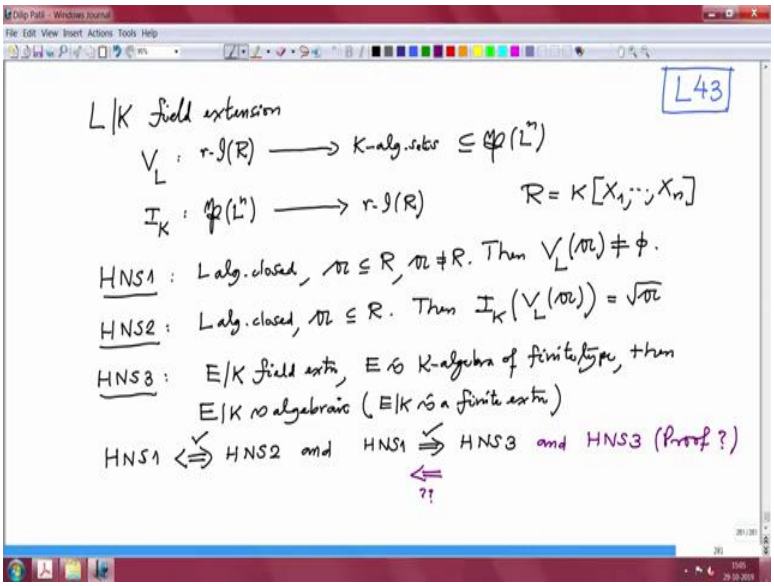
Introduction to Algebraic Geometry and Commutative Algebra
Professor Doctor Dilip P. Patil
Department of Mathematics
Indian Institute of Science, Bengaluru
Lecture 43
Hilbert's Nullstellensatz Contd.

Welcome to this lectures on Algebraic Geometry and Commutative Algebra. In the last lecture, I have stated 3 formulations of Hilbert's Nullstellensatz, and we wanted to prove their equivalence. And, let us recall quickly what we have proved so far.

(Refer Slide Time: 00:50)



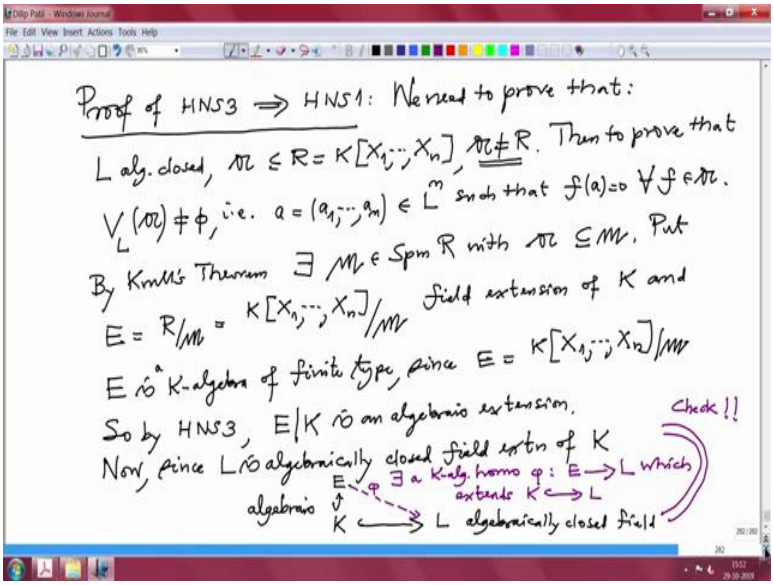
So, what we proved is the following. So, as usual, our notation is L over K field extension. And we have defined the maps VL and IK, these are the maps. This is a map from ideals of, radical ideals of the ring R to the K of finite algebraic sets, K algebraic sets. This is a subset of the power set of L power n. And then we have defined, the map from power set of L power n to radical ideals in I, R. And R is our polynomial ring in n variables over the field, base field capital K. And this actually we have defined for, actually from any ideal.

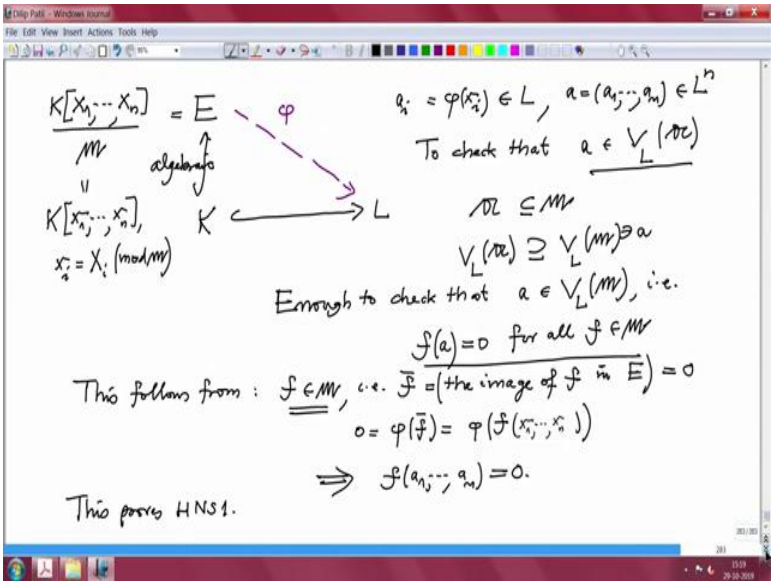
But it depends only on the radical of that ideal. And what is HNS1? HNS1 says if L is algebraically closed and I is an ideal in, not I gothic a. This is ideal in R, and a is not R. Then, VL of this ideal is nonempty. So, that is at least one point in this algebraic set. HNS2 that is, if I take any ideal, again L algebraically closed, a is any ideal in R. Then if I take IK of VL of the ideal a, then you get back not A, but the radical of a.

So, in particular if were a radical ideal, then you get back your ideal a. So, and HNS3, this is completely algebraic formulation, as nothing to do with these maps. So, if I have a field extension, capital, let me write, field extension of this base field K. So, that is E over K field extension and E is K algebra of finite type, then E over K is algebraic. That means, every element of E is algebraic over K. Actually, we will prove that actually E over K is a finite extension, in particular algebraic.

So, finite extensions are algebraic. And what did we prove so far? So far, we have proved that HNS1 if and only if HNS2. And also, we have proved HNS1 implies HNS3, these we have proved already. So, I will just mark this is proved, this is proved. And now, we want to prove therefore, what remains to prove is this implication, this remains to prove which we will do it today. And, proof of HNS3, proof. These 2 things are remaining. So, if we prove these 2 things which we will do it today; then we would have proved that all these HNS 1, 2, 3 are equivalent and they are all true.

(Refer Slide Time: 06:00)





So, now let us prove HNS3 implies HNS1. So, proof of HNS3 implies HNS1. So, what is to be proved? So, we need to prove that, we have given L is algebraically closed. Also, we have given an ideal a in the ring R, which is a polynomial ring over K in n variables. And, a is not the whole ring R, it is a non unit ideal. Then to prove that, VL of a is non empty. That is, we want to find, we want to find a point, we want to find a point a equal to a1 to an, in L power n, such that f of a is 0 for all polynomials f in the ideal a. This is what we need to prove.

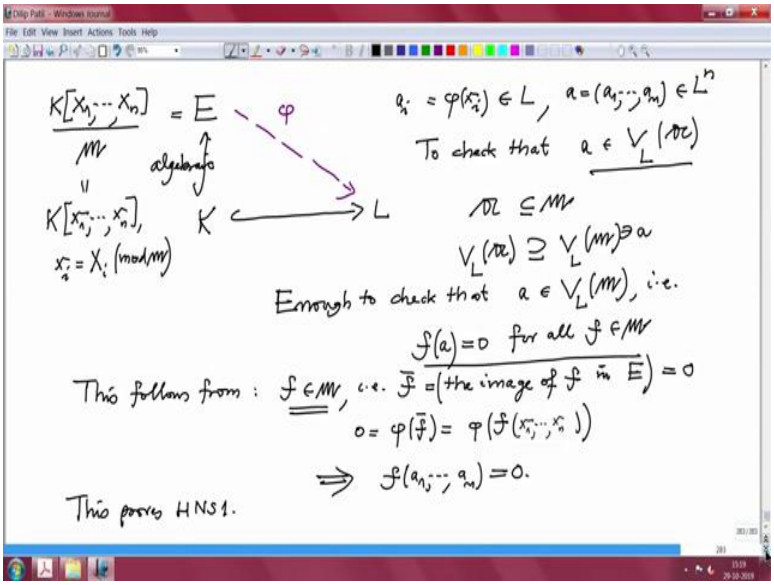
And what is given is, HNS3. That means whenever you have an algebraic, whenever you have a finite type K algebra E which is a field, then it should be algebraic extension. That is what we have given, that is HNS3. So, what do we do? We have given an ideal a, which is not the whole ring. So, by Krull's theorem, we know that there exists a maximal ideal m in the ring R with a is contained in the maximum ideal m. This is Krull's theorem. Because given any non unit ideal, you can always enlarge to the maximal ideal.

And, know we choose that maximal ideal and put E equal to R by m, R by m is polynomial ring in n variables over K modulo the ideal m. So, it is clearly that this E is a field and it is extension of, field extension of the field K. And also, and E is K algebra, is a K algebra of finite type. That is because, this is a residue class algebra of the polynomial ring. And that is precisely, what we mean by the algebra of finite type. So, since E equal to K X1 to Xn modulo m. So, it is a finite type K algebra is the field, therefore by we can use null, we can use HNS3.

So, by HNS3, E over K is an algebraic extension. Now, I want to use one fact from the field theory. So now, now since L is algebraically closed, L is algebraic closed field extension of K. So, therefore, L is a K algebra. So, it is, I want to draw the diagram. So, so that is K to L there is a injective, this is extension on the fields. And there is an extension E here, which is a field of K and we know this extension is algebraic. Let me write little bigger.

This extension is algebraic and also know, this is algebraically closed field. Then, one of the result in basic filed theory says that you can extend this, this inclusion to E. So, that means, there exist a K algebra homomorphism. So, I will write here, there exist a K algebra homomorphism. Let me call it phi, phi from E to L which extends the inclusion. This is fairly easy theorem in field theory. So, I will leave it for you to check this. So, I will only mark here, this check. So, once you have that, then that means what? And remember, so I will draw again the diagram on the next page.

(Refer Slide Time: 13:03)



So, we have E here, which is residue class of the polynomial ring by the maximal ideal m. This is K, and this is algebraic, and this is L. And then we have extended this phi, we have extended it to L, this we called it phi. So, therefore, phi of this, so let me also denote the elements here. K small x1 to small xn, these small xi's are precisely the images of capital Xi mod m, residue class. So, this phi of xi xn, small xi and those are elements in L, so I will call them ai's. And then, therefore

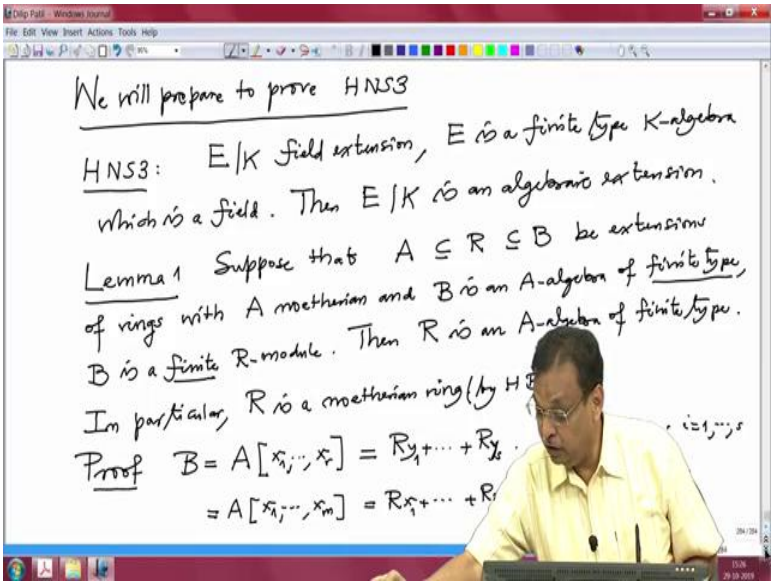
I have a equal to a1 to an, this is in L power n. And then, my natural choice is to check that this element belongs to VL of a.

So, to check that a belongs to VL of the ideal a. But what is the ideal a and m relation, so a is contained in m. So, therefore, a VL is inclusion reversing, so V a is contained in VL of m. So, it is enough to check this, it is enough to prove that it is even in VL m. So, is enough to check that a belongs to VL of m. What does that mean? That means, so that is f of a is 0 for all f in m. But well, this, this phi is a map from these 2 L. So, what is f of a, that is precisely the, so if you take any f in m then this goes to 0 under this homomorphism.

So, phi of, so this is, this follows from, so if f belongs to m, that is f bar which is f, which is f, which is the image of f in E but this image has to be 0, because f belongs to m. Therefore, modulo that it is 0, so therefore this is 0. So, phi of, because phi is a K algebra homomorphism, phi of f bar is also 0. But what is phi of f bar, this phi maps these xi's, xi's that we have called it ai. So therefore, this is nothing but phi of f of small x1 to small xn. But this is 0, that implies f of a1 to an is 0.

So, that proves this, so that proves a is in VL of m. But then it proves, in VL so that, so this proves HNS1. So, with this now we are only left to prove with HNS3. And I have, of course, one can prove any one of them, either HNS1, or HNS2, or HNS3. And then, therefore they will be all true because we have proved their equivalence. And I will choose to prove HNS3, because it is the simplest to prove. Well, one can also prove HNS1. HNS1 is the next simpler to prove and HNS3 is the strongest result, so it will be more difficult to prove. But this equivalence shows that we do not have to prove that.

(Refer Slide Time: 18:57)



Now, we will prepare, to prove HNS3. So once again, what do we need to prove? We need to prove HNS3. So, what we need to prove is, if I have E over K field extension, and E is a finite type K algebra which is a field. Then we want to prove that, E over K is an algebraic extension. This is what we need to prove. Well, and to prove this I will state 2, 2 lemmas. And then, we will use these lemmas to prove this HNS3, and that will complete the proof. So, lemma1, actually I will state lemma1 and prove it, state lemma2 and prove it, and then come to the proof HNS3.

So, what is lemma1, lemma1 is, so suppose, so suppose that A is contained in R, contained in B be extensions of rings, rings always been commutative and with identity elements. With A noetherian ring and B is an A algebra of finite type, and B is a finite R module. You should remember the difference between finite type algebra and finite R module. Finite R module means, it is as an R module it is finitely generated, not finite as a set. And algebra of finite type means it is as an algebra it is finitely generated.

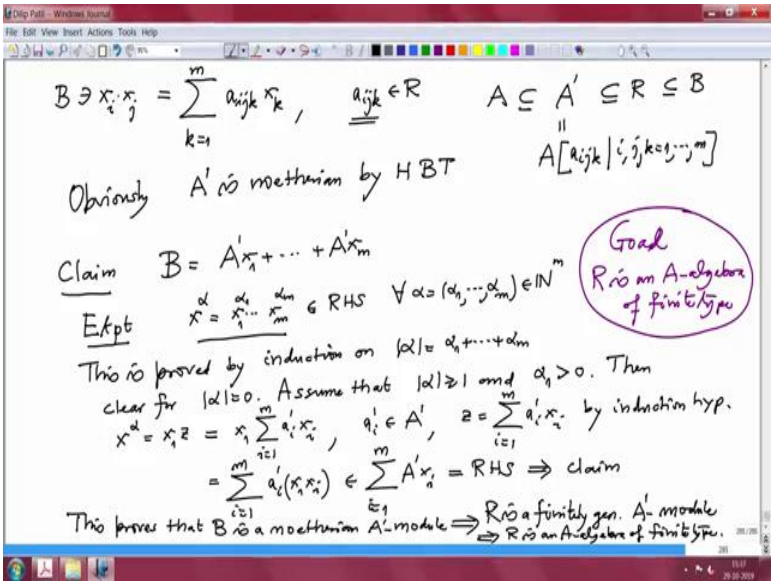
Under these assumptions, then R is an A algebra of finite type. In particular, R is noetherian, R is a noetherian ring. Because A is noetherian we have given, and this R is, conclusion is this R is A algebra finite type. Therefore, by one of the corollary to Hilbert basis theorem, this in particular part is clear. So, in particular part I will just mention here by HBT, Hilbert Basis Theorem. So proof, so let us write down first what are all given, in the notations. So, what is given, A is neotherian that is given, and then we have given that this B is finite type A algebra.

So, we have given that this B is A x1 to xr, it says an algebra is a finite type means, this is generated by as an algebra by these R elements, and this square bracket means as an algebra it is generated by that. Or this means, that this is the residue class algebra of a polynomial ring, over A in R variables, modulus of ideal, that is this given. And then we have also given, this B is a finite R module. So, we have also given that this B, the same B, so I will write equality here. This one is as a module over R it is generated by finitely many elements.

So, this is module over R, this is R linear combinations of finitely many elements y1 to ys, small ys to, small y into small s. Now, what I am going to do is, I am going to put yi equal to xr plus i, for i from 1 to s. And why do I do that? If B is generated by this y1 to ys then I can put more element there also, still it will generate the whole B. Similarly here, so then this will also be equal to A and I will also put m equal to R plus s. Then this A I could write; I added more elements. So, still it will generate because this generating set is contained there.

And similarly, this will be R x1 to xm. Because I have added x1 to xr here, and I have added xr plus 1 to xm here. So, what is the achievement? Achievement is, as an algebra over A, B as the same generating set, and as a module over R it has the same generating set. That is a good achievement, you will see the neatness in the proof because of this.

(Refer Slide Time: 26:17)



So, now this xi and xj if I multiply xi and xj in the ring B, this in the ring B. Because both were elements in the ring B. On the other hand, so this a R linear combinations of the x. So, this is

equal to summation aijk xk, this sum is running over k from 1 to m where this aijk's they are elements in the ring R. Because as a module over R it is generated by this x1 to xm. Now, I am going to concentrate on these coefficients and consider A prime sub algebra of R this, this is a sub algebra of R, A sub algebra of R generated by this (())(27:34) they are finite linear with them.

So, adjoint with A, so A adjoint with aijk, where ijk are varying from 1 to m. So, this contains A, this is a sub algebra A, A sub algebra of R generated by this finitely many elements. So obviously, this is a finitely generated algebra over R. So, obviously, A prime is noetherian by Hilbert basis theorem. Because it is finite type algebra over noetherian ring. So now, what is that we wanted to prove? We wanted to prove that, R is a finite type algebra over A, that is our aim. So, I will write the goal, so goal is what, R is a, R is an A algebra of finite type, that is the goal.

So, first I claim, so claim, as a module over A prime, B. So, B is also module over A prime. We have given A, B is a module over R is finitely generated and it is generated by this x1 to xm. But now I want to claim that, this B is a finite A prime module, with the same generating set. So, claim is B is A prime combination, A prime linear combination of x1 to xm. We know that, B is generated as a R module by x1 to xm, but this says that B is generated as a A prime module by x1 to xm.

So, why is that? So, for this what are the elements of B? Elements of B, we know B is generated in a algebra over A by x1 to xm. That means, every element in B is a sum of monomials in this small xi's. So, it is enough to prove, enough to prove that, every monomial in small x that is x power alpha, this means calculus notation x1 power alpha1 xm power alpha m, this already belongs to RHS for every alpha equal to alpha 1 to alpha m in N power m. Because every element of B, we know that every element of B is a polynomial in this small xi's. I am not saying unique, but it is a polynomial expression in this small xi's. That means it is a finite sum of such mononomials with coefficients in A, that we know.

So, if I prove that all these guys are in RHS, then whole B is in RHS because A is also contained in A prime. And how am I going to prove this? This we will prove it by induction on the, this is proved by induction 1 mod alpha, mod alpha is sum of alpha1 to alpha m. So, the assertion is very clear for. So, clear for formed alpha equal to 0. That means, all these indices are 0, that

means this x power alpha is 1, and therefore it is clearly in A and therefore it is, assertion is clear.

Assume that, mod alpha is big or equal to 1 and we may assume and alpha1 has to be bigger than 1. If alpha1 is 0, then you interchange with some other alpha, interchange xi's. Therefore, we can assume alpha1 is bigger than 1. And then, what is x power alpha? x power alpha will be, x1 will come out time z and now z, z is a monomial in x, small x and the degree has droped by at least by alpha1, which is positive, so at least by 1. So therefore, this z is again a combination of A prime linear combination of this x1 to xm. Therefore, this which is equal to x1 times summation i from 1 to m ai prime xi.

Which belongs to, so where, so I should not where, ai prime they are in A prime. So, this is because we have written z equal to summation i equal to 1 to m ai prime xi, so we have assumed this by induction hypothesis. So therefore, I plugged it in that z here and we got this, and now we push that thing inside. So, this is equal to summation i is from 1 to m ai prime x1 xi, this. But x1 xi, I know again that is in linear combinations of this xk with this coefficient they are now in are A prime.

So, this is clearly belongs to RHS, this clearly belong to summation i is from 1 to m A prime xi, which is RHS. So, that implies claim, this claim that B is generated by this, once you have proved the claim, then what did we prove that, so we have proved, so this proved that it is a finitely generated module over A prime and A prime is neotherian by Hilbert basis theorem.

So, this proves that, this proves that B is a neotherian A prime module. And therefore, every sub module is finitely generated. And R is a sub, A prime sub module of B, so that implies R is a finitely generated A prime module. But this A prime, this is finitely generated A prime module and this is finitely generated A algebra, therefore all together R will be finitely generated A algebra. So, that will prove that a R is an A algebra of finite type. That is what we wanted to prove. So, this proves lemma1 completely and then I will take a short break and after the break we will complete the proof of HNS3. Thank you very much.