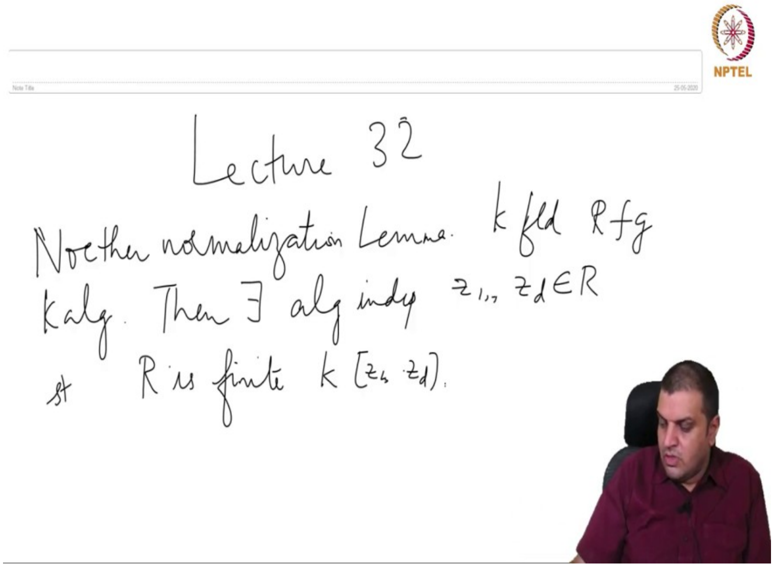
Computational Commutative Algebra
Prof. Manoj Kummini
Department of Mathematics
Chennai Mathematical Institute

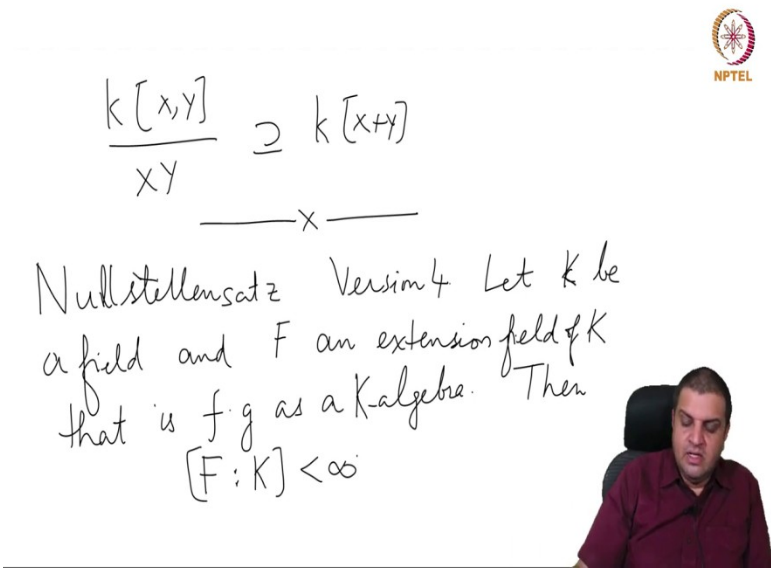
Lecture – 32
Noether normalization lemma – Part 1

(Refer Slide Time: 00:13)



This is Lecture 32. So, in the last lecture we saw Noether normalization lemma, k field, R finitely generated k algebra, or in other words finite type k algebra. Then, there exist algebraically independent $z_1,\ldots,z_d \in R$ such that, R is finite over the sub algebra $k[z_1,\ldots,z_d]$. So, this is isomorphic to a polynomial ring and R over this is finite.

(Refer Slide Time: 01:14)

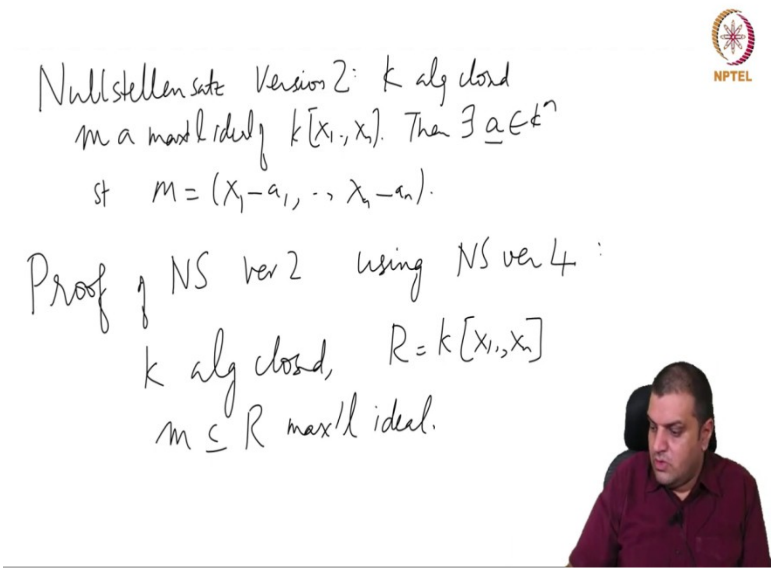


So, we can go back to one of the earlier examples that we had this. So, we can think of the sub algebra $k[x+y] \subseteq \frac{k[x,y]}{xy}$, And this is an example of Noether normalization. So, now, we will prove Noether normalization lemma in a little while, but before that we want to prove the Nullstellensatz.

So, first we will start with a statement. We will call it Nullstellensatz version 3 or version 4. We started with first version, which said something about $V(I)$ being empty. The second version was about maximal ideals. Third version was what we called classical Nullstellensatz or Hilbert's-Nullstellensatz was about the radical of the ideal. And, now we are in version 4. Let K be a field and F an extension field of K that is finitely generated as a K-algebra.

Remember, K to F is a ring homomorphism. And here, we are saying it is finitely generated as an algebra. Then, F is a finite extension field of K that is it is a finite extension. So, it is not at all clear what this has to do with Nullstellensatz and why it is even called a version of Nullstellensatz, so which we will prove now.

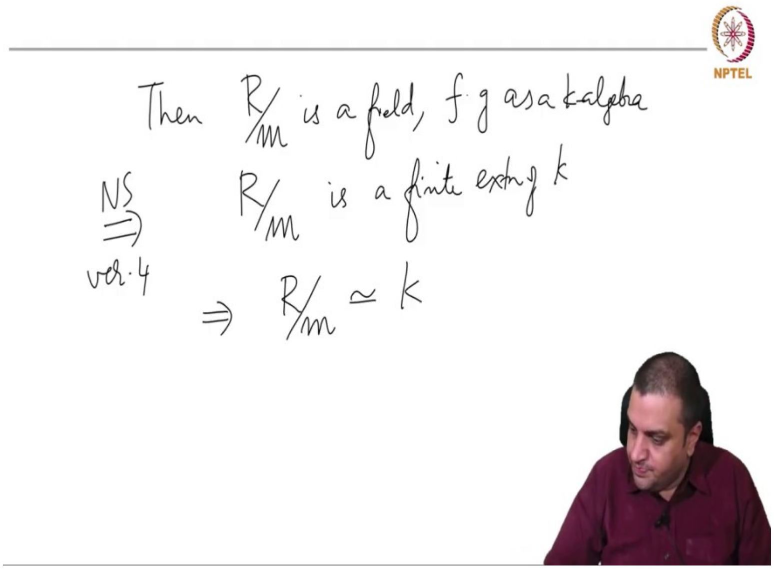
(Refer Slide Time: 03:45)



So, remember version 2 of Nullstellensatz was that k algebraically closed, m a maximal ideal of $k[X_1,\ldots,X_n]$ then there exist some $a \in k^n$, such that $m=(X_1-a_1,\ldots,X_n-a_n)$. This is a version 2. So, now we will prove version 2 using Nullstellensatz version 4.

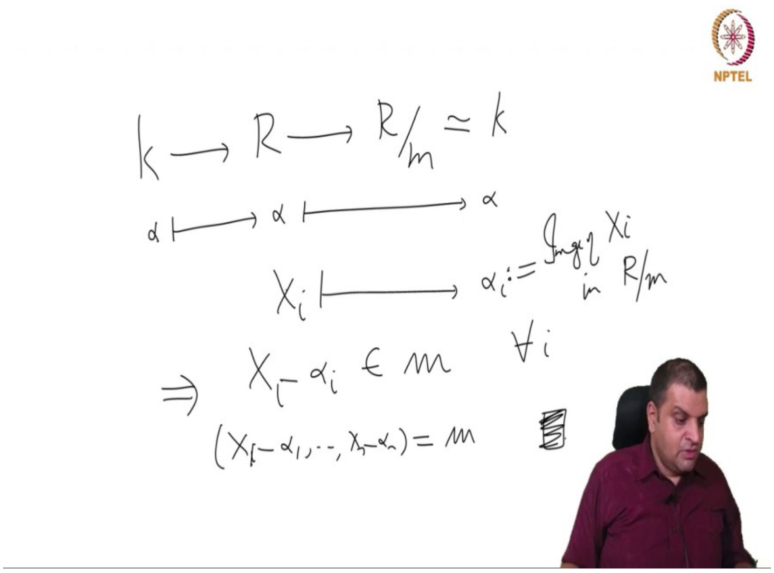
So, this is really I mean, Nullstellensatz was stated as a theorem about zeros of polynomials, this does not look at all anything at all like that, but we would still call it a version of the Nullstellensatz. So, let us we are in this setup. So, let $F=\frac{R}{m}$. So, let R be the polynomial ring. So, k is algebraically closed, $R=k[X_1,\ldots,X_n]$ and m is a maximal ideal of R.

(Refer Slide Time: 05:46)



Then, $\frac{R}{m}$ is a field, finitely generated as a k-algebra, because R is finitely generated as a k-algebra any quotient is also finitely generated as a k-algebra, this is the Nullstellensatz version 4. Nullstellensatz version 4 implies that $\frac{R}{m}$ is a finite extension of k. Remember k is algebraically closed. So, now k is algebraically closed, which now means that $\frac{R}{m} \cong k$.

(Refer Slide Time: 07:00)



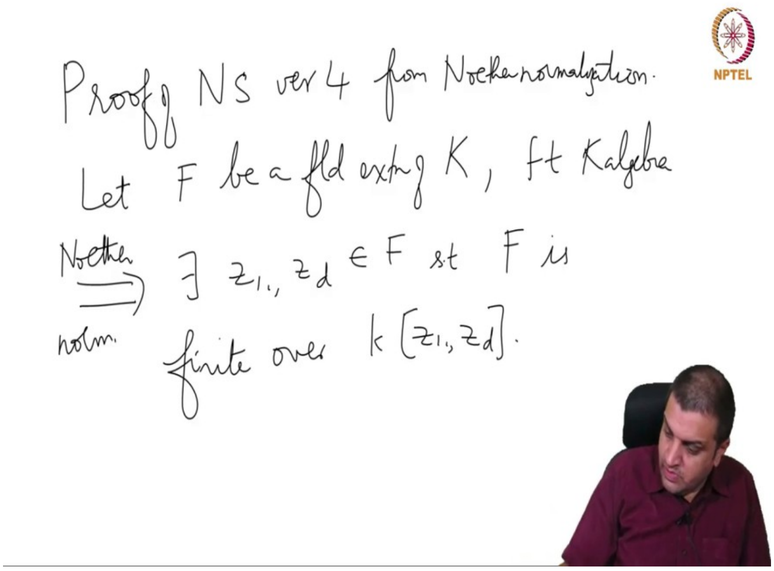
So, now, let us try to look at this. So, there is k here, then there is R here, then there is $\frac{R}{m}$ which is also isomorphic to k. Now, an element $\alpha \in k$ goes to the constant polynomial and goes to α itself here, because this is just going modulus on maximal ideal. So, its residue class is just α itself.

On the other hand, if you X_i will go to some α_i for any i. So, in other words, α_i is the image of X_i under this map. So, because it came from k, α_i went to α_i directly, and the X_i also went to α_i. So, this is inside m, because that is the kernel of this map this is true for all i.

So, remember what is the definition of image of X_i in $\frac{R}{m}$. It give some element inside $\frac{R}{m}$ call it α_i. So, this is inside here. Therefore, $(X_1-\alpha_1, \ldots, X_n-\alpha_n)=m$ because this is a sub ideal of this, but both are maximal. This is a maximal ideal for evaluation, this is given to a maximal ideal. So, therefore, there is equality here. So, maximal ideal is in this form. So, this is the proof of version 2 of the, of Nullstellensatz assuming version 4.

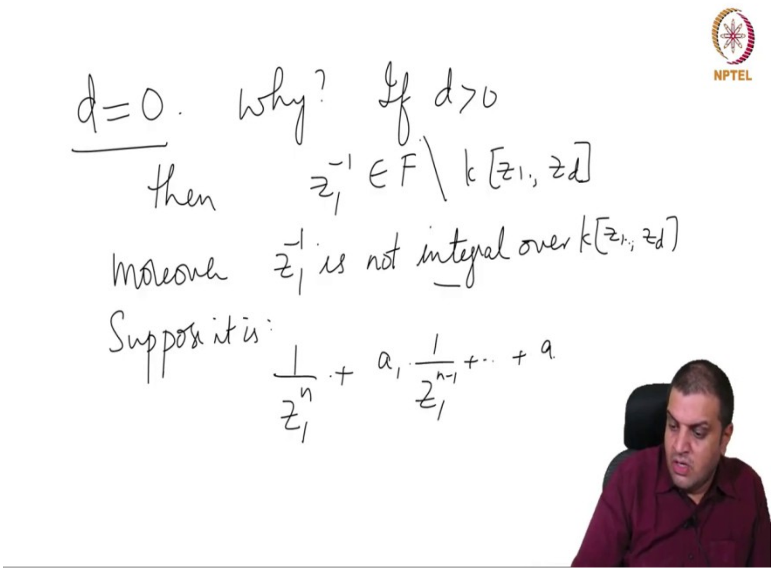
So, now, we will prove version 4 of Nullstellensatz assuming Noether normalization. And then, in the next lecture, we will prove Noether normalization it is a little technical argument playing with polynomials, but we will give a quick argument for some special case in this lecture itself. So, we now need to prove a version 4 of Nullstellensatz assuming Noether normalization lemma.

(Refer Slide Time: 09:47)



So, proof of version 4 of Nullstellensatz from Noether normalization lemma. So, what is the version 4 of the statement was a field extension that is finite type is finite. This is what we have and. So, let F be a field extension of K finite type K-algebra. So, then by Noether normalization, there exists $z_1, z_2, \ldots, z_d \in F$ such that F is finite over $K[z_1, z_2, \ldots, z_d]$.

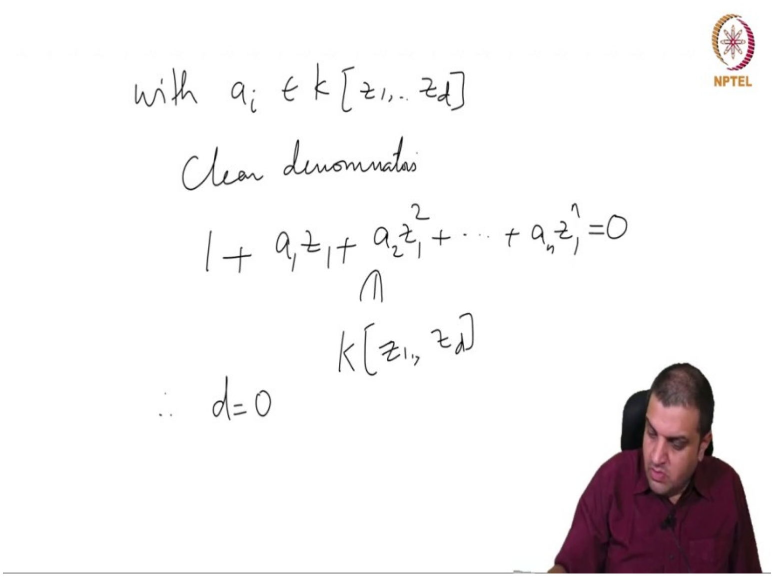
(Refer Slide Time: 11:30)



But what can d be? Well the claim is that d must be equal to 0. Why? If d is positive, then $z_1^{-1} \in F$ ¿$[z_1, z_2, \ldots, z_d]$, that is because, this is a polynomial ring. It does not contain inverses of the variables. So, it will not be inside here, but it is inside F because F is a field I mean z_1 is an element of F. So, its inverse is inside.

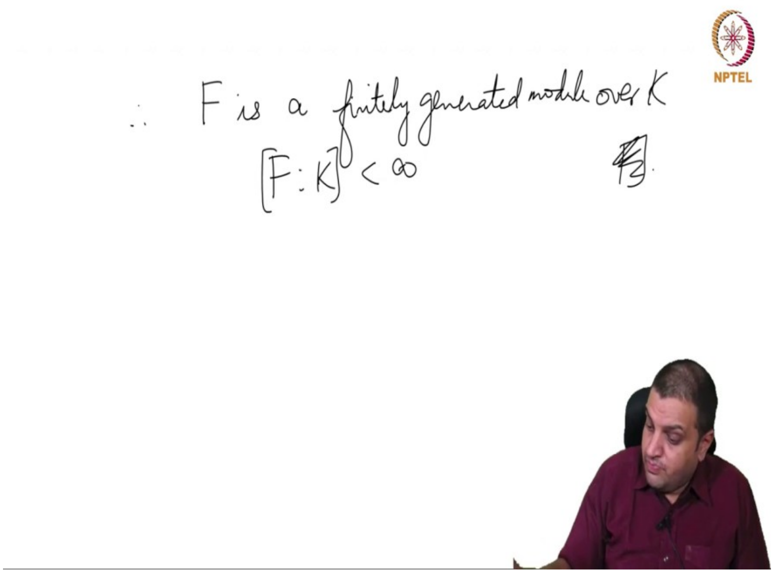
And moreover z_1 is not integral over k, z_1^{-1} is not integral over $K[z_1, z_2, \ldots, z_d]$. So, it goes back to the argument as we did for integers and rationals. So, suppose it is the by way of contradiction, suppose it is then we would get something of the form $\frac{1}{z_1^n} + a_1 \frac{1}{z_1^n} + \ldots + a_n = 0$ 1 with a_i inside the sub ring.

(Refer Slide Time: 13:11)



Clear, denominators we would get $1+a_1 z_1+a_2 z_1^2+\ldots+a_n z_1^n=0$. But, think about in this way, think about it this is a polynomial. So, now, this happens inside the polynomial ring in $k[z_1, z_2, \ldots, z_d]$ that is not possible, because all these terms have no constant term here there is a 1, or say it in other words, these are algebraically independent there cannot be such a relation. Therefore $d=0$.

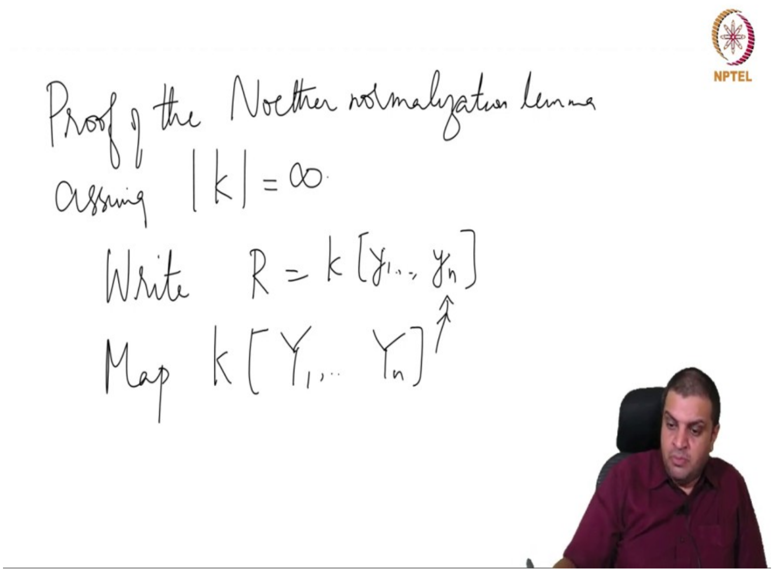
(Refer Slide Time: 14:29)



Therefore, F is a finitely generated module over K which is what we wanted to prove, that is these are field extensions and that extension degree is finite. So, therefore, we are now left to prove Noether normalization lemma, we would give the proof in the next lecture. But before, we will give the full proof of what all we stated in the next lecture.

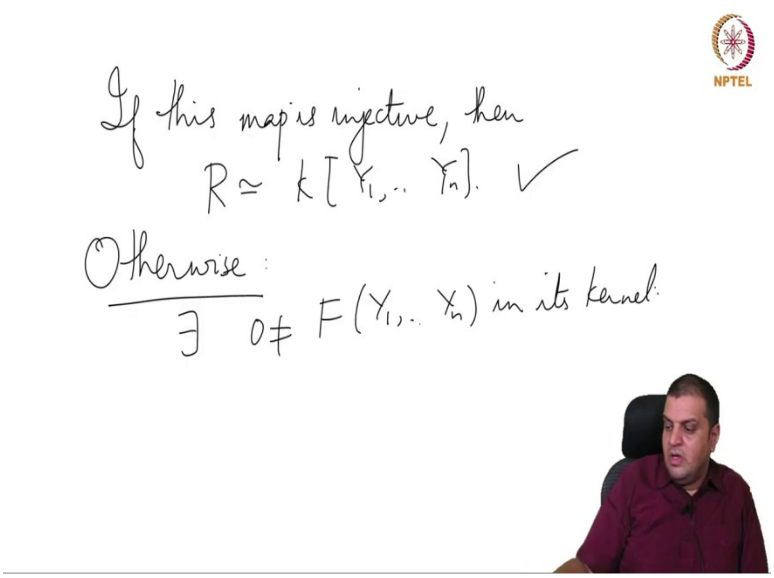
However, let us discuss a proof which will work in for infinite fields, which can also be used at least for fields that are sufficiently large enough can also be used as an idea, as a trick to construct these things in a computer. So, we will do that in the next lecture, but let us just quick give a quick proof of this in the infinite field case now.

(Refer Slide Time: 15:53)



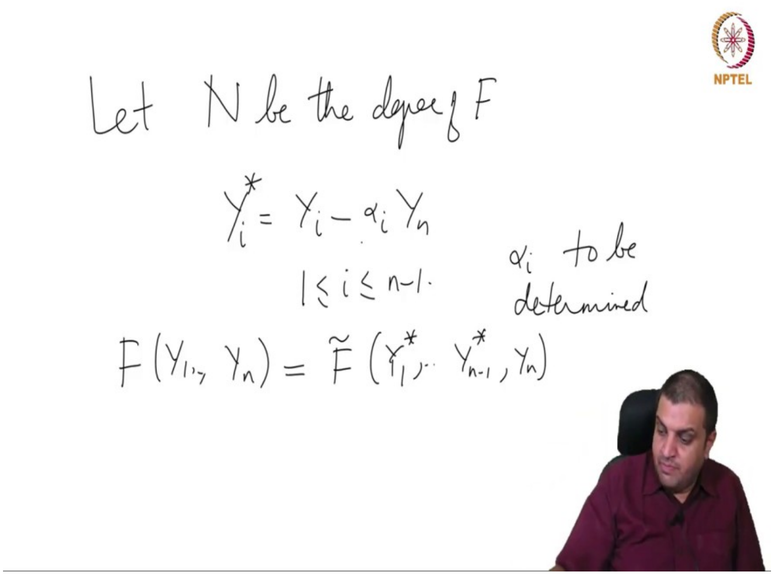
So, proof of the Noether normalization lemma. Assuming k is infinite. So, for example, any field of characteristic zero or any algebraically close field, all of them is finite. So, write $R=k[y_1,\ldots,y_n]$, because it is finitely generated. And map a polynomial ring to this surjectively. If this is injective, then there is nothing to prove, because then it is already a polynomial ring.

(Refer Slide Time: 17:07)



If this map is injective, then R itself is a polynomial ring, and then we are done, because all that we wanted to prove where R is finite over a sub algebra which is a polynomial ring. So, it is just even identity map. Otherwise, there exist some nonzero polynomial $F(y_1,\ldots,y_n)$ in its kernel.

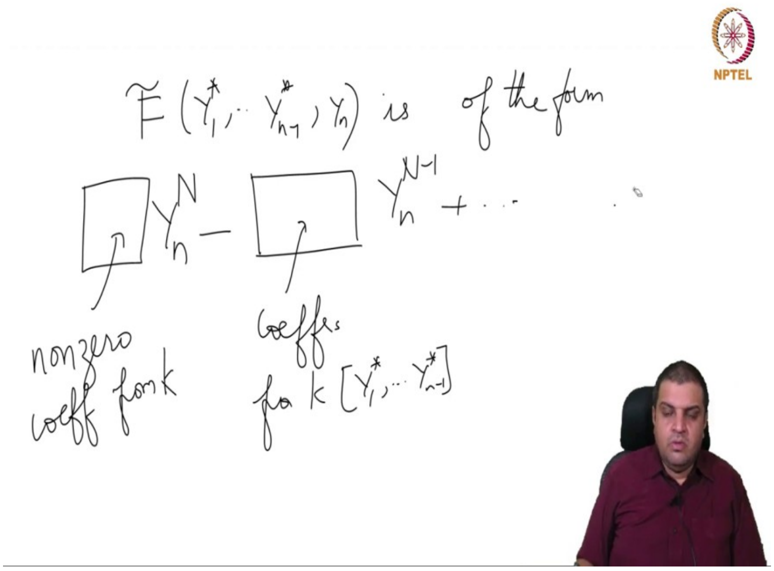
(Refer Slide Time: 18:05)



So, let N be the total degree not individual variable wise degree, but the degree of F, the total degree of F. Now, we do a change of coordinates; we do change of coordinates as

$Y_i^{¿} = Y_i - \alpha_i Y_n$, $1 \leq i \leq n-1$ and α_i to be determined. If you do this, then we can rewrite $F(y_1, \ldots, y_n) = \widetilde{F}(y_1^{¿}, \ldots, y_n^{¿})$. If you choose in fact for almost all choices of these alpha i.

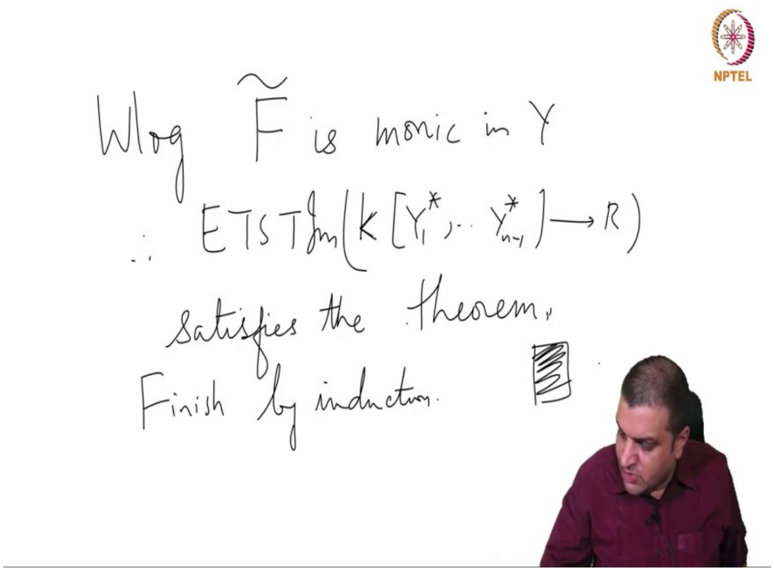
(Refer Slide Time: 19:22)



F tilde is the new polynomial. Notice that the change of coordinates gives an automorphism of the polynomial ring of this polynomial. So, it is just that we are surjecting some other polynomial ring on to R, so it does not. So, we can still study a nonzero element in the kernel y_n^N.

So, there might be, there will be some coefficient which depends on the α's. So, this is a nonzero coefficient from k. Then, here onwards it would involve some coefficients from k adjoint the fewer variables. y^{n-1} and so on lower degree terms. In other words, in these new variables, we get that. So, this is a non-zero coefficient from k, so it is invertible.

(Refer Slide Time: 21:09)



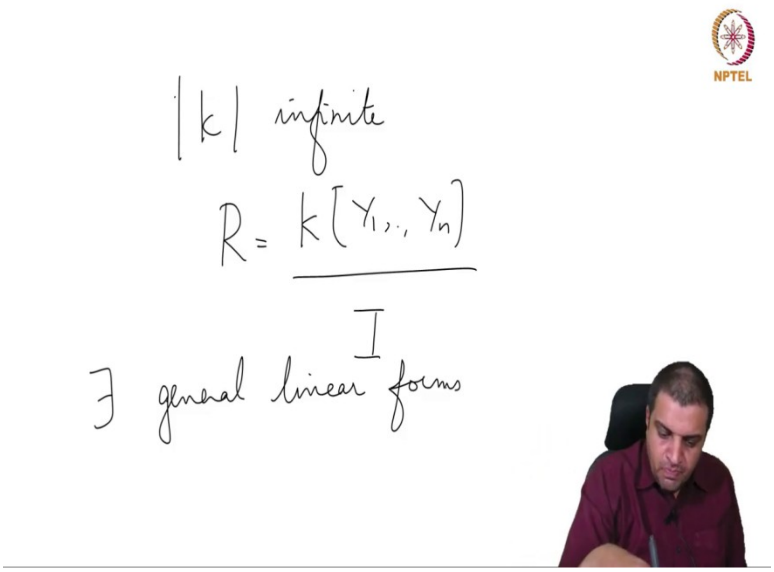
So, without loss of generality, we can relabel things and assume that $\widetilde{F}$ is monic in Y, with coefficients coming from the earlier variables. So, therefore, by transitivity of finite morphisms, it is enough to show that, the polynomial sub algebra generated by $n-1$ elements.

So, so this one's image inside R. So, this one's image inside R. So, if we had y_n also and then took its image it would be all of R, but we, by because of this, we do not need to worry about all of R, we can just remove that y_n.

So, just look at the sub algebra that this one generates inside R. It is enough to show that this image of this thing is satisfies the Noether normalization lemma. And now, I can proceed by induction.

So, then finish by induction, because it cannot come down all the way up, I mean it might come down all the way up to 0, but at some point it has to stop. So, this is the end of this the proof. This is a proof in the special case of where the field is infinite. And, we would so, what does it actually tell us I mean concretely for computations.

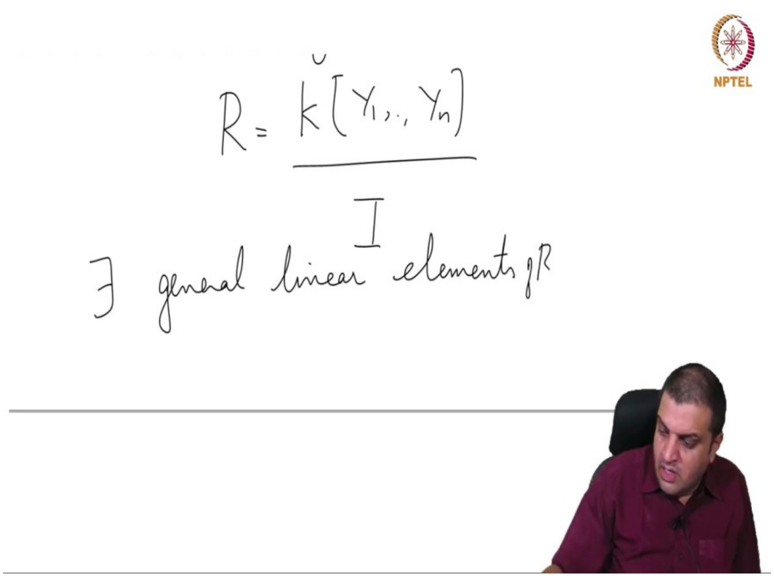
(Refer Slide Time: 23:25)



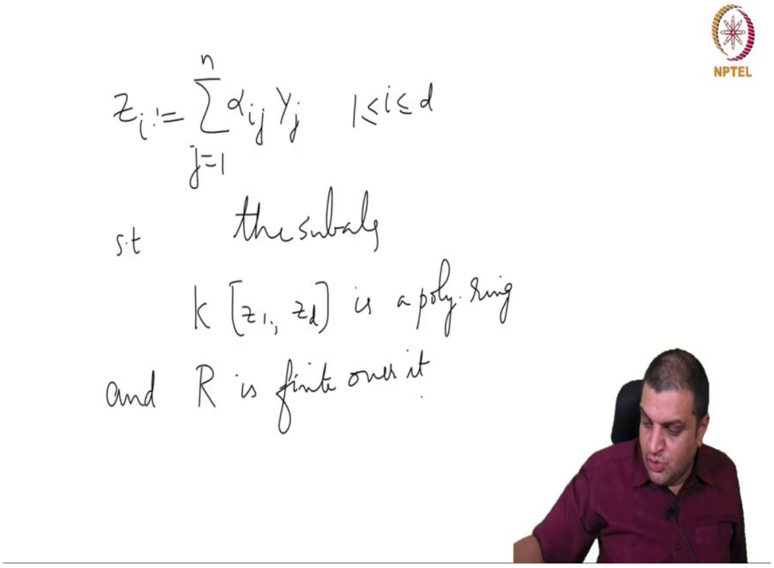
So, suppose we had some k, so let us say k is infinite. So, we are assuming k infinite. $R=\frac{k[y_1,\ldots,y_n]}{I}$ finite type.

So, what it says is there exist general linear forms, what is the value of d that we have not yet determined, it will take us a while for us to understand what the d is. So, these forms will look like well, I should maybe we should not call them because their images of in this thing, linear elements of R of the form.

(Refer Slide Time: 24:27)



(Refer Slide Time: 24:38)



So, these are the $z_1,\ldots,z_d$ such that $z_i=\sum_{j=1}^{n}\alpha_{ij}y_j$, $1\leq j\leq d$ and d will be determined later I mean that there is a d with this property is part of the lemma. How this current proof tells us that? If you take some generic values for α_{ij} and construct these things.

So, let us call this thing z_i. So, this will just take them as elements of R, or in other words we will construct them in the polynomial ring and then look at their residual classes in R. The sub algebra generated by is a polynomial ring, and R is finite over it, finite as a morphism so of rings.

So, this is what the thing. So, we can actually do these things with linear combinations. This is what not every choice of α_{ij} will work, but because k is infinite, there is enough room to choose them randomly and that would work and this may be useful in while trying to compute some things. So we will see some examples a little later.

So in the next, so this is the end of this lecture. In the next lecture we will prove Noether normalization lemma in the generality, so that will finish the proof of Nullstellensatz also. So, this is, and then we will study more about finite integral extensions. And, after we study that a little bit, then we can come back to computational aspects or at least try to see some examples pictures etc.