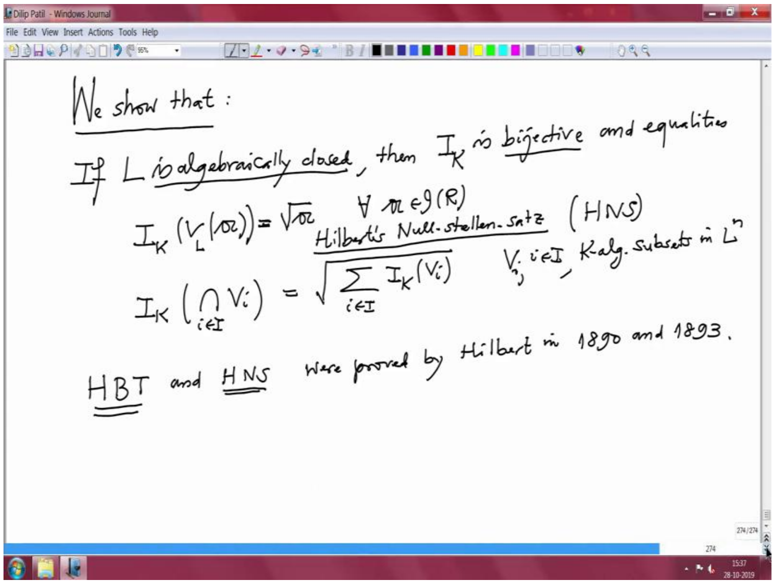
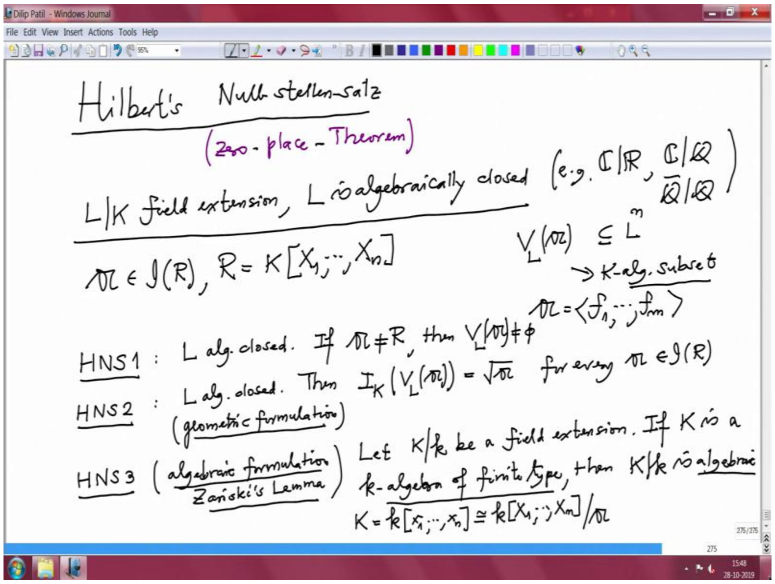
An Introduction to Algebraic Geometry and Commutative Algebra
Professor Dr. Dilip P. Patil
Department of Mathematics
Indian Institute of Science, Bengaluru
Lecture No 42
Hilbert's Nullstelensatz

(Refer Slide Time: 0:40)



Welcome back to this later half of today's lecture. As I said in the earlier half that we will prove Hilbert's Nullstelensatz today and I just want to remind you that L algebraically closed is very very important. So, without that this Nullstelensatz is not true. So, for algebraic geometry it is very important to consider L is algebraically closed and then later on we can specialize L equal to K and K is algebraically closed and then we will get a classical set up.

(Refer Slide Time: 1:10)



So, today now I want to prove Hilbert's Nullstellensatz. It is very easy to pronounce this if you know where to break and at least Indians have some experience those who have learned Sanskrit to give where the breaking should be, so the breaking should be null and stellen. So, that becomes Zero place Theorem. So, theorem which tells you about which places it is 0. So, let us go back. So, I want to little bit write this, Null stellen satz. So, that is where one breaks.

So, the L over K field extension and L is algebraically closed. These are our assumptions. So, this is what we will assume today and typical case for example, so of course C over R is there but also the case C over Q also included or Q bar over Q. This cases are interesting classical at least.

Alright so, and I take a arbitrary ideal a, any ideal I, R where R we are abbreviating for the polynomial ring over a field K in n indeterminates. So, this is what we have ideal and first, so we are using this. We have defined V L of ideal a and this was a subset of L power m and this we called it K algebraic set. So, the first question is when is there is at least one solution? See, it is like when we studied linear algebra and when we have given a system of linear equations, your first question is how do you decide this system is consistent.

Those days in the linear algebra the term consistent is used to say that when do they have common solution? So, the question is when does it have, what condition do you want to put on the ideal a, so that this algebraic set is definitely non empty. So, that means the polynomials which defined this ideal, so if a is defined by the polynomial f1 to fm that means a is generated by these polynomials. Now, the question we are asking is when do this finitely many polynomials f1 to fm in n indeterminates over field K when do they have the common solution and that is precisely what I will call is HNS, HNS1. HNS1 says that so L algebraically closed.

I just want to remind you that we are assuming L is algebraically closed. If the ideal A, obviously if the ideal A is not a proper ideal, if one belongs to that then there is no hope that V L of the constant polynomial 1 will have no 0. So, there is no hope. So, if ideal A is a proper ideal is not the whole ring R then VL of A is definitely non empty. That means this system of polynomials is consistent.

That means they have a common 0 at least 1. How many that is more difficult question and we will not address immediately now, but sometimes we will talk about it. So, this is the Hilbert's Nullstellensatz 1. So, this is also called the classical Hilbert's Nullstellensatz. So, I will just say orally. This is HNS1. It is also called classical Nullstellensatz.

HNS2 is again, remember L is algebraically closed then IK of VL of ideal A equal to the root of the radical ideal of A. This is true for every ideal A in the ring R and sometimes some books will also call this as a geometric formulation. It is called geometric formulation because it gives a bridge between algebra and geometry as we saw.

This equality make, happens when both the map are, the map is bijective. So, therefore it is called a geometric formulation. If you like this is called a classical formulation and third one HNS3, this is also called algebraic formulation or also it is in the literature also it is called Zariski's Lemma because Zariski has proved it, also proved this. So, what is it? So, as you can guess it by the name algebraic formulation that it will not involve geometry at all. In fact it will not involve this language of algebraic sets.

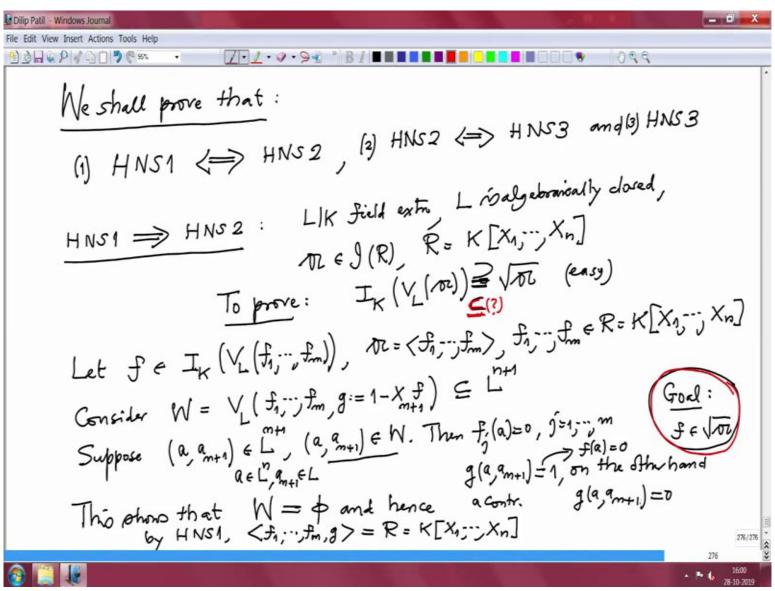
So, I will state in the simple terms that. So, let K over k, capital K over small k be a field extension if the bigger field K, K is algebra, K is, if capital K is a k-algebra of finite type then that extension capital K over k is algebraic extension. So, now I will have to recall you these terms. And obviously this term you already know it, but I will recall it. So, we have these three statements, HNS1, HNS2, HNS3 and as you can see that this HNS3 have nothing to do with algebraic sets and V and I and so on and HNS1 is does not involve the ideal IK but HNS2 involves.

So, it appears that HNS2 looks stronger but I am going to prove that these statements are equivalent. So, and I will recall this concept. So, finite type is what? Finite type means this capital K is a quotient residue class algebra, K algebra of a polynomial ring in finitely many variables over the small k. That is a finite type.

That means as an algebra it is generated by finitely many elements. So, in the notation this means capital K equal to k and generated by this notation. I hope you have not forgotten this notation as an algebra. It is generated by finitely many elements x1 to xn in capital K but this is precisely the quotient of the polynomial ring in n variables modulo some ideal. So, that is the finite type algebra over a field.

Actually we have also studied finite type algebras over arbitrary commutative ring that means they are residue class ring of a polynomial algebra over the base ring A modulo some ideal and algebraic extension means every element of capital K satisfies some non zero polynomial over k. So, this again I will recall when we start proving. So, what are we going to prove? So, let us write down.

(Refer Slide Time: 12:00)



So, we shall prove that, I want to prove they are equivalent. So, I will prove that HNS1 is equivalent to HNS2 and HNS2 is equivalent to HNS3. So, this prove the equivalences. So, we shall prove this if and only if, this if and only if and obviously then if I have to prove that they are all true then I have to prove one of them at least and I will then choose which one is the easiest to prove and namely HNS3.

So, these three things we are going to prove. One is this, two is this and three is this and that will prove that all these are equivalent and they are true. In particular HNS2 is true and that is the geometric formulation and that is very useful for setting up modern algebraic geometry. So, let us prove very easily. So, I am going to first concentrate on this one.

So, first we will prove that HNS1 implies HNS2. So, what is given to us? It is given to us L over K field extension and L is algebraically closed and we have also given ideal a in the polynomial ring R, where R is K x1 to xn. This is given to us and what is want to prove? We want to prove so I will write down here.

To prove IK of VL of the ideal a equal to the radical ideal of a. This is what we want to prove and one implication is easy and that was this. This we have already easy one because if a polynomial is here the power is in the ideal a. That power will vanish and every point here and therefore by definition that power will belong to this ideal IK and because IK is a radical ideal that polynomial itself will belong to the IK.

So, this inclusion was easy. So, the more difficult one is this. I will remind you this is what we are looking for the proof and what are we allowed to use? We are allowed to use HNS1 that means whenever I have an algebraically closed field, whenever ideal a is there which is not a unit ideal then VL of that a is non-empty. This is what we are allowed to use.

So, if you want to apply that we will have to create a situation like that. So, let us start the proof. So, I will start a polynomial on this side. This is ideal in R. So, I will take a polynomial here and I will prove that polynomial is here.

So, let f be a polynomial in IK of VL and as I said this a is generated by finitely many polynomial that we know from Hilbert's Basis Theorem. So, VL of f1 to fm where if you like ideal a is generated by f1 to fm finitely many polynomials, in where f1 to fm are polynomials in R which is a polynomial over K in X1 to Xn variables. So, that is the situation and what is that we want to prove? We want to prove that this polynomial f belongs to this. So, I will write on this corner.

Our aim is Goal f should belong to the radical ideal of a. This is our goal. So, now somehow I have to create a situation so that I can use HNS1. Right now there is no situation. So, consider W is VL of f1 to fm comma g, where g is 1 minus Xn plus 1 times f.

This is now remember I introduced one extra variable here and this is I use this polynomial and this is now algebraic set not in Ln but this is in Ln plus 1 and then I want to check that this set W is empty or non-empty. So, right now it is real of this set. So, suppose there is a point. It has a point in L power n. That means suppose it has a, comma an plus 1 belonging to Ln plus 1 and suppose this point belongs to W.

Then what happens? Remember this a is in L power n and an plus 1 is in L. If it is in W then all these polynomial should vanish there. Then all these f should vanish there. So, fj of a is 0 for j equal to 1 to m and also the g a, an plus 1 now, see when I plug this into fj there is no Xn there, Xn plus 1 present there.

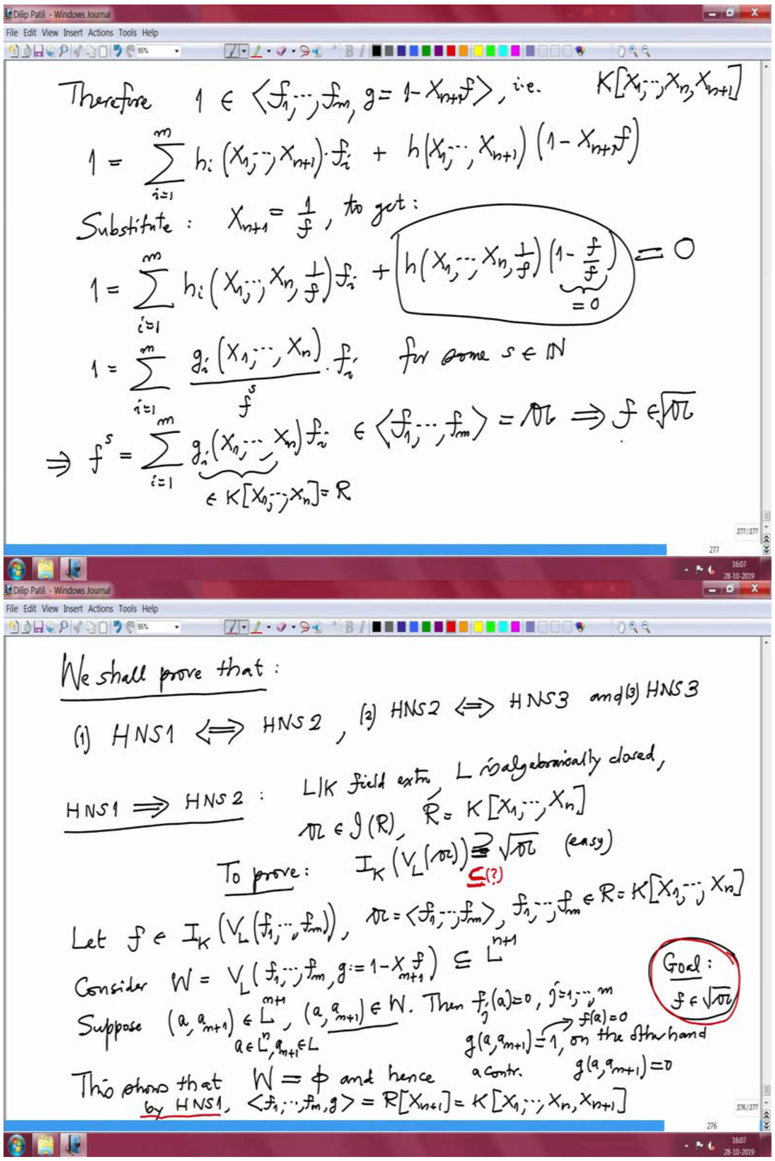
So, therefore it will only be fj at a and this is also 0. This we know by the definition of this W so because it is here but what does one mean by this g is 0. That means when I am plug it in here a and an plus 1, so this will this polynomial f is already 0 there. So, therefore this condition is equivalent to saying so this is already 0 so that means this is not 0 but this is 1. Sorry, this is not 0. This should be 1 because when I plug this there in g this is already 0 at a because f is a polynomial in this and this polynomial should vanish on everybody here.

But this a is already so this means a is already in VL of this. Therefore, this is 1. So, if such a point belong to W then already W g of a at n plus 1 is 0 but this is already contradiction because on other hand g should vanish there. On the other hand g of an plus 1 should be 0. This is a contradiction.

So this is because f of a is 0 because f belong to this. So, therefore there is in this case the W has to be empty. So, if W is non-empty it will have some point and we are getting a contradiction. So, this shows that this set W is empty and then what is our HNS says? If this ideal where not a unit ideal then W has to be non-empty and hence by HNS1, the ideal generated by these polynomials f1 fm comma g this should be the whole ideal R which is the polynomial ring in n variable over K.

Then what happens? Remember our goal is to prove this that f belongs to the root, that is our goal. Alright, this ideal is a unit ideal means 1 should belong to the linear combination of these polynomials with coefficients in the ring R.

(Refer Slide Time: 24:17)



So, that means. So, therefore 1 belongs to the ideals generated by f1 to fm, comma g but remember g is 1 minus Xn plus 1 times f. So, that is I can write 1 as sum polynomials hi's times variables X1 to Xn plus 1 times fi's plus sum polynomial h times g that is 1 minus Xn plus 1.

So, here also to be specific I will write h is X1 to Xn plus 1 times g which is 1 minus Xn plus 1 f because we are working in the ring K X1 to Xn, comma Xn plus 1. So, the coefficient should be from this ring. So, let me just check what did I write up. Alright, so this is not correct, this is R. I should write here R Xn plus 1 which is K X1 Xn, comma Xn plus 1.

You see because W is empty and W is not in Ln but L power n plus 1. Therefore we have to take one more variable. So, we have this equation. Remember both these sides are this is a constant polynomial 1 and this is the other side is the polynomials in the ring polynomial K X1 to Xn plus 1 variables. So, in this polynomial identity I can substitute, so substitute the variable Xn plus 1 equal to 1 over f.

We have seen that in the polynomial we can substitute any element in the K Algebra and K Algebra I will take in the quotient field. So, 1 by f will be there. So, therefore I am allowed to substitute and then what happens? The substitution is a ring homomorphism so I can rearrange the terms addition, multiplication, etcetera. So, therefore this side will not change so to get, what do we get?

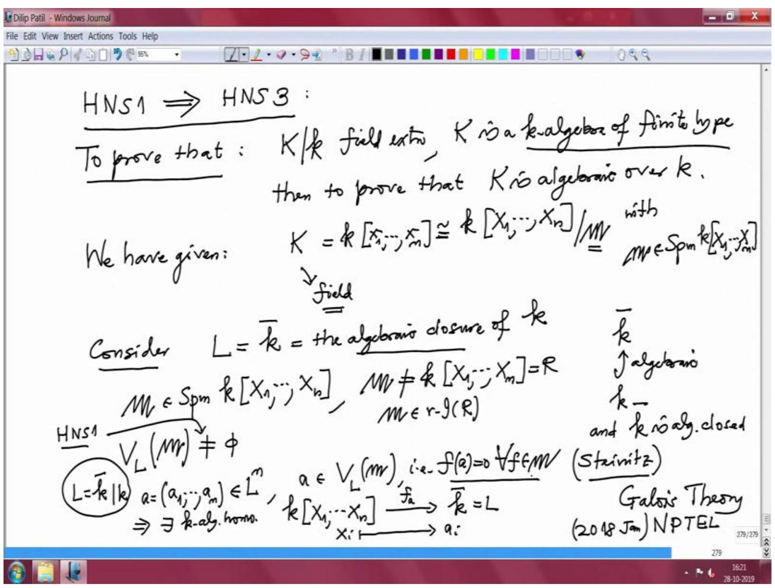
This LHS will not change which will be 1 only. This side, this will become 1 over f, so summation this is from i equal to 1 to m hi X1 to Xn nothing there and this is 1 over f and then fi as it is because there is no Xn plus 1 there and h of Xn to Xn and 1 over f, this. But this when I put Xn plus 1 equal to 1 over f, this is 1 minus f over f and this is 0 then. Therefore, this term altogether will be 0, that is not contributing and this term has 1 over f in the denominator and because this is a polynomial Xn will not have arbitrary large degree terms so I can take the common denominator and write this as so 1 equal to then I want to clear the denominator so this will be equal to i equal to 1 to m and instead of hi there will be some other polynomials gi X1 to Xn and divided by some power of f and I will take by supplying up and down common denominator.

So, it will be f power some power fs and this polynomial fi is as it is for some s a natural number. So, then what do we get from here? Now you cross multiply. You clear this denominator so we will get f power s so this will become f power s will be equal to summation i equal to 1 to m these gi X1 to Xn fi. But these are now where? These are in the polynomials in n variable with coefficients in K which was our ring R. So, this is a R linear combination of this polynomial which belongs to the ideal generated by f1 to fm.

But this ideal was precisely the ideal A. So, we have proved that some power of f belongs to the ideal A so that means the polynomial f itself belongs to the root ideal A. So, and remember I will show you what our goal was. Our goal was to prove f belong to the radical ideal of A and that is where we have succeeded. So, this proves HNS1 implies HNS2. This is what we were trying to prove and the place where we have used HNS1 I will show you. This is the place where we have used HNS1.

That is because W is empty then this ideal has to be the whole unit ideal. So, now the converse that is HNS2 implies HNS1.

(Refer Slide Time: 31:14)



So, conversely to prove HNS2 implies HNS1. So, we want to prove HNS1 by using HNS2. So, as usual what is the assumption we should always write. L over K field extension and we are assuming L algebraically closed and we want to prove if we have an ideal a in the ring R and if this ideal a is proper ideal then to prove, what do you want to prove?

We want to prove that V L of the ideal a is non empty. This is what we want to prove and our assumption is this L algebra is algebraically closed of course and we are allowed to use HNS2. So, suppose on the contrary that V L of this ideal a is empty. Then we should get a contradiction.

Well, if the VL of the ideal I is empty then what will be the I K? I K of V L of a, this will be equal to I K of empty set. But I K of empty set is what?

I K of empty set is a whole ring R. Because that is I K of 0. This was the first property I will state. This is the ring R which is a polynomial ring in n variables. But what do HNS2 says in this situation?

But by HNS2 we have radical of the ideal a equal to I K of V L of a for any ideal that was HNS2. But this is R. So, therefore I proved that the root radical ideal of a is R. Then it is very easy to see that a is also the unit ideal R because 1 belongs here. That means 1 power 1, 1 power any integer n that is also 1 and that will also belong to that ideal a then.

So, this is correct which is a contradiction to our assumption a is not R. So, this proves this completes the proof of HNS1 if and only if HNS2. Now, we will have to prove that next we want to prove that HNS1 and HNS3 are equivalent. So, let us finish that prove also. Now, to prove HNS1 implies HNS3.

So, what is the assumption again? Now, I want to prove HNS1. I am assuming HNS1. That means whenever L is algebraically closed field extension of field K and there is an ideal which is a non unit ideal then V of that is non-empty. That is the assumption and what is HNS3?

HNS3 have nothing to do with algebraically closed and L and K and I and V. So, what is to prove? So, to prove that, to prove what? To prove that, I will write the statement what do we want to prove. Whenever capital K over small k is a field extension, capital K is a K algebra of finite type then what we want to prove, then to prove that K is algebraic over k. This is what we want to prove.

So, let us start proving it. So, I have given K which is K algebra of finite type. So, therefore we have given capital K equal to K generated by finitely many elements as K algebras but this means this is a quotient of a polynomial algebra in n variables modulo some ideal and that ideal because this is a field, that ideal has to be the maximal ideal with m belonging to Spm of capital K X1 to Xn because this is a field. If it is an ideal so that the residue class algebra is a field then this ideal must be a maximal ideal.

That is a characterization of maximal ideal. So, that is the field or that is the maximal ideal. Now, consider ultimately we want to use HNS1. That means we have to have algebraically closed field and then so consider L equal to k bar, small k bar. This is the algebraic closure of the small k.

What is algebraic closure? Algebraic closure by definition is the smallest algebraically closed field which contains k. That means this k bar is algebraic over k. This extension is algebraic and if there is any other algebraic (ex) and then k bar has no algebraic extension. So, this is 1 and k bar has no proper algebraic extension.

Or in other words, so let me write in other words this is an algebraic extension and k bar is algebraically closed. It is a theorem of Stainitz that every field has an algebraic closure. In particular this given k, small k has an algebraic closure. If we have not seen this theorem I will recommend you to have a look at the course I gave in the last year on Galois Theory. So, all these things are proved there very precisely and very neatly.

This is NPTEL course 2018 Jan. So, we assume that every field has algebraic closure and L equal to that we take and then now this m is a maximal ideal. So, m is a maximal ideal in the polynomial ring in n variables and therefore it is a proper ideal. So, m is therefore is not equal to the whole this and n and this is a small k.

I also want to correct here. This is also small k it is not capital K. This is also small k and this is also small k. So, this is not proper ideal. Therefore, it is polynomial not the whole ring. So, it is a proper ideal.

Therefore if I take VL of this ideal m, m is also maximal. So, prime, so therefore m is actually a radical ideal, so m is a radical ideal anyway that is not needed here. So, this is my ring R now and I am applying HNS1 to this algebraic set. So, HNS1 to the pair, L equal to k bar over k. This is what I am applying HNS1. So by HNS1 applied to this and this. So, this is non-empty. This is by HNS1. Therefore, there is a point here. So, that means I can find here a, a1 to an in L power n.

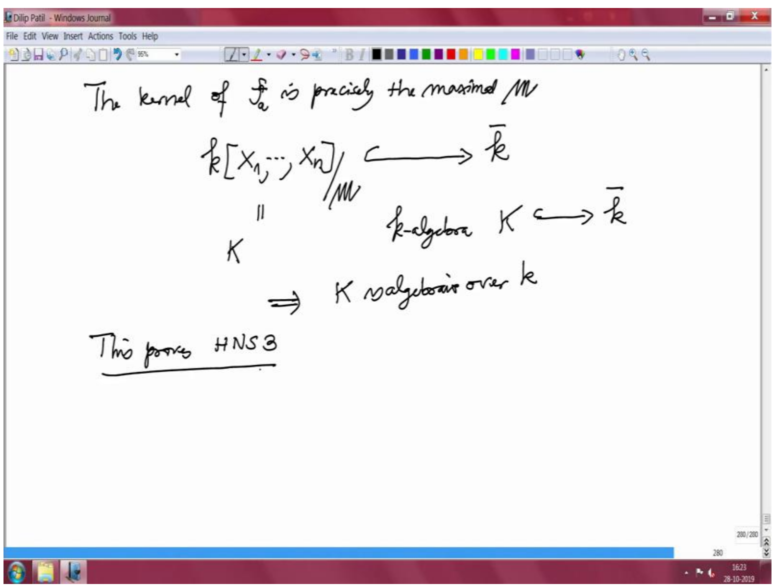
Let us abbreviate it a and which belongs to a belongs to VL of m because it is non-empty. So, there is a point there but now I look at the K algebra homomorphism. So, that means this a will vanish at every polynomial in m. So, that is f of a is 0 for every f in the maximal ideal m. But this means I have a map.

So, this means look at the k algebra homomorphism. So, that I have to define it in the polynomial ring X1 to Xn. I just have to give where the variables go and the k algebra here is the k bar which is L. So, here I take the substitution map by Xi going to ai. This is a substitution map.

If I call this as f suffix a, this is a substitution map. That means what? This proves that, there exist a k algebra homomorphism. That implies there exist a K algebra homomorphism which maps Xi to ai and therefore a polynomial each so I want to assert from here. So, what is a kernel?

Kernel is a by all the kernel of this f is precisely this m because of this. So, let me write on the next page.

(Refer Slide Time: 45:00)



So, the kernel of this k algebra homomorphism, f suffix a is precisely the maximal ideal m but then it will induce a ring homomorphism, k algebra homomorphism from this modulo m inside k bar. But this ring is precisely this residue class ring is precisely our given field capital K. So, that means there is a small k algebra homomorphism from k to k bar.

But this is injective. That means capital K as a field is sitting inside k bar. So, that implies capital K is algebraic over k. So, this proves HNS3. Now, the converse, in the next lecture we will prove the converse and also we will prove HNS3.

So, that will complete the proof of these three formulations of Hilbert's Nullstellensatz and in exercises I will give you many more (())(46:38) HNS4, HNS5, HNS6. Some of them I will do it in lectures and some I will put it in assignments. So, with this I thank you very much and we will continue in the next lecture.