Galois' Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture No 15
Minimal Polynomials

(Refer Slide Time 00:25)

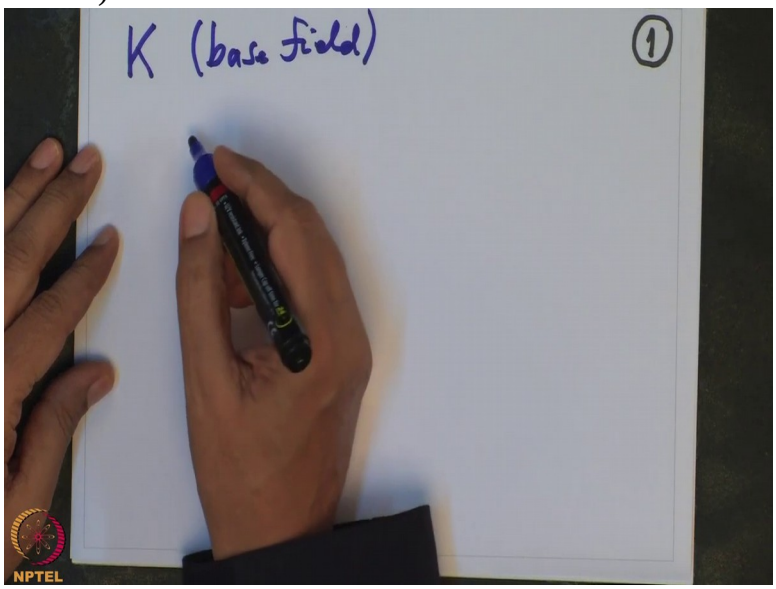
In the last lecture I have defined what are algebraic elements over a field and I have given some examples. Today I will

(Refer Slide Time 00:38)

give a characterization of algebraic elements. This will allow us to examine whether some given element is algebraic or not in an efficient way.

Ok, so let us recall our notation was K as usual, our base field and let me remind you

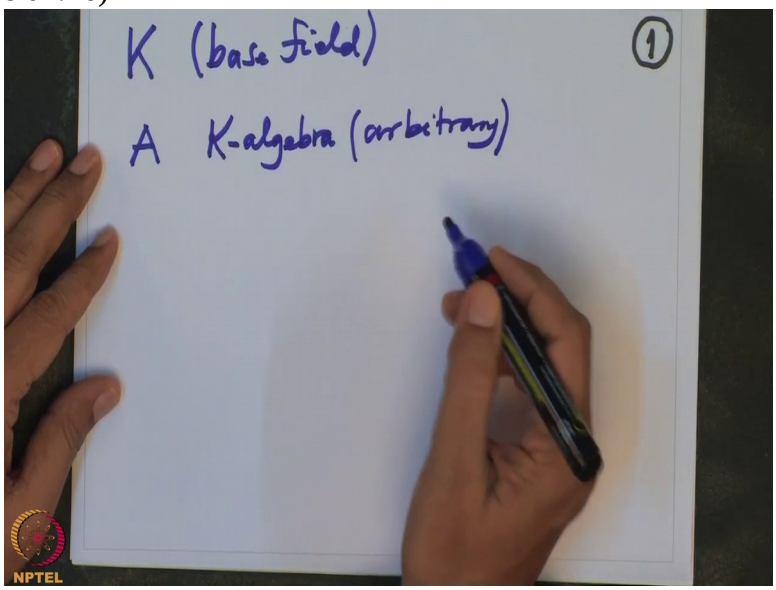
(Refer Slide Time 01:07)



once more, we are considering K-algebras. A is a K-algebra, arbitrary K-algebra.

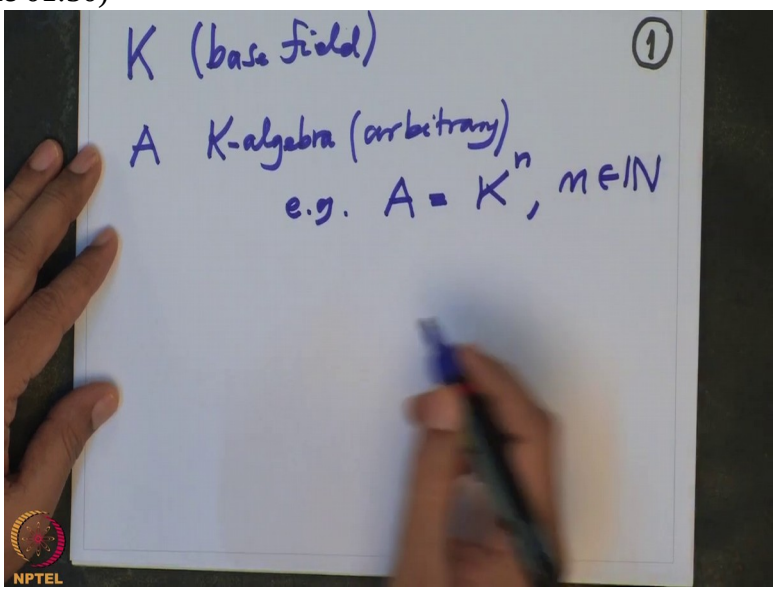
It may be

(Refer Slide Time 01:26)



a field; it may not be a field. It may be integer domain; it may not be an integer domain and so on. A typical example we saw that in case of commutative, for example we could also take A equal to K^n where n is some natural number.

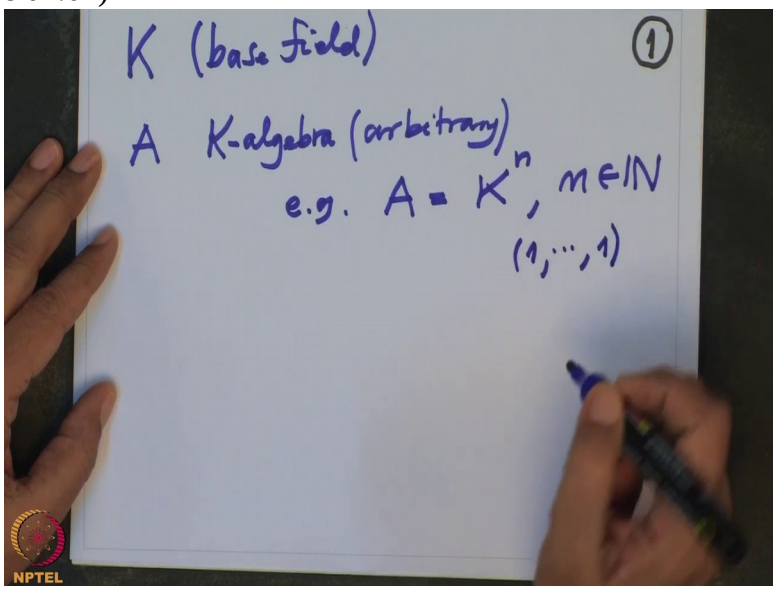
(Refer Slide Time 01:50)



This is the K-algebra. The addition is component wise and multiplication is also component wise.

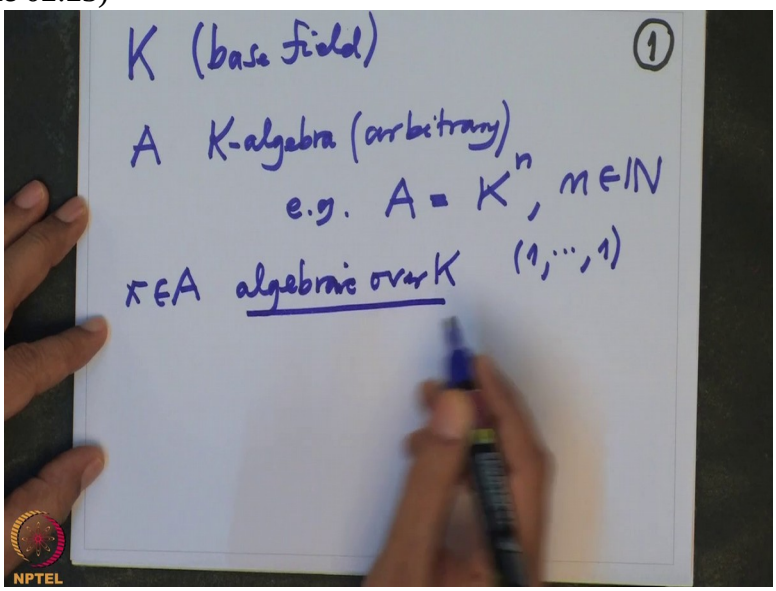
In particular see this (1,... ,1), this is a multiplicative identity

(Refer Slide Time 02:02)



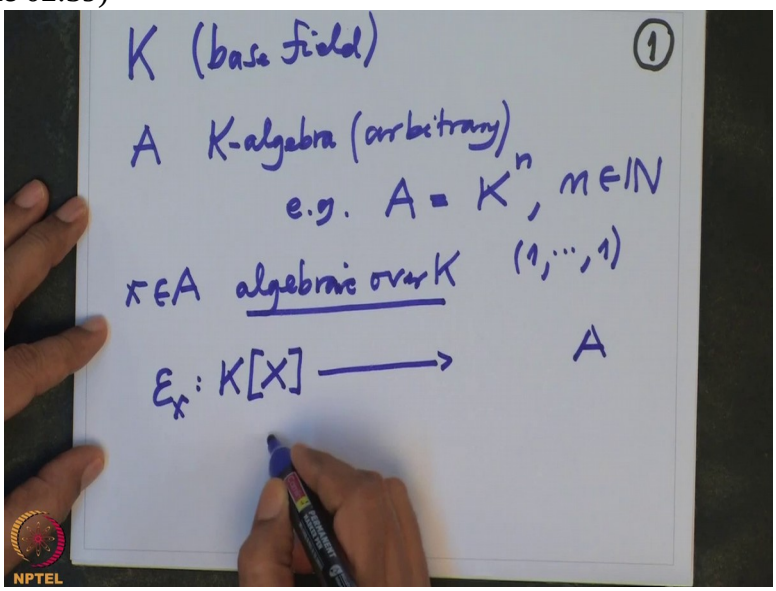
and (0,…, 0) is the additive identity. Anyway, so how did you define an element? $x \in A$ is called algebraic over K if we have

(Refer Slide Time 02:23)



looked at the substitution homomorphism ϵ_x , this is a homomorphism from the polynomial algebra in X over K to A,

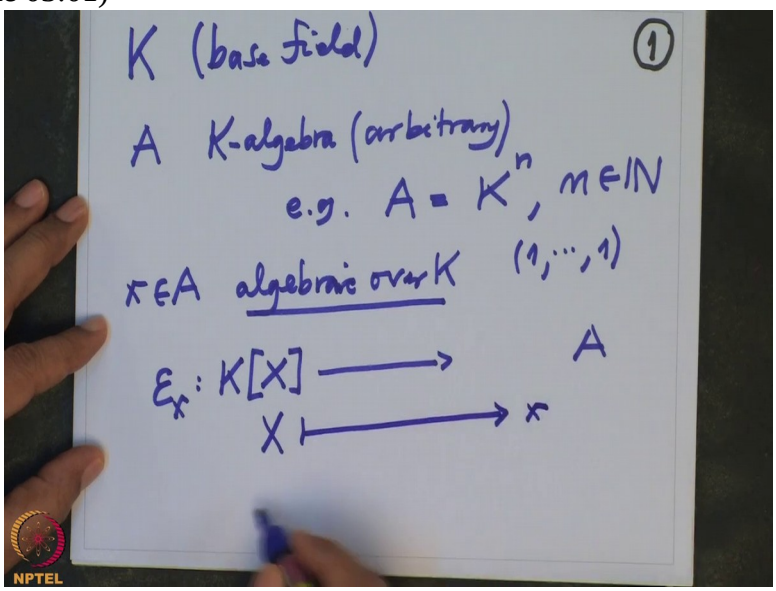
(Refer Slide Time 02:39)



the homomorphism is just evaluating the polynomial at given x.

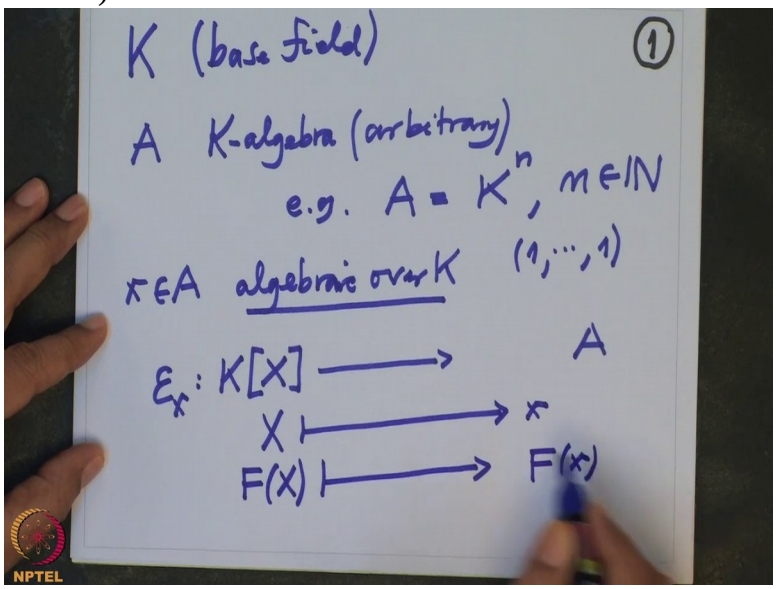
So for that also you could also give only value where capital X go and then once you want K-algebra homomorphism then it is dictated where the arbitrary polynomial will go. So if I map X to small x,

(Refer Slide Time 03:01)



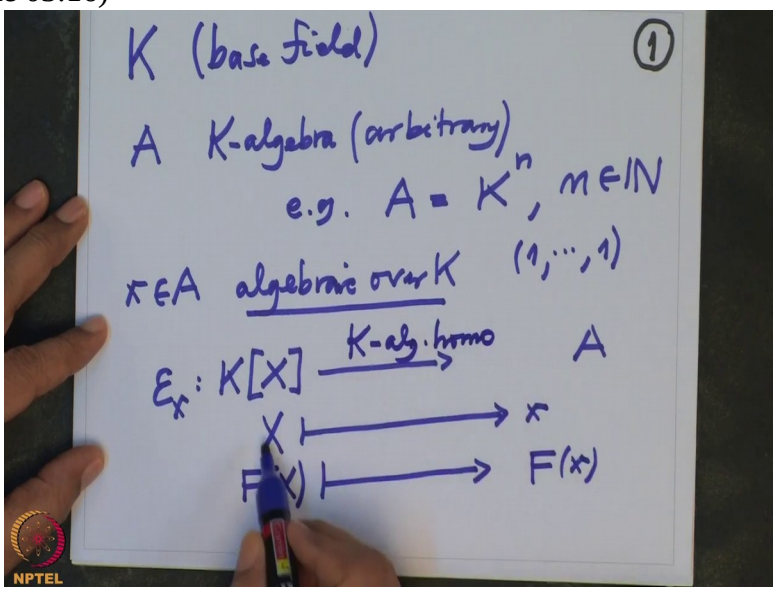
then F, F of X, arbitrary F has to go to F of small x because

(Refer Slide Time 03:09)



we want K-algebra homomorphism. Because once

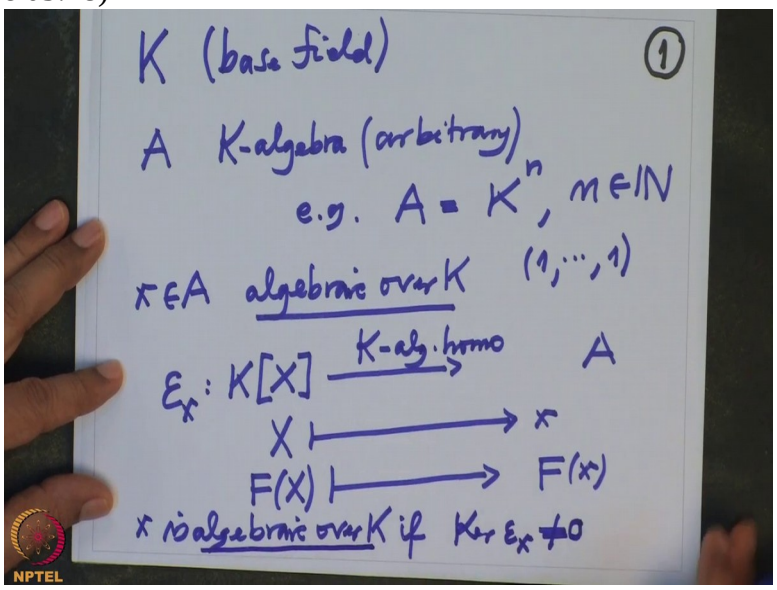
(Refer Slide Time 03:16)



you know where X go, it is clear where X^2 will go and it is also clear where linear combination will go.

So this K-algebra homomorphism, and if the kernel of this, if x is algebraic over K, if the kernel of this substitution homomorphism is non-zero then we say that it is algebraic over K.

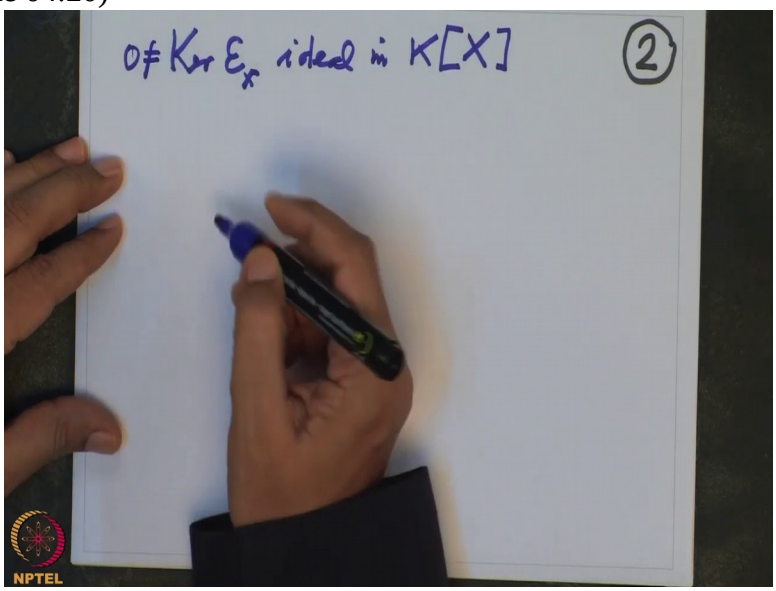
(Refer Slide Time 03:48)



So, and we want to characterize this in a efficient way, easier way, Ok.

For that let me just set up some notation. We have seen earlier that this kernel ϵ_x or E_x is an ideal in $K[X]$ and we know it is a non-zero ideal

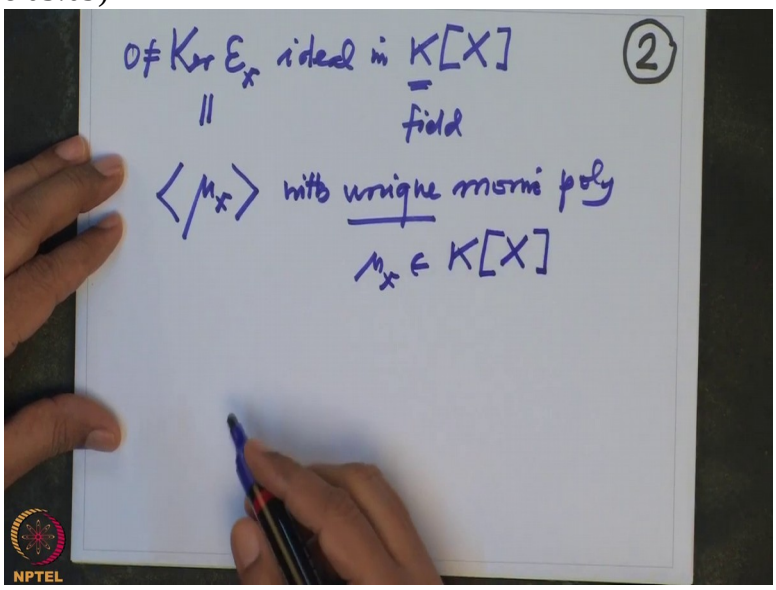
(Refer Slide Time 04:20)



assuming X is algebraic and we have seen the ideals in a polynomial ring over a field in K, K is a field is very important.

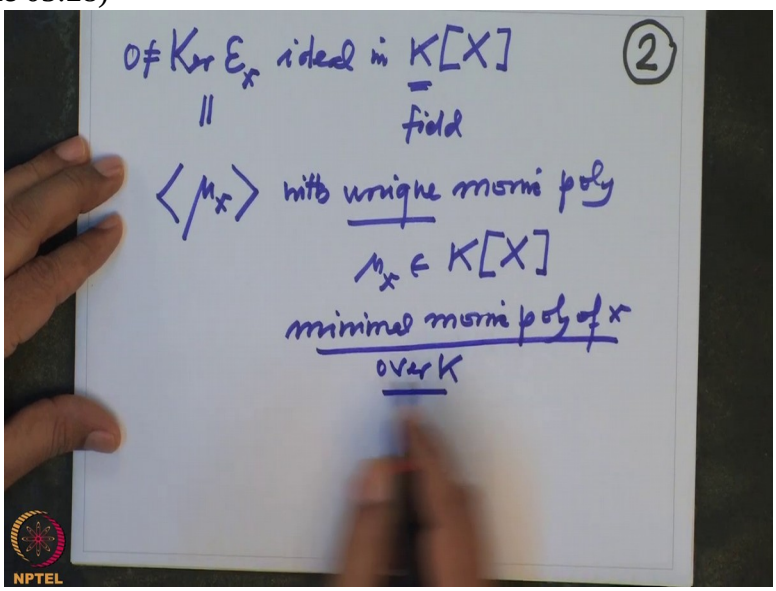
This is a field is very important, so such non-zero ideals are generated by single polynomial and that monic, that polynomial is also uniquely determined by this ideal if you assume that the generator is monic. So this is generated by, I will use this notation, μ_x with unique monic polynomial μ_x in $K[X]$.

(Refer Slide Time 05:09)



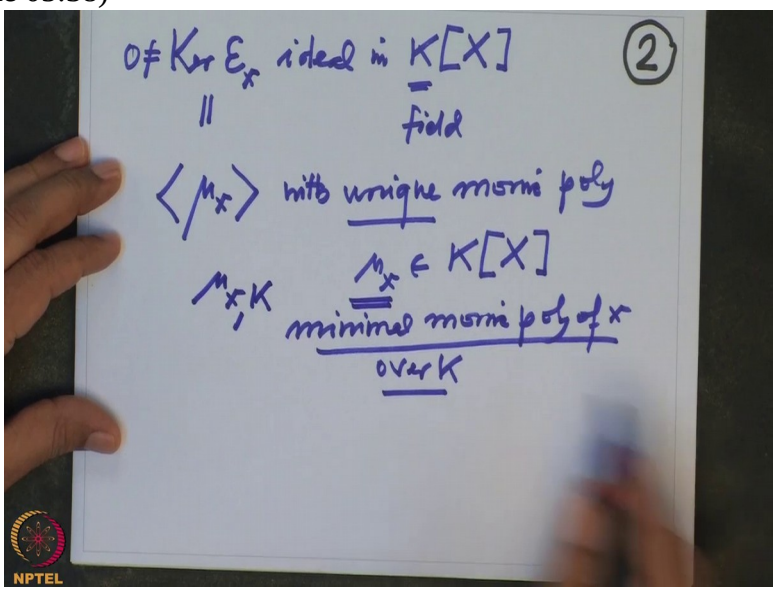
This polynomial is called minimal monic polynomial of x over K. Strictly speaking

(Refer Slide Time 05:28)



I should also use, instead of μ_x I should also, better I should use $\mu_{x,K}$ just to keep track where

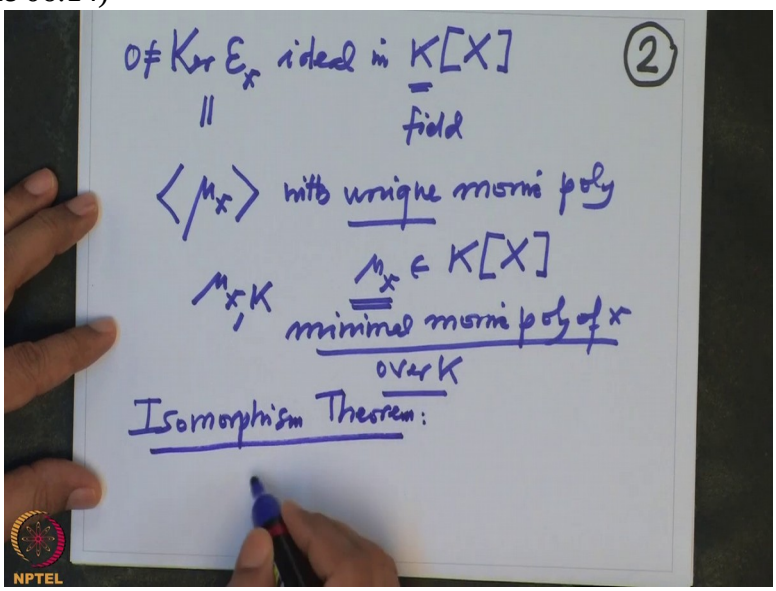
(Refer Slide Time 05:38)



the coefficients are. But when the context is understood it is better to simplify the notation by dropping that K, Ok.

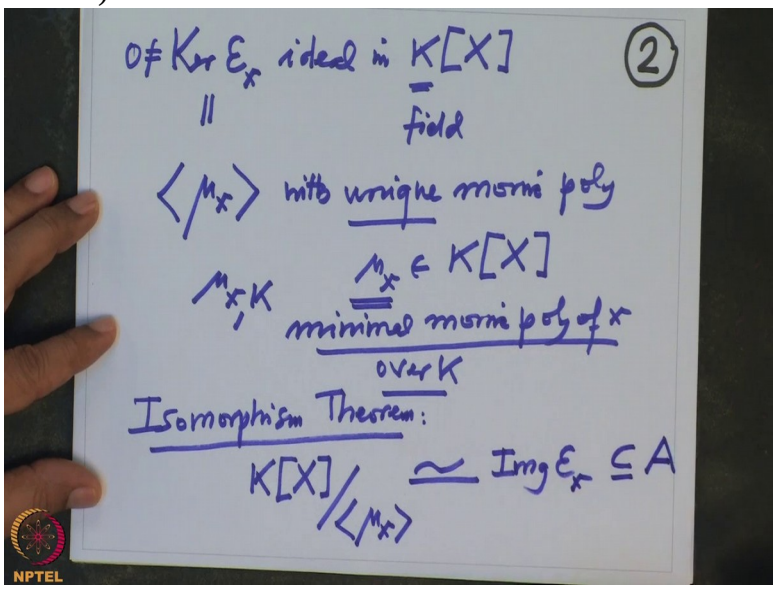
So now what did we learn in the first course on algebra? That whenever you have a ring homomorphism then the kernel and image, how are they related? Isomorphism theorem says, theorem says that

(Refer Slide Time 06:14)



if I take this ring $K[X]$, K-algebra $K[X]$, and go modulo the kernel which is generated by μ_x , this is isomorphic to the image of this ϵ_x which is a sub algebra of

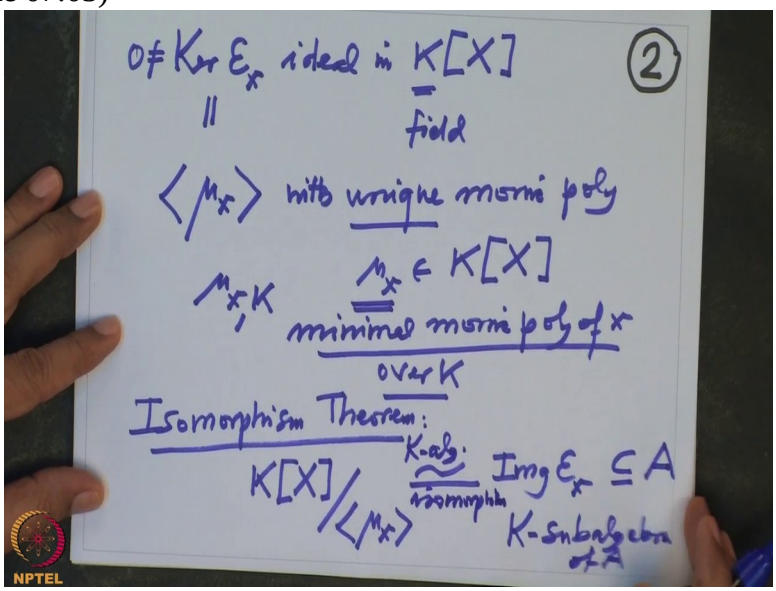
(Refer Slide Time 06:35)



A because this map is from, ϵ_x is from $K[X]$ to A.

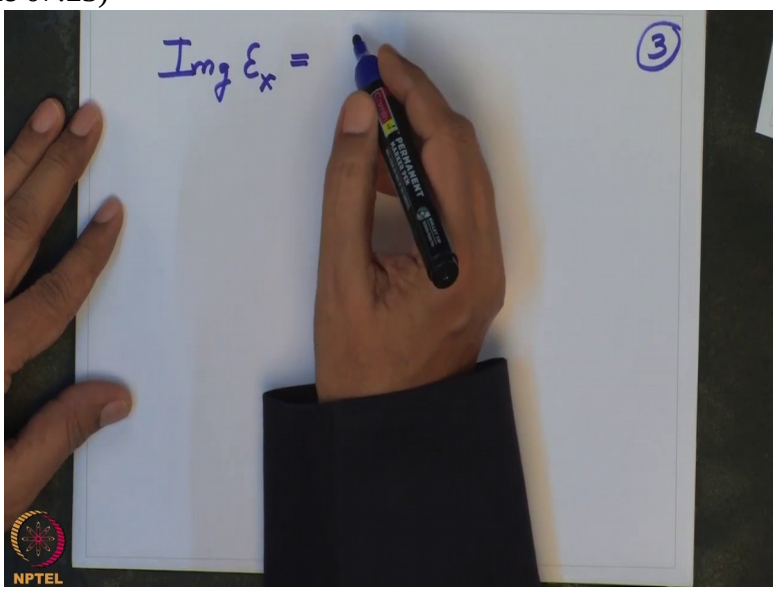
So image is definitely a sub algebra. This is a K sub algebra of, of A. And this isomorphism is a K-algebra isomorphism. But you know what

(Refer Slide Time 07:03)



is the image? Image also you can describe neatly. So the image, the image is nothing but, image of ϵ_x is nothing but it is generated by

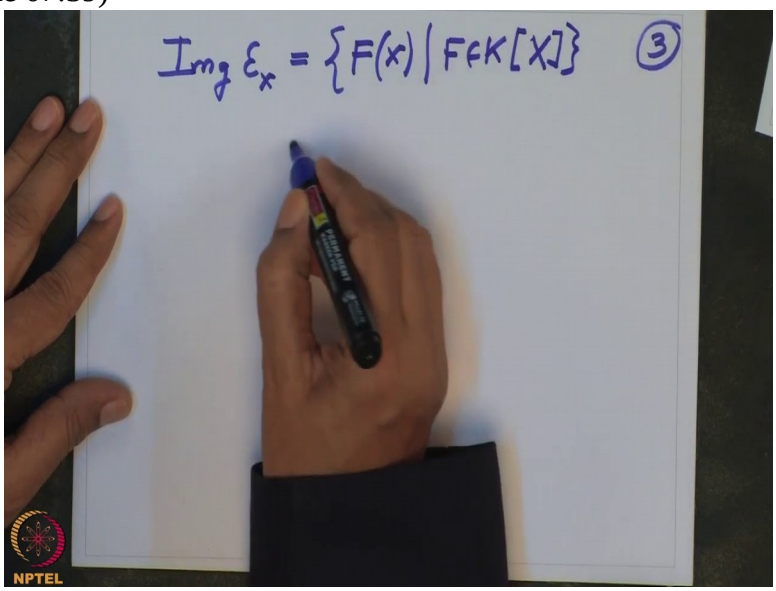
(Refer Slide Time 07:23)



X as algebra because, so what is the image of this?

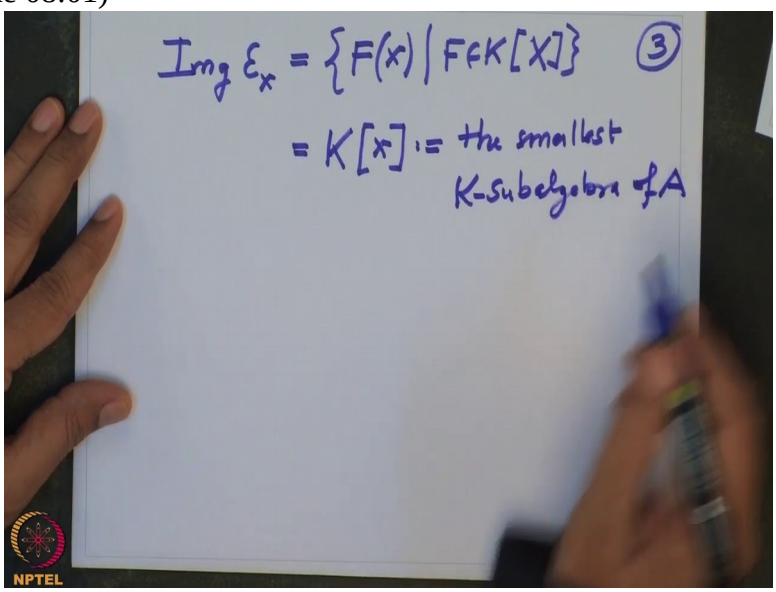
These are all those polynomials evaluated at x where F varies in $K[X]$. This is the image. So this is

(Refer Slide Time 07:39)



precisely K small x. And what is this, by definition? This is the smallest case of algebra of A

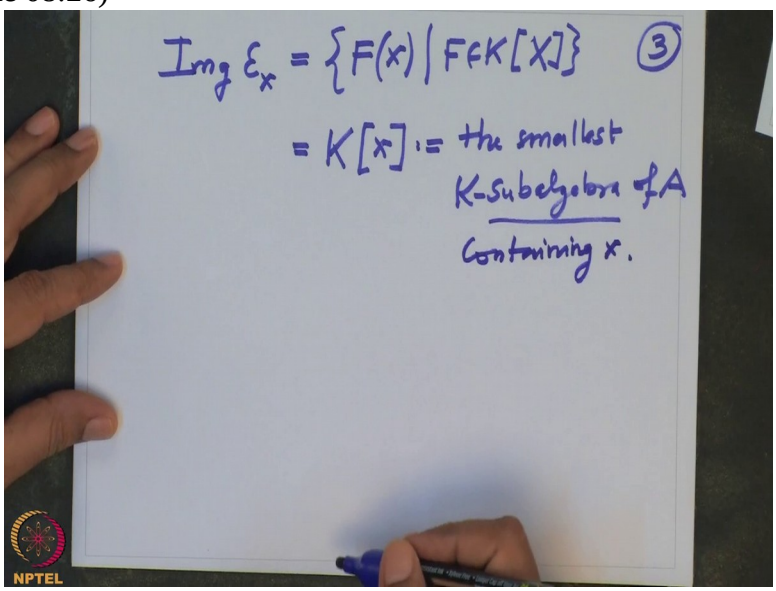
(Refer Slide Time 08:01)



because once x is there and it is a sub algebra, all polynomials in x is also there. Only thing we have is 2 polynomials may give the same evaluation but may be different polynomials.

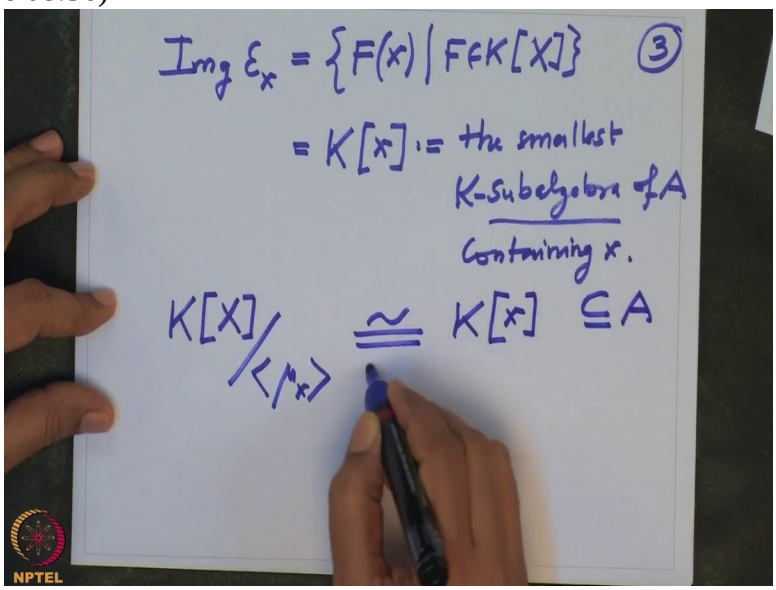
So this is the smallest case of algebra of A containing x.

(Refer Slide Time 08:26)



Once it contains x, it contains x^2 . It contains x^3 , it contains all powers of x and also their combination. So it is, in particular it is a sub algebra. Therefore our isomorphism theorem tells $K[X]$ mod ideal generated by μ_x this is isomorphic to K small x which is a sub algebra of A

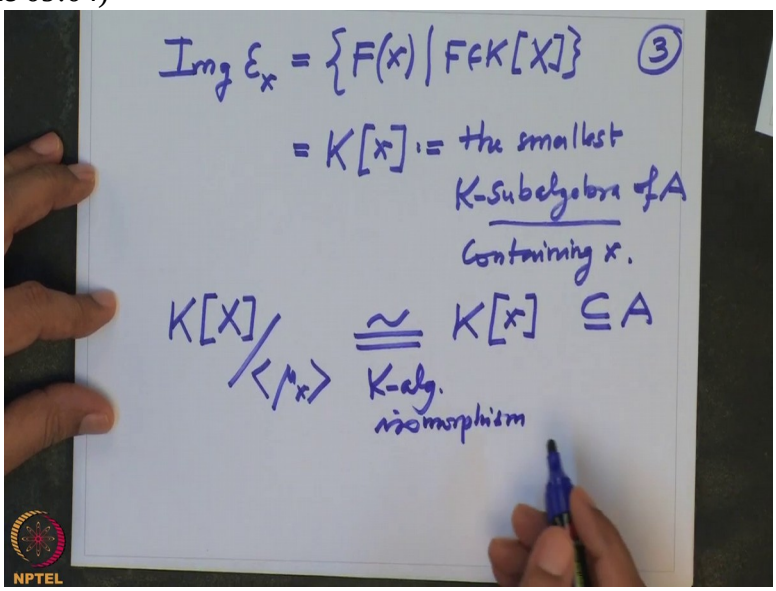
(Refer Slide Time 08:56)



which is a K-algebra isomorphism.

Once it is

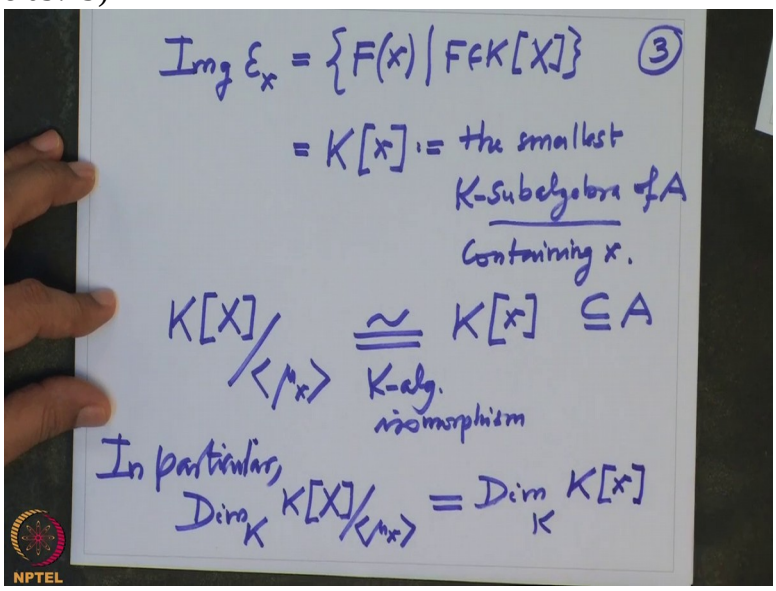
(Refer Slide Time 09:04)



a K-algebra isomorphism, it is also K vector space isomorphism and isomorphism as ring also, together.

So therefore, because it is a vector space isomorphism in particular their dimensions are also equal. In particular dimension of O as a vector space over this, $K[X]$ mod ideal generated by μ_x is same as dimension of, as a vector space $K[x]$.

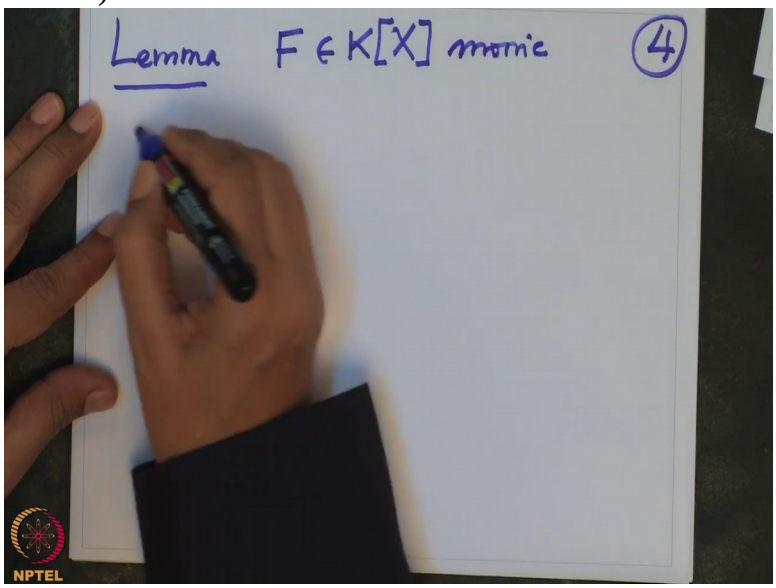
(Refer Slide Time 09:49)



We have this, but between the two we know that this quotient ring very well because mu is monic and we can compute the dimension easily. So let me state, let me remind you this is already we knew from your basic algebra course. So let me state it as a lemma and lemma I will state it more generally so, so this is a lemma.

So F is monic polynomial in $K[X]$ and in this K may not be a field, monic is very important,

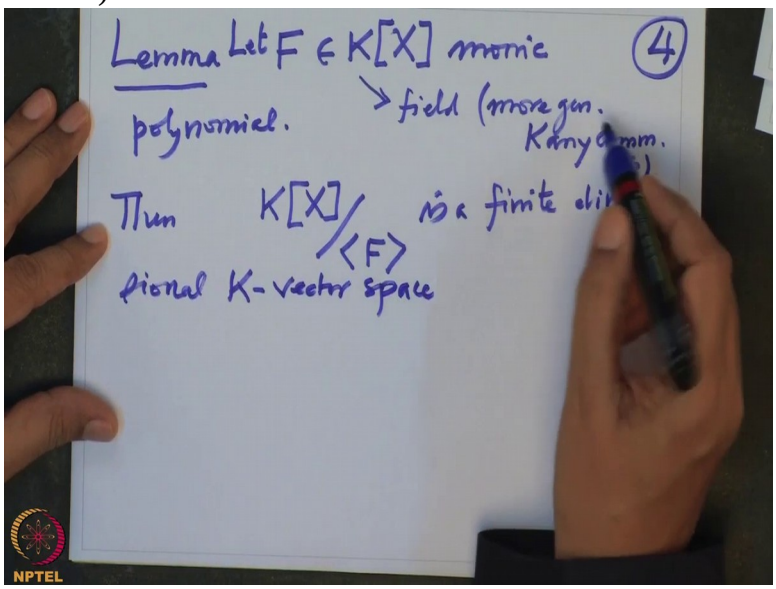
(Refer Slide Time 10:30)



monic polynomial. Let F be a monic polynomial in $K[X]$. K assume, K is a field or more generally any commutative ring. Then $K[X]$ mod ideal generated by F is a finite dimensional K vector space.

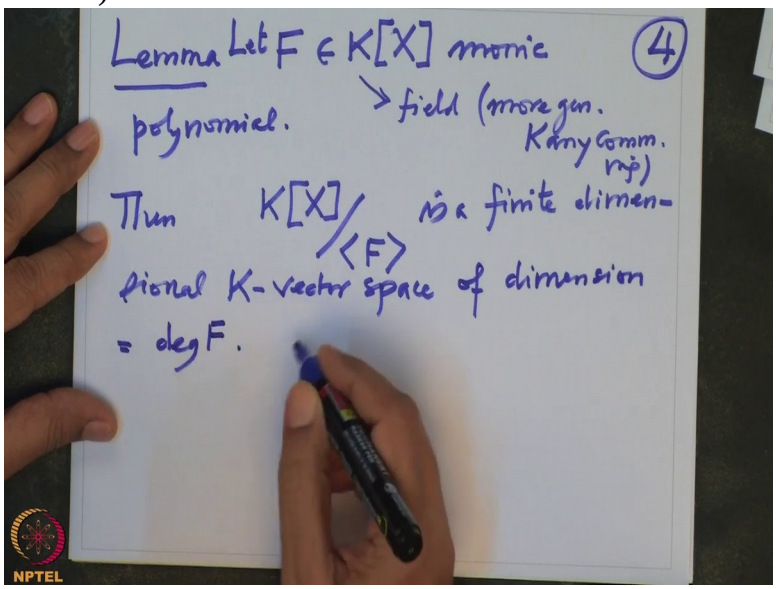
If it is not a field

(Refer Slide Time 11:28)



then one should say it is a free module of finite rank. But I am not going to write it here. I will just state only because we do not need in this course, may be. When I need it I will say it, of dimension equal to degree of F.

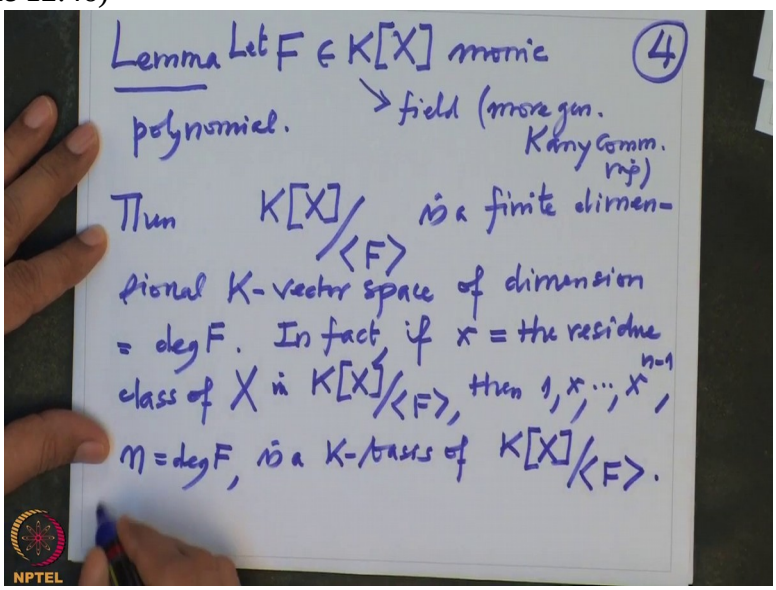
(Refer Slide Time 11:52)



In fact we can give a basis.

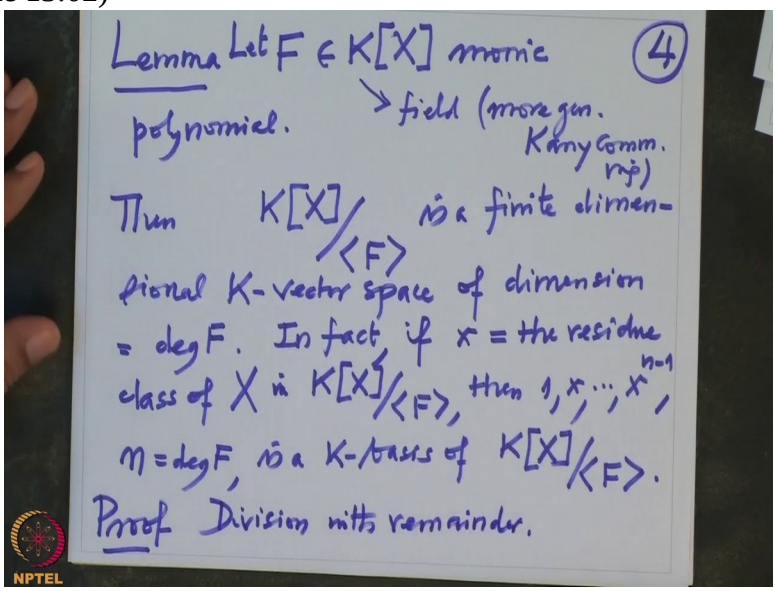
If small x equal to the residue class of capital X modulo F that means in this ring, $\frac{K[X]}{F}$ then 1 x up to x^{n-1} where n equal to degree of F is a K basis of this quotient residue class algebra, $\frac{K[X]}{F}$.

(Refer Slide Time 12:46)



Proof which is immediate form what is called division with remainder.

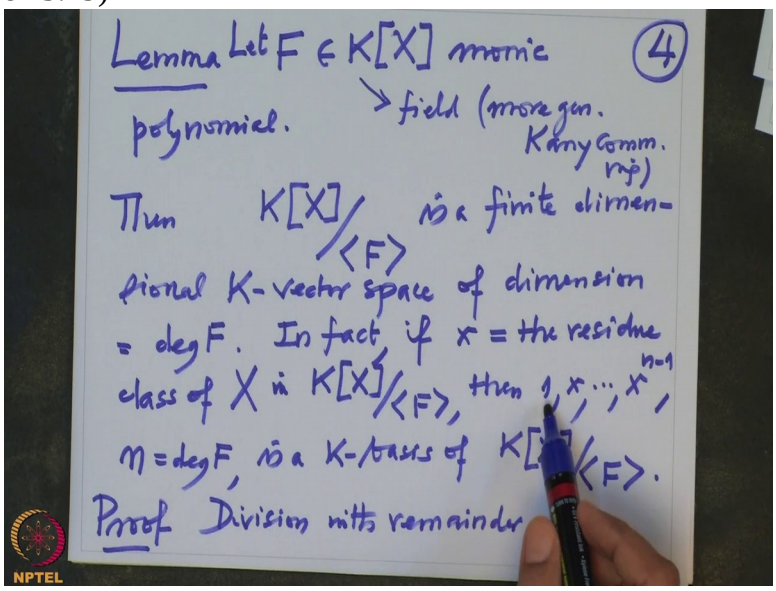
(Refer Slide Time 13:02)



That is immediate because we know that division, the remainders are unique and remainders will have smaller degree equal to the degree of F because we are dividing by F.

So therefore remainders can have at most degree n minus 1 that means

(Refer Slide Time 13:19)

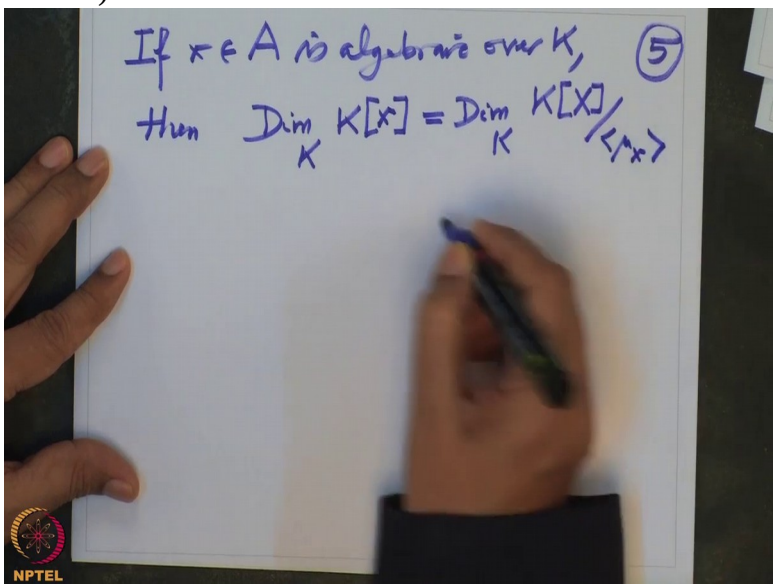


mod F the remainder is a linear combination of this and is unique because the remainders have degree less than n, degree of F that is the proof.

So in particular our problem therefore, therefore what we know 5, therefore what we, I will summarize it here, if x is in A is algebraic over K then dimension of, vector space dimension

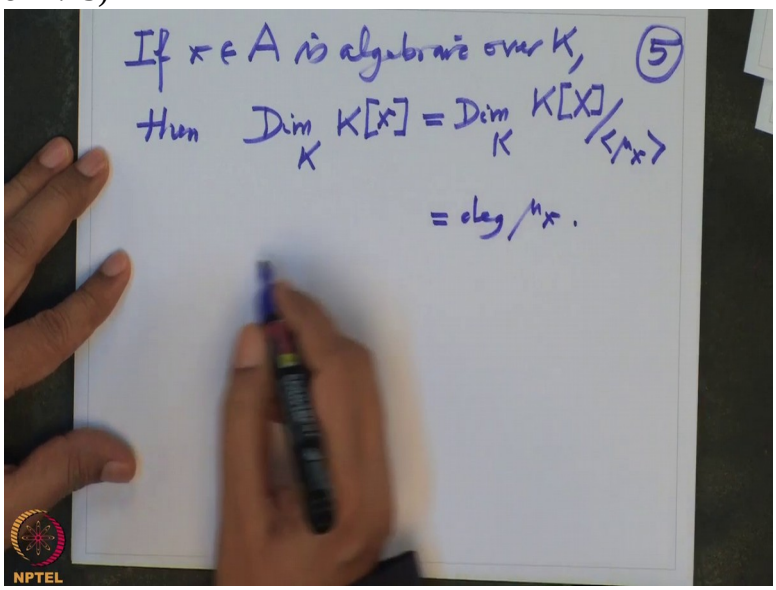
of the sub algebra generated by x is same thing as dimension of the vector space $K[X]$ mod the minimal polynomial

(Refer Slide Time 14:20)



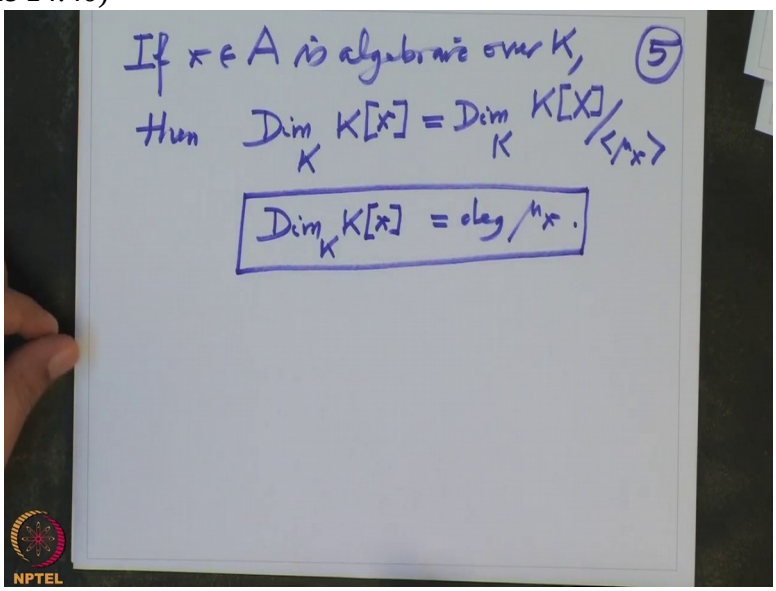
which is equal to the degree of the minimal polynomial.

(Refer Slide Time 14:25)



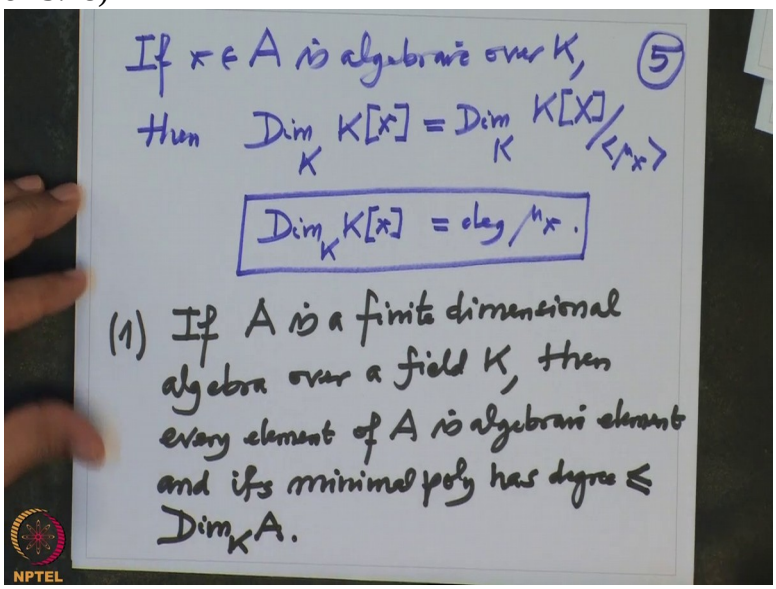
So dimension $K[X]$, this formula.

(Refer Slide Time 14:40)



So 1, if capital A is a finite dimensional algebra over a field K then every element of A is algebraic element and its minimal polynomial has degree small or equal to the dimension of A over K.

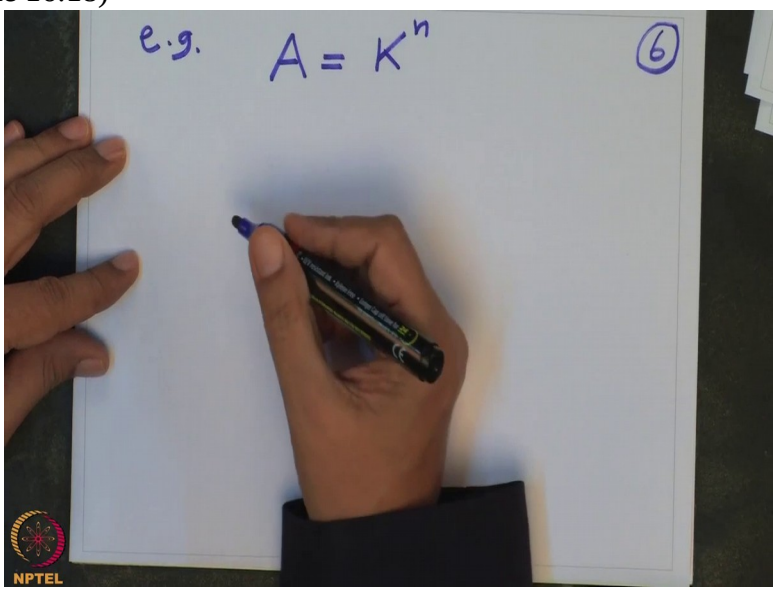
(Refer Slide Time 15:48)



Small or equal to because the minimal polynomial, the degree of the minimal polynomial is dimension of the sub algebra, not dimension of A but dimension of the sub algebra, sub algebra generated by x. So A may have more dimension but this will, for example so let us see explicit example.

If I take A to be equal to say K^n

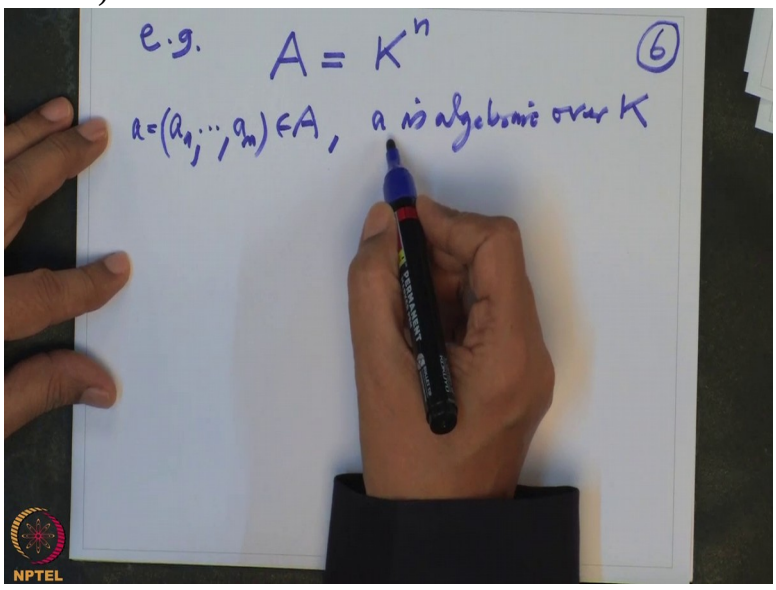
(Refer Slide Time 16:18)



this is a finite dimensional algebra over K namely dimension is n, Standard e_1 to e_n is a basis, so the dimension is n. Now suppose I take an element $(a_1,\ldots,a_n)$, this is my element $a \in A$. Then we know a is algebraic because a is finite dimension but we do not know what is the degree of the minimal polynomial.

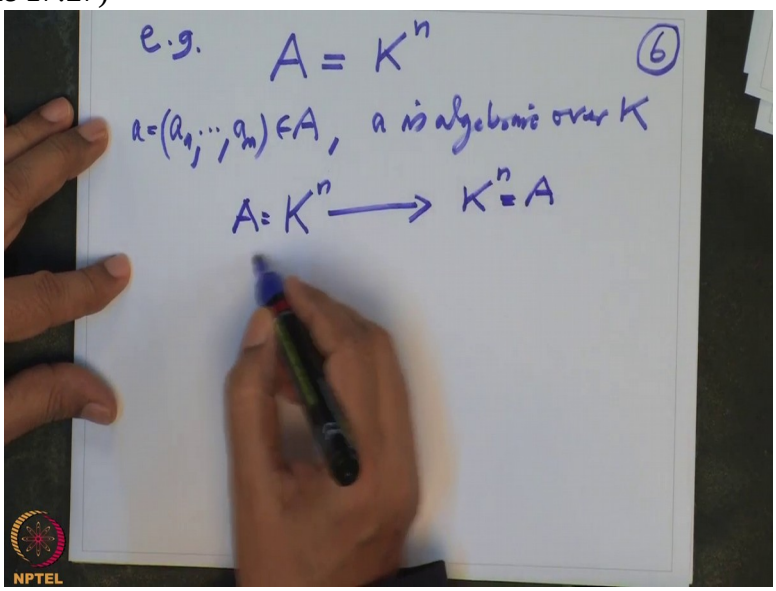
So let me write a recipe how do you find a minimal polynomial. So minimal

(Refer Slide Time 17:03)



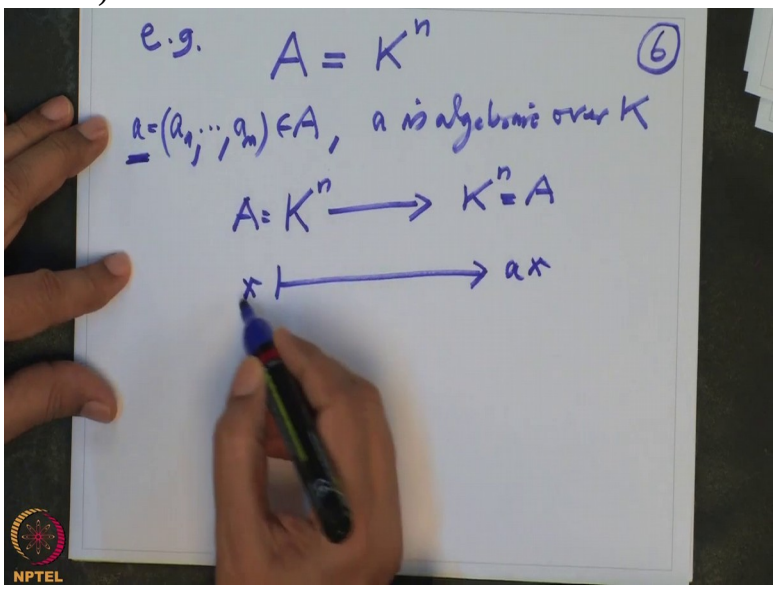
polynomial you want to find the following. So you have this A. So think of linear, so look at the map $K^n \to K^n$, A to A, let me write A, A equal to K^n , to A.

(Refer Slide Time 17:27)



And the map is any x going to ax, multiplication by a, this a. This a is fixed.

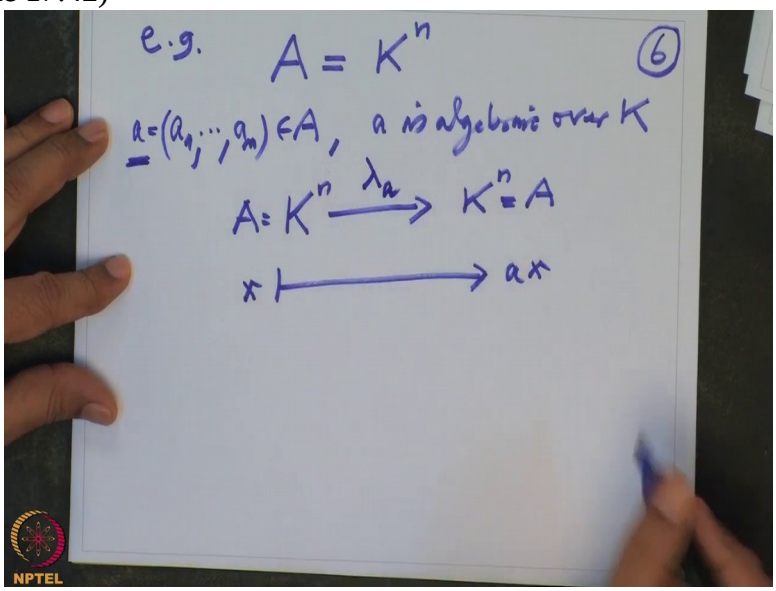
(Refer Slide Time 17:36)



Arbitrary element is mapped to multiplication map.

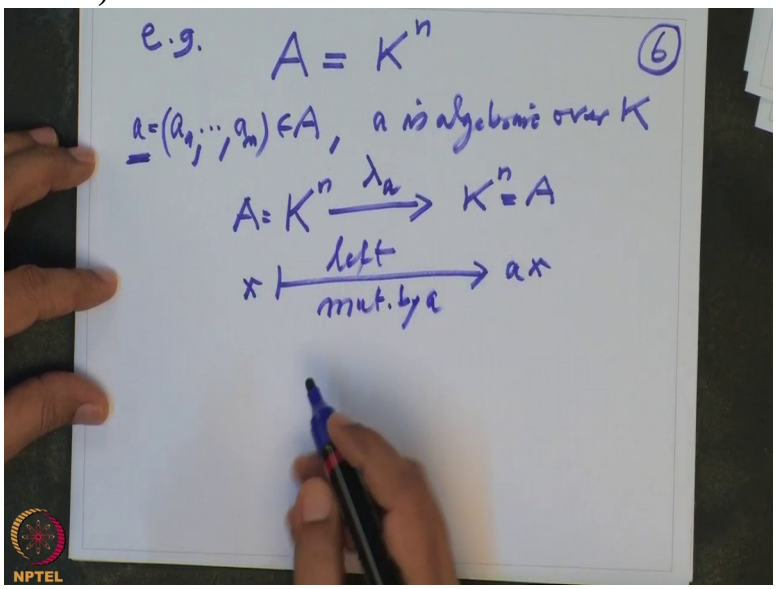
This map I am going to denote by λ_a.

(Refer Slide Time 17:42)



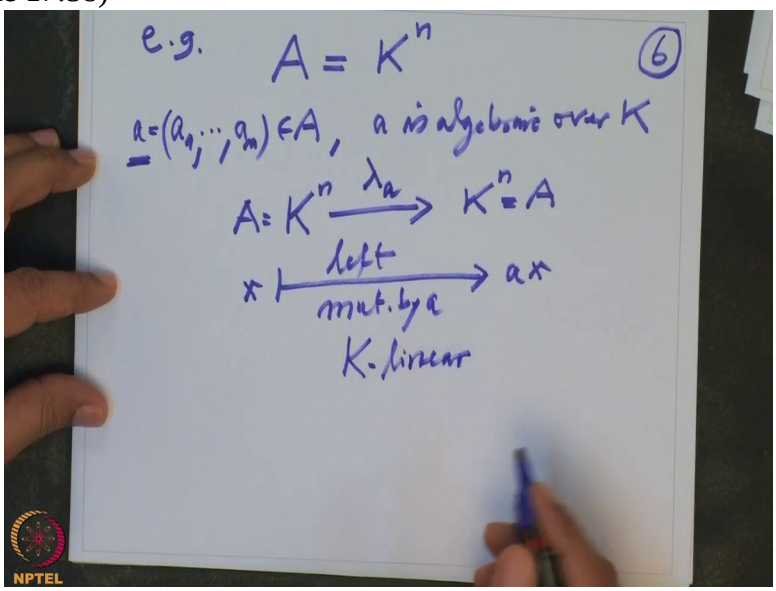
lambda is for left multiplication. This is a left multiplication by a.

(Refer Slide Time 17:53)



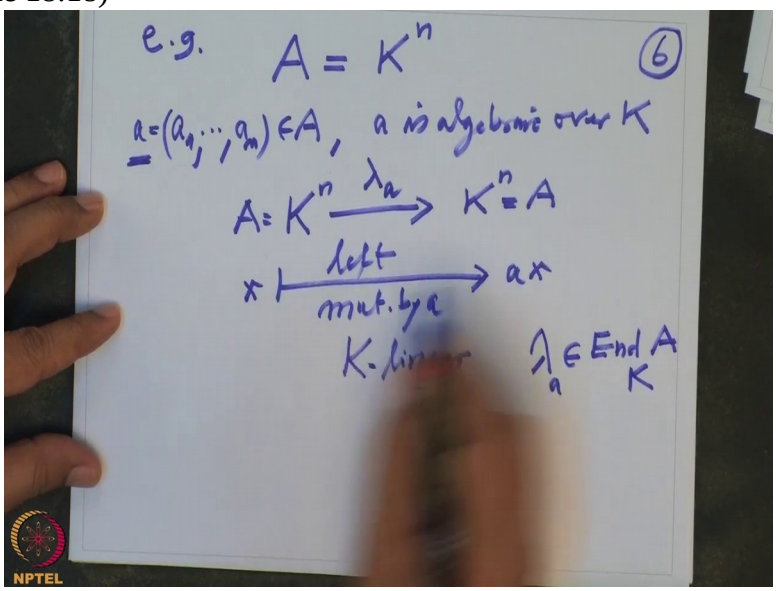
So it is clearly K linear.

(Refer Slide Time 17:58)



It is a K linear map and therefore I want to use some linear algebra. So this λ_a therefore is an endomorphism of the vector space A over K. Endomorphism means

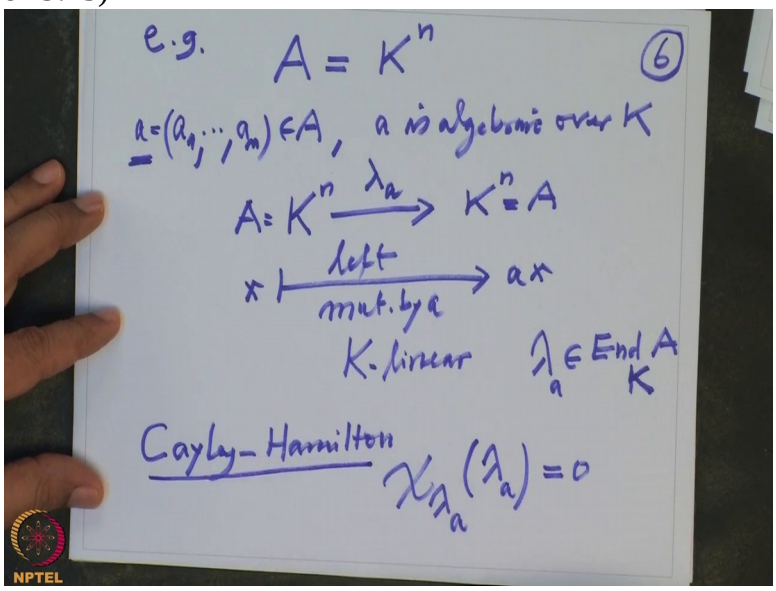
(Refer Slide Time 18:18)



the map from A to A and the suffix here means it is K linear. It is the map of the vector space. So we know, because, what do we know?

We know that this map satisfies a Cayley Hamilton, last time also I have said that Cayley Hamilton says the characteristic polynomial of λ_a , this is the standard notation, this is, this satisfies, λ_a satisfies that, that means this is 0. As a map. So this is a polynomial. And in that polynomial I have substituted this linear operator λ_a can be 0. That is precisely what Cayley Hamilton theorem

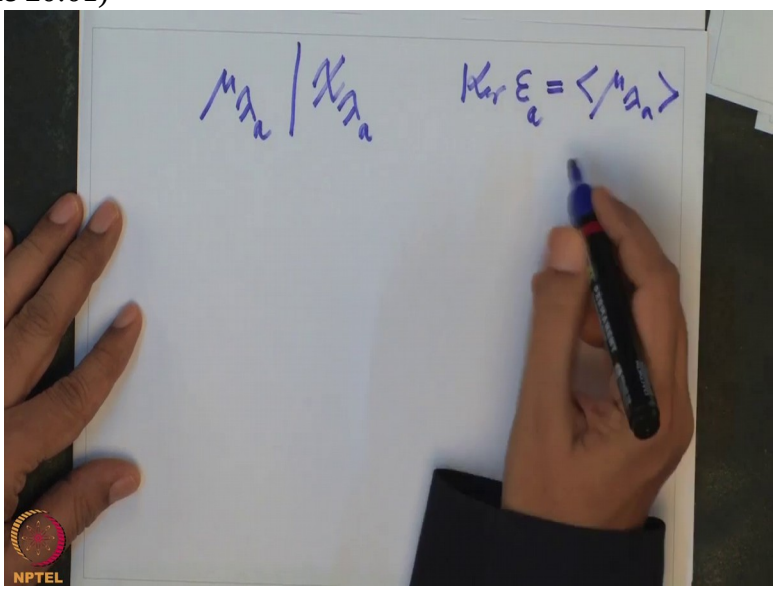
(Refer Slide Time 19:13)



says.

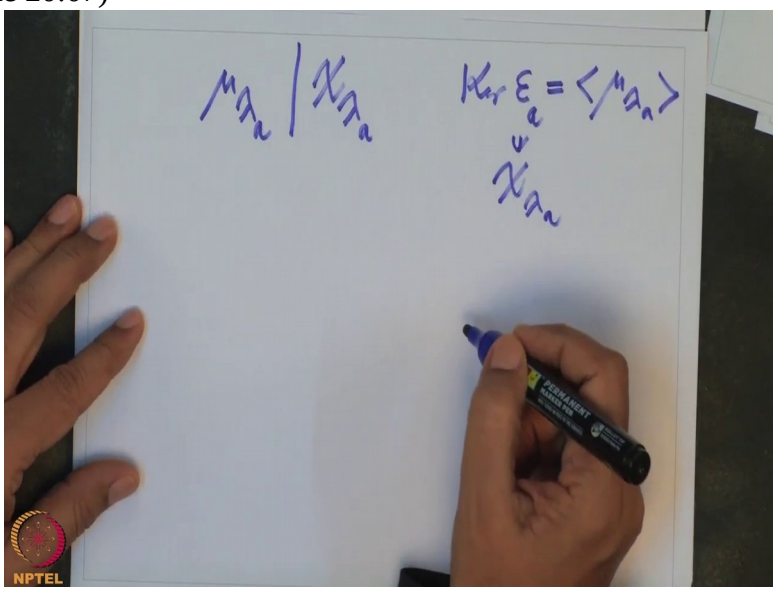
So therefore in any case, what we, what it checks is λ_a is algebraic, a is algebraic over K but minimal polynomial is the generator. So by definition mu of λ_a is the minimal polynomial. So minimal polynomial divide the characteristic polynomial and this kernel of, what did I call it, epsilon a homomorphism this is precisely generated by μ of λ_a

(Refer Slide Time 20:01)



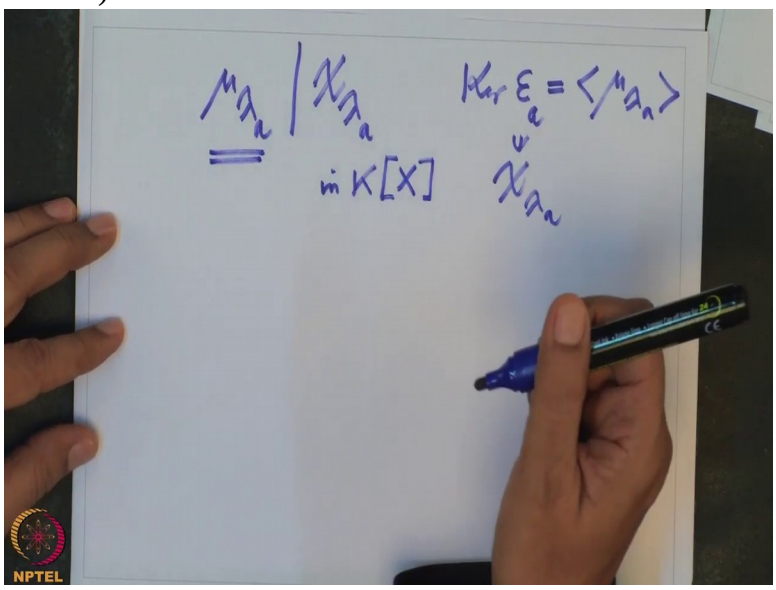
and χ of λ_a is an element here.

(Refer Slide Time 20:07)



So Therefore mu divide this in $K[X]$ and our problem is to find this. Because this will be the, this will give the degree of,

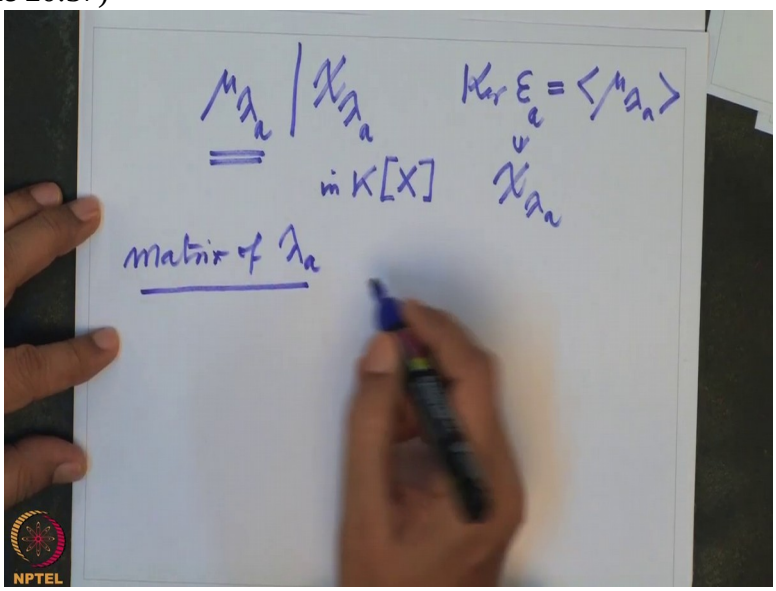
(Refer Slide Time 20:17)



this will tell us what degree polynomial A satisfies. So how do you find the minimal polynomial of the linear operator λ_a ?

I have to find the matrix of λ_a , and how do I find the matrix of λ_a ?

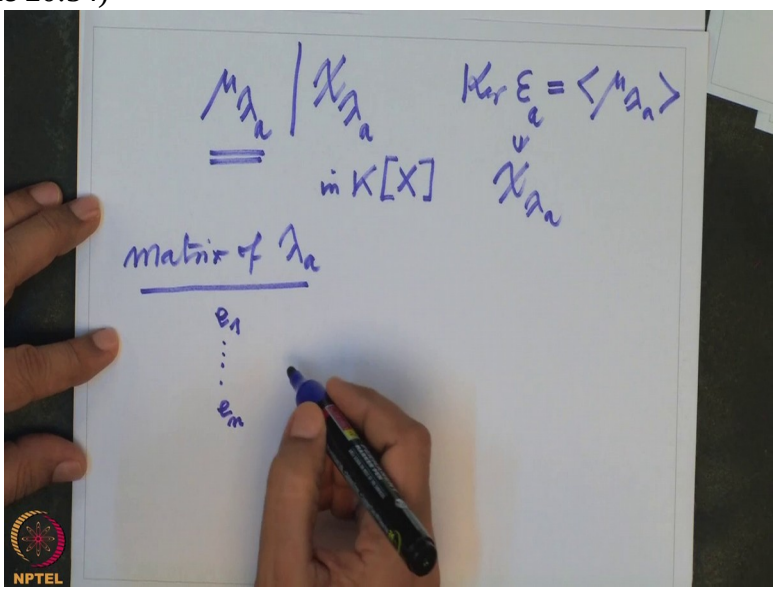
(Refer Slide Time 20:37)



I take a basis, fix basis and see where that basis goes and write down the matrix and find the minimal polynomial of that matrix.

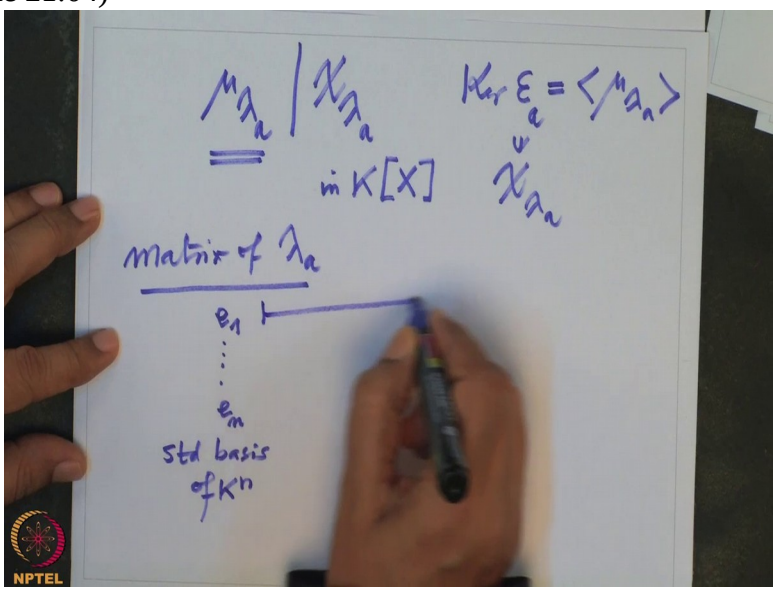
So therefore I will use the basis e_1 to e_n . This is the basis of that K^n

(Refer Slide Time 20:54)



standard basis, this is a standard basis of K^n , and I have to know where do these

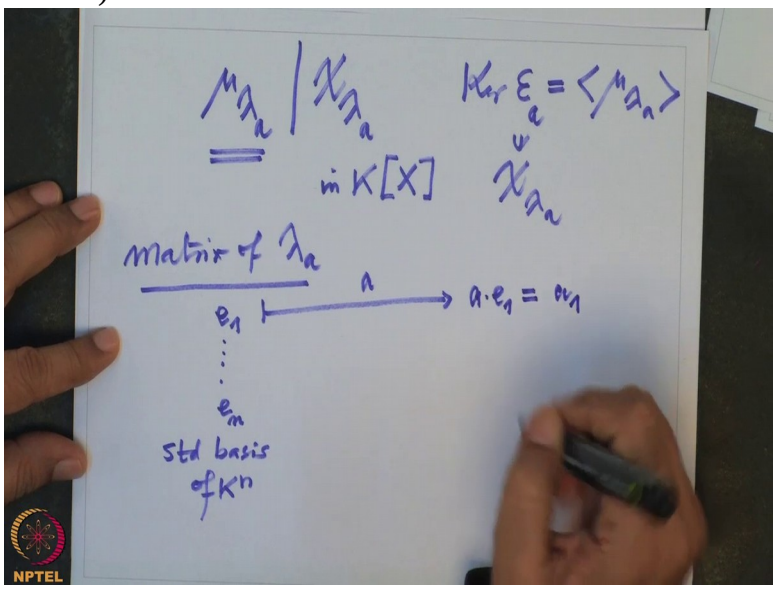
(Refer Slide Time 21:04)



go under multiplication by a? So under multiplication by a this goes to a times e_1 .

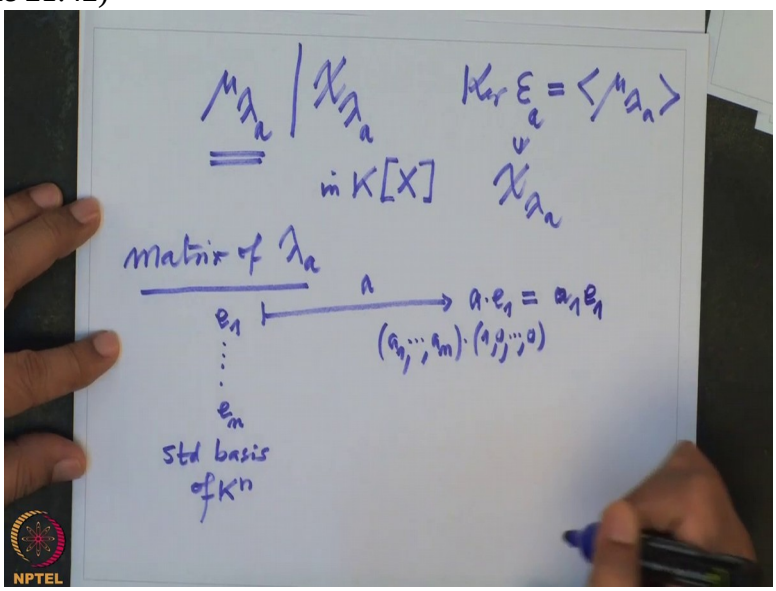
But a times e_1 is the first coordinate of a, a_1 .

(Refer Slide Time 21:15)



a times e_1 ,

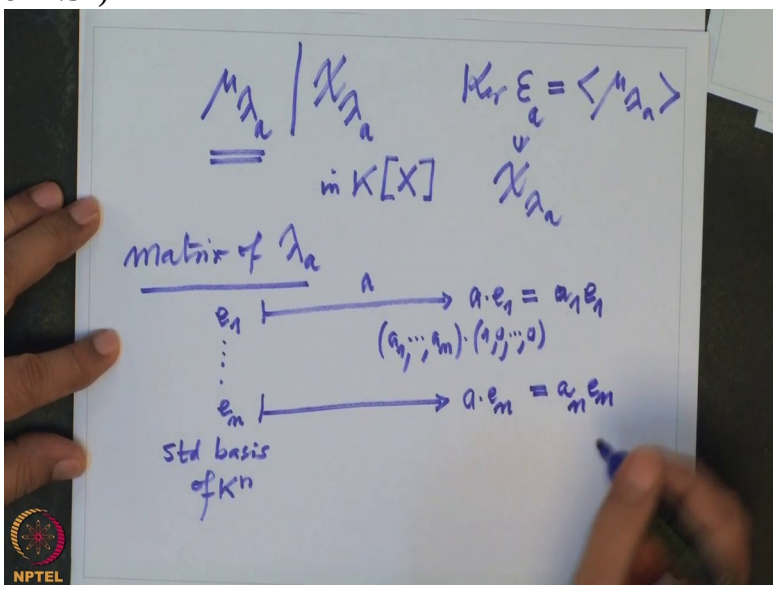
(Refer Slide Time 21:42)



so a_1 , a_2 n times e_1 , e_1 is $(1,0,\ldots,0,0)$. So this is $e_1 a_n$ and e_1 is $(1,0,\ldots,0,0)$. So when I multiply component wise I get only a_1 .

Strictly speaking I should write it as a_1 , a_1 times e_1 . So where do e_n go under multiplication by a? That is $a_n e_n$.

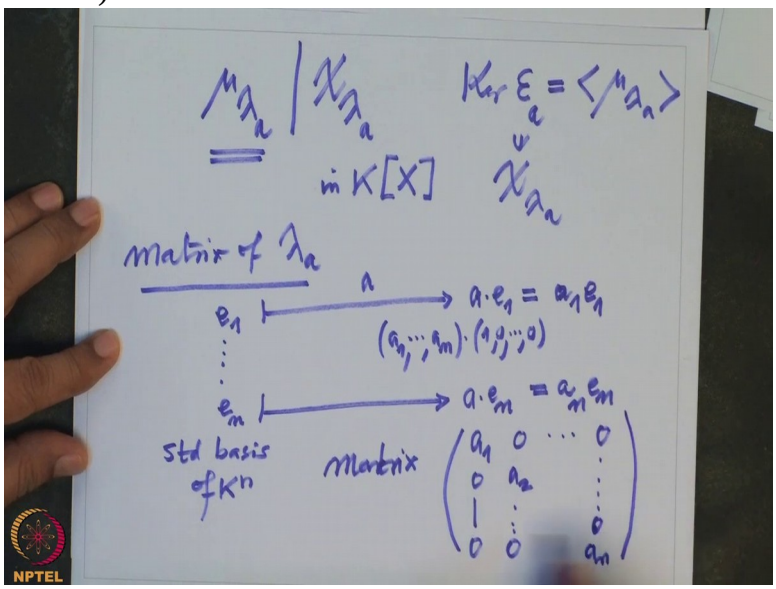
(Refer Slide Time 21:54)



That is how it goes. So what is the matrix? Matrix is therefore, the first vector should go to the column. So that is a_1 , e_1 only so $(0,..,0)$. Next one will go to $a_2 e_2$ so that is $(0,a_2,0,\ldots,0)$ and so on the last column is $(0,\ldots,0,a_n)$.

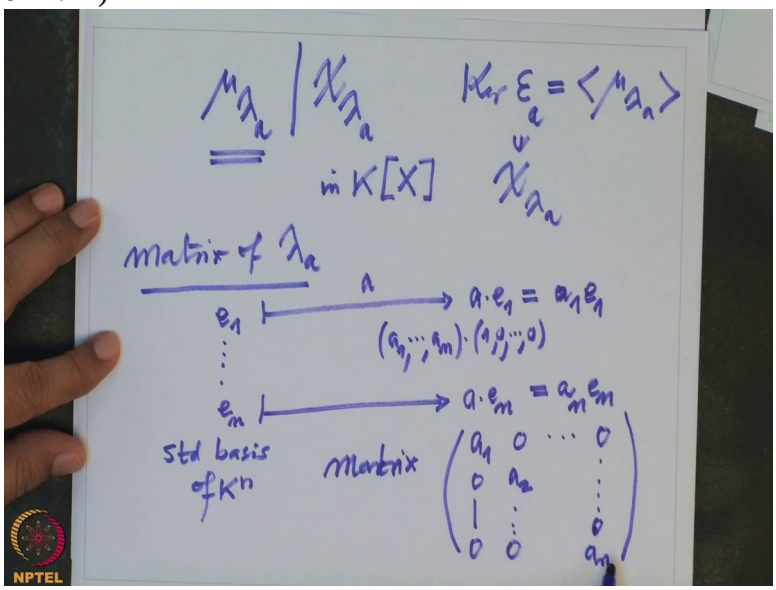
So therefore the matrix

(Refer Slide Time 22:22)



is a diagonal matrix where it is easy to conclude what is the minimal polynomial.

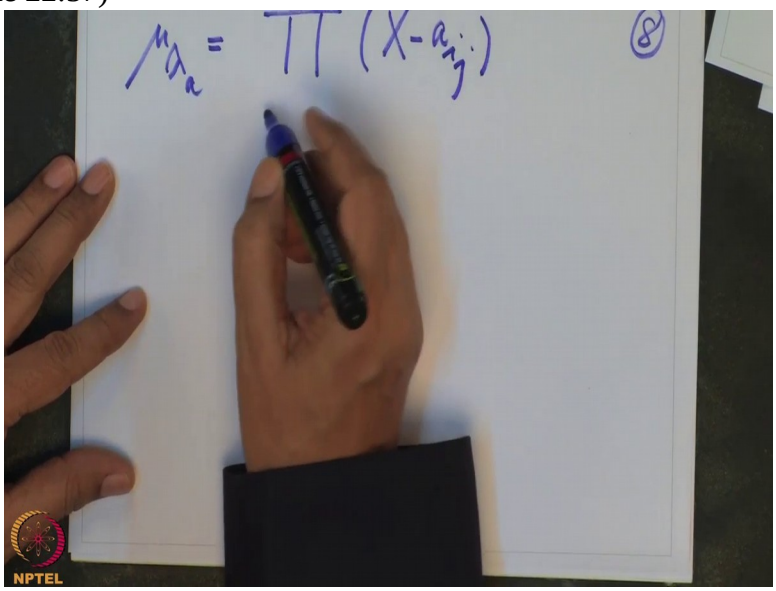
(Refer Slide Time 22:27)



And the minimal polynomial is precisely the product of the distinct factors. So I will write the answer on the next page.

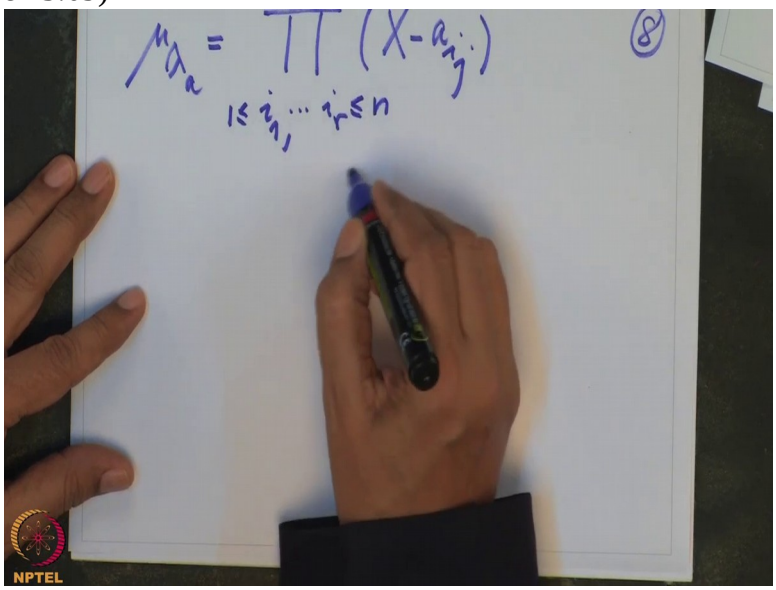
So the minimal polynomial therefore is, minimal polynomial of λ_a is product $X - a_{i_j}$ this product is running

(Refer Slide Time 22:57)



over $1 \leqslant i_1, i_r \leqslant n$

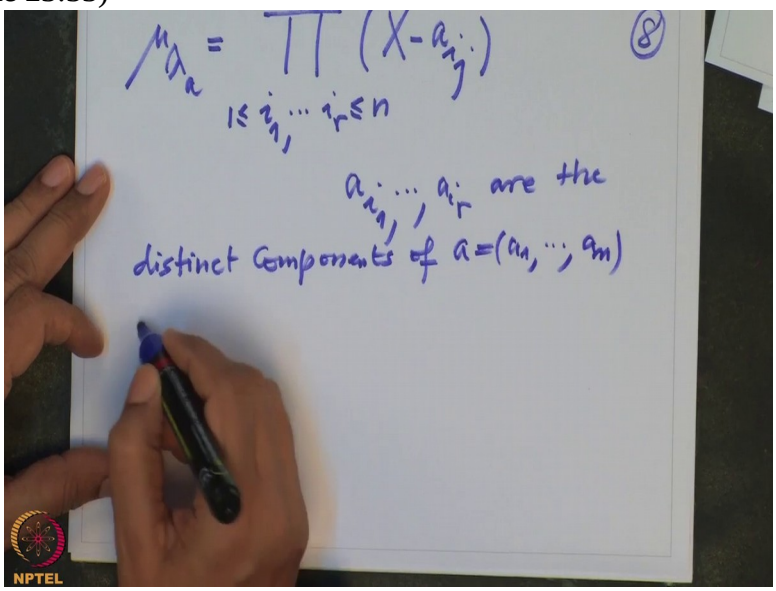
(Refer Slide Time 23:09)



where a_{i_1} to a_{i_r} are the distinct components of a which is a_1 to a_n .

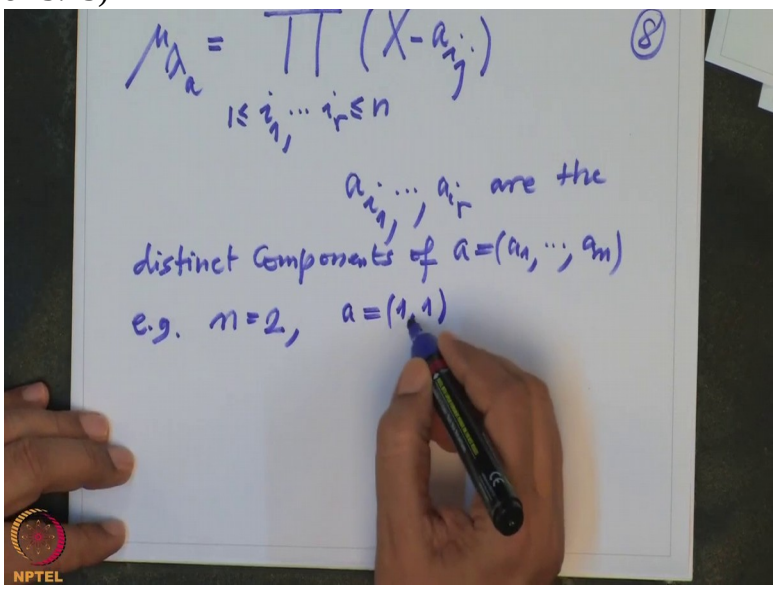
So for example

(Refer Slide Time 23:33)



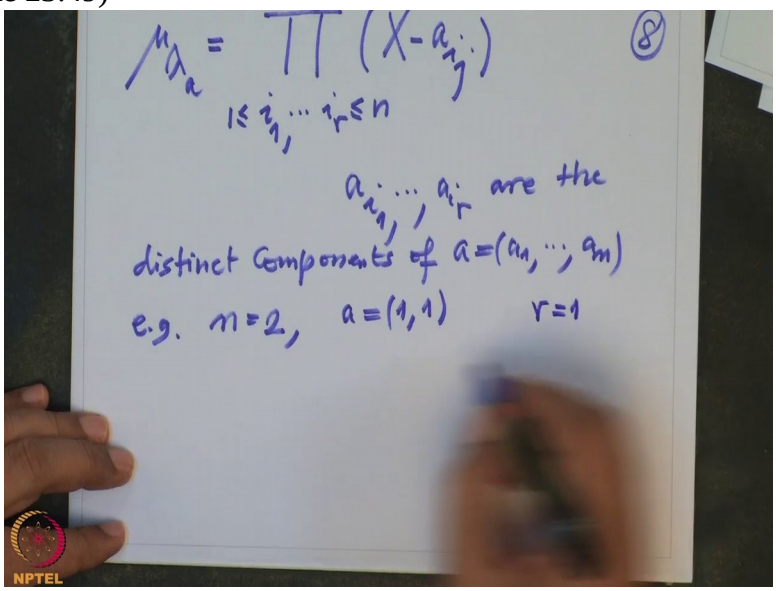
if I take n equal to 2 and a equal to $(1,1)$ then number of distinct components are only

(Refer Slide Time 23:45)



1, so r is 1 in this case and only

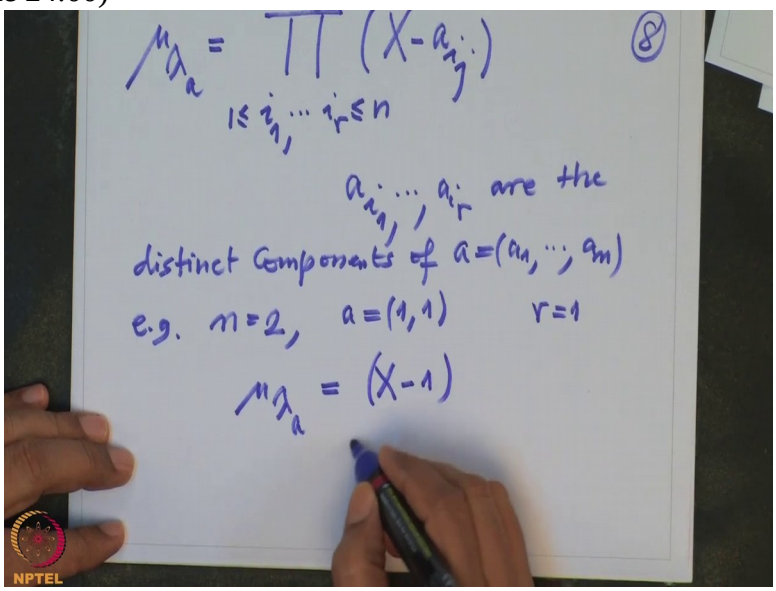
(Refer Slide Time 23:49)



1 a that is, and the minimal polynomial of lambda a will be just $X-1$.

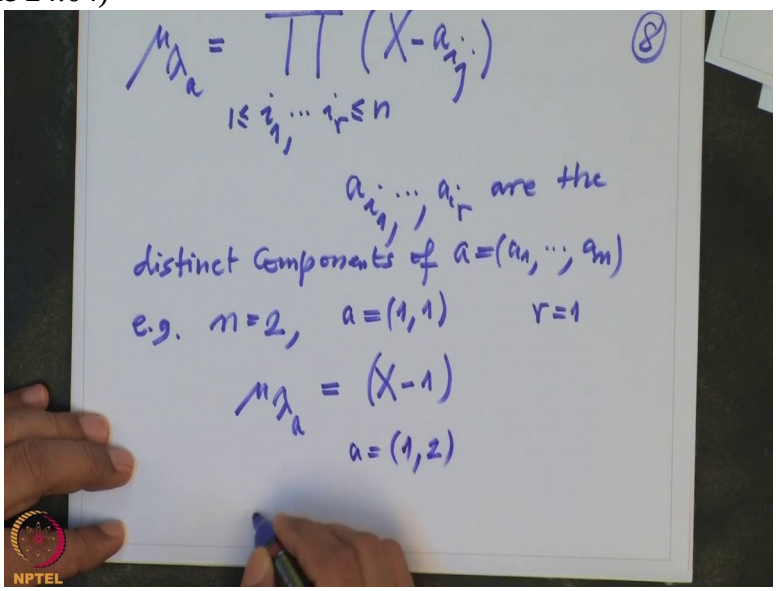
Where as if I take

(Refer Slide Time 24:00)



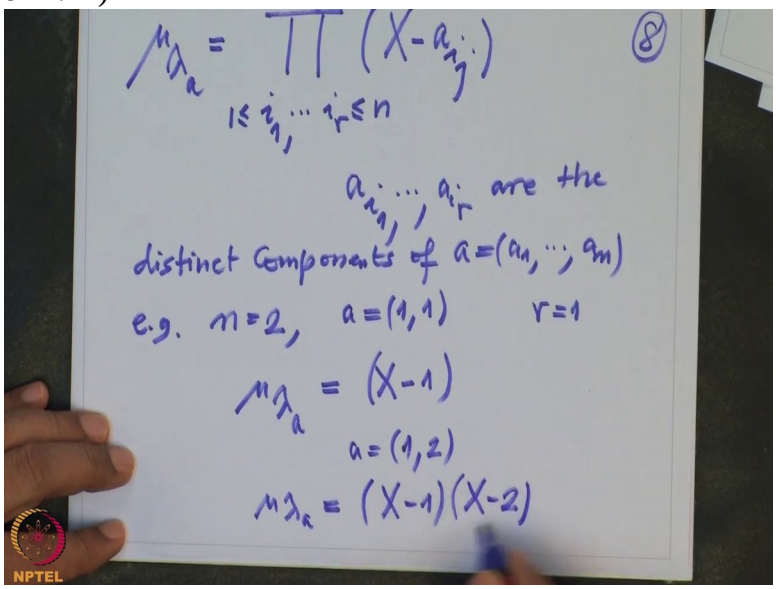
a equal to $(1,2)$,

(Refer Slide Time 24:04)



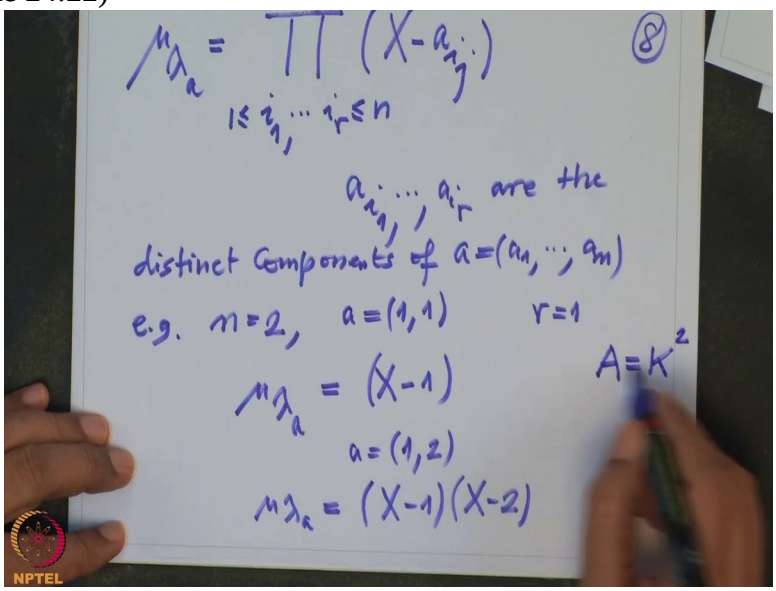
then the minimal polynomial will be equal to $(X-1)(X-2)$.

(Refer Slide Time 24:12)



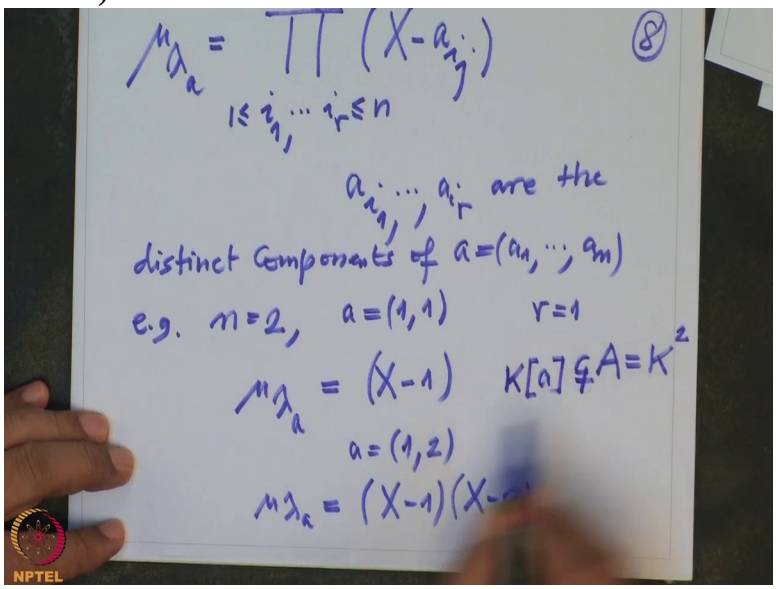
In this case the degree is 2; in this case the degree is 1. The algebra we are working with A equal to K^2 so this is two-dimensional.

(Refer Slide Time 24:22)



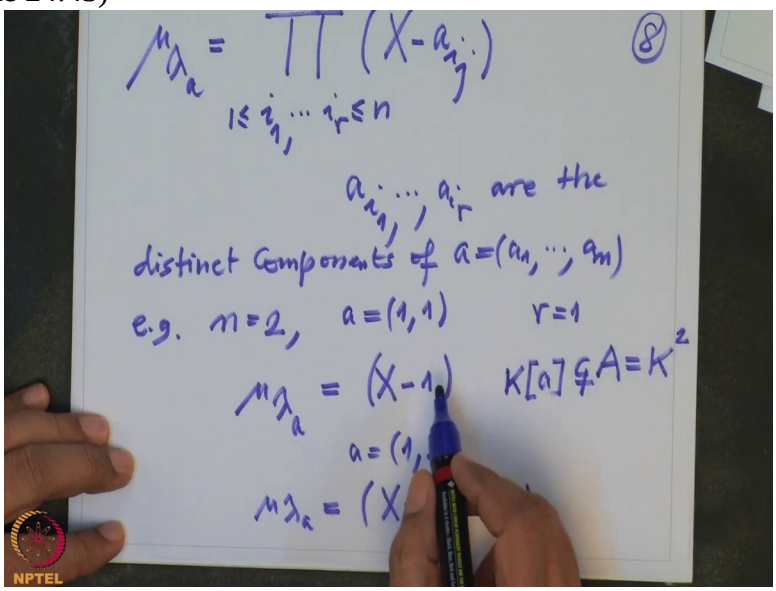
In this case the sub algebra generated by A will be just K a and this will be proper because

(Refer Slide Time 24:34)



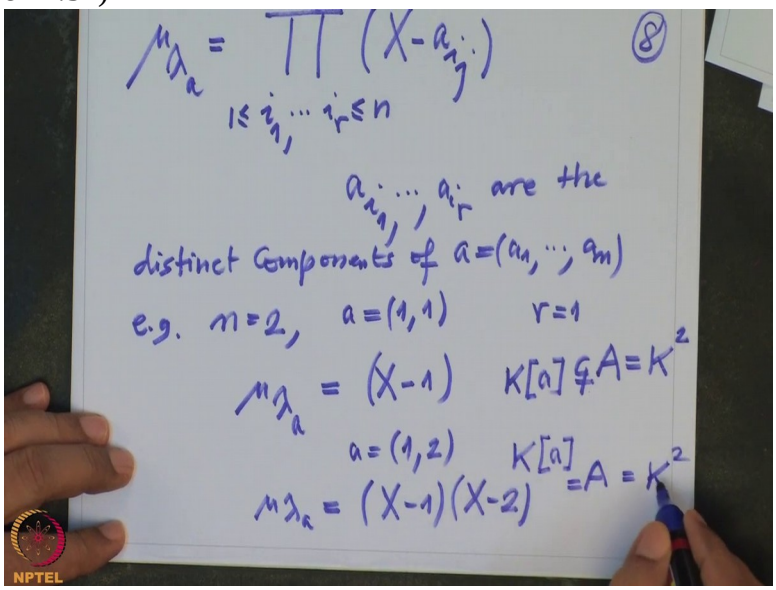
this is one-dimensional, and this is one-dimensional because of degree is 1 and we have seen sub algebra has a dimension equal to degree of

(Refer Slide Time 24:43)



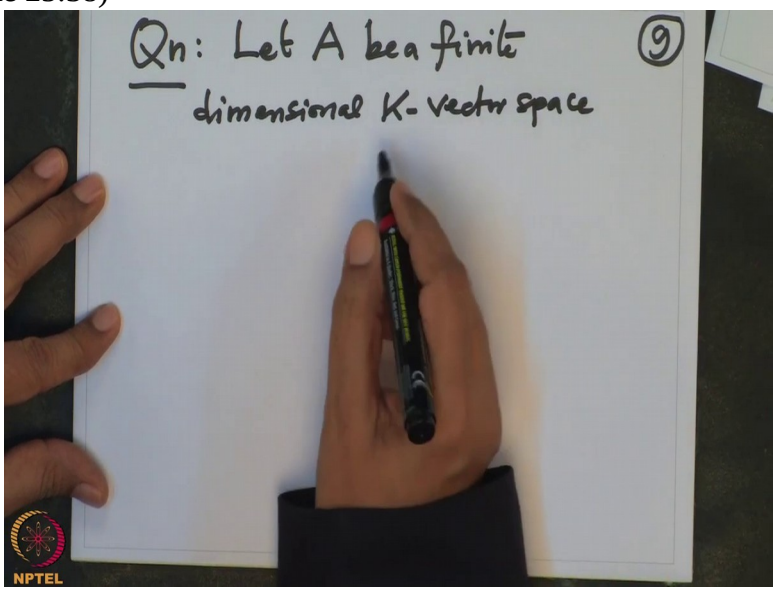
the minimal polynomial. So this is proper. In this case it is two-dimensional therefore it has to be equal. This will be equal to K a in this second example.

(Refer Slide Time 24:57)



So this is how we compute many things. Ok so this also tells us, this also asks the question, this also allows us to ask the question, so this is a question. So let A be a finite dimensional K vector space. Then we know

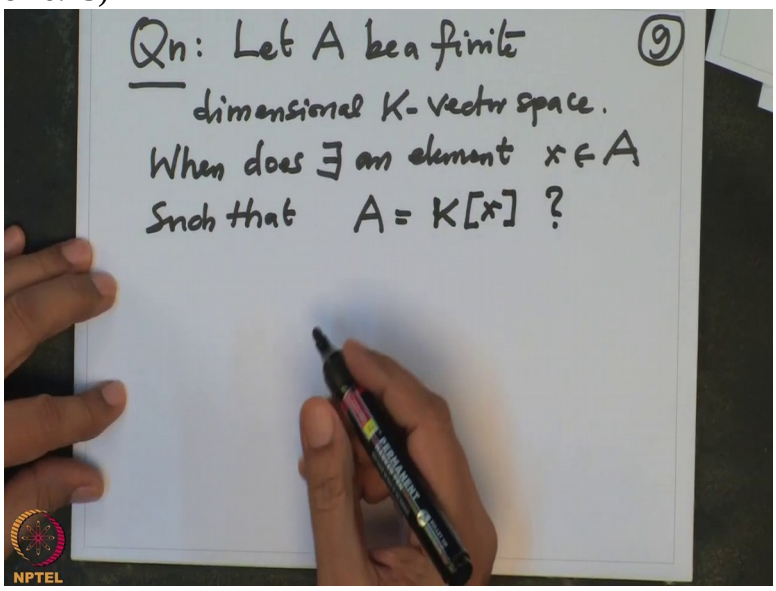
(Refer Slide Time 25:38)



that every element of A is algebraic over K. We know that.

Question is when does there exist an element small x in A such that A is equal to sub algebra generated by x? So

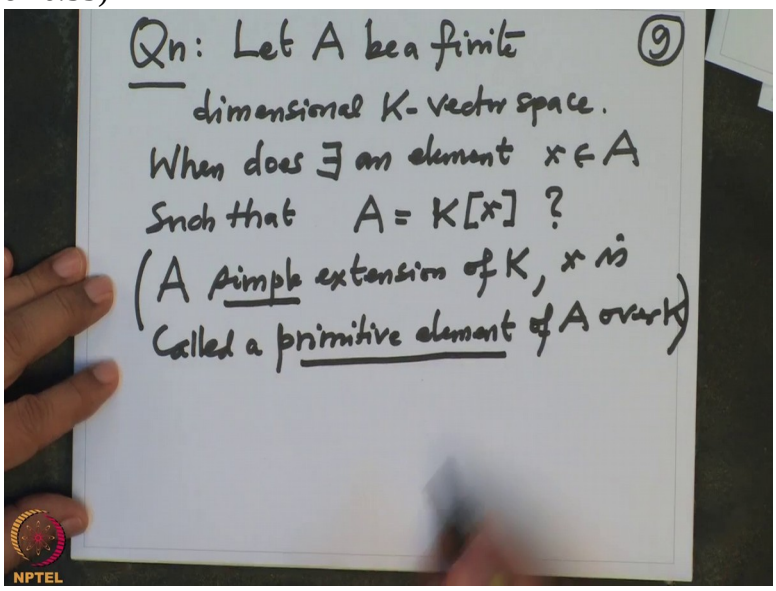
(Refer Slide Time 26:15)



such an element is called, so such a, such a A is called, such a A is called simple extension of K and that element x is called a primitive element of A over K.

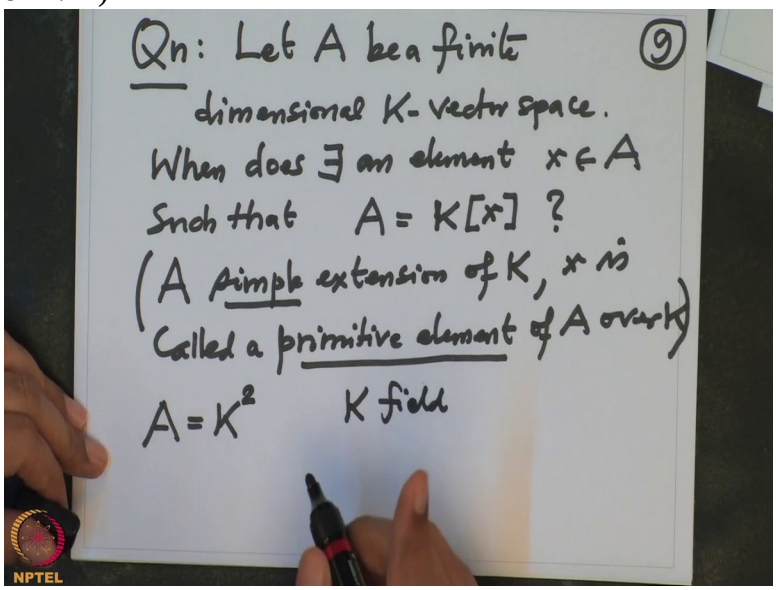
Simple extension and primitive element. And one of the main important observation of Galois that whenever K an extension of $\mathbb{Q}$, finite extension of $\mathbb{Q}$, they all have simple extension and they have a primitive element.

(Refer Slide Time 26:53)



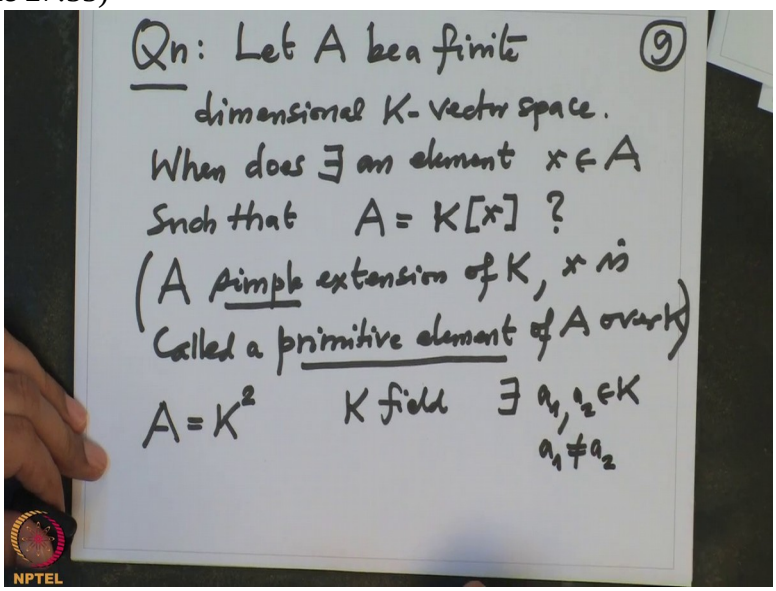
And one of the main problem in the Galois theory was how do you find that primitive element? And how do you use that primitive element to compute Galois groups? This is what we will also do. So in this case we know that in, in, in this case, in the two-dimensional case, field has at least 2 elements. So you can always find, for example $A = K^2$. K is a field. So field has at least 2 different elements.

(Refer Slide Time 27:44)



So there exists a 1 and a 2 in K which a 1 is not equal to a 2, then this is simple. We have just checked that this is simple because this is, as an algebra over K generated by a 1 a 2 where a 1 is not equal to a 2.

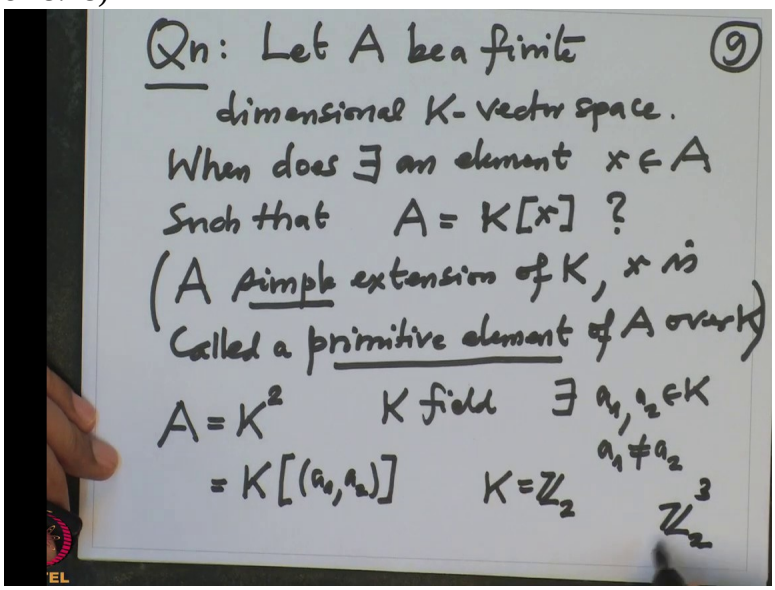
(Refer Slide Time 27:55)



But for example if you want to know whether, whether K^3 is always simple and you will need at least 3 elements different.

And obviously you can write down an example, where for example you can take a field $\mathbb{Z}_2$ and you can take $\mathbb{Z}_2^3$,

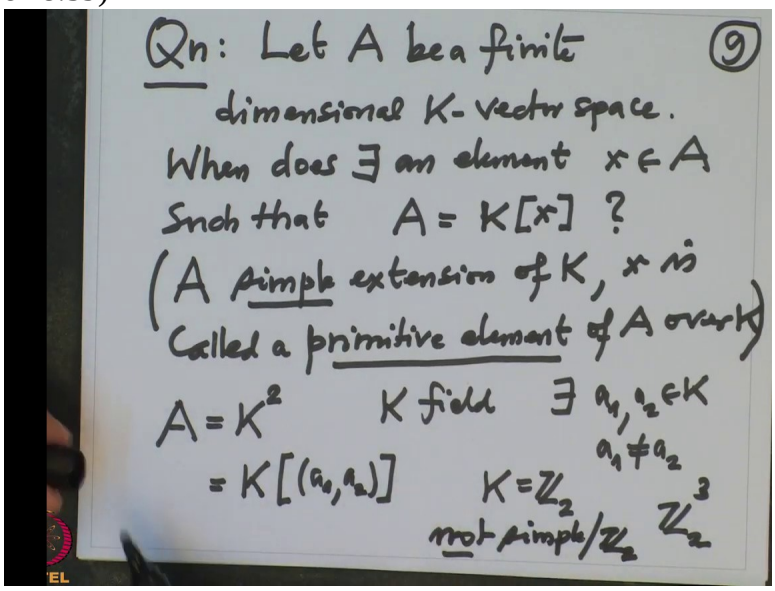
(Refer Slide Time 28:28)



then here no matter what you do, three tuples; at most 2 will be different. And then we know in that case the minimal polynomial can have at most degree 2.

It can never be degree 3 where as the dimension of algebra is 3. So such algebra is, this algebra is, for example, is not simple over $\mathbb{Z}_0$. So over a finite field it becomes

(Refer Slide Time 28:59)



more difficult. Ok, for finite field

(Refer Slide Time 29:03)

you will have to use something else. So I will take a break and then we will continue with this discussion.