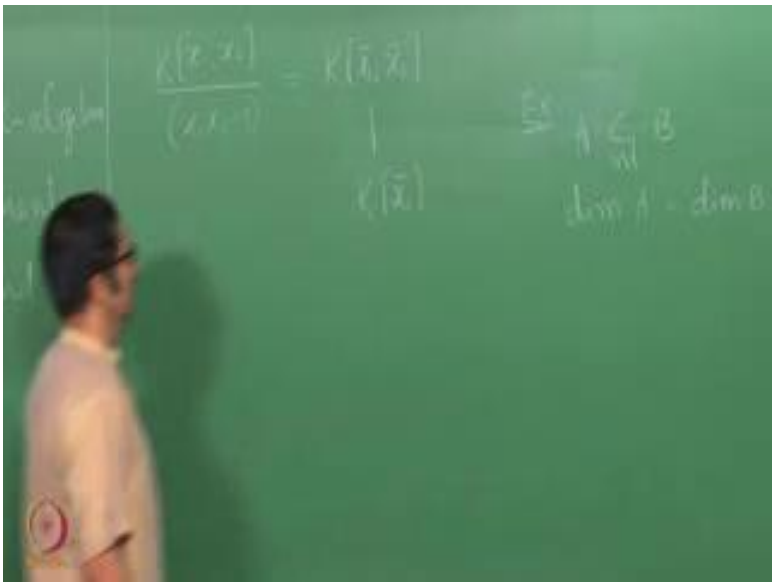
Commutative Algebra
Prof. A. V. Jayanthan
Department of Mathematics
Indian Institute of Technology, Madras

Lecture - 38
Hilberts Nullstellensatz

(Refer Slide Time: 00:25)

So let us quickly recall Noether normalization, let R be a finitely generated K algebra then there exists variables; algebraically independent elements z 1 up to z r in R such that K z 1 up to z r injection to R and R is a finitely generated, let us call this S module. So, I mean we proved this when the field K is infinite, I am not going to repeat the proof, but I will quickly go through the steps. So, here what we did was we proved this by induction on n, but what is this n I am looking at? So, when I write this K X 1 up to x n, I mean R is a K algebra generated by x 1 up to x n. These need not be variables, if you are; if you have confusion yeah, I will just simply write like this. See for example, we discussed this or you know over K.

(Refer Slide Time: 02:42)



So, if I look at this K algebra x 1, x 2 minus 1. So, this I can write as K algebra generated by x 1 bar x 2 bar. Now this is see x 1 bar as it is algebraically independent over K because it does not satisfy any equation over K, but now if I look at this one; x 2 satisfies and algebra equation over K X 1 which is x 1 x 2 minus 1.

So, if I look at this x 1 bar T minus 1, this is a polynomial.

Student: (Refer Time: 03:45)

No. So, this is not integral, this x 2 satisfies a polynomial, but does not satisfy an integral equation, the extension being integral, one big advantage of extension been being integral is that the dimensions are same, yeah, it will be finite first of all. Secondly, the dimension of A, so if I have an integral extension A contained in B, so we defined the scroll dimension; maximal length of chain of prime ideals. So, if this is integral then scroll dimension of A is same as scroll dimension of B. So, in this case, x 2 is not integral over this ring, but it satisfies is an algebraic equation. So, when I write R equal to this form I mean x 1 up to x n are generators of R over K as a K algebra they need not be algebraically independent here x 1 bar and x 2 bar are not algebraically independent that is one remark I wanted to make.

Now, so how did we prove? We proved first of all if x 1 up to x n are algebraically independent, we are through we can just take R to be equal to n itself, we do it by

induction on n if n is 0 you can take R to be 0, suppose n is bigger than 0, if they are all algebraically independent we can take R to be equal to n and z i equal to x i and we are through. Suppose we have a polynomial which is satisfied by this, we look at a homogeneous component of I mean all the homogeneous components of the polynomial which is satisfied by this then we look at the leading homogeneous term that is the homogeneous term of highest degree.

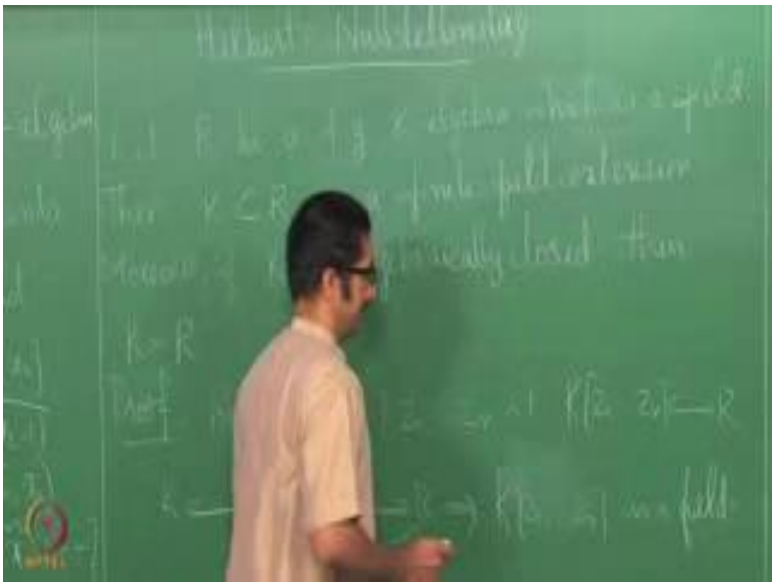
Now what we do is that we make coordinate changes so that this becomes a monic polynomial in one of that variables say x n. So, how do we do that? Given a homogeneous polynomial, we proved that lemma saying that there exists an n minus 1 tuple such that f i mean, it does not vanishes it that which is not a root of the given homogeneous polynomial there we use the fact that the field is infinite for that part we need the field to be infinite otherwise we cannot really say this. So, so that that using the fact that it is infinite we convert the given polynomial into a monic polynomial and that gives me the I mean I just change the twist I mean tweak the generators and get in a slightly new form y 1 up to y n such that they satisfy the same polynomial which is monic as a polynomial in y n.

So therefore, what we get is that y n is integral over K y 1 up to y n minus 1. Now K y 1 up to y n minus 1 has only n minus 1 generator as a K algebra therefore, we can

Student: extended.

Up, we can apply induction and say that there exists variable z 1 up to z r such that K is z 1 up to z r injects into K y 1 to y n minus 1 and the extension is finite. Now K y 1 up to y n minus 1 to K y 1 up to y n it is again finite because it is integral y n is integral over.

(Refer Slide Time: 08:52)



Student: (Refer Time: 08:25)

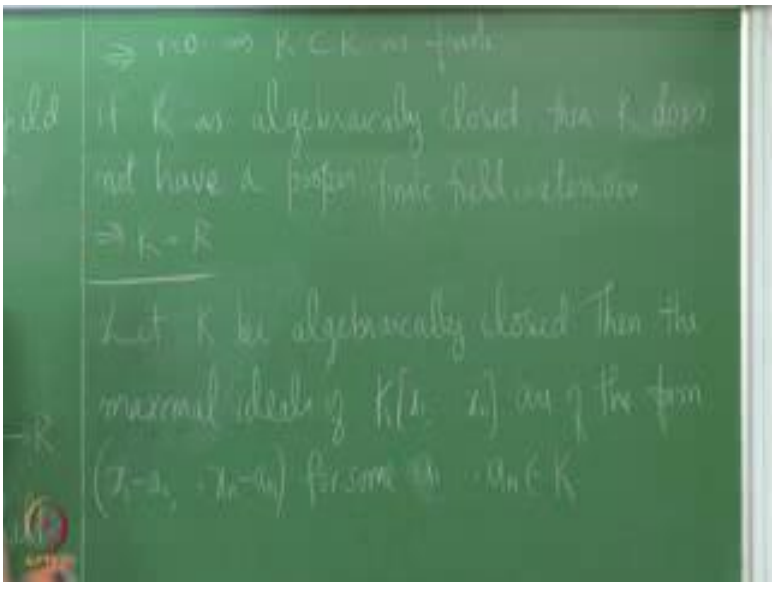
K y 1 up to y n minus 1 therefore, we have K z n up to z r to R is finite that is how we proved the Noether normalization lemma. So, as a corollary to Noether normalization lemma we proved Hilberts Nullstellensatz; Nullstellensatz in German, I mean this is German word meaning theorem of 0s. So, there are three forms we will be discussing three forms of Nullstellensatz. So, the first form is called weak form the says let R be a finitely generated K algebra which is a field if let R be yeah then K over R is finite field extension moreover if K is algebraically closed then K is equal to R.

So what this says is that if I have a finitely generated K algebra which is a field which is a field as well as finitely generated K algebra it has to be a finite field extension finite field extension means as a vector space over K see finitely generated C x 1 x 2 mod x 1 x 2 minus 1 this is. So, if I write this as C x 1 bar x 2 bar if this I mean this is a finitely generated C algebra, but this is not a finite extension see this is not a finite C module because you have many more algebraically independent elements see if I take x 1 x one square x 1, I mean images of one bar x 1 bar x 1 bar square, these are all independent over C right there is no polynomial that this x 1 up to say x n I mean x 1 x one square this set satisfies over C not over x 1 x 2 over in over C this is a linearly independent set. So, therefore, this is not a finite field extension I mean of course, this is not a field, but this is not a finite module I am say.

So here the situation is if R is a finitely generated K algebra which is a field then there are no other option and it has to be a finite field extension I mean the second part follows directly from here if R is all if K is algebraically closed which means you cannot have any finite field extension of K which means K is equal to r. So, first let us prove this part. So, R is a finitely generated K algebra now we have this Nullstellensatz which says by I mean we have the Noether normalization which says there exists z 1 up to z r such that K z 1 up to z r is contained in R now R is a field. So, I have K contained in K z 1 up to z r contained in R. Now R is a field and this is what we did proved is that this is an integral extension this is a finitely generated module over this one therefore, and this is a field therefore, this is also field thus we proved some time back I mean this what we indeed proved is that this is an integral extension.

The proof of Noether normalization say is that this is an integral extension by induction we proved at each step you can get an integral extension. This is integral, this is field, therefore, this is a field how can this be a field the only way is R is 0 a polynomial ring K X this can never be a field unless I mean K X now this one K X 1 up to x n can never be a field unless n is 0.

(Refer Slide Time: 15:25)



So therefore, this implies that K z 1 up to z r is a field what does that say that says that R is 0 that says that K to R is finite. Now if R is sorry, if K is algebraically independent sorry algebraically closed then R is then K does not have a proper finite extension and

that implies that K is equal to R, it can have infinite extension for example, see the field C.

Student: (Refer Time: 16:52)

Yeah, it is algebraically closed you cannot have a finite extension of c, but you can still have like this right you attach a variable this is an extension.

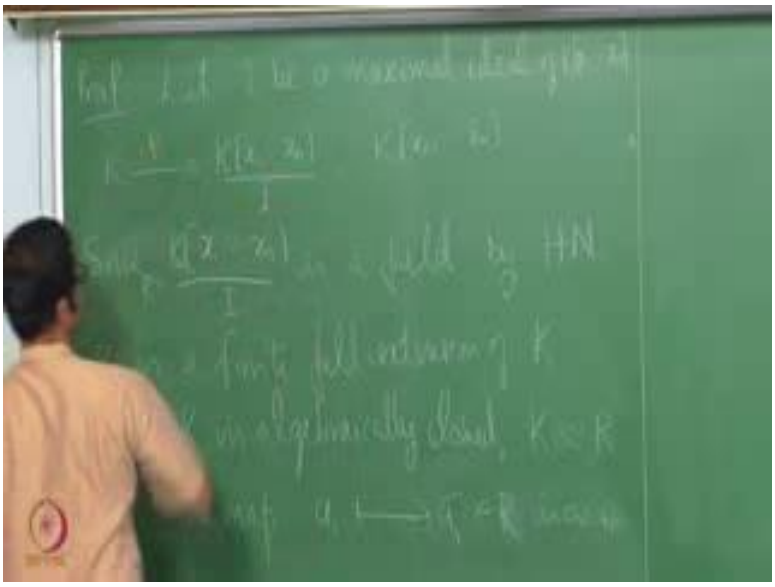
Student: sir why not finite?

Finite will imply algebraic you cannot have any algebraic extension of C, you cannot have an algebraic extension of C in particular, you can have you cannot have a finite extension of c, but this is neither algebraic nor finite. So, similarly what here if see K is algebraically closed R has to be equal to K another very important form of Nullstellensatz is the one which describes the maximal ideals of polynomial rings over algebraically close fields.

So look at; let us look at another form there is another corollary let K be algebraically closed then the maximal ideals of K X 1 up to x n are of the form x 1 minus A 1 up to you must have seen A the 1 variable version of this in say for see if you look at the if you look at the polynomial ring C x.

Student: maximal is A x minus.

(Refer Slide Time: 19:44)



Maximal ideals are always of the form x minus alpha; alpha varies over, but now this theorem says that maximal ideals of this are precisely the maximal ideals are precisely the element I mean ideals of this form. So, let us proof this let I be a maximal ideal K X 1 up to x n then I have this map K injects into K X 1 up to x n, modulo I, this is the map is a i mapping to a i bar for any K algebra case its inside the K algebra and this form K is a field. So, this map is always injective if it is non 0 it has to be injective if I is a maximal ideal this map has to be non 0 therefore, it has to be injective. So, this Ks its inside this in the natural manner, but now what we know is that I is a maximal ideal therefore, this is a finitely generated K algebra which is a field by the weak form of Nullstellensatz.

Student: (Refer Time: 21:21)

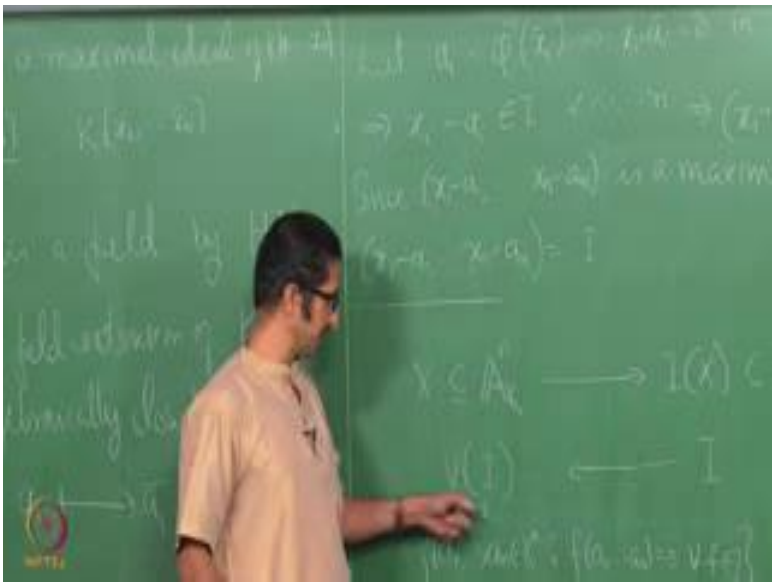
It says that this is a?

Student: finite.

Finite extension of finite field extension of K since this K X 1 up to x n mod I is a field by Hilberts Nullstellensatz weak form. So, let me call this R is a finite field extension of K, but now K is algebraically closed which means K has to be R has to be equal to K.

since K is algebraically closed K has to be equal to R or you know this K has to be I should write K has to be isomorphic to R K its inside here that image has to be equal to R or in other words a i the map a i going to a i bar in to R is an isomorphism that is what it says now if I take. So, I have this K X 1 x 2 up to x n x 1 bar. So, I write this as K X 1 bar up to x n bar. So, let me call this map phi.

(Refer Slide Time: 23:26)



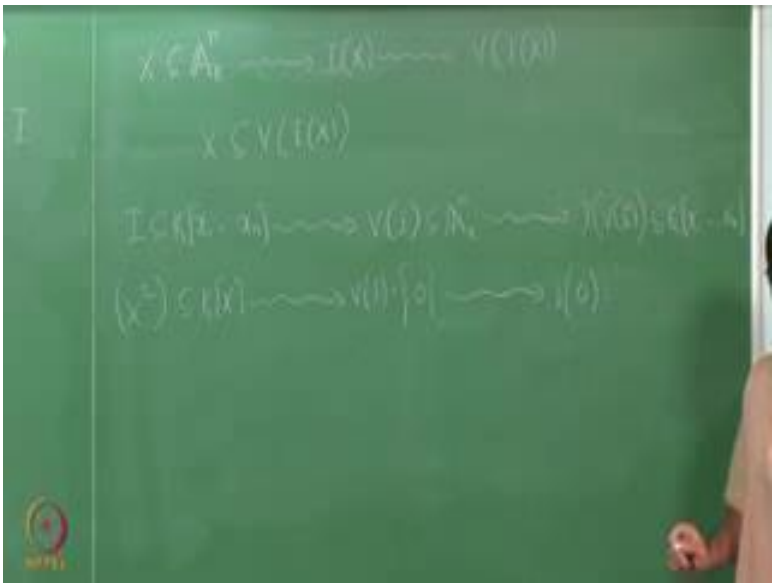
Let a i be equal to phi inverse of x i bar this is uniquely determined then what would be the. So, that says that the ideal I is precisely x 1 minus a 1 up to x n minus a n because a 1 see in this one if a i denotes this x 1 minus a 1 has to be 0 in x 1 minus a 1 has to be 0 in R similarly x i minus a i has to be 0 in R or in other words x 1 minus a 1 comma x n minus n is contained in i, but this is a maximal ideal x 1 my the ideal generated by x 1 minus a 1 up to x n minus a n is a maximal ideal therefore, they have to be equal let me this implies that x i bar minus a i bar is 0 in R which is K X 1 up to x n modulo I that implies that x i minus a i is in I for all I from one to n that implies that the ideal generated by these elements this is contained in I. Now this is a maximal ideal I is maximal is a maximal ideal they are equal that is precisely what we wanted to prove every maximal ideal is of this form.

Now the third form of Nullstellensatz talks about how you know how closure of a variety looks like or in other words I will. So, given a set X in a and K, I can now go to the polynomial ring by looking at I of X the ideal in K X 1 up to x n. Now given an ideal I in the polynomial ring I can look at all the common 0s of I V of I V of I is set of all a 1 up to a n in K n. In fact, A n K you can say such that f of a 1 up to a n is 0 for all f in I all the common 0s. So, if I start with an algebraic set I can get an ideal and then come back here I go back to this one, I again land up with a set here, I start with an ideal here, I come to this one to get a set in A n K and then go back to get an ideal here what are the relations between these 2.

Student: (Refer Time: 27:55)

So, if I start with let us start with an element X in A n K and then get an ideal I X and then go to V of I of x can we say some relation between them.

(Refer Slide Time: 28:02)



Student: (Refer Time: 28:32)

X is contained in V of I of X, can we say that these 2 are equal.

So, let us look at the other one, I start with an ideal I in K X 1 up to x n I have V of I which is a variety in a in K and then I get back to I of V of I sorry, K X 1 up to x n. Let us start with a simple example here, suppose I take X suppose I take the ideal X square, what does X square in K X; what is the 0 set here? ASll elements which vanish on all elements of ideal, what would be V of I?

Student: 0 only.

0 only, V I will be 0 only that is the only element which will vanish on every element of this. Now what if I go back I of 0 I am looking at now I am looking at all the polynomials in forget about this, what we started with, now I have this set I am looking at all polynomials in K X which vanish on 0.

Student: all the (Refer Time: 30:30) term 0.

Which is the ideal generated by X? So, what is the relation between these 2?

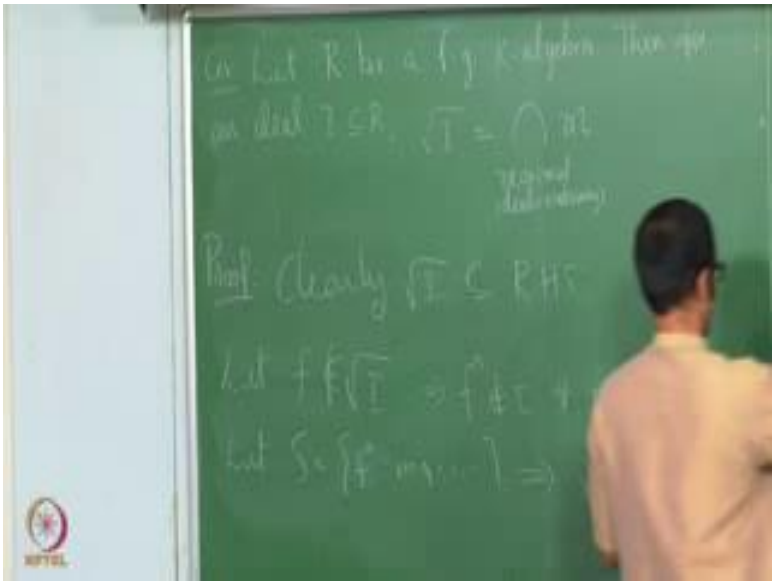
Student: (Refer Time: 30:46)

This ideal is contained here and what does the exact relation between these 2 ideals? Can you give me a precise relation between these 2 ideals? Ideal generated by X square and ideal generated by X.

Student: (Refer Time: 31:06)

Yeah or in other words, radical of this is yes and that is precisely what the Hilberts Nullstellensatz says that you start with an ideal form variety and then take the ideal of that variety what you get is nothing, but the radical of the ideal that we started with.

(Refer Slide Time: 31:41)



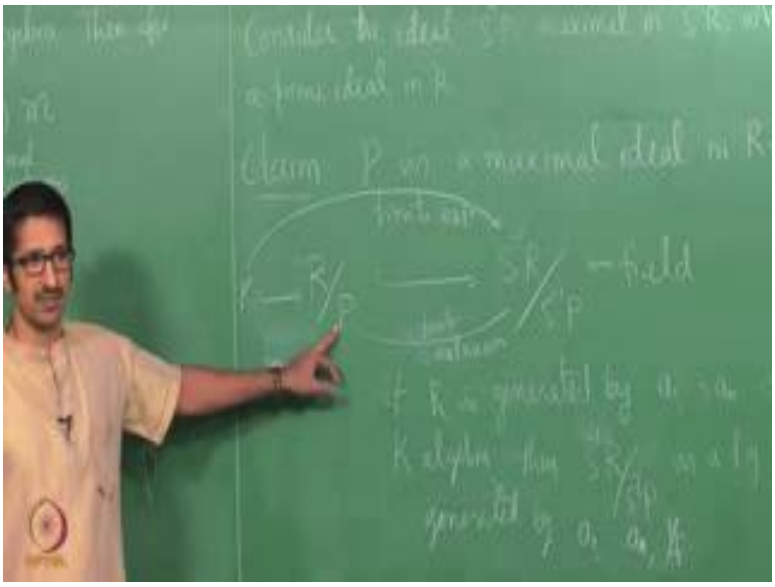
We first prove, a slightly more general form, let R be a finitely generated K algebra then for an ideal I radical of I. So, we have already seen the definition of radical it is the you know all elements with some power of the elements contained in I we then proved that it is nothing, but intersection of all prime ideals containing I, but now in this specific situation that ideal I is contained in a finitely generated K algebra radical of I is nothing, but set of all maximal ideals containing I. So, in this one inclusion is clear.

Student: this is contained.

This is contained here right clearly radical of I is contained in the right hand side.

Now what we need to show is that if there is an element which is not here I want to say that there exists a maximal ideal that misses that element. So, let f be not in radical of I; that means, f power n does not belong to I for all n or in other words if I take I look at this set f power n and from 0 1 2 and so on then S intersection I is empty.

(Refer Slide Time: 34:14)

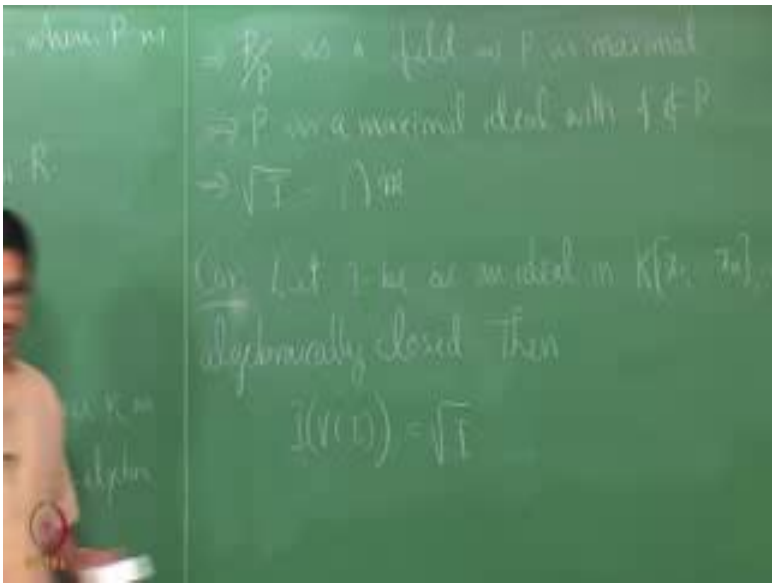


So, consider the ring S inverse p yeah maximal in S inverse R I look at the ring S inverse P sorry consider the ideal S inverse p maximal ideal in S inverse R and P is prime and see the correspondence between prime ideals of S inverse R and R we already know that you know they are all prime ideals that do not intersect with S. So, therefore, this is a prime ideal where P is a prime ideal in R. Now I claim that P is indeed maximal in R suppose I prove that P is maximal in R that would say that f cannot be in P naturally because f is in S this f this is in S if I say that P is maximal in R S inverse S inverse P is maximal ideal if P is maximal in R I have obtained a maximal ideal which do not contain f and that is exactly what we want. So, I claim P is a maximal ideal in R now how do I do this I have. So, I basically want to show that R mod P is a field. Now look at this R mod P see this is certainly an integral domain. So, I have an integral sorry I have an injection from here to S inverse R mod S inverse P, R mod P injection to S inverse R mod S inverse because R mod I mean this is an integral domain.

So therefore, I have this extension now this is a field yeah. So, this is a field yeah K yes see again you know the trick goes back to the; say that this is yeah this is a finite field

extension. So, this is yeah see this extension is finite now this extension is also finite why is this finite if I look at the generators of R if R is generated by let us say a 1 over K as K algebra then the S inverse. So, what we know is that R is a finitely generated K algebra right. So, this is a finitely generated K algebra, I want to say sorry, yeah then S inverse R mod S inverse P is a finitely generated K algebra as well generated by a 1 up to a n and 1 by f. So, therefore, this is a finitely generated K algebra which is a field therefore, by Noether and Nullstellensatz weak form this is a finite extension; that means this is a finite extension.

(Refer Slide Time: 40:47)



Now, R mod P is an integral domain you have this is a field that says R mod P is a field therefore, so this is R mod P is a field that implies P is maximal.

Student: (Refer Time: 41:02)

This is a finitely generated K algebra which is a field therefore, this is a.

Student: (Refer Time: 41:14)

Which one?

Student: S inverse (Refer Time: 41:17)

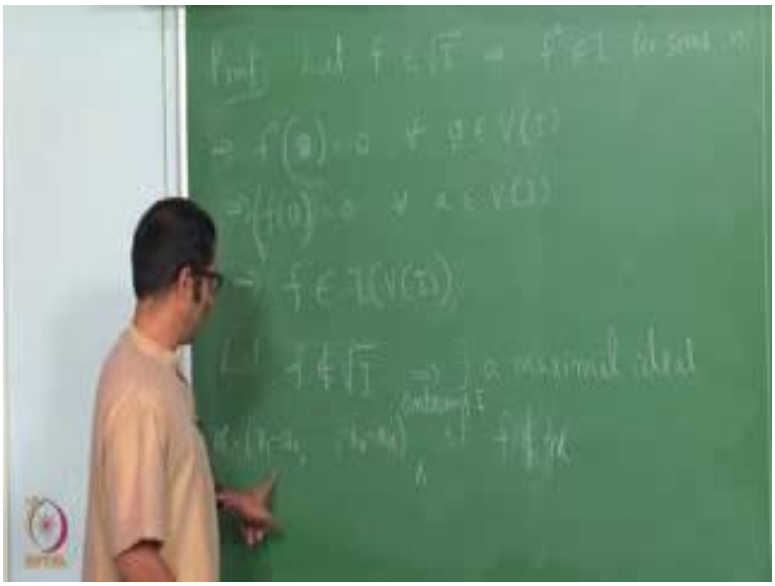
This is a; why is it a finitely generated K algebra? That is exactly what I am written if so our assumption is that R is a finitely generated K algebra.

So if R is K, suppose it I write this like this then. In fact, S inverse R itself S inverse R would be nothing, but K a 1 up to a n 1 by f.

Student: should be a 1 bar a?

So, here it is a 1 bar 2. So, S inverse R itself is a finitely generated K algebra and here we are looking at S inverse R mod S inverse p. So, this is a finitely generated K algebra which is a S inverse this is a finitely generated K algebra which is a field this is finite extension this is finite extension this is field therefore, this is field; that means, P is a field yeah sorry P is maximal ideal and that is exactly and now that implies P is a maximal ideal with f not in P because S inverse P is a maximal ideal f cannot be in p. So, that proves that radical I is intersection of maximal ideals. So, another corollary is let I be an ideal in K X 1 up to x n K algebraically closed then I f V of I is equal to radical of I this is. In fact, we do not require I to be algebraically closed one can prove this for any infinite field and in that case there is a, I mean there are you know if you just search Google there are you know a lot of proofs different proof using different techniques for this one, but there is a nice proof using Rabinowitsch trick which I will you know leave it you to check read on your own, but I will you know write it as a corollary of this the earlier result.

(Refer Slide Time: 44:42)



So suppose let f be in radical of I that implies that f power n is a is in I for some n; that means, f power n, I will write this point as f power in a is 0 for every a in V of I by

definition it is an element in I what is the definition of V of I? V of I those elements in I those elements in K n those points in K n.

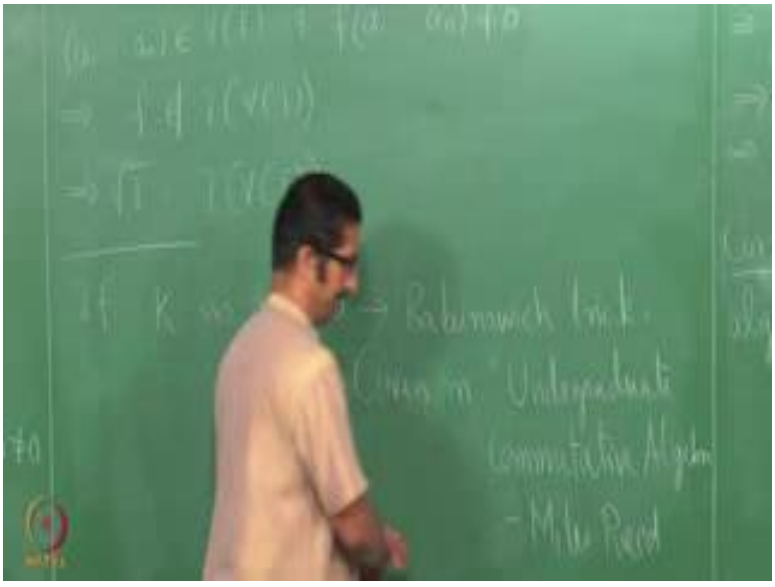
Student: (Refer Time: 45:54)

Sorry, yeah f is in this means this is 0 for every a in V of I and that directly implies that f power n: no.

Student: (Refer Time: 46:18)

So, this no, no, this says that f power n of a is 0 implies that f of a has to be 0 because it is you know f power n of a is nothing, but f of a whole power n right; that means, f of a is 0 for every a in V of part and that implies that f belongs to I of V of I. So, now, let f be not in radical of I, if f is not in the radical of I; that means, by earlier previous proposition there exists a maximal ideal x 1 minus a 1 up to x n minus a n such that f is not in. So, let me f is not in m what does that mean? See I want to say that f is not in the I of V of I this one maximal ideal containing I it has to be. So, here there exists a maximal ideal m containing I containing I such that f is not in m.

(Refer Slide Time: 48:36)



Now see m is contained in I implies that a 1 up to a n is in V of I. Write this point has to be in V of I because every element is see every element in m is a polynomial combination of this. So, if you put x 1 up to x n equal to 0 that has to be 0 therefore, this is a 1 up to a n is in V of I, but now I want to say that I of f is not in I of V of I yeah of

course, yes yeah this is see and this is not in m implies that f of a 1 up to a n is non 0 because f is in I mean this is characterization f is in m if and only if f of a 1 up to a n is 0 for every I mean a 1 up to a n is 0.

So, f is not in m implies f of a 1 up to a n is non 0 a 1 up to a n is here and f of a 1 up to a n is non 0 implies that f is not in I of V of I. So, that implies radical of I is equal to. So, that finishes the proof for Nullstellensatz. So, there is weak form of, there is a another proof if K is infinite; need not necessarily be algebraically closed then there is a proof using what is called Rabinowich trick, you can search for this in you know this proof is given in undergraduate commutative algebra by Miles Reid. I would like you to go through the proof. So, we stop here.