INDIAN INSTITUTE OF TECHNOLOGY BOMBAY

IIT BOMBAY

NATIONAL PROGRAMME ON TECHNOLOGY ENHANCED LEARNING (NPTEL)

CDEEP IIT BOMBAY

COMMUTATIVE ALGEBRA

PROF. DILIP.P. PATIL
DEPARTMENT OF MATHEMATICS,
IISc Bangalore

Lecture No. – 14
Hilbert's Nullstellensatz

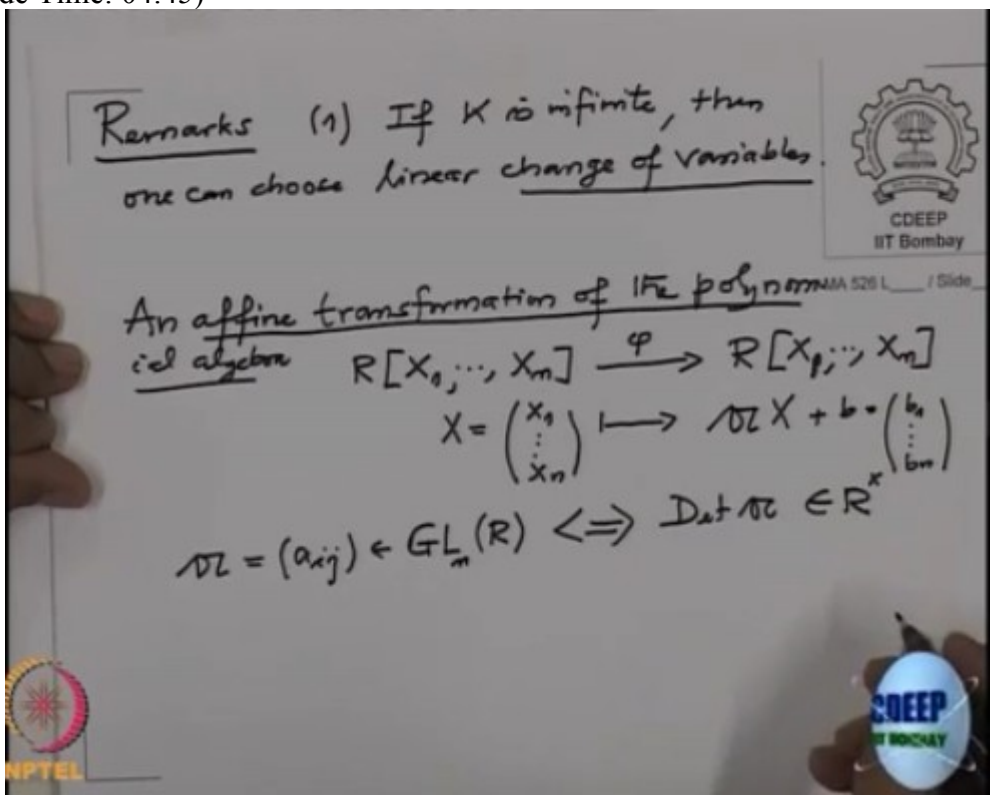
Okay, so I want to give couple of remarks on this proof. And then we will start reducing the corollaries, okay. So the first remark is, so remarks first one is see here in this proof we have never use any special structure of the field K, whether it is finite, infinite and so on, it works on arbitrary field.

If moreover if you assume that K is in infinite field, if K is infinite, then this change of variable, the automorphism we are define here it was not linear because it depended on the γ_i 's, the γ_i 's could be bigger, so but in case of infinite field one can choose linear change of variables, okay. For future we probably I want to say little bit more, so this change of variable time, so for example when one say the affine, an affine transformation of the polynomial algebra in, and not necessary over a field, so allow me to use arbitrary measuring, because what we've used it for a field, but the definition makes in for arbitrary measuring of $R[X_1,\ldots,X_n]$, affine transformation of the polynomial algebra over R means it's a map automorphism of special type X_1, ϕ , which is given by like this, so let us write capital X has a column X_1 to X_n .

So if I want R automorphism I just have to give values on capital X's, so I just have to tell you where this column goes, so this column let's say it goes to $AX+B$, B is also B_1 to B_n , and where these A is? A matrix, (a_{ij}) is a matrix, it's in $GL_n(R)$, clear? If the matrix is in $GL_n(R)$ means it has inverse, so over a wing it's complicated to check whether a matrix is in $GL_n(R)$, all that we have to check it determinant should be unity in, determinant of A should be unit in R.

In case of field we just have to check it is a nonzero function, so such automorphisms are called affine transformations of the polynomial algebra.

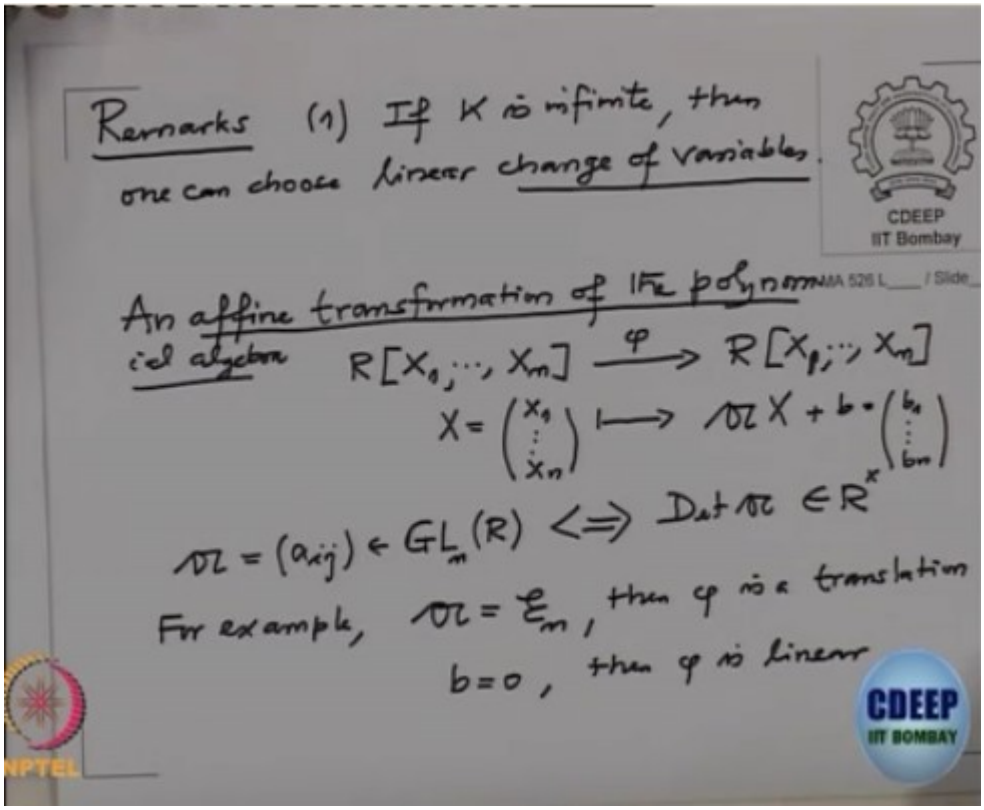
(Refer Slide Time: 04:45)



So for example, for example if you take the matrix A to be the identity matrix E_n, then this is translation, then it is ϕ is a translation.

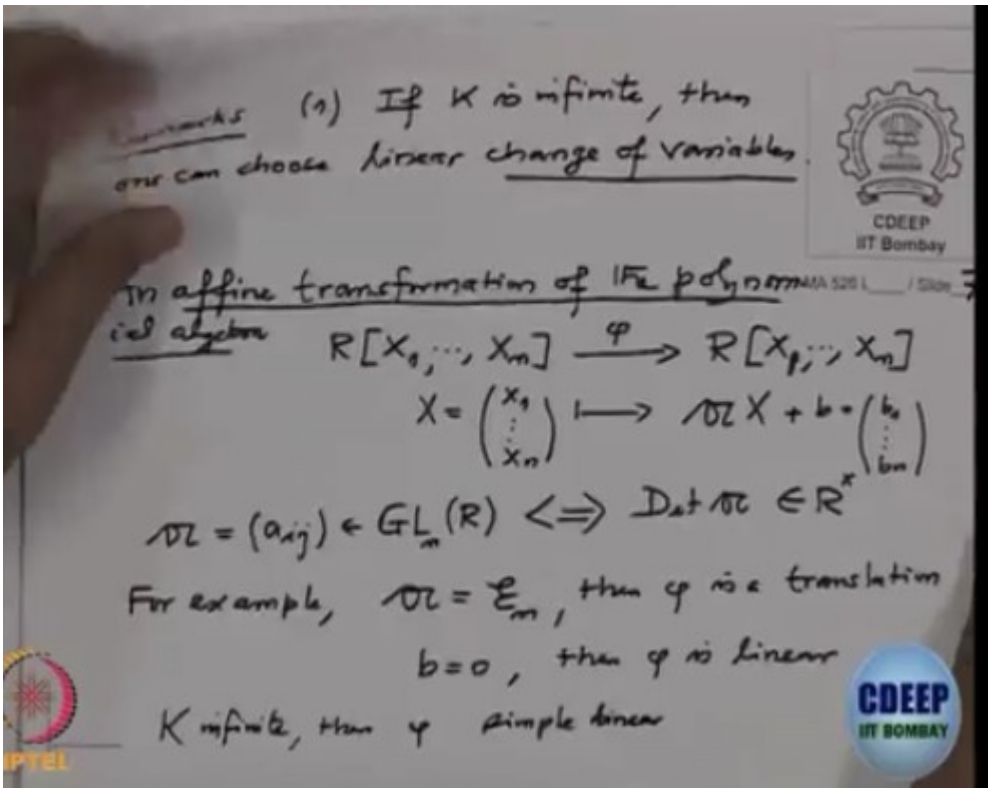
And on the other hand if B is 0, then it is linear.

(Refer Slide Time: 05:23)



See in our case if B is 0 but it's not linear, right, so these are not the automorphism we are given in the prove of lemma that is not of this type, but if you take, if you assume we're field to be infinite, then you can actually choose like a transformation.

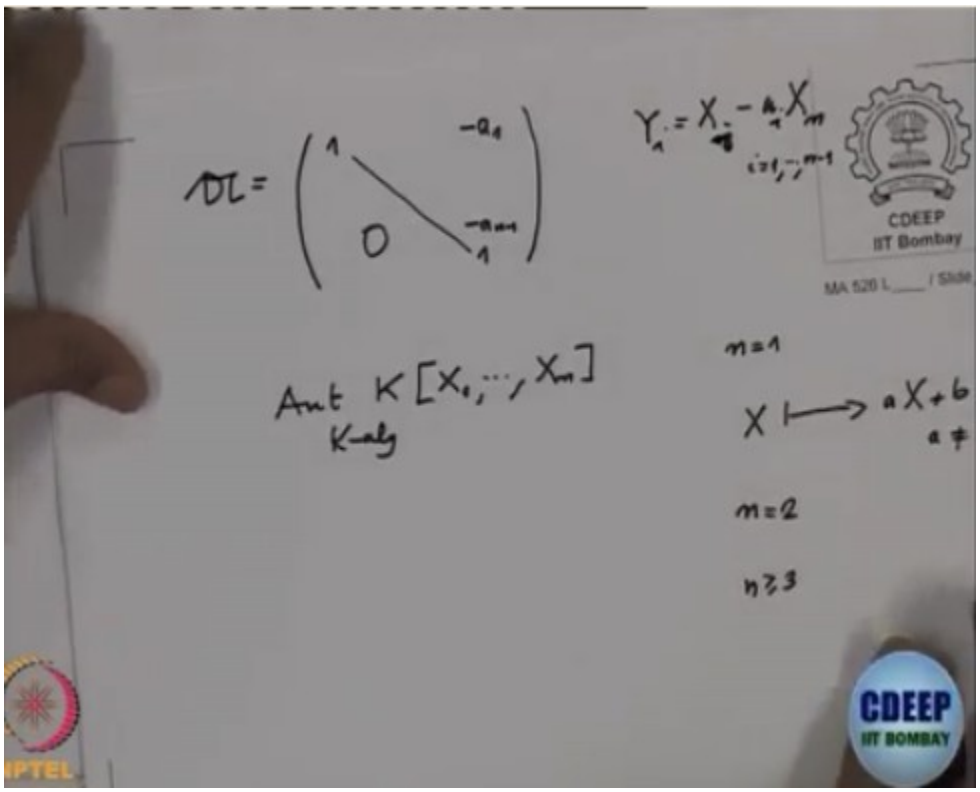
Actually so K infinite, then you can actually choose, then you can take ϕ to be what is called simple linear, so the matrix, so to give such a transformation I have to give a matrix,
(Refer Slide Time: 06:18)



so in that case you can take the matrix like this A = diagonal 1, below it is 0 and here you can take $-a_1$ so on $-a_{n-1}$, so that simply means you can take Y_i to be equal to $X_i - A_i X_n$, I someone to N units. See we have taken in the lemma $X_i - X_n$ power somebody, so if K were infinite then you can get away with this small such linear one and clearly this matrix is you can see, it's a nice matrix, such transformations are called simple.

In general it is the group of odd, if I write this odd even for a field $K[X_1,\ldots,X_n]$ as K algebra, so K algebra automorphism of the polynomial algebra over a field in n variables, this is your group, and these group is very complex shown as n, for example it is easy to see when N =1, what are the automorphisms of K algebra automorphism of polynomial in 1 variable that is very easy, they just tell affine linear ones, they're off the type X going to AX+B, and A is nonzero, so that's very easy to check for n = 1.

Already n =2 it's a difficult task, and your $n \geq 3$ it's even more difficult, and even $n \geq 3$ it's an open question, so what is the structure of this group?
(Refer Slide Time: 08:36)

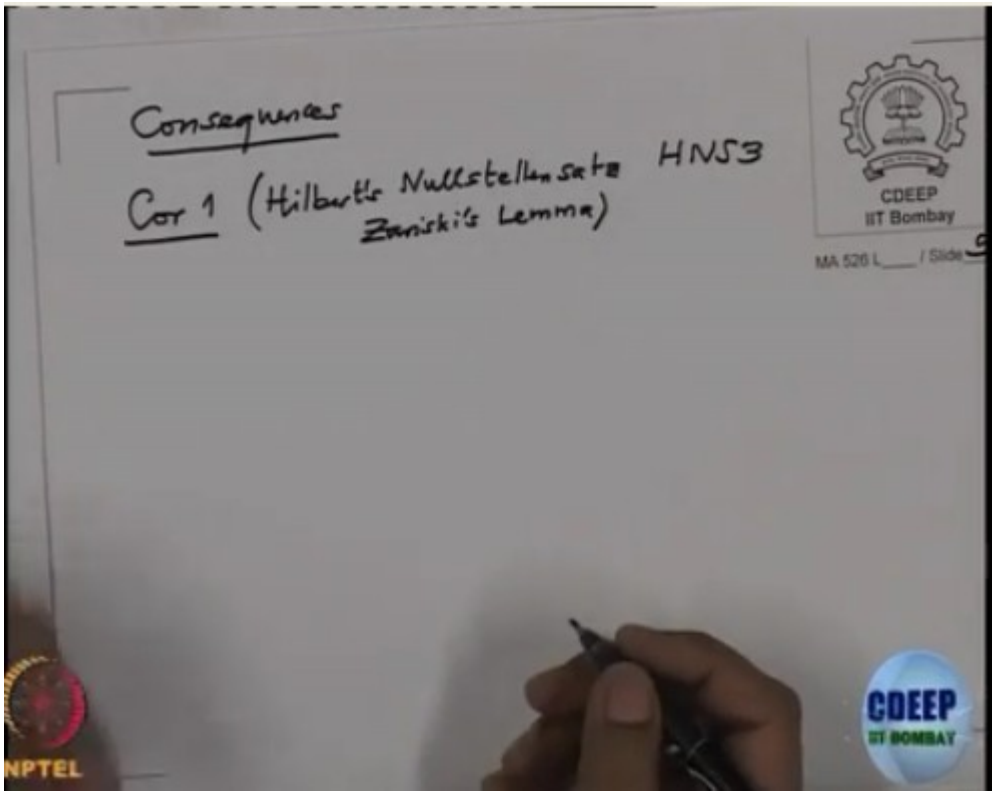


And n = 2 is also quite difficult but known, okay.

So now let us draw some consequences already from the classical version, and then we will go on to prove the more complicated one which is due to Nagata which was proved in 60's. So now, so consequences, these consequences have lot of geometric meaning, so but I want to do that geometric meaning after I have little bit language from the geometry.

So today there will be only the algebraic consequent, written in terms of algebra, so corollary 1, this is one form of, this is also called algebraic version of Hilbert's Nullstellensatz, so Hilbert's Nullstellensatz, this is, I'll abbreviated as HNS, and just I'll give some number, 3, this numbering comes from the way I've arranged the lectures sometime back, so this is also called Zariski's lemma,

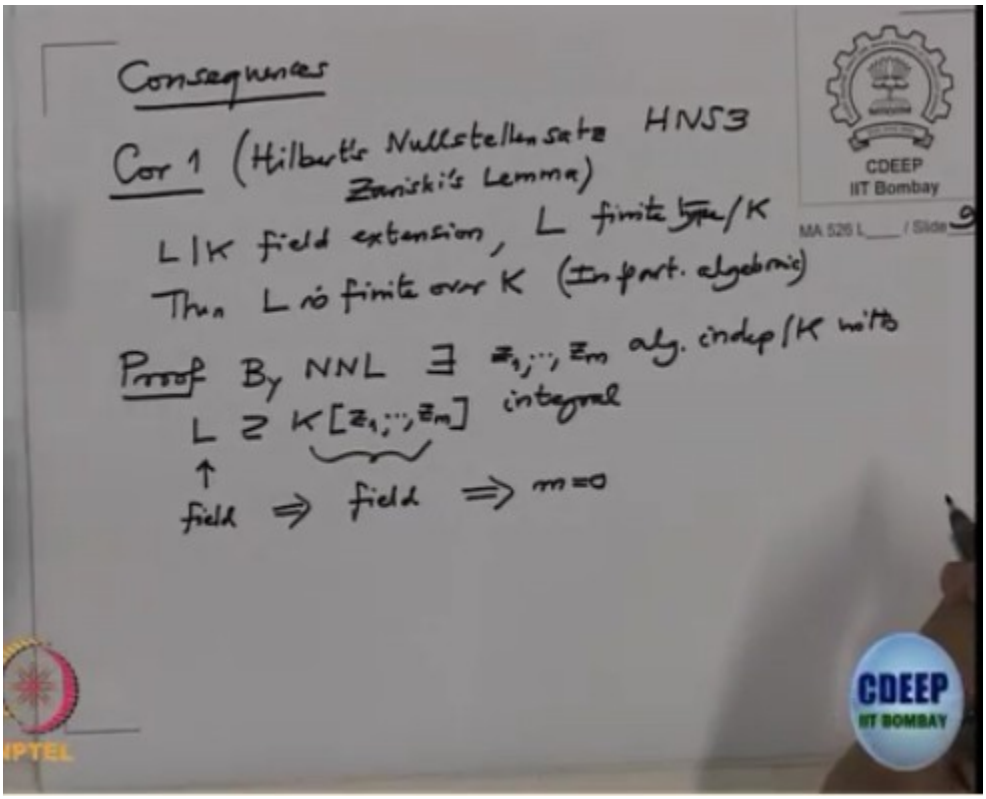
(Refer Slide Time: 10:28)



it says if you have a field extension L or K with field extension, and L is finite type over K, L is algebra of finite type over K, then L is actually finite, L is finite over K, so in particular algebraic, in particular algebraic over, okay, finite extensions are algebraic.

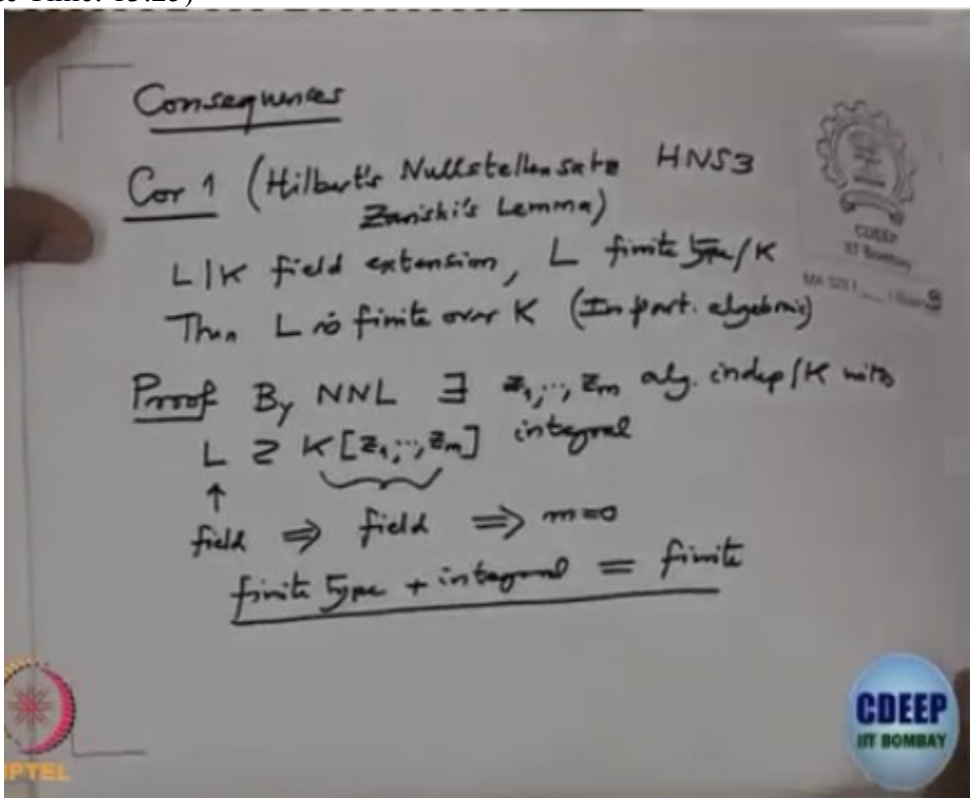
So proof, alright, so by NNL, L is the finite type over K therefore by NNL there exists LMN $z_{1,\dots},z_n$ such that L is integral over the sub algebra generated by this, and this elements are algebraic independent, so there exists $z_{1,\dots},z_n$ algebraically independent over K with L containing this is integral, integral, L integral over $K[z_1,\dots,z_n]$, but L is a field, this is a field and this is a polynomial algebra, and if a field is integral over summering then you would have seen that z_1 is also field, so therefore this is also field , so this is a field, because it's integral, but when can such a polynomial algebra be a field? The only chance is when m is 0, so that implies m is 0. And so that means L is integral over K, but integral in case of basis field in same thing as algebraic,

(Refer Slide Time: 12:59)



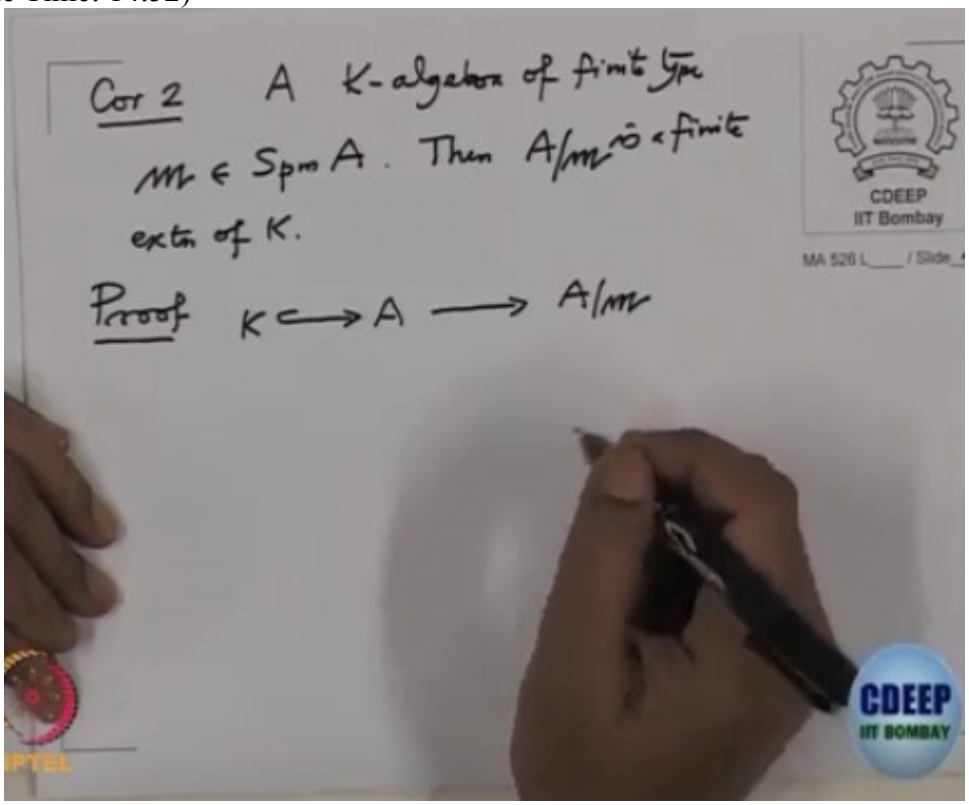
but and it's finite type, finite type algebraic is finite, so finite type, actually finite type + integral, this is equivalent to finite.

(Refer Slide Time: 13:25)



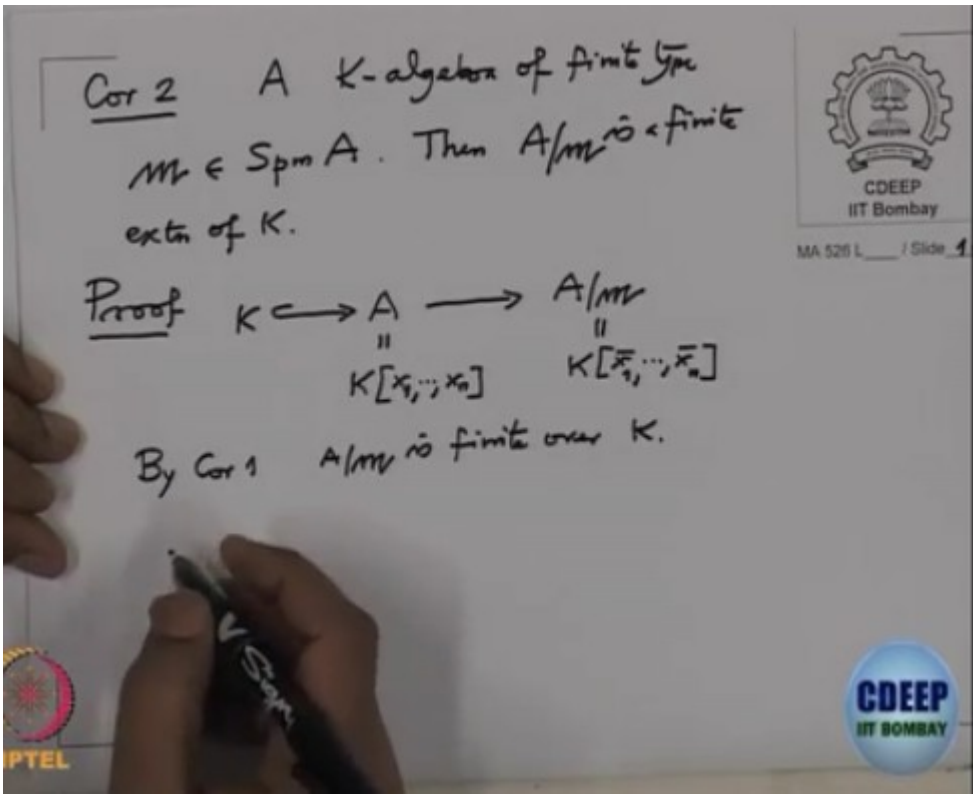
Okay, the next one corollary 2, suppose is A is finite type, A is algebra of finite type, and suppose m is a maximal ideal, m belongs to SPM A, then the residue field $\frac{A}{m}$ is finite extension of K. Proof, see A is algebra finite type so A is here, this residue field is $\frac{A}{m}$ is here, K is here, K contain, K is contained in A, this is finite type, so therefore this is also finite type over K, the images of algebra generators of A will generate $\frac{A}{m}$ as a algebra,

(Refer Slide Time: 14:52)



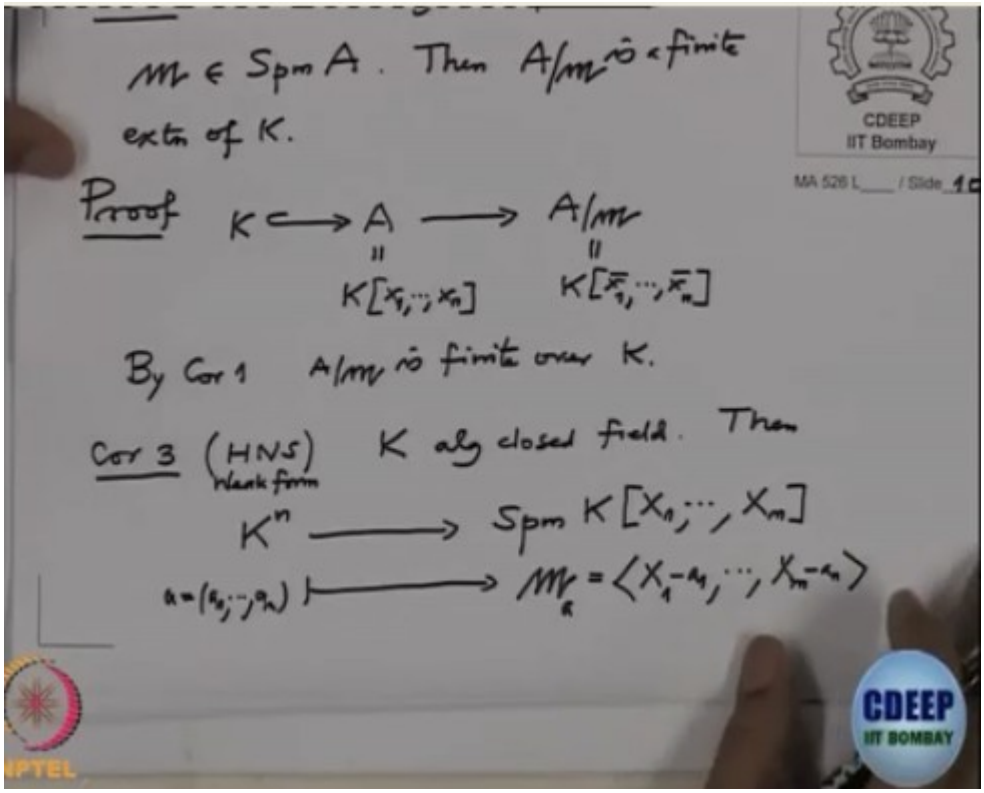
so if this is generated by this small elements $x_1, \ldots, x_n$ then there images, further images they will generate $\frac{A}{m}$, so this $\frac{A}{m}$ is also a finite type over K, and the earlier corollary says in this case this is an algebraic extension, that's what we wanted to proof finite, so by corollary 1 $\frac{A}{m}$ is finite over K, okay.

(Refer Slide Time: 15:32)



Corollary 3, so this I will call, this is also called weak form of HNS, I'll not give the number now, when I write the notes I'll give you the number properly, so this is weak form, K is an algebraically closed field, then we have a map from K^n to SPM of $K[X_1,\ldots,X_n]$, maximal ideals in $K[X_1,\ldots,X_n]$ namely if I have a tuple a is $(a_1,\ldots,a_n)$, then apply to m_a, m_a is the ideal generated by $X_1-a_1,\ldots,X_n-A_n$, note that clearly this is maximal ideal,

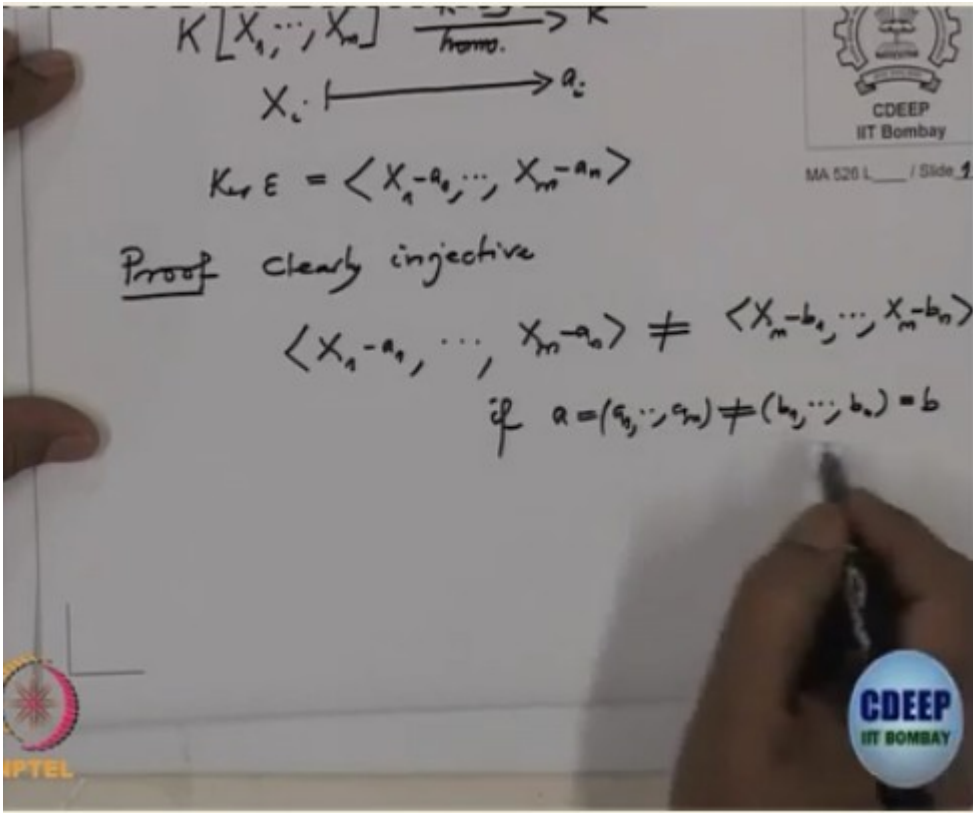
(Refer Slide Time: 16:53)



that is because the easiest way to see that is, let me go to the next one, so the easiest way to say that look at the evaluation map $K[X_1,\ldots,X_n]$ to K, and the K algebra homomorphism is XI going to A, this is K algebra morphism, and kernel let's call this as ϵ, kernel of ϵ is precisely generated by $X_1-a_1,\ldots,X_n-a_n$, and it's clearly subjective, therefore this mod kernel is actually the residue field is K, so it's not only maximal ideal but it's residue field is K, okay.

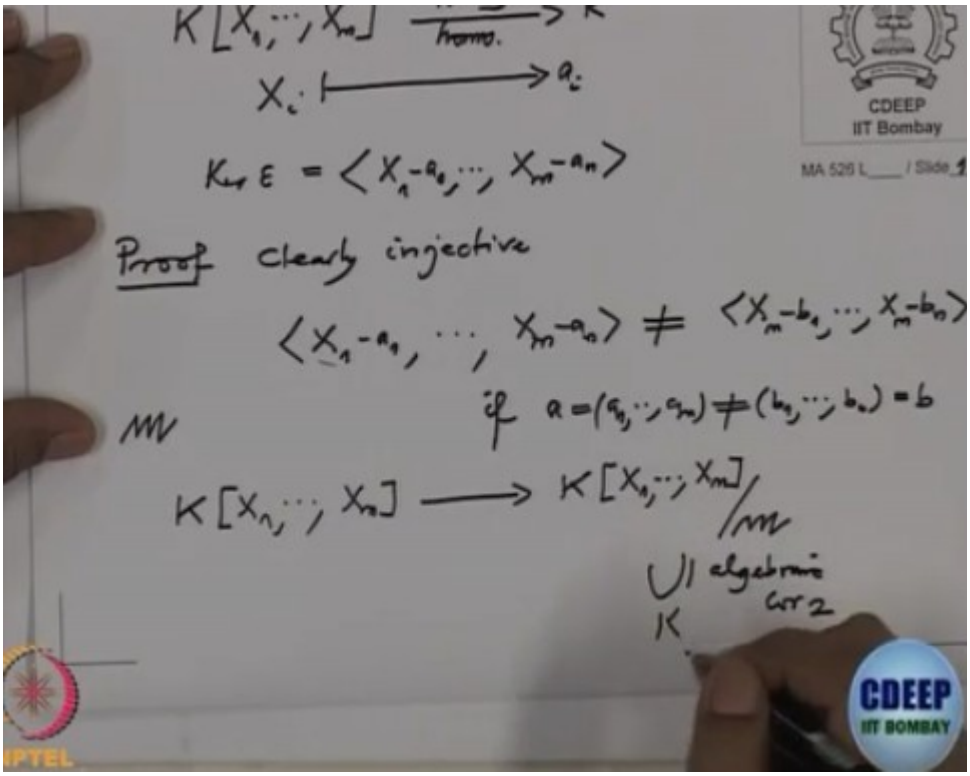
So we want to prove this map is, then the map is bijective that is assumption, so proof this map is clearly injective, clearly injective, simply you have to check that the ideal generated by $X_1-a_1,\ldots,X_n-a_n$, and if you take a different point $X_1-b_1,\ldots,X_n-b_n$ these are different if $a=(a_1,\ldots,a_n)$ is different from $(b_1,\ldots,b_n)$, this is clear because if they are different at least one of the component is different

(Refer Slide Time: 19:01)



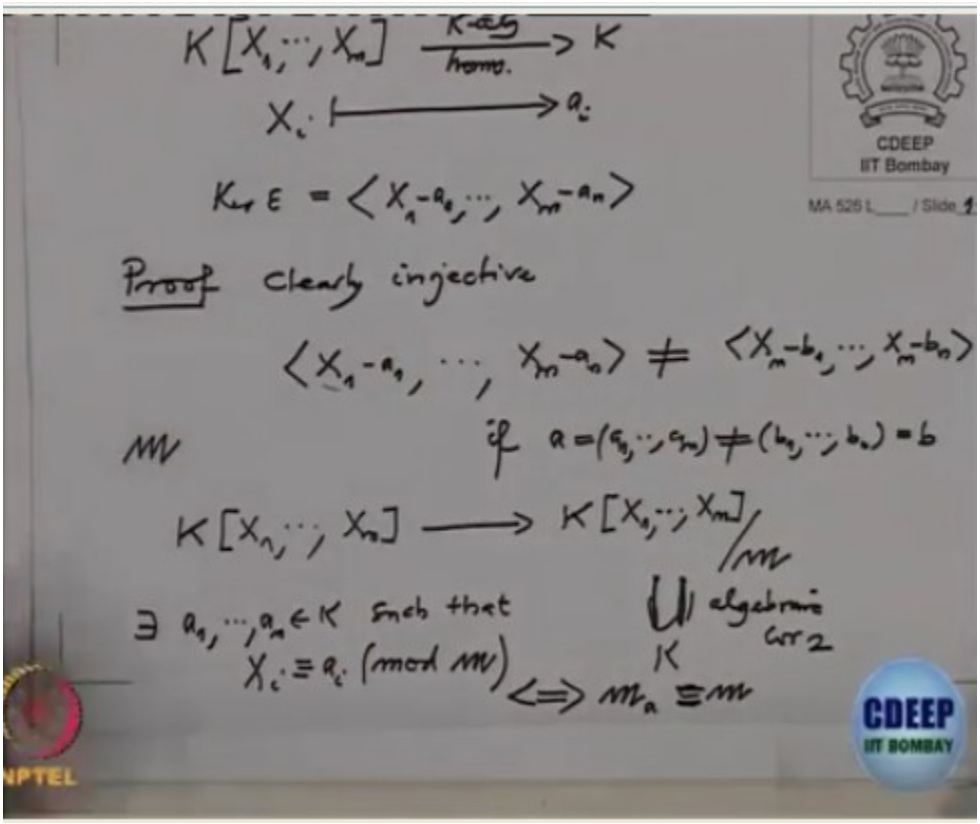
and then the difference if this ideals were equal then it will contain both the polynomials X1, let's say without dash, without loss a_1 is different from b_1, then this if there were equal then this and this polynomial both are there, so there difference is there so $a_1 - b_1$ is there, but $a_1 - b_1$ is different, then 0, so it's unit and therefore it's not possible, so clearly it is injective, so injective because look at the map $K[X_1, \ldots, X_n]$, so take any maximal ideal m and take, look at this map $K[X_1, \ldots, X_n]$ and then go mode it, this is the natural subjection and then we have, because K is algebraically closed we are assuming this extension, this extension is algebraic that is what we approved in corollary 2, because this is algebra of finite type, this is maximal ideal mode, so this is finite type field over K, but K is algebraically closed, so there is no algebraic extension rather than itself,

(Refer Slide Time: 20:16)



so it's equality here, but then there exists $a_1, \ldots, a_n$ in K such that they are the lift of this so $X_i - a_i$ or X_i is congruent to A_i mod m, but that is equivalent to checking that this point ideal m_a, I wrote now, reading are this m_a is contain in m, but this is maximal, so equality here, so that proves that each maximal ideal is coming from point, such maximal ideals are called points.

(Refer Slide Time: 20:14)



So I think it's time, we will stop here and I will continue more consequences in the next time, because we should see the power of this normalization lemma, so one more lecture I will lead for consequences and then we will go on to the more stronger version of normalization lemma which is due to Nagata.

Prof. Sridhar Iyer

NPTEL Principal Investigator
&
Head CDEEP, IIT Bombay

Tushar R. Deshpande
Sr. Project Technical Assistant

Amin B. Shaikh
Sr. Project Technical Assistant

Vijay A. Kedare
Project Technical Assistant

Ravi. D Paswan
Project Attendant

Teaching Assistants

Dr. Anuradha Garge **Dr. Palash Dey**

Sagar Sawant **Vinay Nair** **Pranjal Warade**

Bharati Sakpal
Project Manager

Bharati Sarang
Project Research Associate

Riya Surange **Nisha Thakur**

Project Research Associate **Sr. Project Tehnical Assitant**

Project Assistant
Vinayak Raut