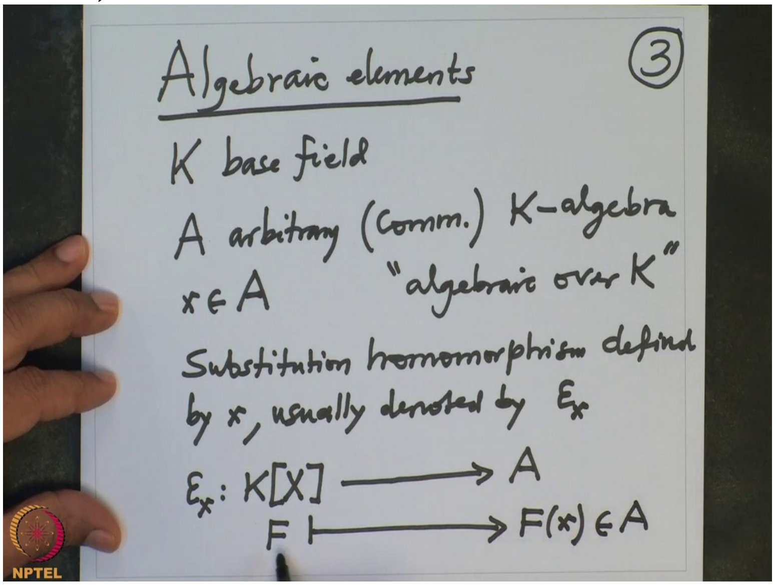
so what is it? Any polynomial F, I will map it to F evaluated at x.

(Refer Slide Time 08:39)



So wherever there is a capital X I will substitute with small x. And note that the resulting element, this is an element in A because F has

(Refer Slide Time 08:50)

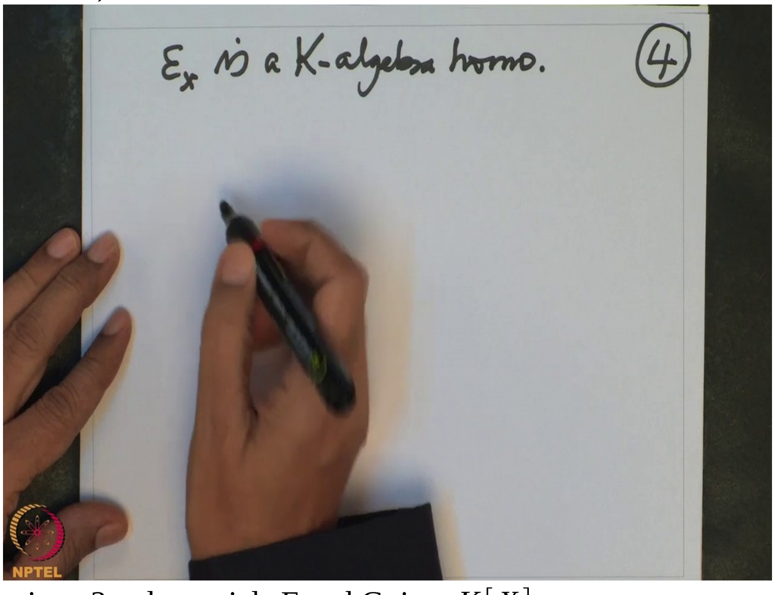


coefficients in K and A is the K-algebra so this is a combination, K linear combinations of the powers of x.

And because it is algebra, it is a ring therefore powers of x are also there. So substitution homomorphism is a map from $K[X]$ to A, and it is easy to say that this epsilon x is for K-algebra homomorphism.

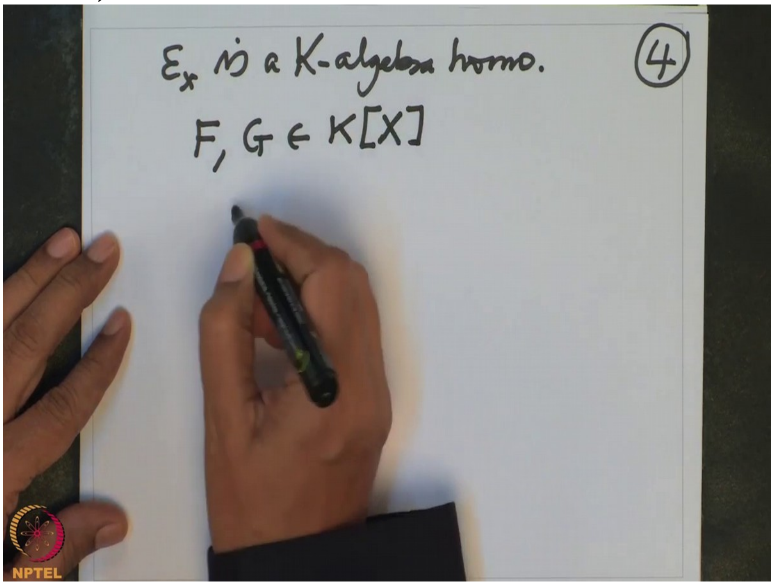
What does that mean? That mean

(Refer Slide Time 09:28)



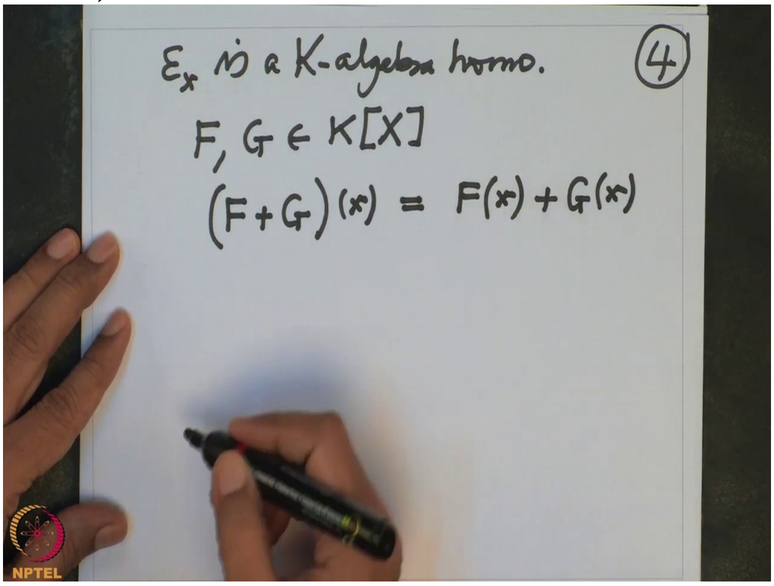
whether if I have given 2 polynomials F and G, in $K[X]$,

(Refer Slide Time 09:37)



whether I add 2 polynomials first and then evaluate it at x, this result is same as $F(x)+G(x)$.

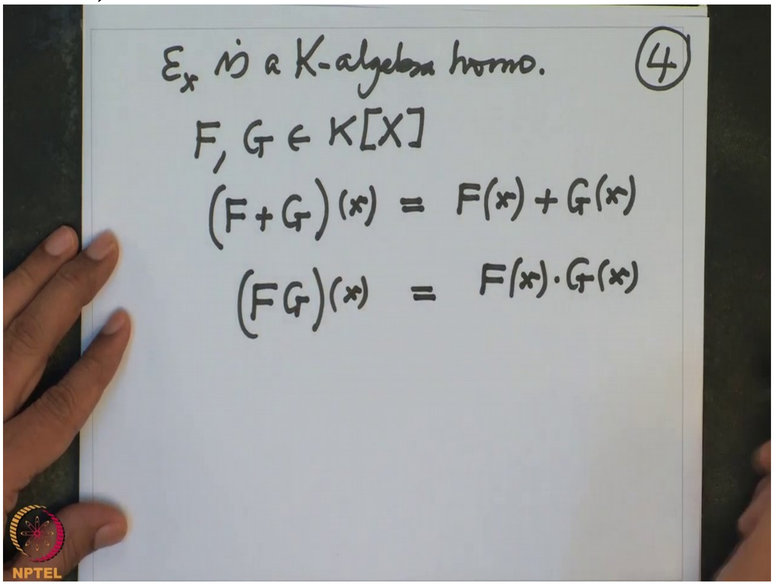
(Refer Slide Time 09:51)



This is one.

And if I multiply 2 polynomials and then evaluate at x, or if I evaluate the polynomials at x and then multiply them in A, this multiplication is in A, this addition is also in A but remember we are writing the same but it is clear from the context that

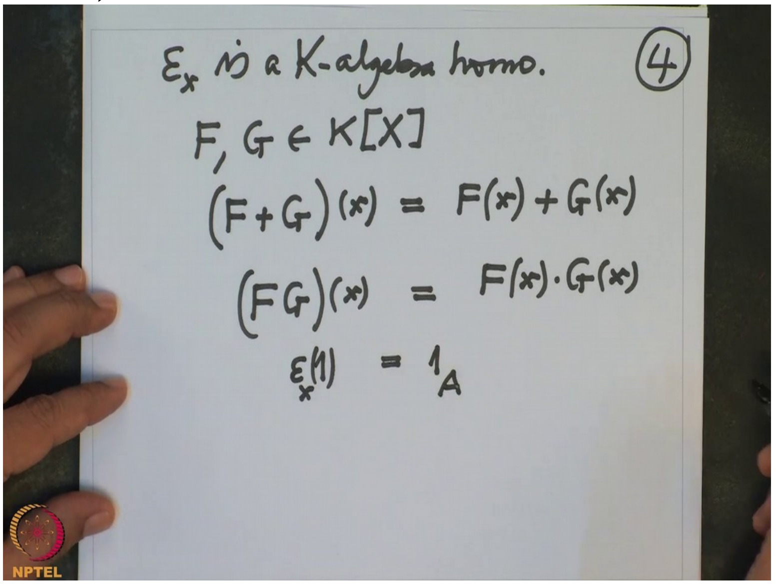
(Refer Slide Time 10:16)



where the multiplications and additions are defined.

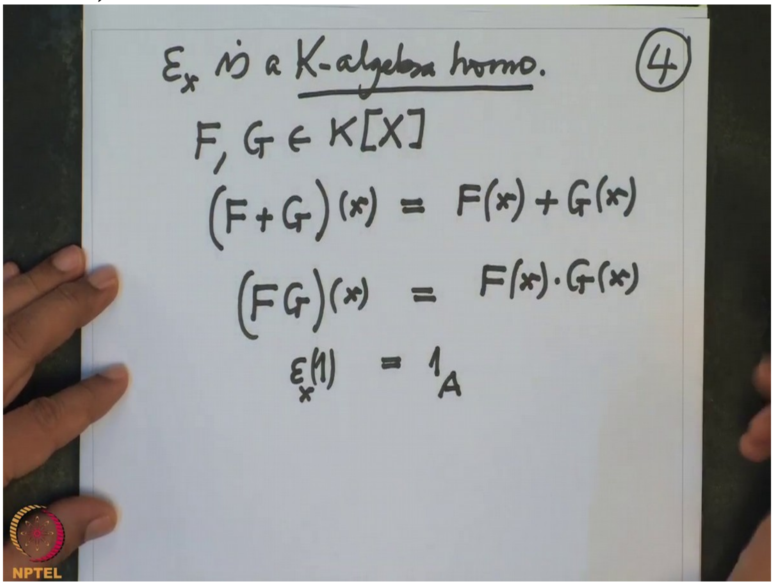
This plus also we are assuming that 1 in this ring, 1 in $K[X]$ goes to, 1 is same as 1_A and if I, ϵ_x that means I have to put, wherever there is capital X, I have to put small x, but there is no capital X in this so this is same as 1, and this 1 is the 1 in the algebra A, 1_A .

(Refer Slide Time 10:50)



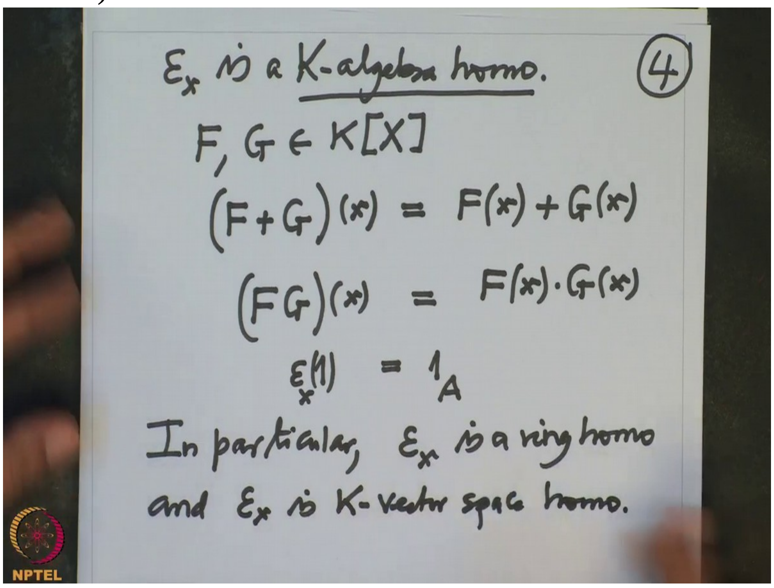
So altogether this means that it is a K-algebra homomorphism.

(Refer Slide Time 10:57)



In particular it is a ring homomorphism. So in particular, ϵ_x is a ring homomorphism. And ϵ_x is the K vector space homomorphism, K vector space homomorphism together and

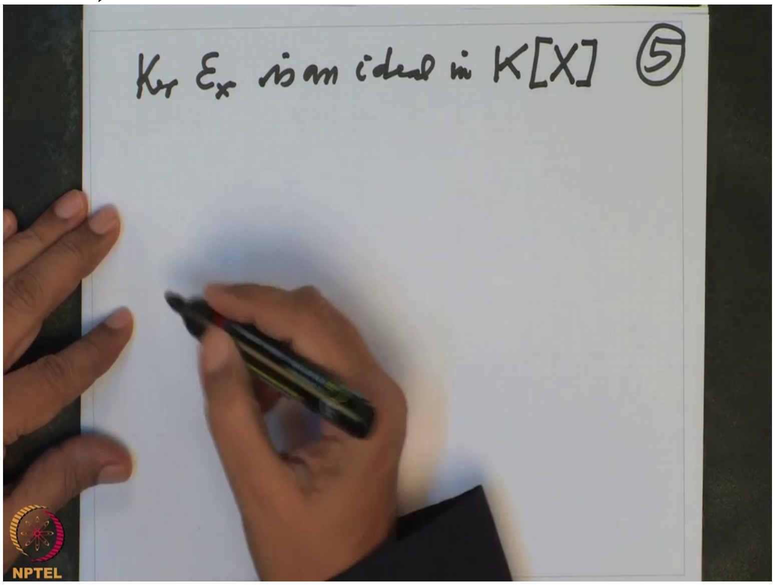
(Refer Slide Time 11:27)



operations are obviously compatible.

Now whenever you have homomorphism between the rings, last time we saw we talked about the kernel and also we have seen so ϵ_x , the kernel of ϵ_x , this is an ideal in, is an ideal in polynomial ring in one variable over K.

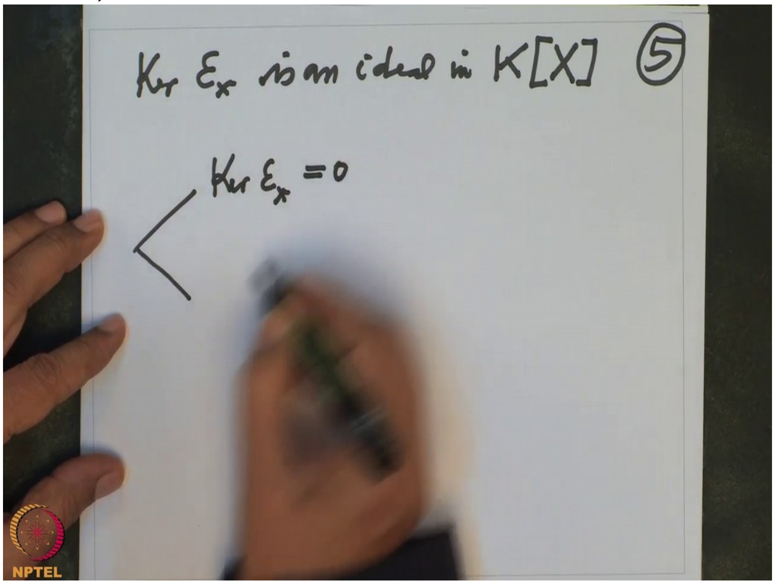
(Refer Slide Time 11:58)



And we, just now I told that last time we also have the structure of, we know all ideals in the polynomial ring $K[X]$, all ideals are principal. So either the generator is zero or non-zero.

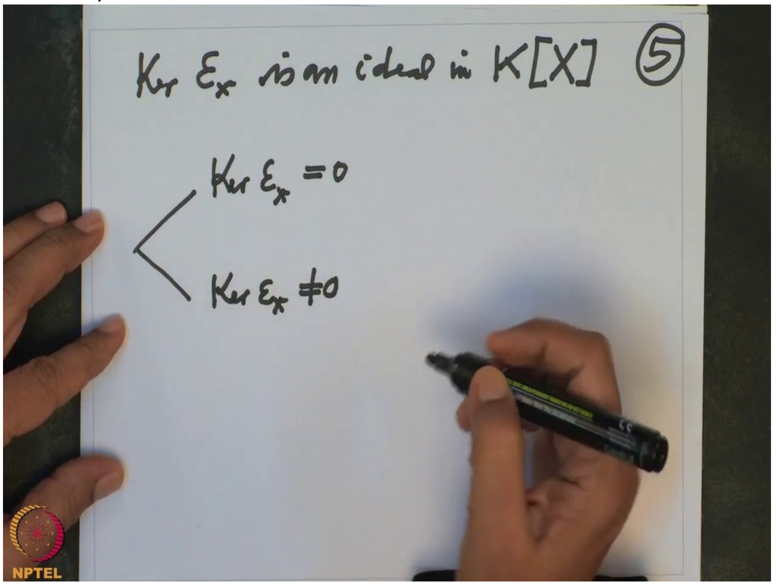
So we have two cases. Kernel of ϵ_x is 0

(Refer Slide Time 12:26)



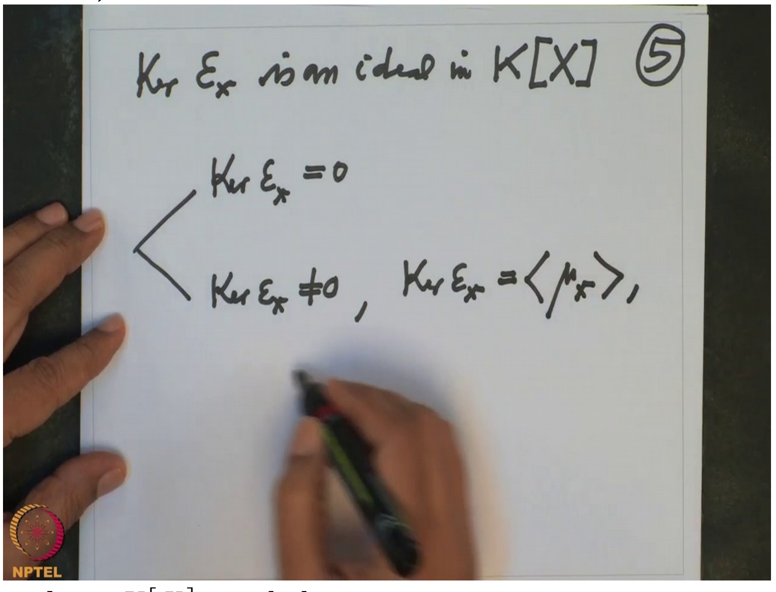
or kernel of ϵ_x is non-zero.

(Refer Slide Time 12:31)



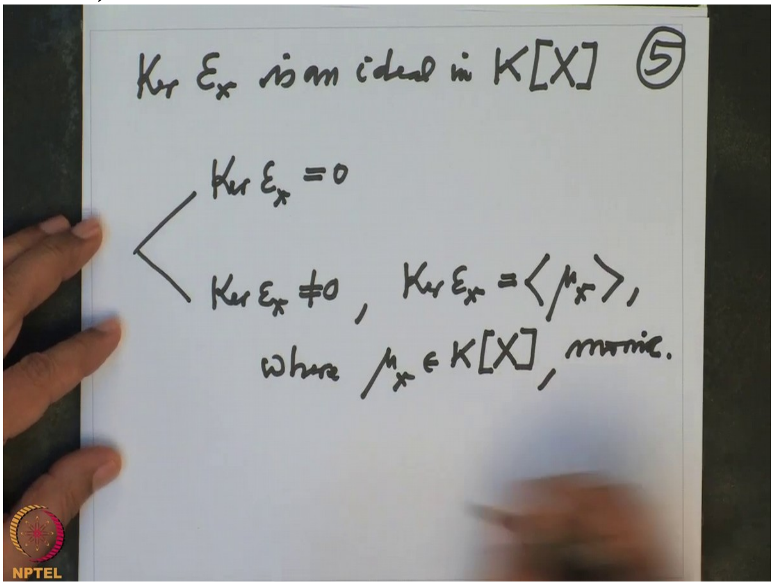
And in this case we know that kernel of ϵ_x has a unique generator if we choose it to be a monic. So kernel of ϵ_x is generated by monic polynomial μ_x where

(Refer Slide Time 12:49)



mu x is a polynomial in $K[X]$ such that it is monic.

(Refer Slide Time 13:02)

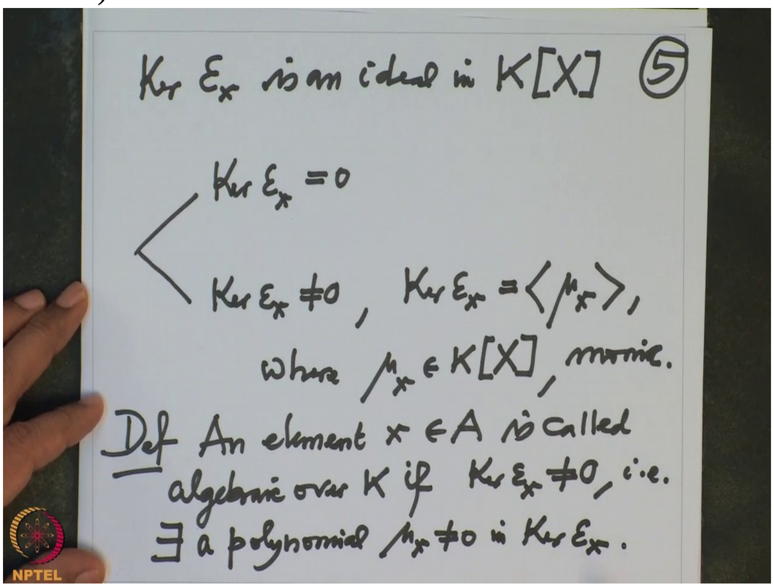


This is what we know from the last lecture that all ideals are like this.

Now we will analyze further but just before I go on, I just make a definition here.

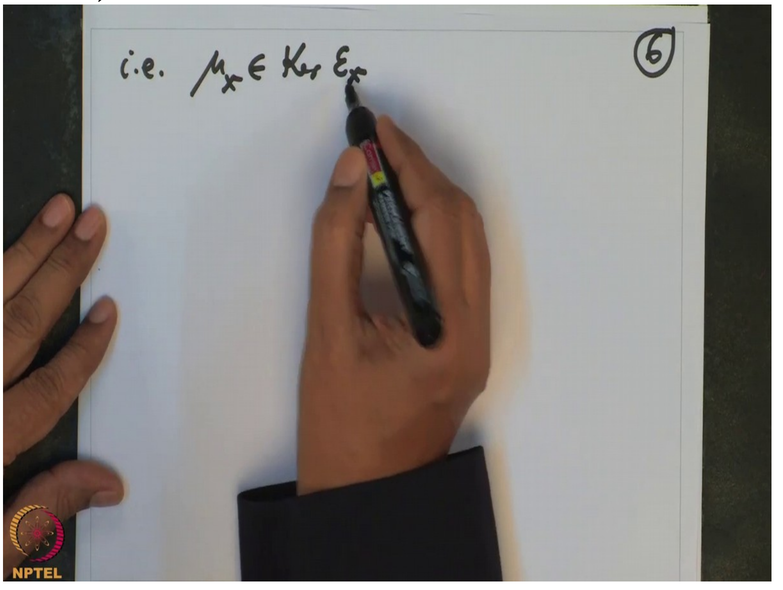
An element $x \in A$ is called algebraic over K if kernel of ϵ_x is non-zero. So that simply means that if there exists a polynomial μ_x non-zero in kernel of ϵ_x and remember

(Refer Slide Time 14:01)



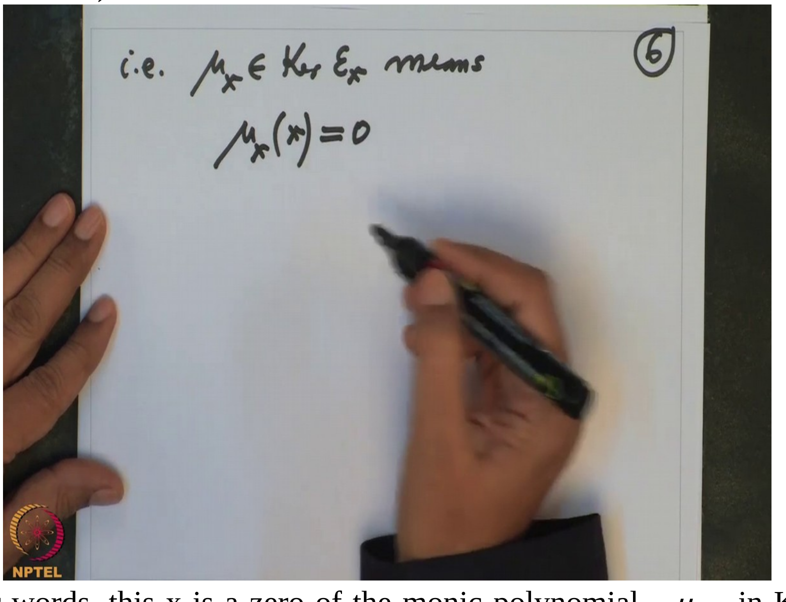
the polynomial in kernel of ϵ_x if, so that is μ_x is in the kernel means, μ_x is the polynomial in the kernel means μ_x is the polynomial in 1 variable and

(Refer Slide Time 14:22)



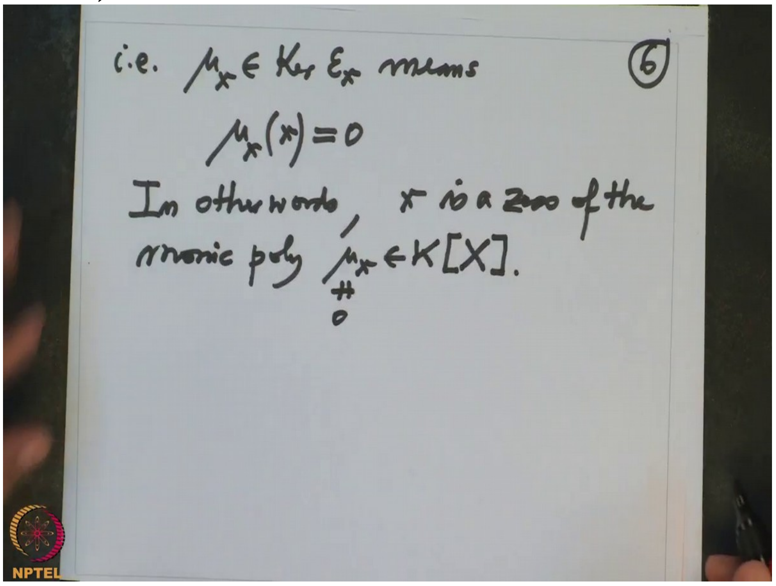
it is in the kernel means whenever I substitute capital X equal to small x it is zero. Means μ_x evaluated at x is 0.

(Refer Slide Time 14:35)



But this in other words, this x is a zero of the monic polynomial μ_x in K. And μ_x is non-zero. Then

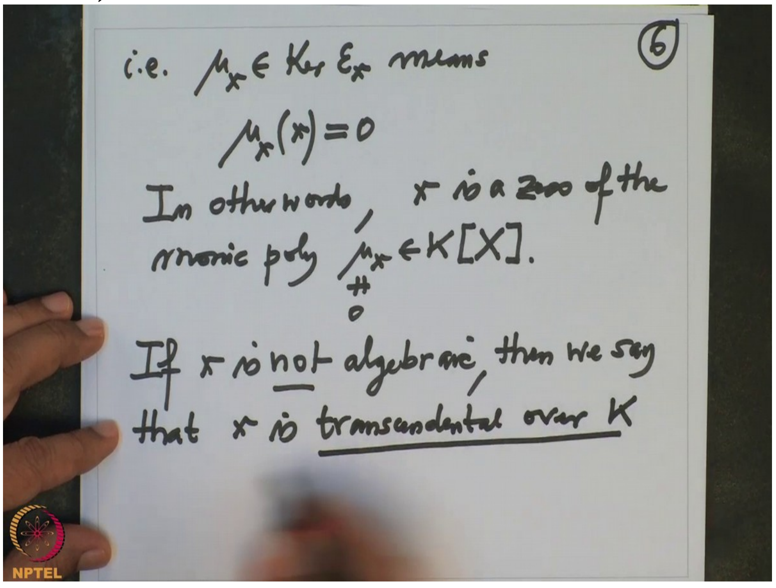
(Refer Slide Time 15:07)



we call such an element to be algebraic over K. Now there are several observations. I want to make about this μ_x first and then we will go on. So first of all we should see some examples that where the element is algebraic and where the element is not algebraic.

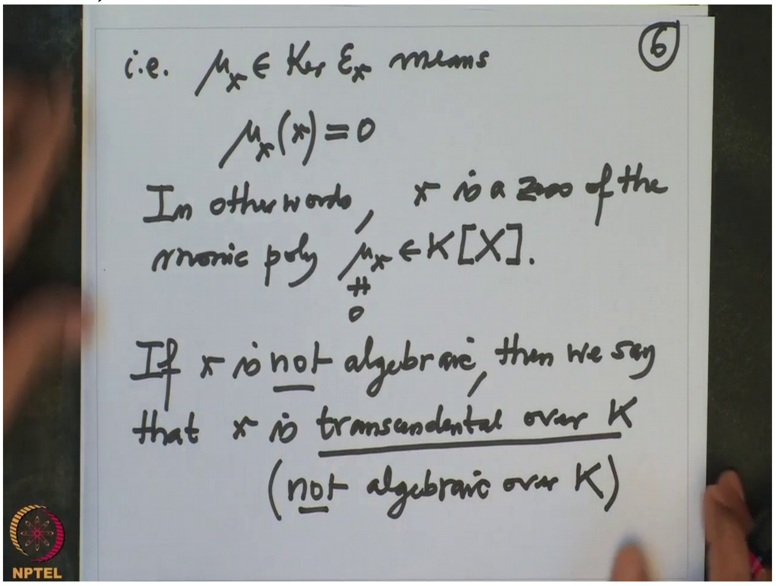
So before I go on, if x is not algebraic, then we say that x is transcendental over K. This is

(Refer Slide Time 16:03)



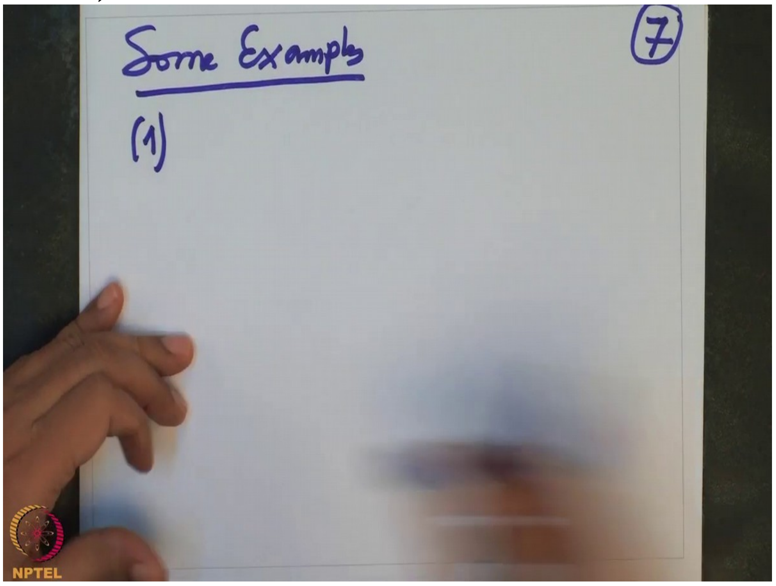
same as saying not algebraic over K. And then

(Refer Slide Time 16:14)



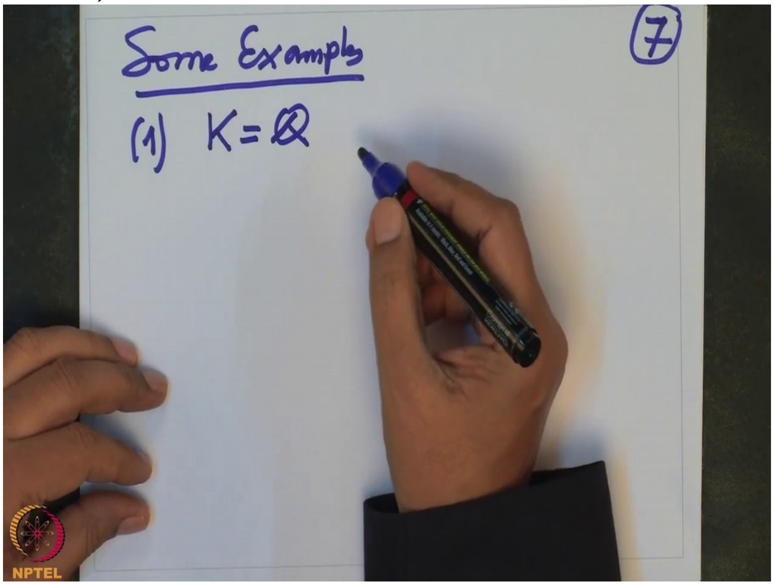
first we want to see some examples, some examples. One,

(Refer Slide Time 16:25)



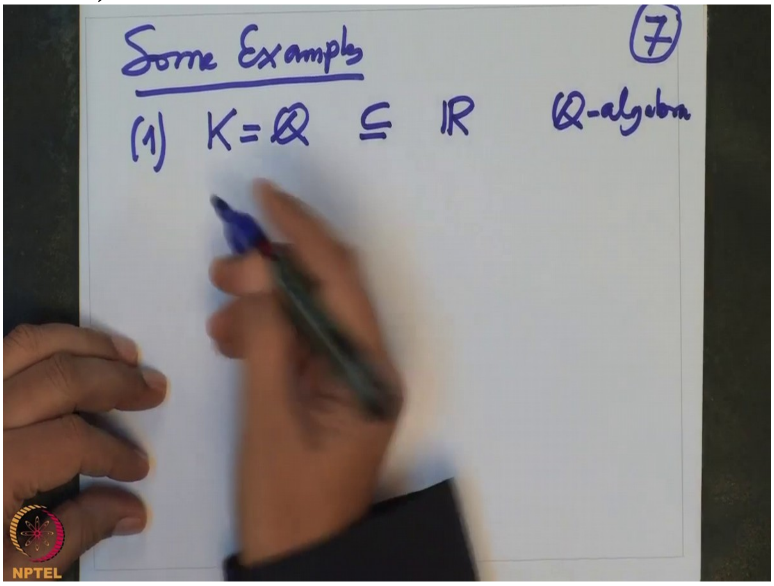
for example my base field is Q

(Refer Slide Time 16:34)



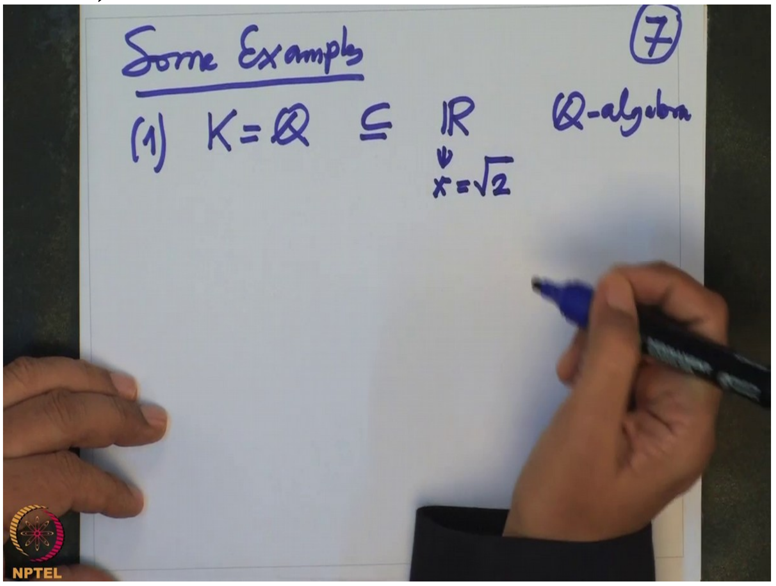
and the algebra I take is for example, $\mathbb{R}$. This is field extension so think of $\mathbb{R}$ as a $\mathbb{Q}$ algebra.

(Refer Slide Time 16:49)



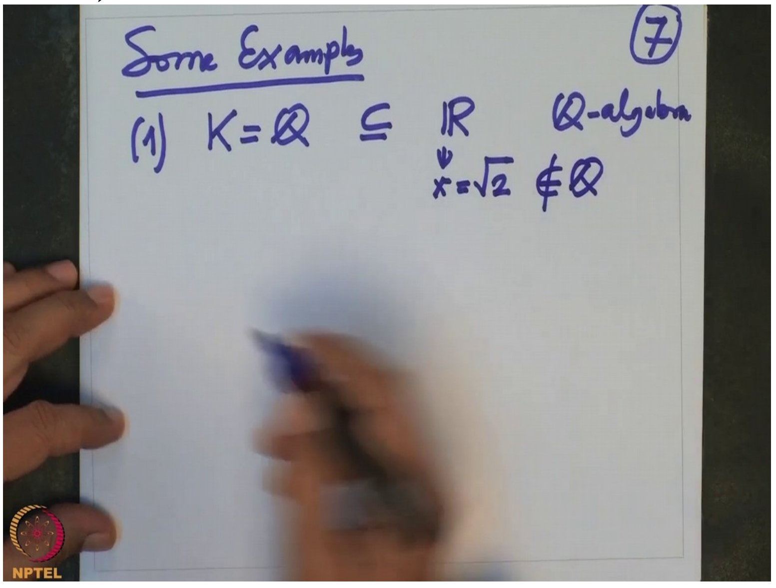
So, and look at the element x in $\mathbb{R}$ which is, say $\sqrt{2}$.

(Refer Slide Time 17:00)



Everybody knows that $\sqrt{2}$ is a real number. There is a $\sqrt{2}$, there is a $\sqrt{2}$ is a real number and which is not a rational number. So this is not rational.

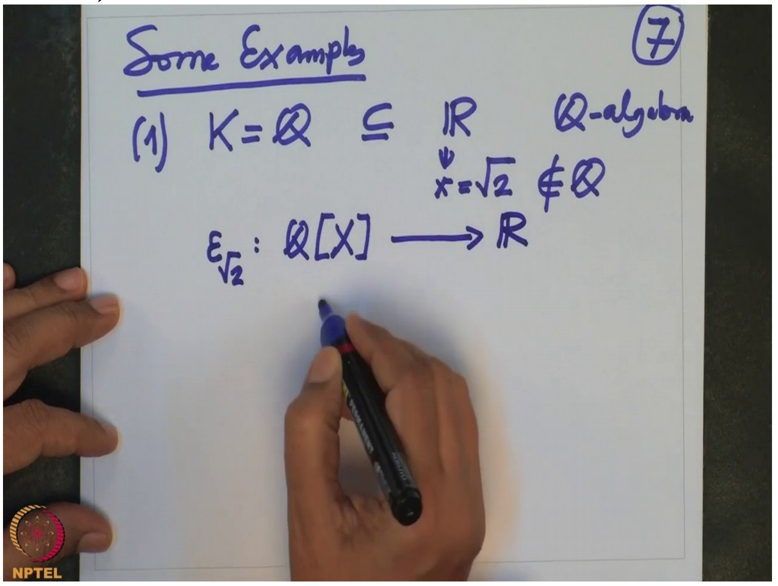
(Refer Slide Time 17:14)



This is, in fact very easy consequence of the fundamental theorem of arithmetic.

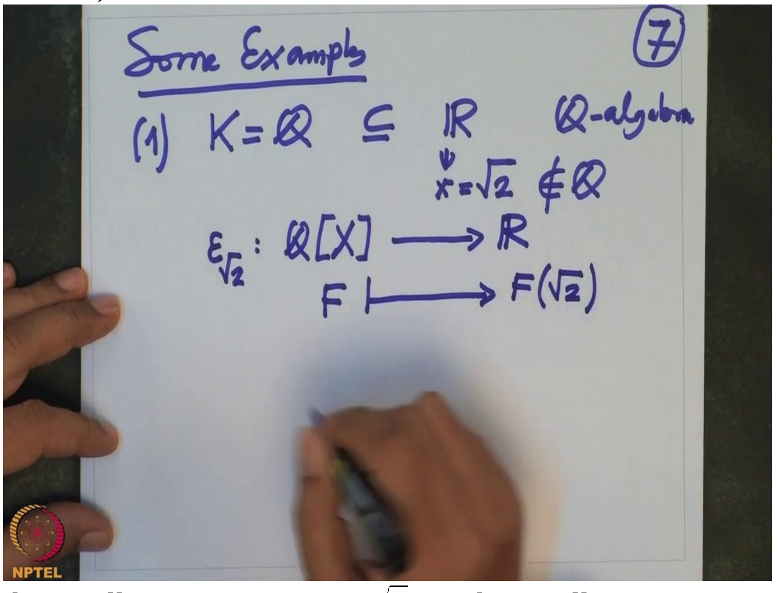
Ok, so and what is the map? The map we are considering is evaluation or substitution map at $\sqrt{2}$. So this is a map from $\mathbb{Q}[X]$ to $\mathbb{R}$.

(Refer Slide Time 17:39)



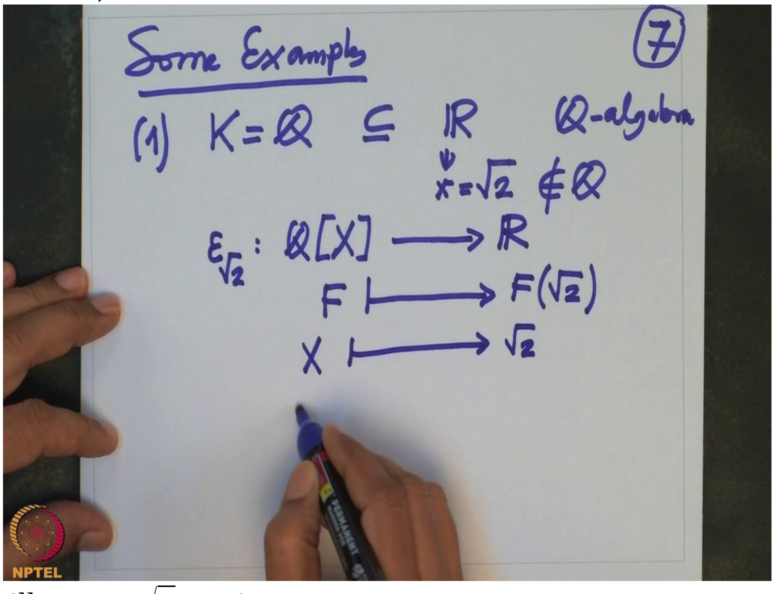
The map is any polynomial F, you take F and substitute F equal to $\sqrt{2}$, X equal to $\sqrt{2}$. So F of $\sqrt{2}$.

(Refer Slide Time 17:47)



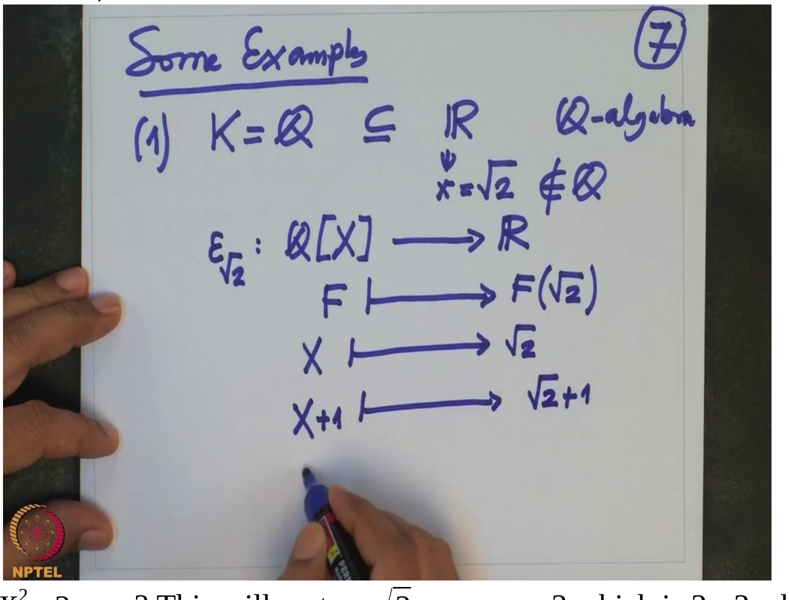
So for example where will X go? X goes to $\sqrt{2}$. Where will

(Refer Slide Time 17:55)



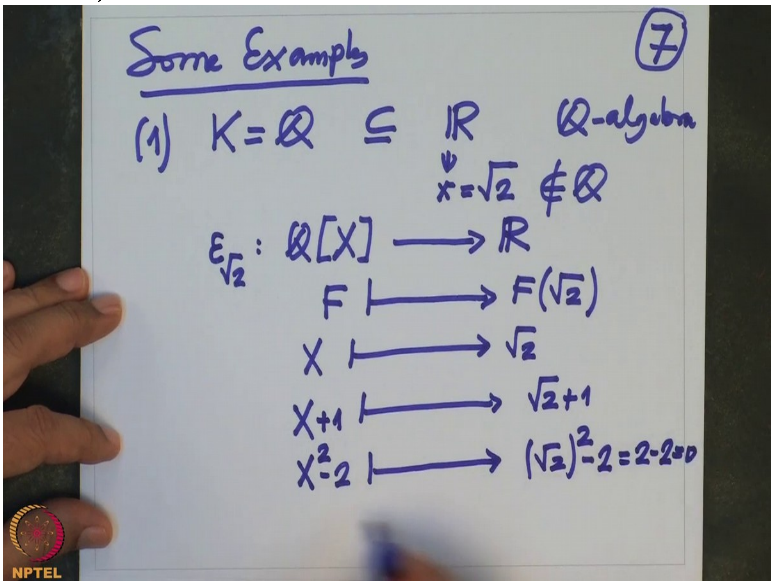
X + 1 go? This will go to $\sqrt{2}$ + 1.

(Refer Slide Time 18:02)



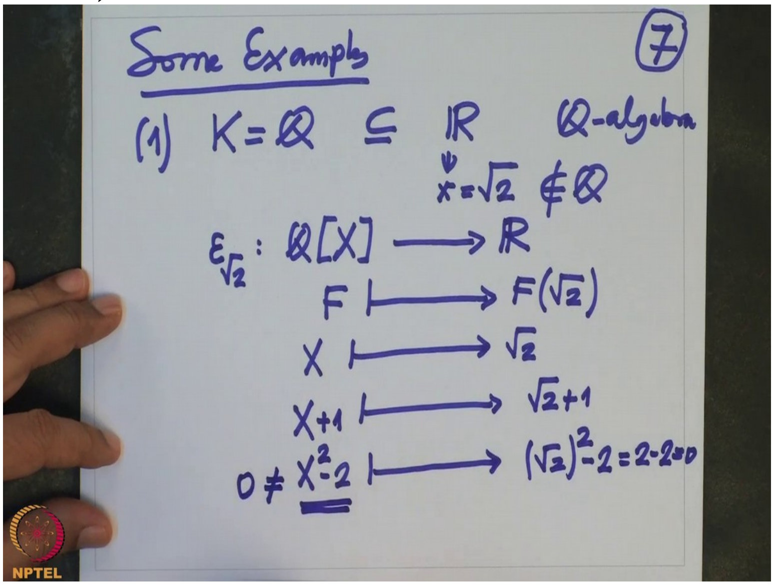
So where will $X^2 - 2$ go? This will go to $\sqrt{2}$ square - 2 which is 2 - 2 which is 0. So

(Refer Slide Time 18:17)



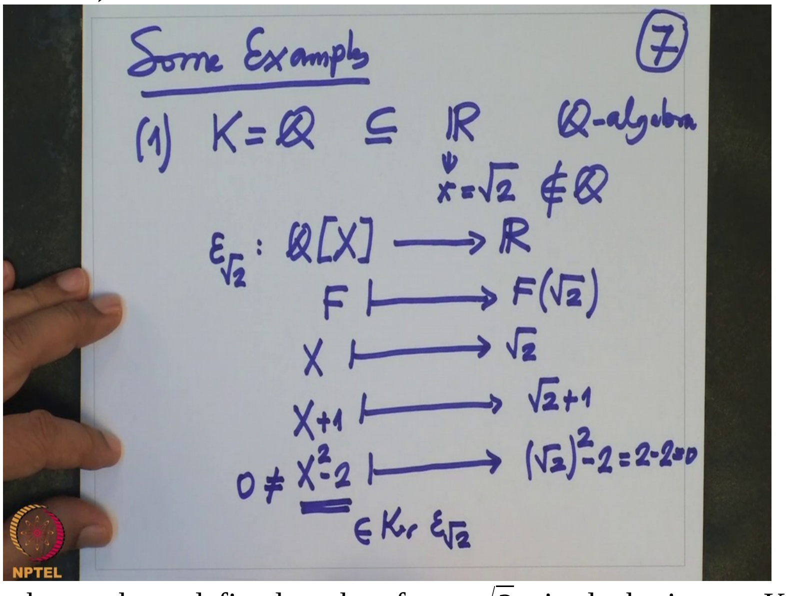
here is a polynomial which is non-zero

(Refer Slide Time 18:22)



and it goes to zero, so that means this polynomial does belong to the kernel of $\epsilon(\sqrt{2})$.

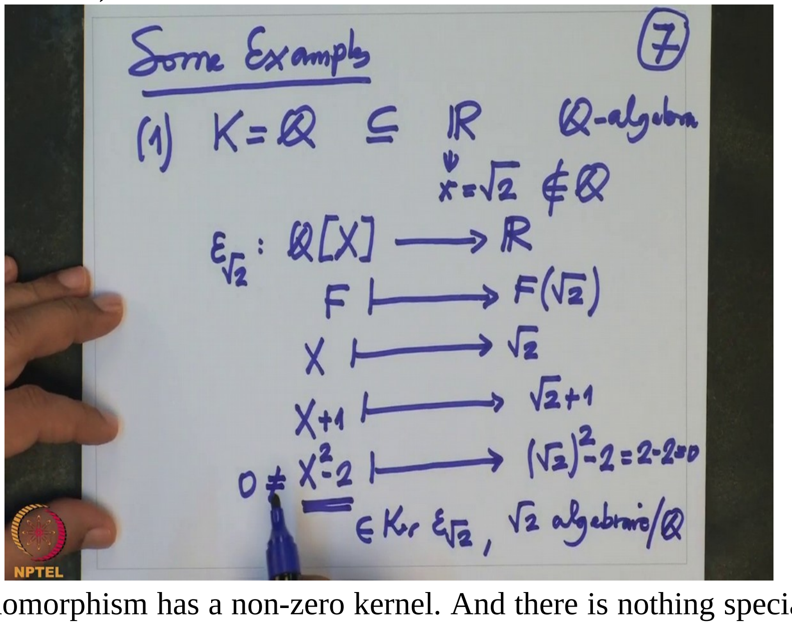
(Refer Slide Time 18:30)



This is precisely what we have defined at; therefore $\sqrt{2}$ is algebraic over K.

We just have to test whether this

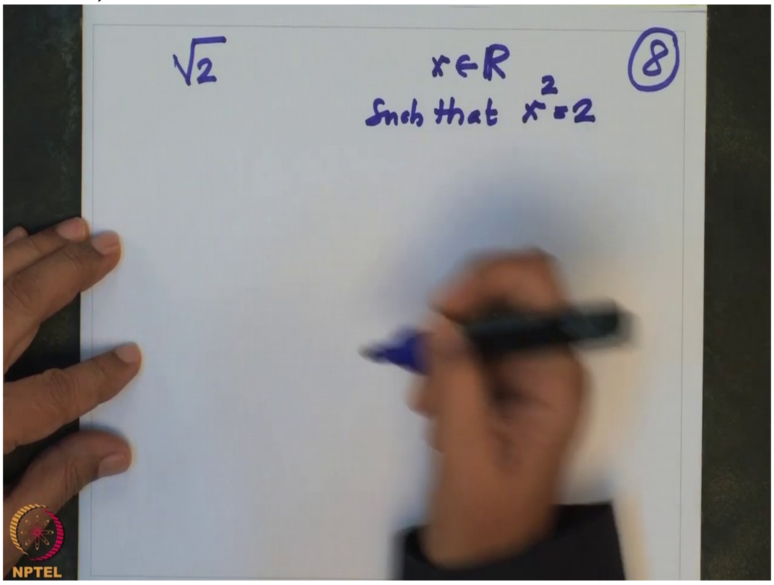
(Refer Slide Time 18:44)



substitution homomorphism has a non-zero kernel. And there is nothing special about $\sqrt{2}$. So here also I want to clear one confusion or one, not confusion but writing style which one should improve; that is I am not going to write $\sqrt{2}$. So 8, so instead of writing $\sqrt{2}$, this is because it is ambiguous; whether you are taking a positive sign or a negative sign.

And when one writes this one will have always thing in mind, whether you are taking positive sign or negative sign. In order to create, to be more precise with this, instead of this I am going to write small $x \in \mathbb{R}$ such that $x^2 = 2$.

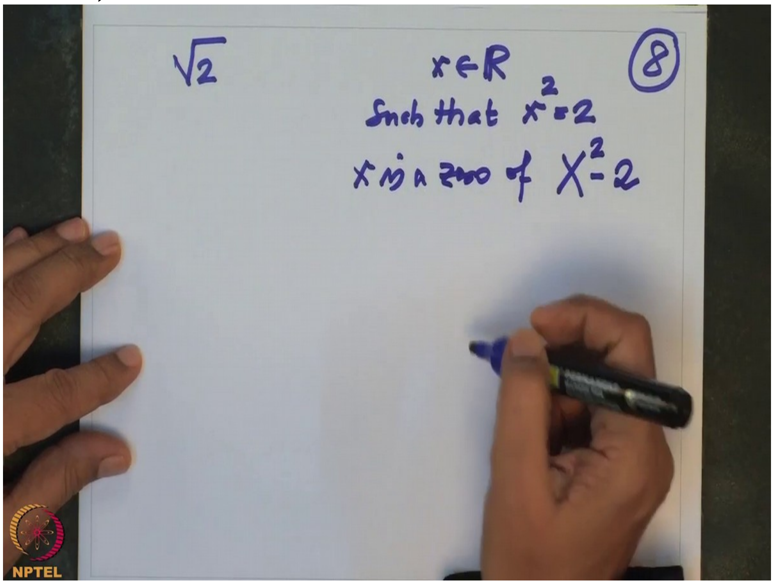
(Refer Slide Time 19:44)



And how many possibilities are there?

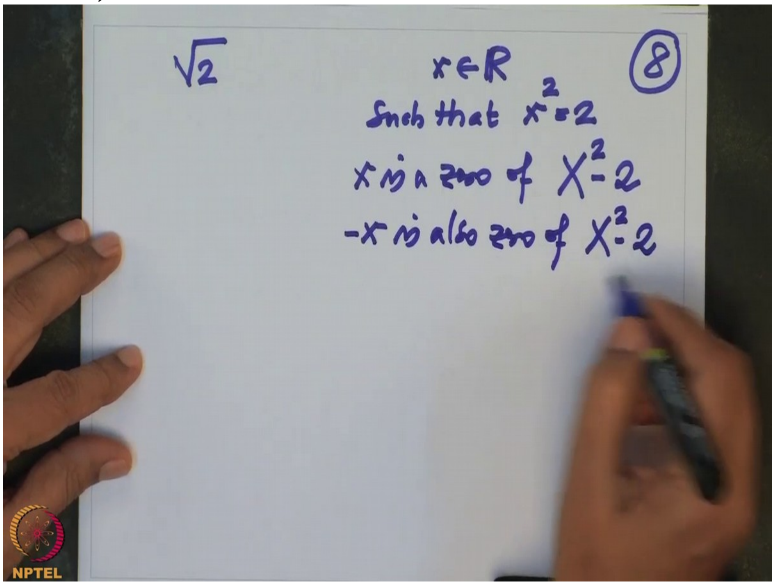
We say that means, this means that x is a zero of the polynomial capital $X^2 - 2$.

(Refer Slide Time 20:01)



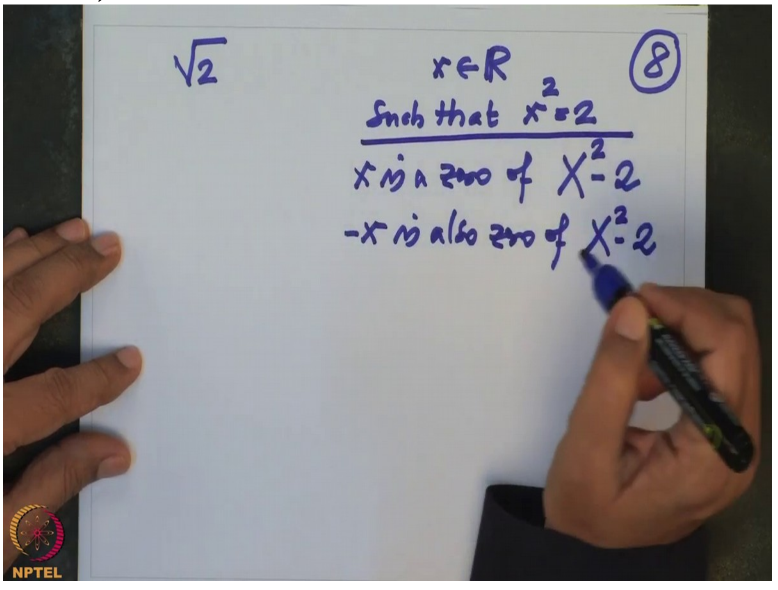
And we know if x is a zero then -x is also zero, of the same polynomial because when you square it,

(Refer Slide Time 20:14)



whether you take minus x or small x it is same. So therefore our standard writing will be x such that $x^2=2$.

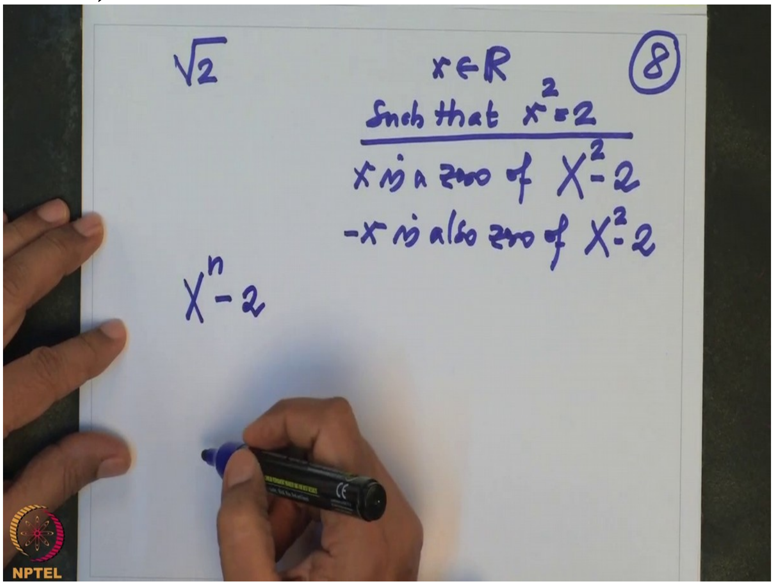
(Refer Slide Time 20:25)



So there is no question, we are not talking about sign or anything here.

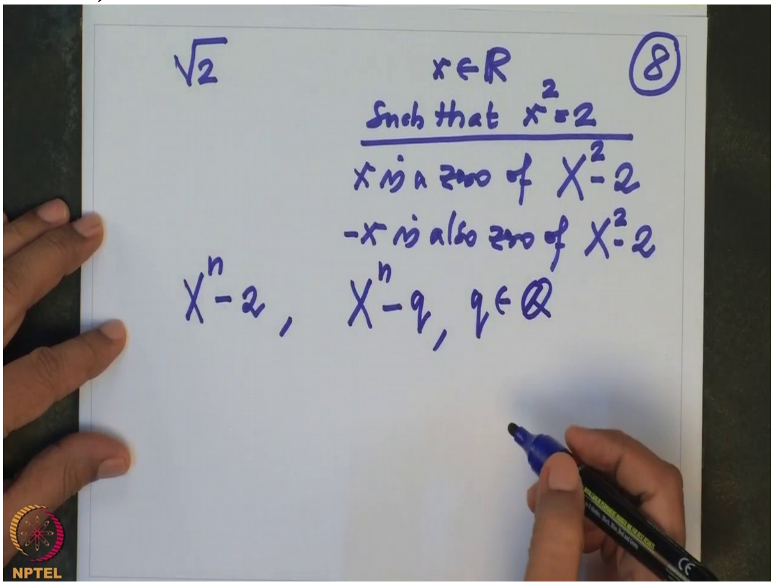
And I think special about $\sqrt{2}$, we could have taken any polynomial of this type $X^n - 2$

(Refer Slide Time 20:45)



or y, z, X^n - any rational number q, q is any rational number.

(Refer Slide Time 20:56)

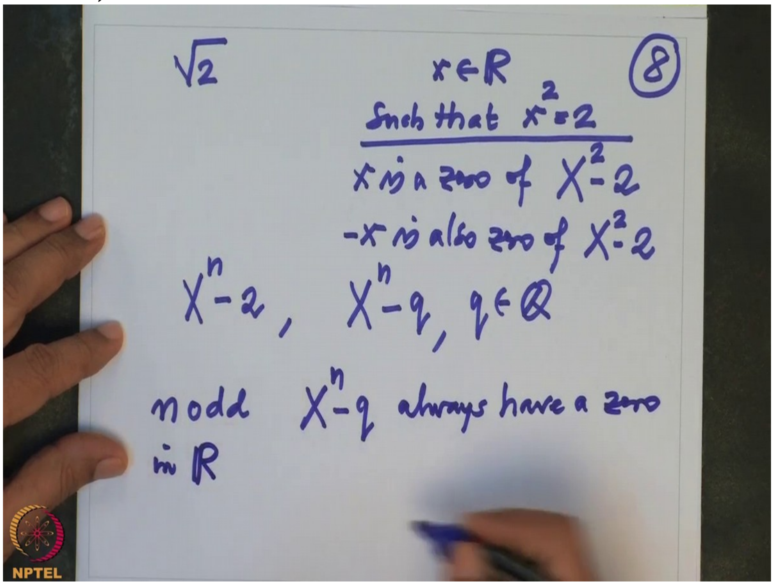


So that means what, we are looking at the zeroes of this polynomial.

And we have noted that this polynomial has at most n zeroes and now, you would have seen in the definition of real numbers that when do you definitely know that such a polynomial has a zero over real numbers, that is when n is odd.

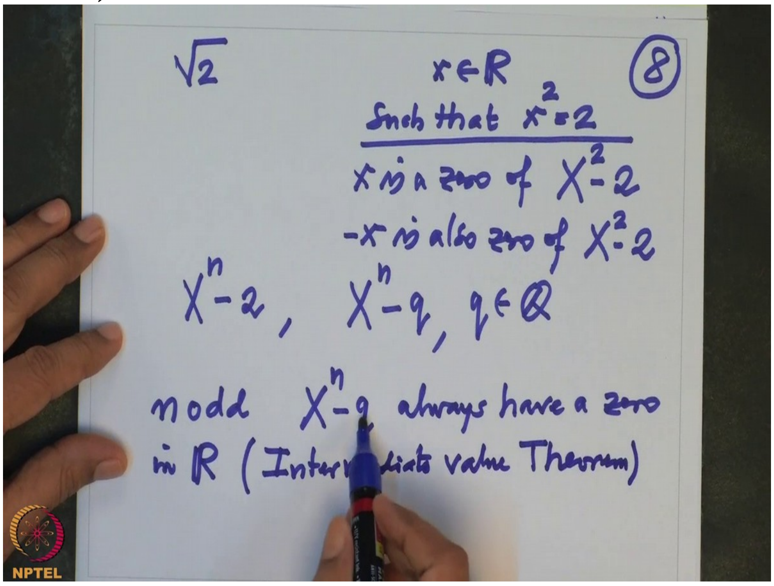
And n is odd, $X^n - q$ always have a zero in $\mathbb{Q}$, in $\mathbb{R}$.

(Refer Slide Time 21:41)



This is precisely what you prove in your college days, in so-called Intermediate Value theorem, Intermediate Value theorem. So in other words,

(Refer Slide Time 22:01)



given a rational number $\mathbb{Q}$ it always have a nth root as a real number.

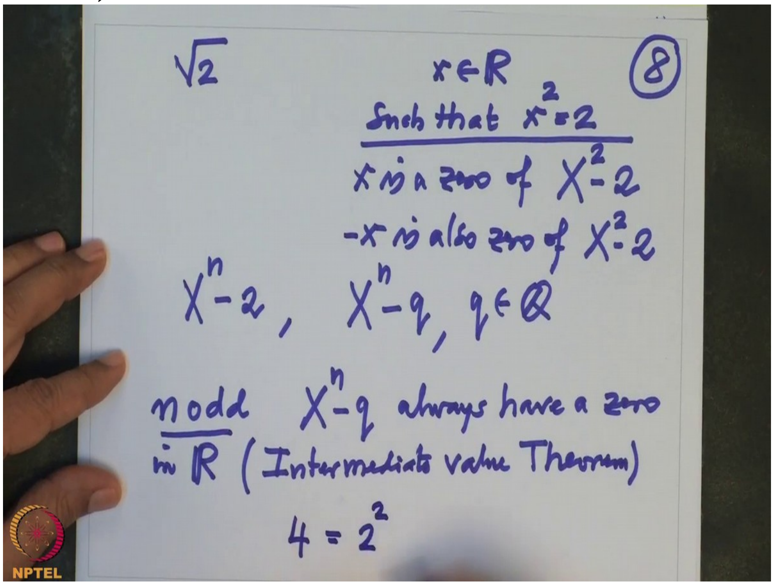
The roots are not rational numbers in general but if n is odd, then definitely there is a real number who is a zero of this and those real numbers are called nth roots of q.

And one can also give the criterion when the rational number has a rational nth root. That will only when, that will depend on the prime decomposition of $\mathbb{Q}$. I will not go there, into that, but it is possible by looking at, that is much easier.

If you, if I know prime decomposition of $\mathbb{Q}$ and if all exponents of the primes, which occur in the prime decomposition of $\mathbb{Q}$ are divisible by n, then this also has a nth root in $\mathbb{Q}$ already.

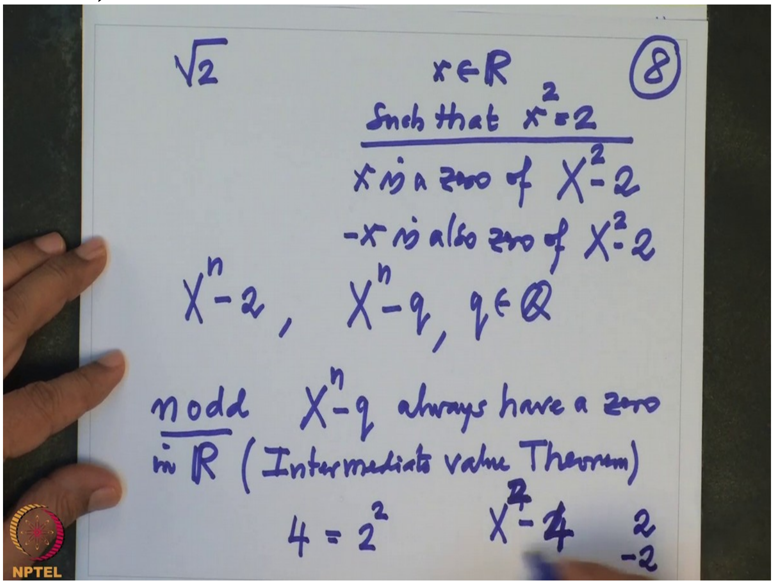
For example, 4, 4 prime decomposition is 2^2 .

(Refer Slide Time 22:59)



So when I take a zero of X^4-2, X^4-4, X^2-4 that has a square root rational number, that is namely 2 or -2.

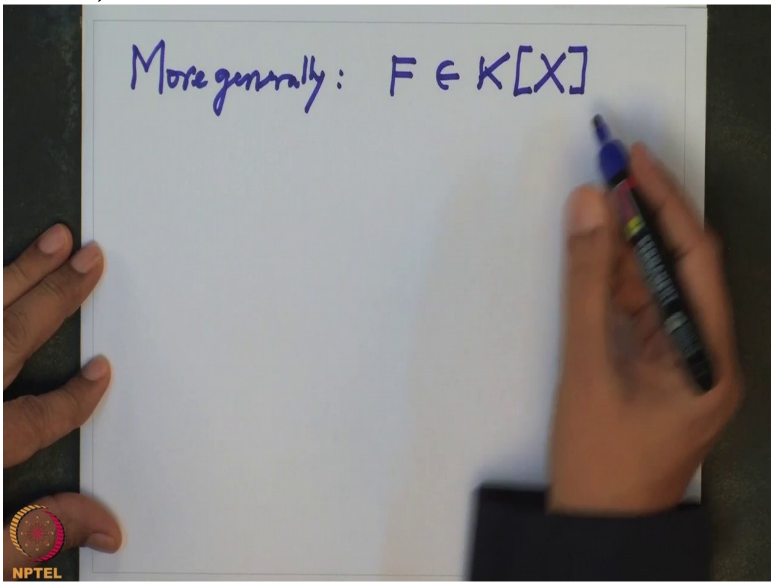
(Refer Slide Time 23:19)



These are the square roots of this. So that, that is much easier criterion to say that when such a polynomial has a rational zero. So also when n is odd one can assert that this polynomial has a real zero.

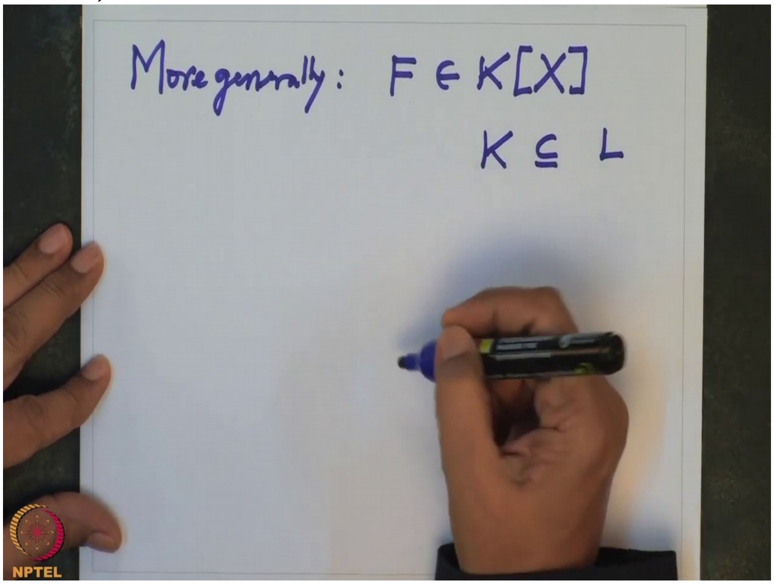
And all these zeros are by definition, therefore algebraic over q. So more generally if I have a polynomial F over any field $K[X]$

(Refer Slide Time 24:03)



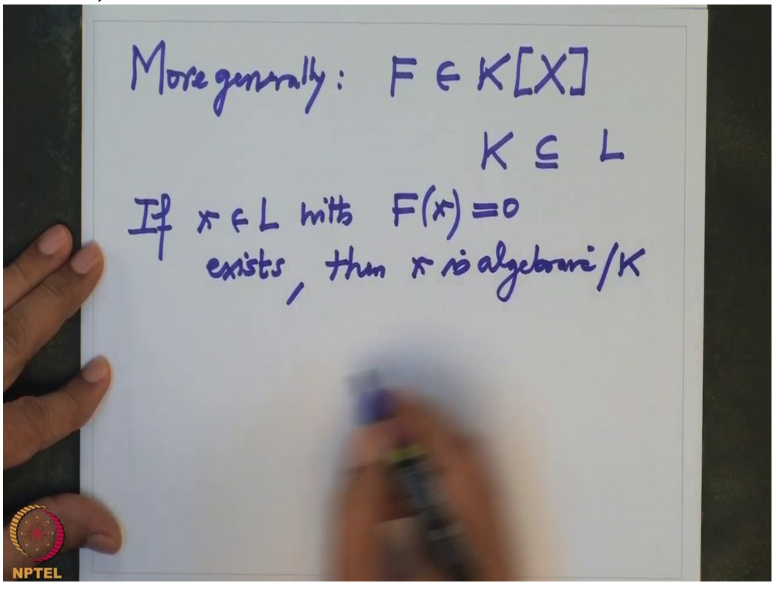
and if I have a bigger field L

(Refer Slide Time 24:07)



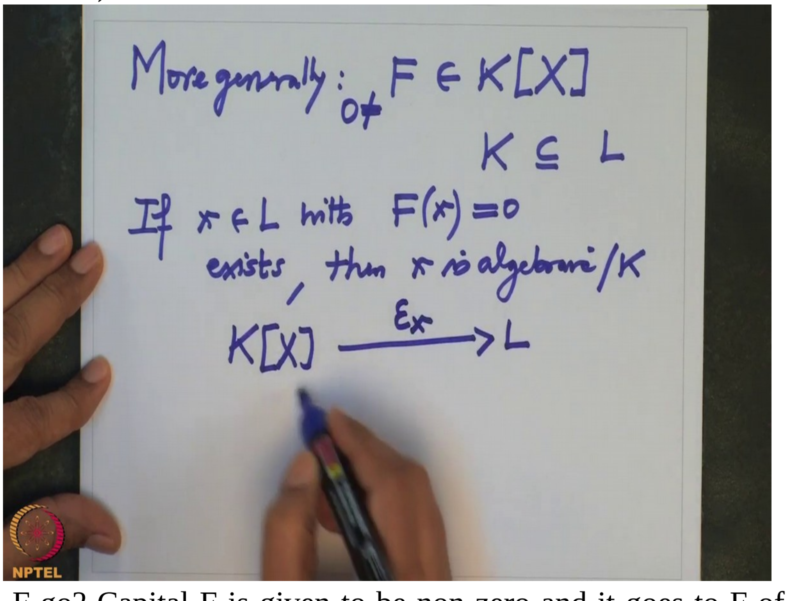
and there if x is in L with F of x is 0, if such a x exists then that x is algebraic over K. Then x is algebraic over K.

(Refer Slide Time 24:38)



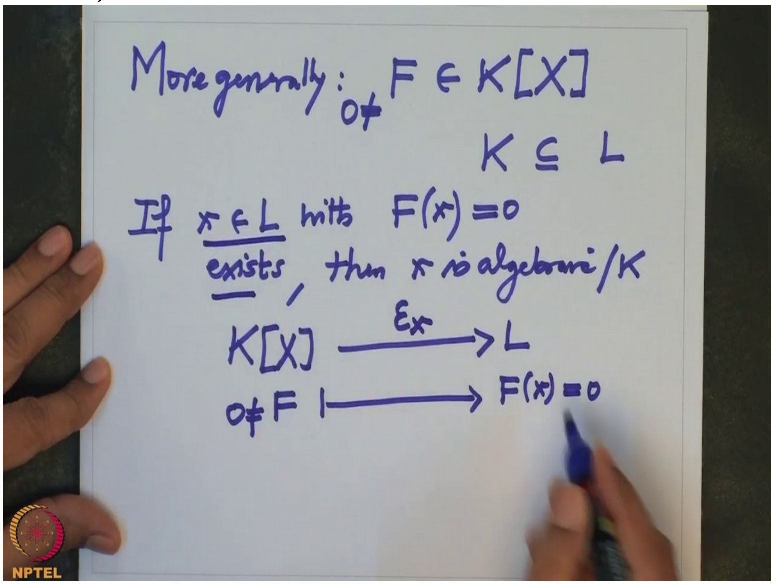
And of course F is non-zero. So that is because you see all that we need to check that is, if I take this substitution homomorphism from $K[X]$ to L ϵ_x

(Refer Slide Time 24:52)



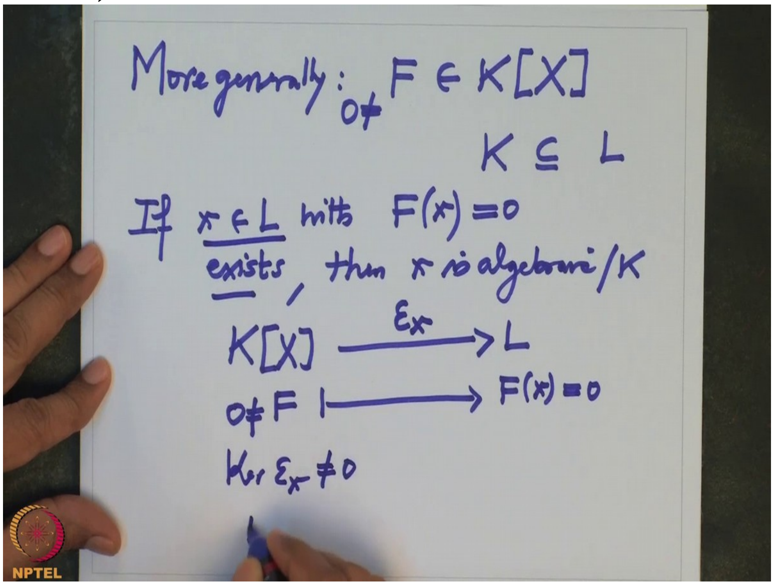
where do capital F go? Capital F is given to be non-zero and it goes to F of x but F of x is zero. That is how x is chosen.

(Refer Slide Time 25:03)



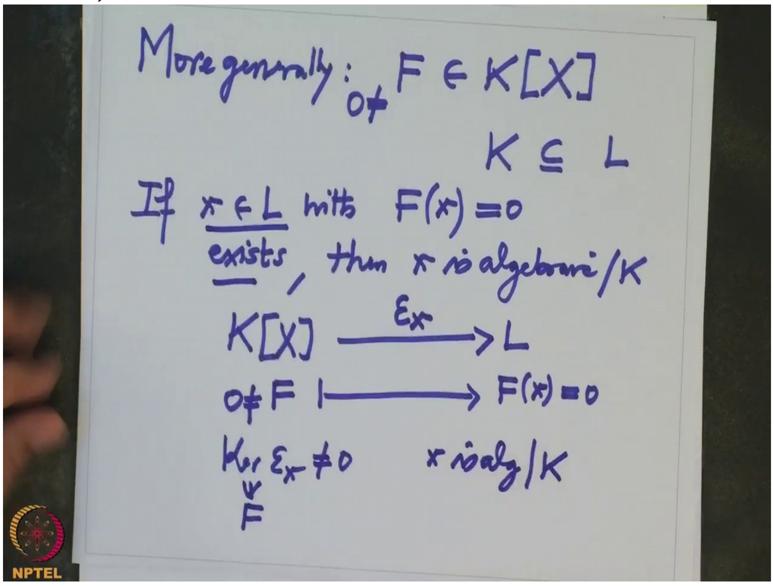
That means kernel of epsilon x is non-zero, in fact F

(Refer Slide Time 25:11)



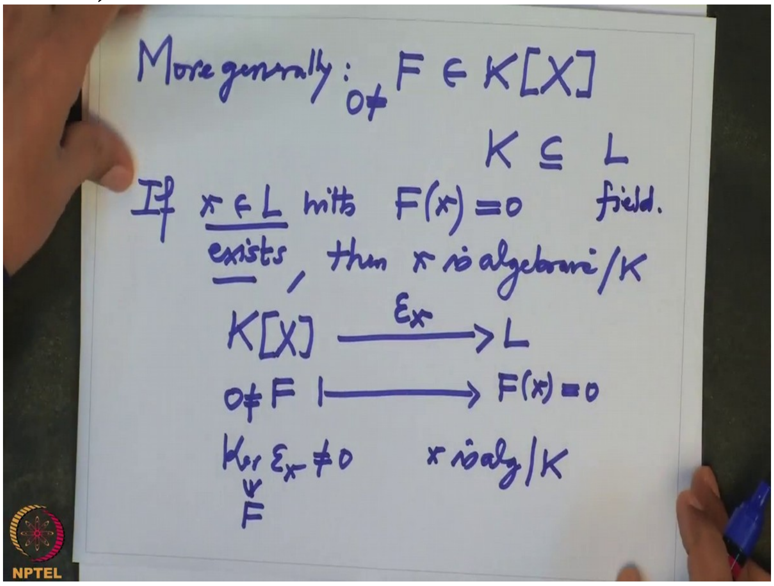
belongs there and therefore we say that F is algebraic over K.

(Refer Slide Time 25:19)



So you see the zeroes are very closely connected to algebraic elements. So this was the field case. But I want to also show you

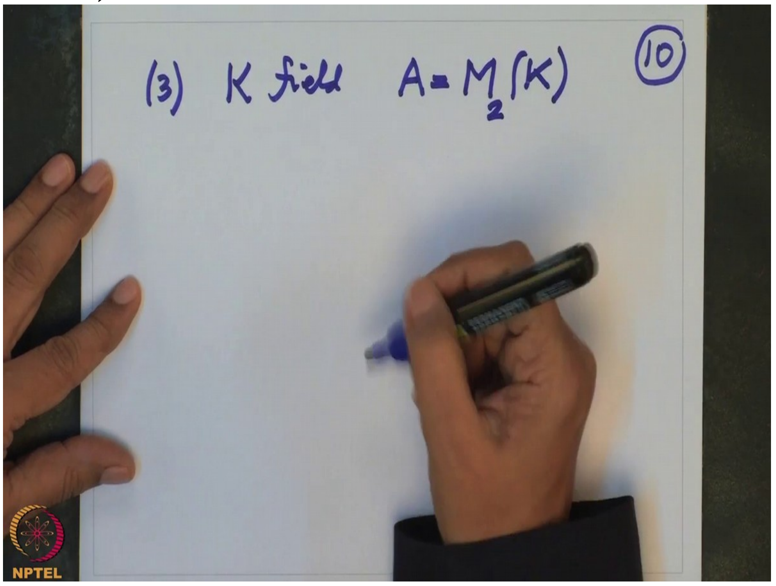
(Refer Slide Time 25:29)



is natural to consider an example where L is not field. For example, this example is now I want to remind you that I am not assuming that the algebra that I am considering in this example is commutative.

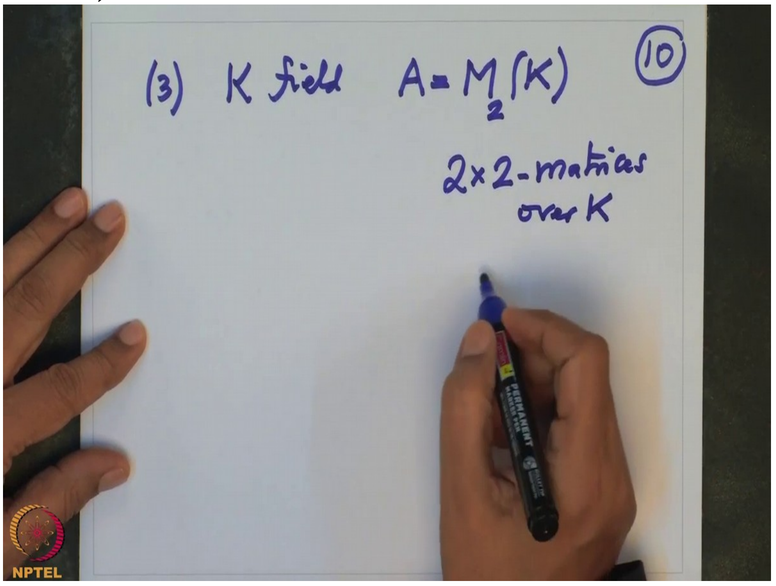
So this example, give it 3, so K is any field and A is the algebra I am taking, $M_2(K)$ let us say.

(Refer Slide Time 25:58)



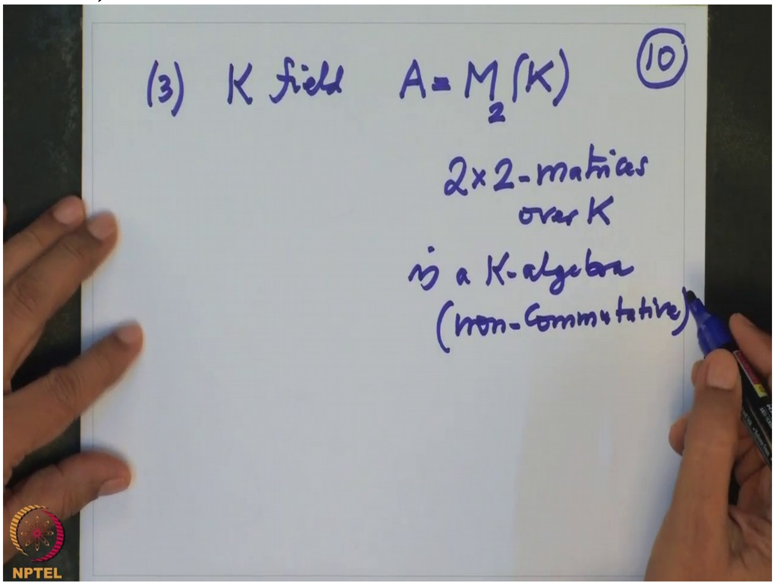
$M_2(K)$ is algebra. This is 2×2 matrices with entry in K, over K and we know how to add 2 matrices, how to multiply 2 matrices,

(Refer Slide Time 26:14)



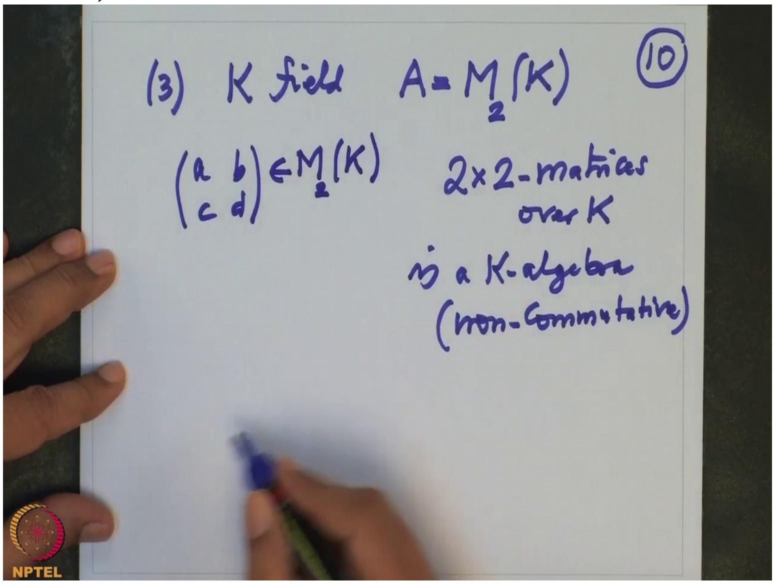
how do I multiply scalar with a matrix. So with those operations we know this $M_2(K)$ is a K-algebra. And it is definitely non-commutative.

(Refer Slide Time 26:36)



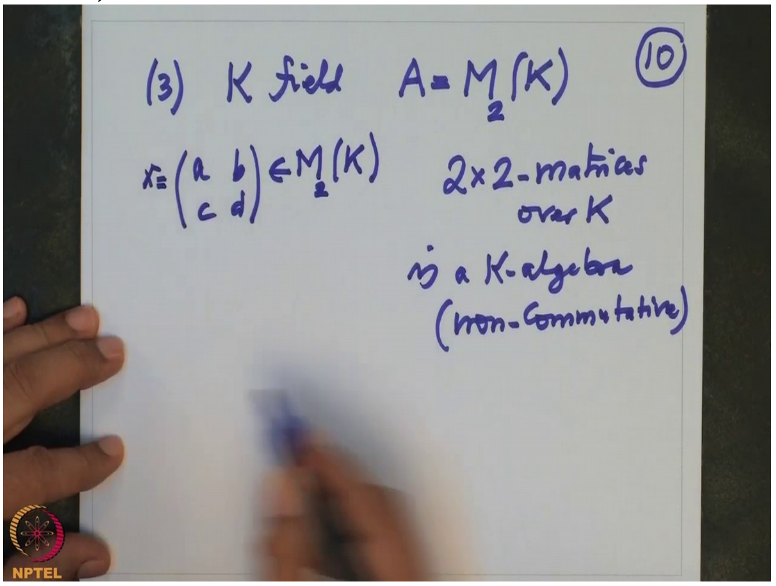
And now I take arbitrary matrix, so $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, this is a 2 by 2 matrix with entries in K

(Refer Slide Time 26:53)



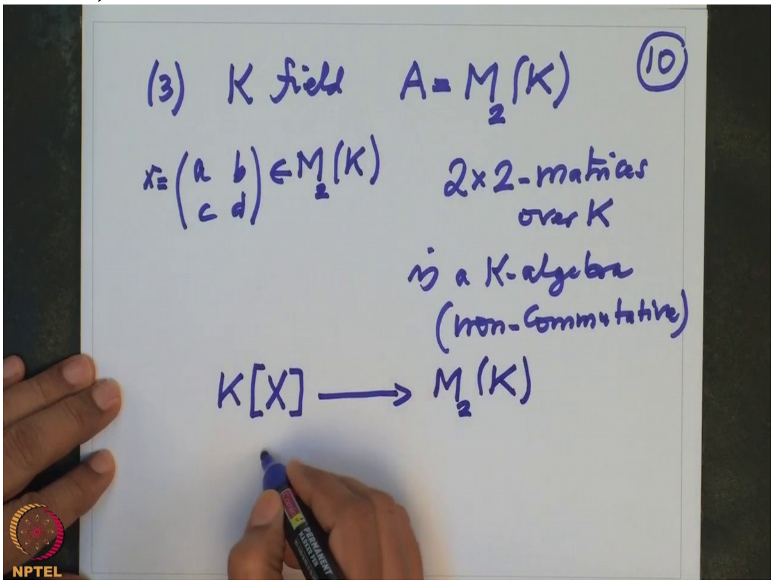
and I want to now show you that this element is algebraic over K. So this is my x.

(Refer Slide Time 27:02)



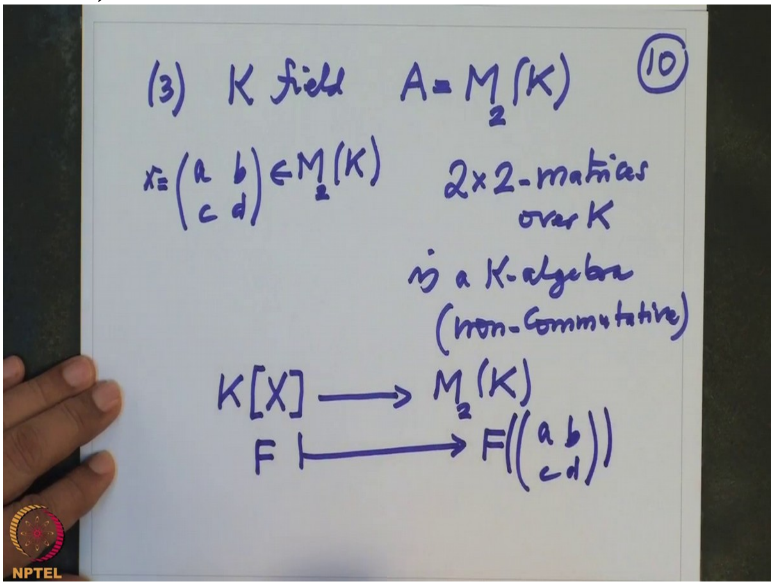
To show that x is algebraic over K I have to consider this as substitution homomorphism capital X $K[X]$ to $M_2(K)$ which

(Refer Slide Time 27:15)



any polynomial F is mapped to, F of, if you substitute instead of X, this matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

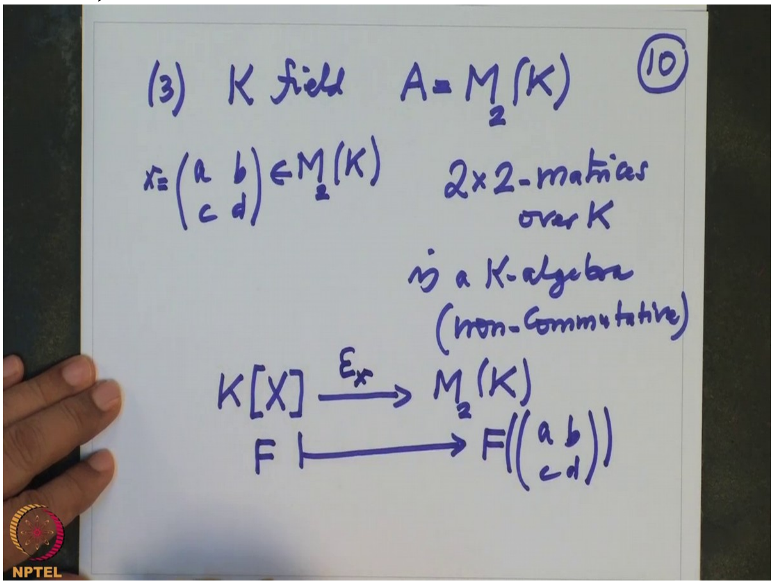
(Refer Slide Time 27:27)



And what do we need to check?

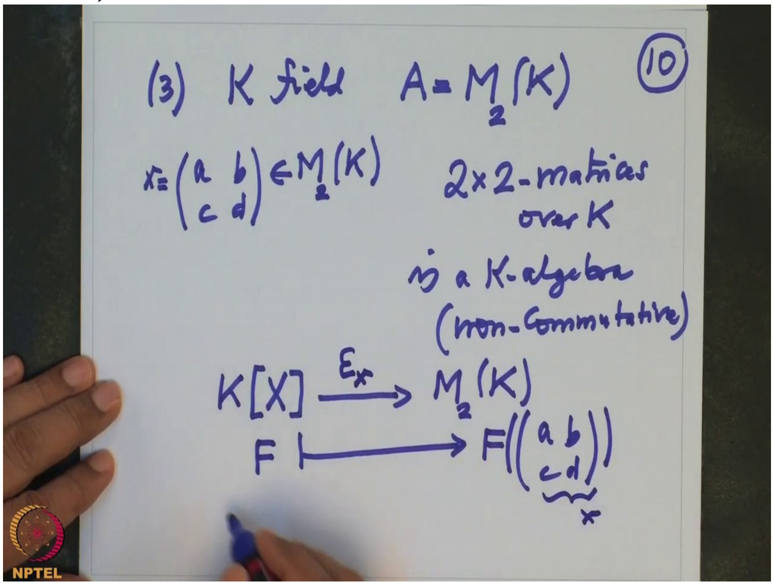
We need to check that there is at least, this is substitution homomorphism by x,

(Refer Slide Time 27:35)



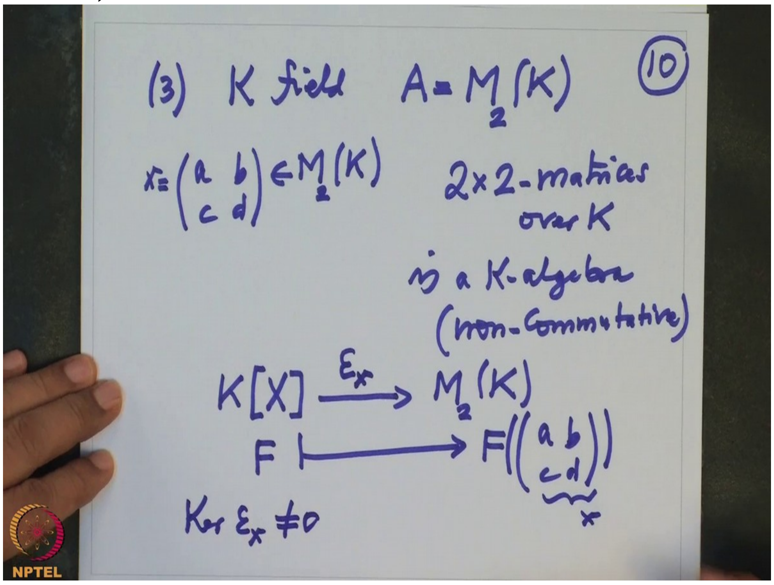
this is our x now, we need to

(Refer Slide Time 27:38)



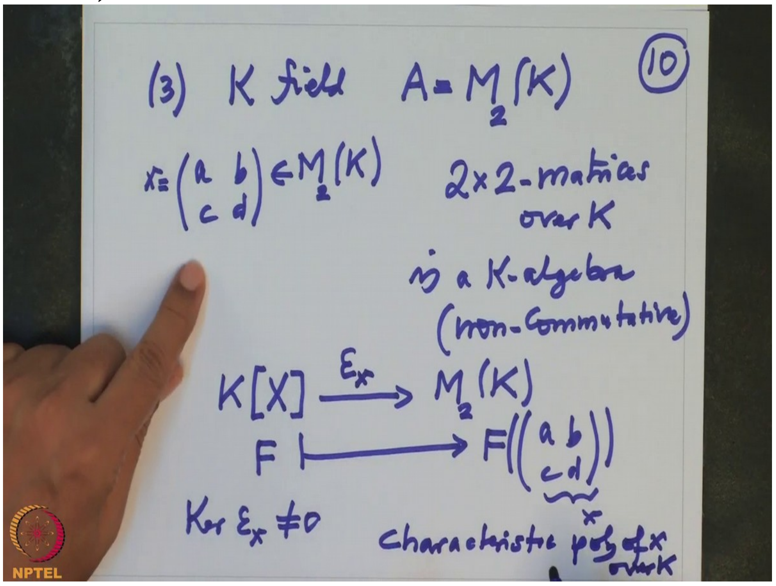
check that kernel of ϵ_x is non-zero.

(Refer Slide Time 27:43)



Well the right candidate for that, one might have guessed that is if you look at the characteristic polynomial of this x, so characteristic polynomial of, polynomial of x over K, in this case we know

(Refer Slide Time 28:06)

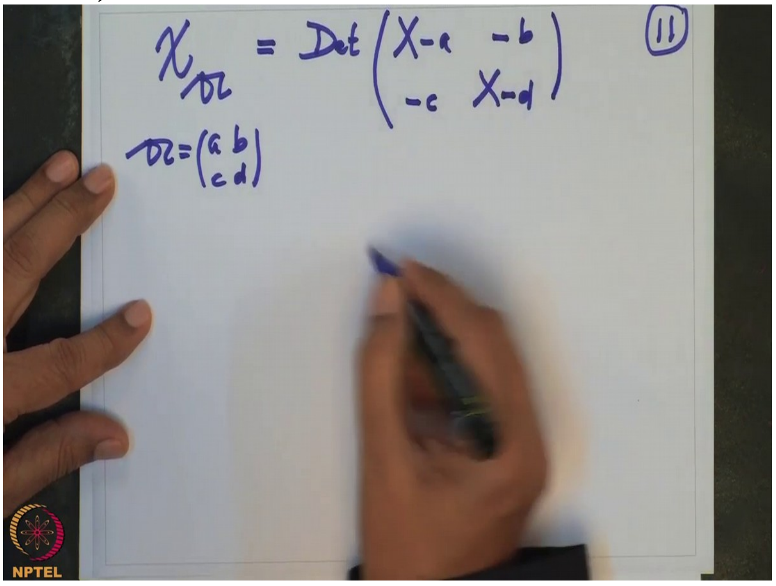


it is a, it is a monic polynomial of degree 2.

So the characteristic polynomial of this 2 by 2 matrix is usually denoted by characteristic polynomial and that let me denote A as a matrix. A is this matrix.

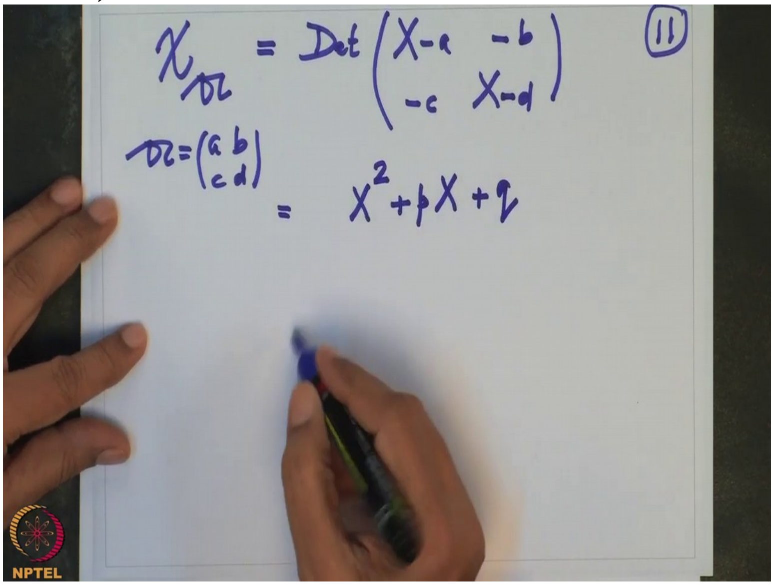
Then this is by definition the determinant of $\begin{bmatrix} X-a & -b \\ -c & X-d \end{bmatrix}$.

(Refer Slide Time 28:37)



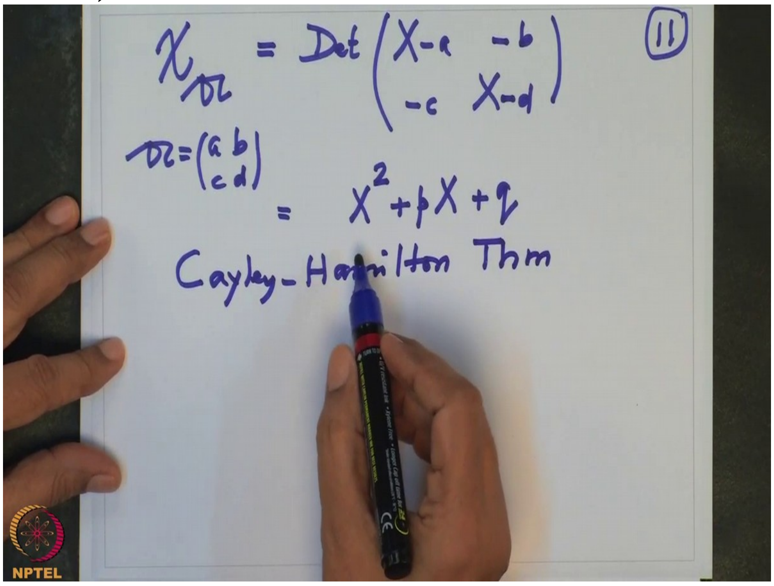
This is, whatever polynomial, it is a polynomial of degree 2, monic so it is X^2+pX+q .

(Refer Slide Time 28:47)



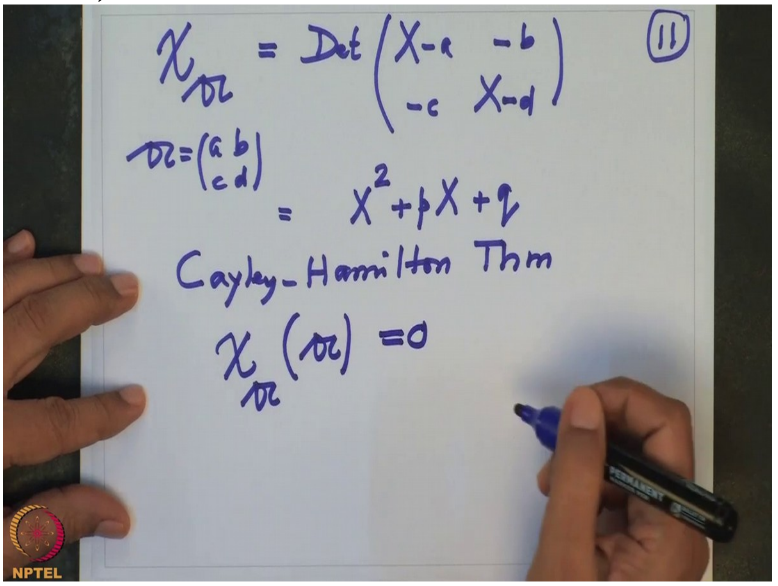
And your famous Cayley Hamilton theorem says, it says that if I substitute instead of X

(Refer Slide Time 28:59)



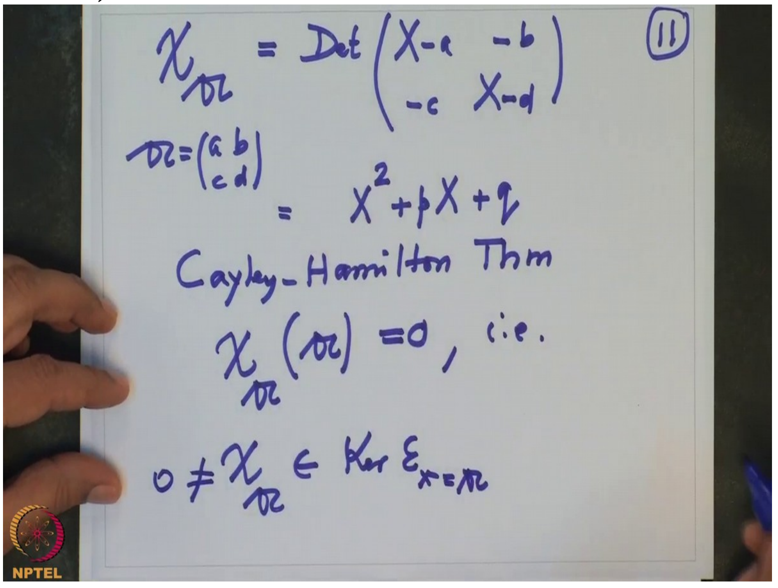
the matrix, the original matrix that I started with, then I get it zero. That means $\chi_A(A)$, this is actually zero matrix.

(Refer Slide Time 29:10)



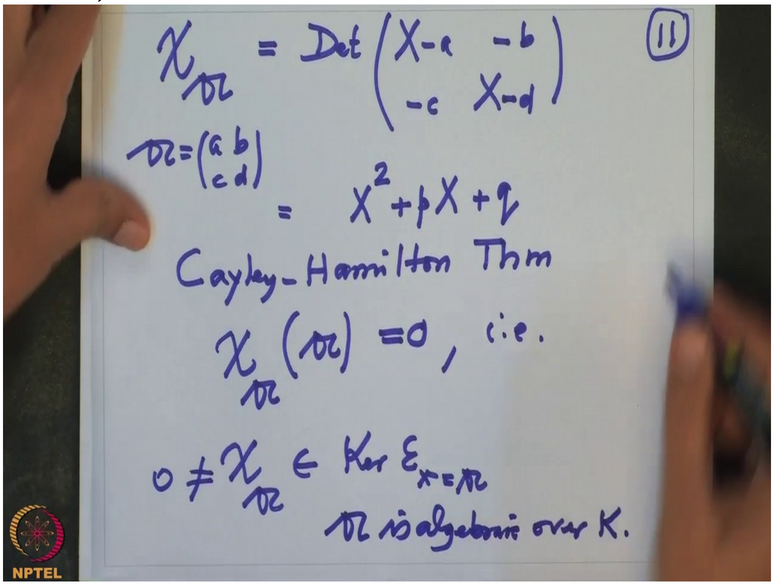
That precisely means, so in other words this χ_A is a polynomial inside the kernel. Remember X I have called it A. So therefore this is a non-zero polynomial because it is monic and

(Refer Slide Time 29:29)



degree is 2. And therefore what we conclude from here is this matrix A is algebraic over K. And there is nothing special

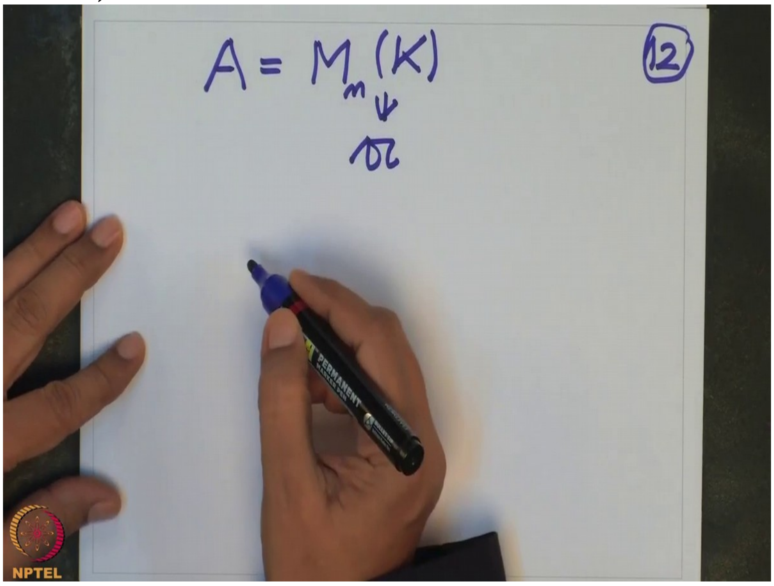
(Refer Slide Time 29:41)



about 2.

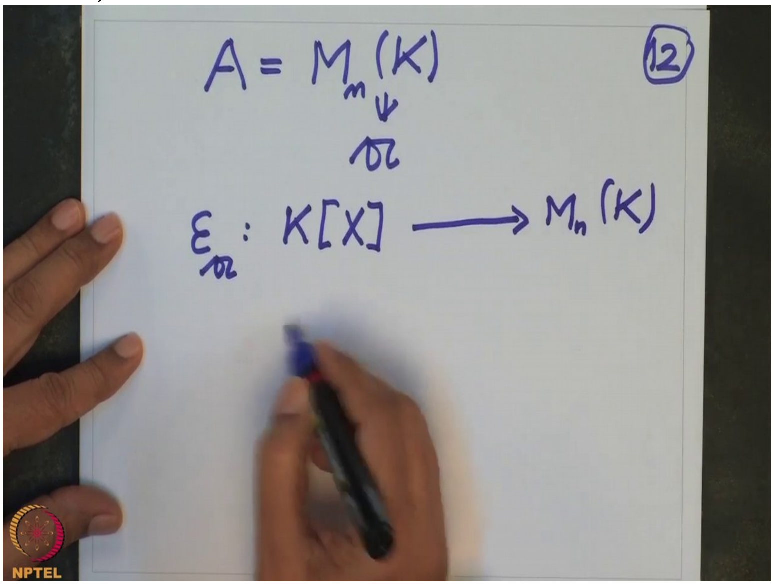
So this, so more generally what do we note, the same proof tells you that if I have, if I take A to be $M_n(K)$, $n \times n$ matrix is over K and I take a fix matrix A

(Refer Slide Time 30:00)



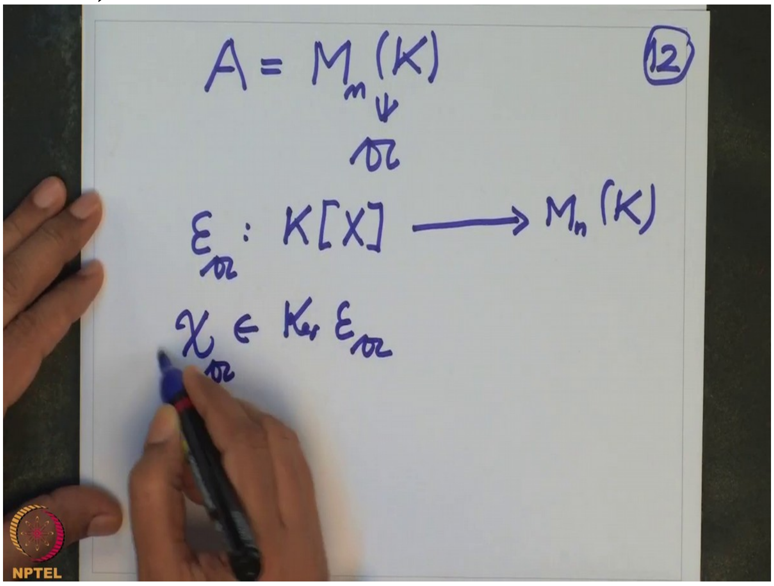
and I take the evaluation for substitution homomorphism defined by this A, that is the map from $K[X]$ to $M_n(K)$, then this

(Refer Slide Time 30:13)



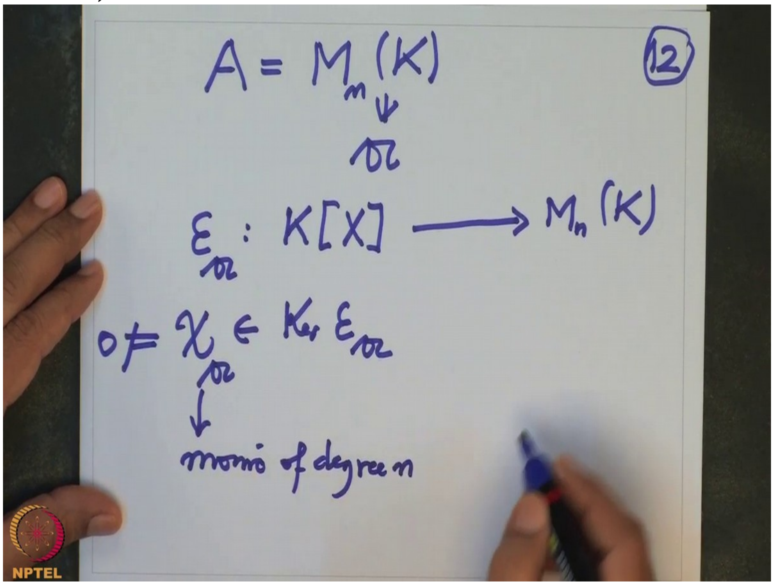
kernel of this epsilon A definitely contains the characteristic polynomial of A

(Refer Slide Time 30:20)



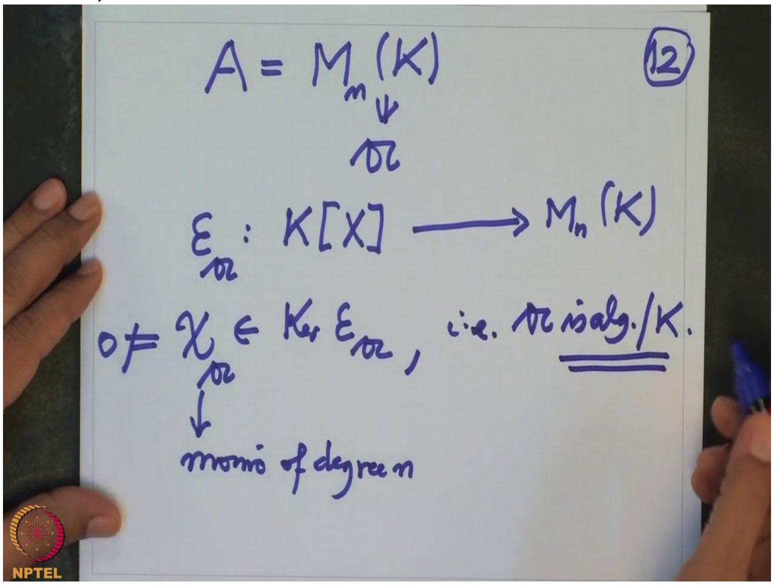
which is a non-zero polynomial monic of degree n.

(Refer Slide Time 30:30)



So that simply means in our language, that is A is algebraic over K. So all

(Refer Slide Time 30:40)



matrices are algebraic over K and this is very important, in fact any algebra as you have noticed is centered around studying the characteristic polynomial, zeroes of the characteristic polynomials and therefore we have lots of ready examples to go on.

And with this definition I will, next time, next couple of minutes I will deduce how do you check, this is only a definition and we know examples. And also I will give

(Refer Slide Time 31:15)

examples which are not algebraic and we will also study how do we see the elements are algebraic or not, how do you find a economical criterion for elements to be algebraic or not. So this I will continue after the break, thank you.