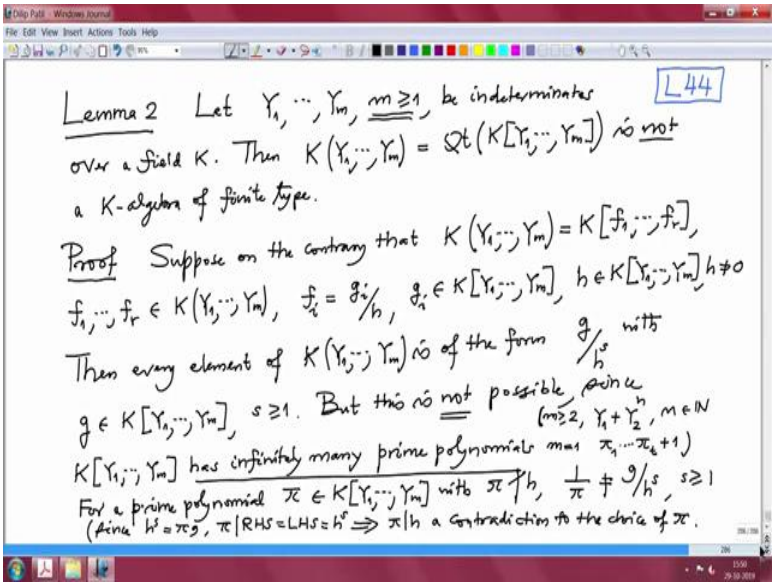
Introduction to Algebraic Geometry and Commutative Algebra
Professor Dr. Dilip P. Patil
Department of Mathematics
Indian Institute of Science, Bengaluru
Lecture 44
Proof of Zariski's Lemma HNS3

(Refer Slide Time: 00:27)



Come back to this second half of today's lecture, where we are proving, we are preparing to prove HNS3. This is the third formulation of Hilbert's Nullstellensatz. So, we have proved already lemma 1 and I need another lemma, which is not so difficult. So, lemma 2 this is again lemma from field theory actually, this is about the field extensions. So, so suppose, so let, Y1 to Ym, m is at least 2, m is at least 1 not 2, be indeterminates over a field capital K. Then this K round bracket Y1 to Ym which is, this is the quotient field of Qt of the polynomial ring.

So, elements of this field are precisely the rational functions, that is polynomial divided by polynomial. So, then this is not, not a K algebra of finite type. Remember, this polynomial algebra is algebra of finite type over the field K. But if I take the quotient field, that is not anymore K algebra of finite type. This is very, very important fact and I will give you at least two proofs of this. The first proof will depend on the fact that this polynomial algebra over a field is a UFD Unique Factorization Domain, that one usually learns in the first basic course on algebra.

So, that is called the theorem of Gauss. So, I will assume that, so proof. So, how does one proof such a statement that it is not an algebra of finite type? That means, that means we want to prove that it is not generated as a K algebra by finitely many elements. So, suppose on the

contrary, suppose on the contrary that K round bracket Y1 to Ym is finite type algebra. That means what? That means it is generated by finitely many elements. So, finitely many f1 to fr, where f1 to fr are not polynomials, but they are rational functions.

They are elements in K Y1 to Ym round bracket not the square bracket, but any case they are rational function. So, I will again make the common denominator and assume that fi's are of the form, some polynomials gi's divided by h, where these gi's are polynomials in Y, Y1 to Ym, with coefficients in K. And this h is also an element there, h is also polynomial in Y1 to Ym and h is not 0.

So, if they have different denominator, then I will multiply numerator and denominator by more and this fi will not change, but the denominator will be a common. This is a standard trick, when one is applying this trick right from the school days. So, what does this equality means? This equality means that every rational function is a polynomial in this fi's over K. And once, it is a polynomial in this, that means it is polynomial in this rational function with coefficients in K. So, that means I can clear this denominator again.

So I will, so that will mean that every rational function will be, so this assumption, this, so then every element of this rational function field K Y1 to Ym is of the form some polynomial g divided by some power of h, with the same h. So, g belonging to K polynomial Y1 to Ym, and s is some integer big or equal to 1. 1 is needed because these fi's are of that form. It could be more, because if, when I write this g, when this rational function as a polynomial in this, you might need to, that might come, fi might come in that with power 2 because it is algebra generator and therefore, I have to clear h square.

So, therefore it will be like this. And I want to say now this is not possible, but this is not possible. Since, not possible since, at least I should give you an element where I should give you a rational function, which is not of this form. Since, this K Y1 to Ym has infinitely many prime elements, infinitely many prime polynomials. That we know, this statement is very easy.

Why is that? First, how do I apply this? So, if this h is one polynomial and therefore it will have only finitely many prime factors and I am going to choose a prime factor, which is a prime polynomial, which is not a factor of h. So, first let me finish why it is not possible. So, for a prime factor from a, for a prime polynomial pi in K Y1 to Ym with pi does not divide h, 1 over pi cannot be written in this form, g by h power s for any s is not possible.

Why? If it is possible if yes, then I cross multiply. And then, we will get h power s equal to g h. So, since, I will write in the bracket, since h power s will be equal to pi g, and pi divides RHS which is LHS which is h power s. And pi is a prime polynomial therefore, if pi divides power of h, then pie will divide h, a contradiction to the choice of pi.

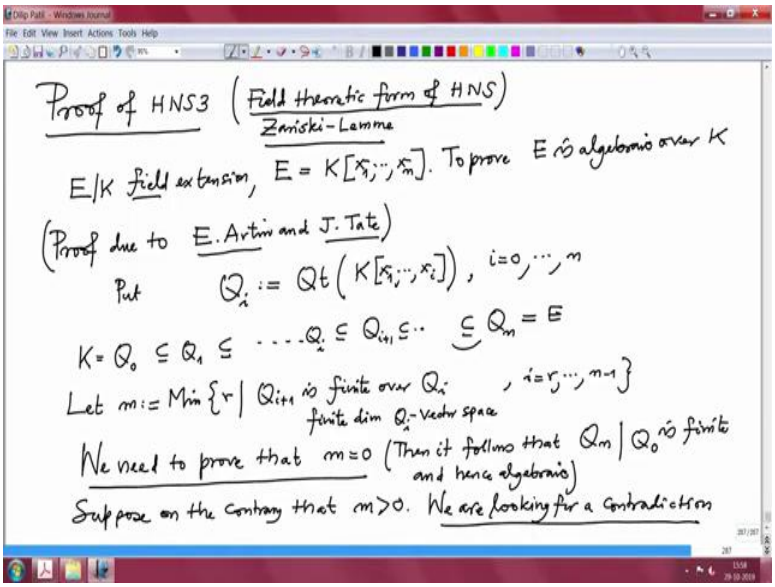
So, if we know that there are infinitely many primes in this polynomial ring, then we are done. And how do you check that it is, there it has infinitely many primes, that is where we use the assumption m is at least 1. And why is that? For example, I will give. So, this I want to prove this statement that it has infinitely many prime polynomials that does not require much space, so I will write here. So, if m is big or equal to 2 just, that means there are at least two variables, two indeterminates. Then look at the polynomials Y1 plus Y2 power n, where n is any natural number.

All these polynomials are prime polynomials, that is easy to check. And if m equal to 1, there is a standard trick, if you have only finitely many prime's the Euclid's trick. If pi1 to pi are the only primes, pi 1 to pi t are the only primes, then you look at pi 1 to pi t product and add 1 to that and we know now, this ring is a unique factorization domain. That means, and this polynomial, this is a polynomial is non constant polynomial. Therefore, it should have a prime factor and that prime factor have to be different from pi 1 to pi t.

So, that is the proof that this polynomial ring has infinitely many prime polynomials. And with that we proved that, this 1 over pi cannot be in this form. So, that means, this statement is not true that, every element of rational functions is of the form this, this is not true. Therefore, our assumption is not true. Therefore, the lemma is true. So, that proves the lemma.

And I also said that, one can also give more elementary proof than this which does not use the fact that the polynomial ring infinitely many variables is a unique factorization domain. But this simple proof I will write as an assignment. So, now we have prepared for the proving HNS3. And now, I will come to the proof of HNS3.

(Refer Slide Time: 12:29)



So, proof of HNS3. And remember this, this is purely field theory statement, this is also called sometimes some books also call it a field theoretic form, field theoretic form of HNS. This is also known as, Zariski lemma. HNS1 is called, and some people call it algebraic formulation. Because that gives a maximal ideal. And HNS2 is a strongest one, which is also called a geometric formulation.

So, what is, what do you want to prove? We have given E over K field extension and E is a field, now E is actually field. If E is a finite type algebra over K, so E is generated by over K by, by x1 to xn, finitely many elements. Then I want to prove, to prove E is algebraic over K. That means every element satisfies a non-zero polynomial with coefficients in K. So actually, it is enough to prove that these xi's are algebraic over K.

So, that is what we are going to prove and the prove I am going to give, so this proof is due to, proof due to Emil Artin and John Tate, John Tate was student of Emil Artin. So, so we have this E and we want to prove it is algebraic over K. So, let us denote some notation. Let us call this, put Ei, not Ei, Qi this is quotient field of Qt of K. You take algebra, sub algebra of E generated by x1 to xi. This is an integral domain, because it is a sub ring of E, sub ring of a field and therefore it is an integral domain.

Therefore, quotient field make sense. And I am taking i is from 0 to n. So, what is the diagram? So, when I take i equal to 0, it is a Q0 which is a quotient field of K, i is 0. So, there is nobody attached to K. Therefore, it is quotient field of K, but K is already field. So, K is

already Q naught contained in Q1. And so on, it is a chain and the last one is Qn, which is already E. Because when I take i equal to n, this is already E, and E is given to be a field. Therefore, it is already E.

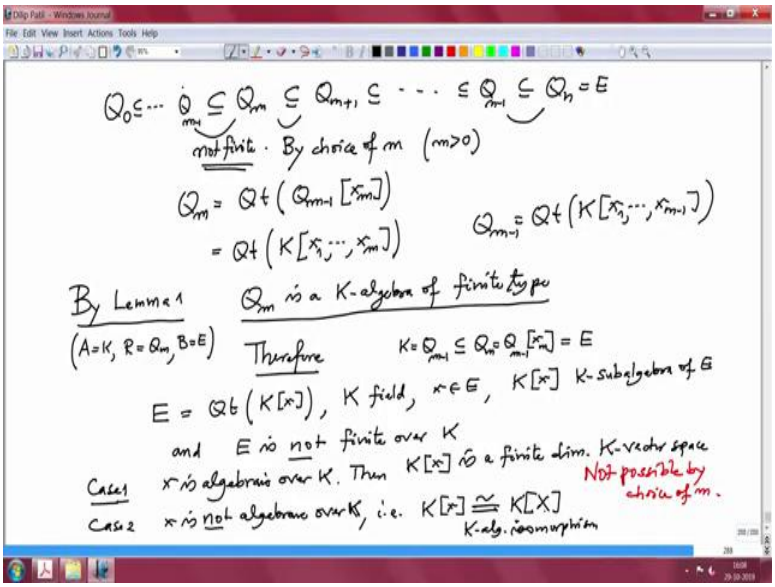
So, I have such a chain of fields. And what so we want to prove? I want to prove this E is algebraic over K. So, let us put, let m equal to minimum of R, such that this Qi plus 1 is finite over Q, over Qi. See, Qi is, Qi plus 1 is somewhere here and Qi is here. So, I take where this is finite over Q. This simply means that these Qi plus 1 is finite dimensional Qi vector space. Look at all this i's and take, and i is varying from r to n minus 1. So, what I am saying? Look at this is, this is, if this is finite vector space keep it go to the next, if it is finite keep it go to the next one.

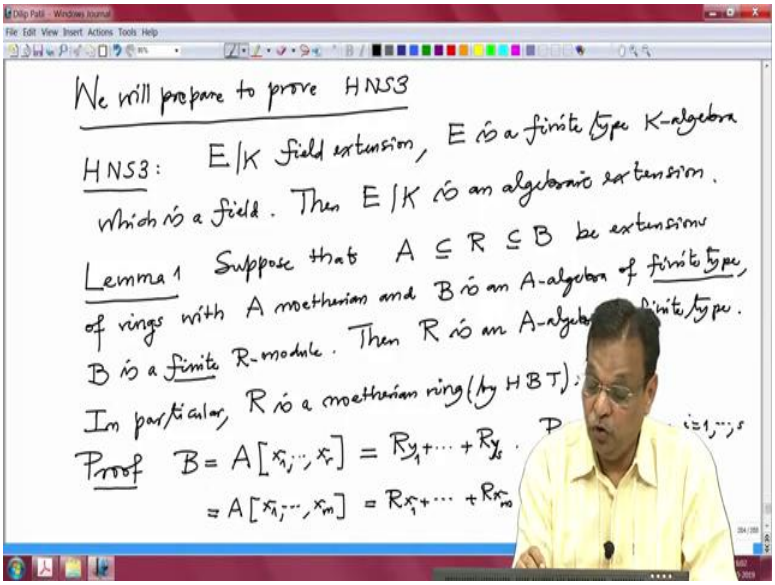
So, you choose, choose R so that R is minimum with this property that, all these later ones they are finite vector spaces over the earlier one. So, takes such R, what does this mean? This means, now what is to be proved now? See, if this is finite over Q then it is already algebraic. So, this is algebraic, this is algebraic, this is algebraic, so up to R they are definitely algebraic. And therefore, we need to prove what? We need to prove that these R has to be, this minimum m has to be 0. So, we need to prove, to prove that m equal to 0.

Because if we would have proved m equal to 0, that means all these extensions are finite extensions, and finite extensions are algebraic and algebraic, algebraic properties are transitive properties. So therefore, if this is algebraic, this is algebraic, then this is also algebraic. So, I have to prove m is equal to 0, m equal to 0 that is, if I prove m equal to 0, then it will, then it follows that Qn over Q naught is finite and hence algebraic, but this is precisely En over K.

Finite field extensions are algebraic, so as I said, actually this proof also shows that we are actually proving it is finite. So, we want to prove m is 0. So, if we assume, so if, suppose on the contrary, that m is positive, on the contrary that m is positive. Then we are looking for a contradiction, we are looking for a contradiction. So, let us see.

(Refer Slide Time: 21:16)





So, so let me draw this Q0 is here, Qm is somewhere here, and Qm plus 1 is here and this, this is Qn here which is E here, and this is Qn minus 1, and so on. And this is finite, this is also finite, and now this is not finite Qm minus 1 this is not finite. That is how we have chosen our m. So, this is by choice of m.

And obviously, we are assuming m is positive. So, what is Qm, so note Qm was what? Qm was the quotient field of, quotient field of you take that field earlier one Qm minus 1 and the attached xm. Actually, Qm was by definition it was the quotient field of this integral domain x1 to xm. But this is same as, this is not same as this but, because this is a quotient field and this Qm minus 1 is also contained there. Because this a quotient field of Qm minus 1 is a

quotient field of K x1 to xm minus 1. So, this is a field, and therefore this is a smallest field which contain K x1 to xm and therefore both these are equal.

So, then we know by what did the, what did we prove in lemma1? So, here it is. So, I will write here by lemma 1, Qm is a K algebra of finite type. Remember, what is the lemma1? Lemma1 if you have in between thing, that is this is my R, this is your B and this is our K. So, this is A, this is R, and this is B. And this E is finitely, finite over Qm that we know, and this Qm over this, this is, this is a ring in between. And so, therefore by check, by lemma 1 this is actually, K algebra of finite type.

So, I will show you, what we proved in lemma 1. So here, this situation this B, B was our E. E is an, B is A algebra of finite type, that is the assumption we have given in HNS3. This R, B is finite R module, that is also given by our choice of m. And then what is the conclusion? This is A is noetherian, but A is over field K, therefore noetherian. And the conclusion is, this R is A algebra of finite type that is precisely, what I have written. See here, so here I will say apply to A equal to K, R equal to Qm, and B equal to E.

So therefore, it is an algebra of finite type. Therefore, therefore we will consider, therefore I want to clean up little bit notation, therefore, we reduced to the following case. So, E is a quotient field of some sub algebra, see this is generated by one element only. So, I want to take, I want to enlarge, I want to forget K and work with Qm and minus 1. So, let us look at the situation. This is my K, which is Qm minus 1 and then this one is, next one is Qm, Qm which is, which is Qm minus 1 xm and this is contained in E.

Ultimately, we are getting, we want to get a contradiction. So, I will forget this E, and call this as E. So, in the new notation. This is my E, so I will forget this E and call this as E, and forget this Q and call this Qm minus 1 as Q. And, and now I want to get a contradiction to the fact that this is a K algebra of finite type. So, this is, if it is a K algebra of finite then it will be K algebra of finite, finite over Qm minus 1 also. So, we are in this situation.

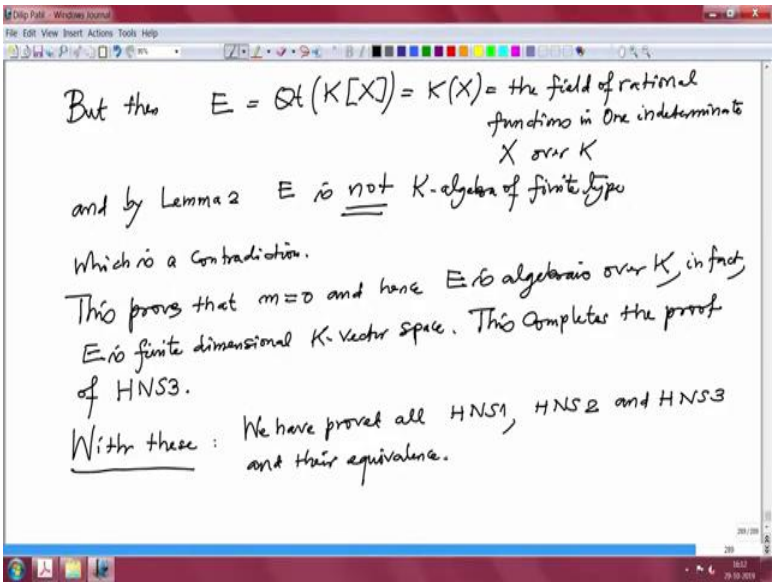
E, this is the quotient field of the sub algebra Kx. Where K is, K is a field and x is an element in E. And this Kx is therefore, K sub algebra E, in this situation, we are in this situation. And, and this is not finite, and E is not finite over K. That is how we have chosen over m that this is not finite, this is not finite. So, this is my K, this is my Kx and, so we are in this situation. And what do you want to prove? I want to, I am looking for a contradiction. Because we assume that, this m is positive, so looking for a contradiction. So, there are 2 cases. So, case 1 x is algebraic over K or not, x is not algebraic over K.

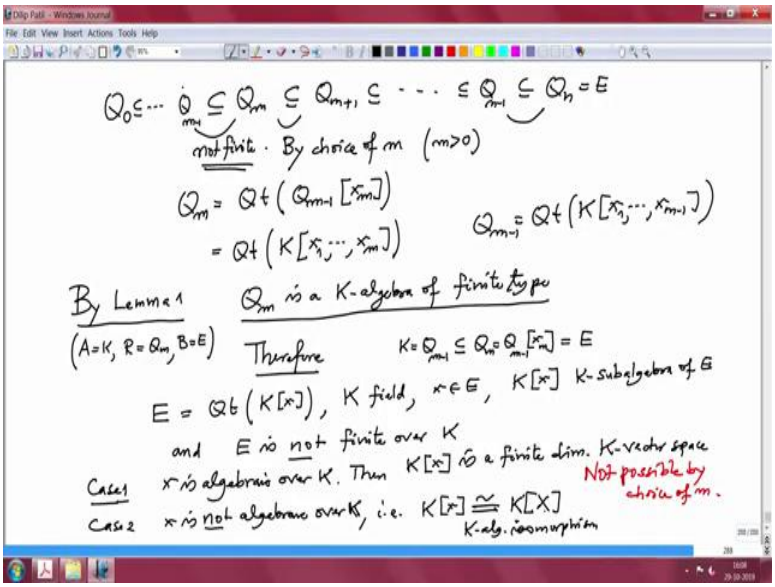
There are only two possibilities. I will say that the first possibility does not occur, why? Because if it is algebraic then this, this is a finite dimensional vector space, finite dimensional K vector space. But that is not the case, we are assuming it is not finite dimensional. So, we are assuming, remember we are assuming it is not finite dimensional by our choice of m. So, this is not possible. This is not possible, not possible by choice of m.

So, it is not algebraic that means what? That means it is transcendental. So, that is this Kx is a polynomial algebra. It does not satisfy any, any polynomial over K that mean this is a transcendental alone, so this is isomorphic as K algebra isomorphism. That means the, the map which sends this capital X to small x, this is clearly surjective and also it has to be injective because if it is not injective, the kernel will contain a non-zero polynomial in that and that will mean that X is algebraic.

But because of our assumption X is not algebraic, that has to be an isomorphism. So, this is isomorphism as K algebras. And now, what is E then, E is a quotient filed, so.

(Refer Slide Time: 31:42)





But then E is nothing but the quotient field of the polynomial algebra in one variable, which is field of rational functions. See, this is the field of rational functions. Functions in one indeterminate X over K.

And what do the by lemma 2 says? Lemma 2 says such a field of rational function the variable is at least one, that cannot be finite type over K. So, and by lemma 2 E is not K algebra of finite type. But that, which is a contradiction. See, because look here, what we are assuming. This is a, so this is finite, this is by lemma 1 this is finite type, this was finite type over E, but that is a quotient field of this which is E. And so therefore, it is not possible therefore, so this proves that m must be 0 and hence E is algebraic over K. In fact, E is finite dimensional K vector space.

So, this completes, completes the proof of HNS3. So, with these, with these we proved all HNS1, HNS2, and HNS3, and their equivalence. So, this was, this is a big step. This is in fact, the beginning of modern algebraic geometry. And in the next lecture, and the next 2 lectures, I will draw a lot of consequences from Hilbert Nullstellensatz. Where I will be allowed to use any formulation that one likes, because we all know that they are equivalent. So, I will draw many nice applications of this Hilbert Nullstellensatz, some are geometric, some are algebraic. And that will give us a interplay, between algebra and geometry.

Some results which look harder to prove in geometry, we will prove them by, precisely by using algebra. And some results, which are algebraic will be proved by the geometric statement. And then further, we will strengthen this study and study more basic properties of the Zariski topology and their algebraic meaning, by using the Nullstellensatz. So, with this I

will stop and we will continue in the next lecture, the Consequences of Nullstellensatz. Thank you.