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

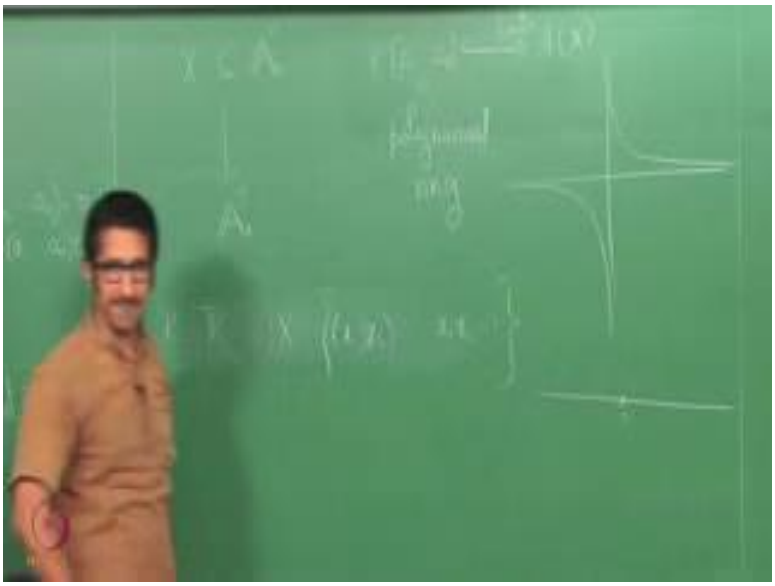
Lecture - 37
Noether Normalization

(Refer Slide Time: 00:25)

So let us do Noether Normalization. This is one result in commutative algebra which is quite important in the geometric point of view as well; let me just try to explain the vaguely explain the geometric situation. So, suppose here you have a even algebraic set in K n K is a field. So, we call this a fine space you must have already done the exercises in a Atiyah McDonald that finds the K n with Zariski topology is usually denoted by A and k and this is called a fine space. So, if you have an algebraic if you have a subset X of k n then I can define this ideal I of x set to be set of all f x 1 up to x n in K x 1 up to x n, such that f of a 1 up to a n is 0 for all a 1 up to a n in x; then this is an ideal in K x 1 up to x n; the ring A x usually denoted by A x, K x 1 up to x n modulo I of x is called the coordinate ring of the algebraic set X.

So, the idea of the Noether normalization is the following.

(Refer Slide Time: 03:11)



Suppose you have an algebraic set X in some in some A n k; the question is whether we can we do have a projection onto A r k.

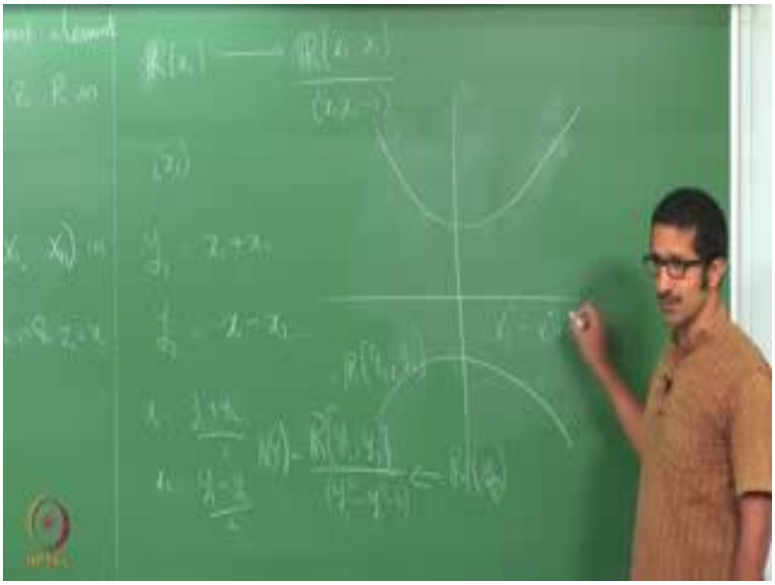
So, suppose I have a projection like this suppose I have a map between; I mean suppose I have a surjective map like this, then I have an injection from. So, I have an injection from K let us say some z 1 up to z r to the coordinate ring A of X. So, this is injective map; what does this if I have a projection like this then I have a map like this. What and what we are looking for in geometry what one looks for is can we have a projection like this. So, that this becomes a finite extension, A x become a finite extension of this polynomial ring, once you have this is a polynomial ring and this is a finite extension.

Student: (Refer Time: 05:04).

Z 1 up to z r. So, if I have a map from X to A r A k r then correspondingly I have. So, this will be the coordinate ring of this, because you have only the 0 polynomial that. So, if I have a map from X from you know K x 1 sorry; A n k to Y in A m k if I have a Morphism like this what I mean there is something called Morphism, then correspondingly I have a map between the coordinate rings of Y and X; that is what we have here, this is the coordinate ring of this variety because there is only 0 polynomial that vanishes at all points of this. So, this is polynomial ring modulo the 0 ideal.

So, the question here is whether we can have such a projection so that this becomes a finite extension it. So, turns out that it need not always be the , we need not always have such a projection giving something like this always for example, if you take. So, let us take K equal to R, X equal to the 0 set of all x 1 x 2. So, that x 1, x 2 is 1 its basically the this set.

(Refer Slide Time: 07:58)



Now, if I look at this, this as my r equal to 1, if I take the projection I will miss the point 0. Accordingly if I look at correspondingly if I have C x 1 I have C x 1 to not c does not (Refer Time: 08:06) R x 1, x 2, x 1 x 2 minus 1; this is the coordinate ring of this variety, I have this map. Now this is I do not have see if I look at the ideal generated by x 1 here this is a prime ideal here there is no prime ideal here that is lying over x 1. So, therefore, this does not become a finite extension. Now we do a small trick here everything remains the same, I do a twist here I just change my axis instead of the standard axis I change my axis to take y 1 equal to x 1 plus x 2, and y 2 equal to x 1 minus x 2.

So, when I make this transformation, the act the variety becomes like this. So, what we are doing is we are just twisting 45 degrees right this becomes the axis becomes this these 2 lines sorry. So, I denote no, is this correct.

Student: (Refer Time: 10:19).

At 1 not 0; so, this is like this at 1 it comes twisted by 45 degrees, because what happens when what is x 1? X 1 is y 1 plus y 2 by 2 and x 2 is y 1 minus y 2 by 2. So, the axis this is this line and the other one is this line. So, it is basically 45 degree.

So, you become and the variety becomes this, there is no change as such for the variety only thing is we are looking at in a different angle. Once we twist this, now what happens to the variety now? So, we are now in R y 1 y 2 and what is. So, let us call this to be the new variety to be A of Y, A of Y the coordinate ring of A of Y becomes this becomes Y 1 Y 2. So, if I take x 1 x 2 to be x 1 x 2 the product right, this becomes.

Student: Y 1 (Refer Time: 11:58).

Y 1 square minus y 2 square.

Student: Minus (Refer Time: 12:09).

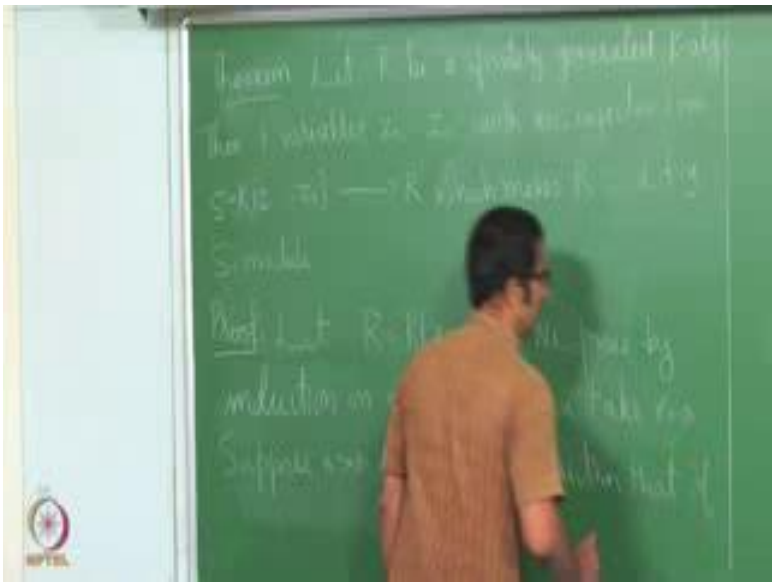
Four now this, this is see y 1 square. So, if I can take let us say I can send R y 1, now y 1 y 2 is integral over this ring, y 2 is integral over this ring not this, this one right because it satisfies the polynomial t square minus.

Student: Y 1 square.

Y 1 square minus 4, y 1 bar square minus 4. So, over this ring also y 2 is integral. So, what we are have is, this is a finite extension now because it is generated by y 1 y 2 I mean this becomes a finite extension because it is generated by y 1 y 2 sorry 1 y 2 and y 1 y 2, after that you can create y 2 square is y 1 square minus 4.

So, this gives me a method of getting into getting a finitely I mean finitely generated k algebra as a finite module over polynomial ring. Now this number that appears here or the number that that appears here this is called dimension of the variety, it is I mean not defined by this way, but it turns out to be that this becomes what is called dimension of a given variety.

(Refer Slide Time: 14:35)



So the idea is this, let us try to prove this. So, first let me make the statement let R be finitely generated K algebra, then there exists variables Z 1 Z 2 up to Z r such that K sorry with an injective homomorphism from K Z 1 up to Z r to r such that. So, let me call this S, R is a finitely generated S module maybe I which makes. So, here I will do the proof assuming that the field is infinite, when the proof is or when the field is finite the proof is slightly more complicated and I will leave it you to read it on your own. It is not very different or too difficult, but it is slightly more linking uses some more intricate arguments; I will leave it you to learn it yourself. The proof for theorem when the field is infinite is not very difficult aspect.

So, there are only I mean very few changes that are required for the proof to be valid in the case of finite fields, but that lemma 1 needs to be careful in proving. So, let us a theorem for the case of a infinite fields. So, first let R be and it is a finitely generated K algebra. So, I can write R as some x 1 up to x n, we prove the theorem by induction on N if n is 0 r s k we can take r small r to be 0 itself, everything works then take r to be 0 itself that works.

Now, suppose n is positive, now let us assume by induction that if I have a finitely generated K algebra, generated by less than or equal to n minus 1 elements then I can find some Z 1 up to Z r. So, that this becomes inclusion and R becomes a finitely generated S module.

(Refer Slide Time: 19:31)

So, let us write down the induction hypothesis; if R is a finitely generated K algebra generated by n minus 1 at most n minus 1 elements, then there exists Z 1 up to Z let us write r prime, such that there exists variables K Z 1 up to Z R prime to R is injective, and r is. So, call this s prime is a finitely generated S prime module.

Now, the idea is to prove by induction. So, the idea is to bring it down to the case of n minus 1, case of a finitely generated K algebra having n minus 1 generator. So, let us look at the situation, we have now let R be equal to K x 1 up to x n. See if all these x 1 up to x n they are all algebraically independent, then we can take n to be R itself that is there are no polynomial f that vanishes on all the I mean no polynomial f such that f of x 1 up to x n is 0, they themselves are variables if x 1 up to x n all of them are variables then we do not really have to worry and we can just take n to be r itself.

So, for any f let us say polynomials in K X 1 up to X n, f of x 1 up to x n is nonzero for any nonzero polynomial, then take n e r equal to n and Z i equal to x i we are through I mean this itself is a polynomial ring. There are no polynomial relations among x 1 up to x n, which means this itself is a polynomial ring they are all algebraically independent. See here there is a relation between y 1 and y 2 right that is y 1 square minus y 2 square minus 4 is 0 in on this ring.

So, this I can write this as R y 1 bar y 2 bar, but in this one y 1 alone does not have a relation, but y 2 has y 1, y 2 satisfies a relation; what is that? Y 1 square minus y 2

square is 4. So therefore, this is I mean these 2 are not algebraically independent, if I take the polynomial x 1 square minus x 2 square minus 4, and put y 1 equal to x 1 I mean x 1 equal to y 1 bar and y 2 equal to x 2 bar this becomes 0.

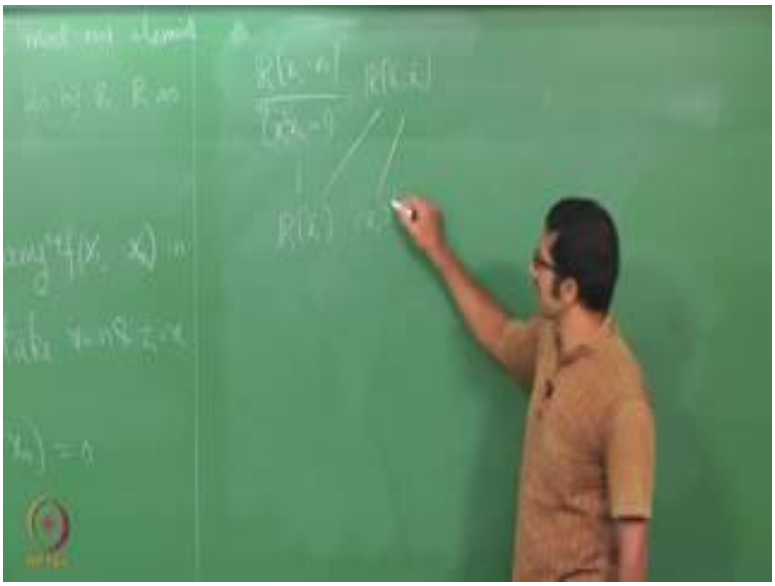
If we do not have any such situation that you know x 1 and x 2 are no way related, not only linear relation no order relation no higher order relation; that is there are no polynomials satisfying x 1 up to x n, then you can take I mean then the what that says is that all of them are variables they are all algebraically independent. So, they are I can take z n r to be n and each j I to be x i. So, in this case we are through. So, suppose there exists f X 1 up to X n nonzero polynomial, such that f of X 1 up to X n is 0; suppose this is 0.

(Refer Slide Time: 25:17)

Now, see as in the case of this example that we discussed can we you know the idea is again, the idea is to bring this down to a case like this, I have R I want to bring it down to a situation like this x 1 up to x n minus 1. Where this is finite, once you have this situation then by induction I can say that I have a K z 1 up to z r, polynomial ring K z 1 up to z r such that this is finite.

Now, if this is finite and this is finite, this is a finite module over this ring and this is a finite module over this ring then R is a finite module over this ring we are through, but then we need to make sure that I can have a finite integral extension like this.

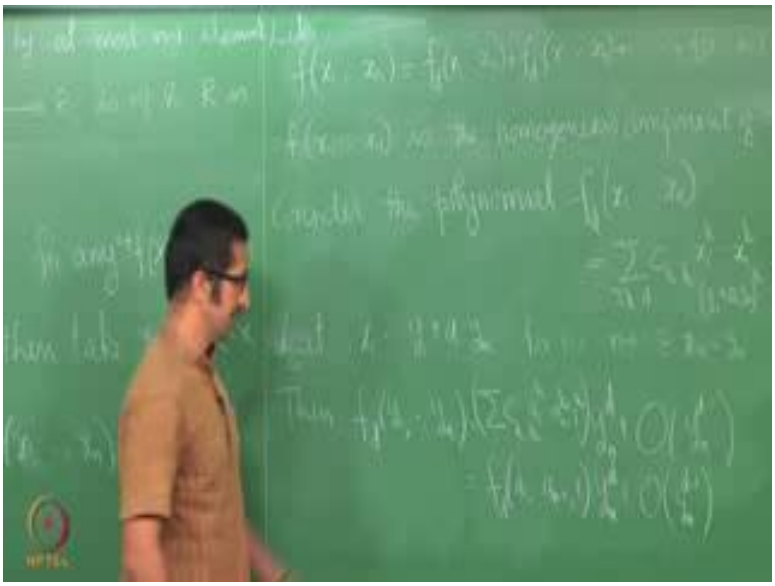
(Refer Slide Time: 26:23)



But then, as we saw in the earlier case for example, in the case of R x 1 x 2 modulo x 1 sorry x 1 x 2 minus 1, in this case neither x 1 nor x 2 is integral or . See if I look at the ring R x 1 , then x 2 bar is not. So, let me call this R x 1 bar x 2 bar, then this is not integral x 2 bar is not integral over this because you are the polynomial that you are considering is not Monique right this is not Monique polynomial. So, this extension is not integral if this is integral if you take this if this is integral, then given any ideal prime ideal here I will have a prime ideal here containing the given prime ideal. But if I look at this is a prime ideal here right, but then I do not have a prime ideal here containing x 1 bar, if it contains x 1 bar it will become the whole ring. So, there are no prime ideals here which contain this one.

Therefore, this is not an integral extension. So, if I simply take some variables that might not work. So, we you know what we did here was we twisted the axis. Similarly we can try to twist the axis and try to see if we can get an integral extension. So, let us see a let us see how we can do this. Now I have a polynomial such that this is 0. So, the question is whether we can get we can make a twist so that one of the variable has leading coefficient 1. Look at the example that we did we made x 1 equal to y 1 plus y 2 and x 2 equal to y 1 minus y 2 or the other way, and then when we substitute it one of the variables became y 1 became Monique, I mean the leading coefficient of y 1 became Monique right. So, over see y 2 it became an integral extension. So, therefore, in this case the question is whether we can indeed do this twist.

(Refer Slide Time: 29:48)



So, let us see how we can do that. Let us write f of x 1 up to x n as a polynomial. So, let us let degree of this, let f 1 the le let us write like this f d x 1 up to x n, where f i is the homogenous component of degree i. To understand this, the homogeneous component means the terms of degree i. So, if I take the x 1 square plus x 1 x 2 cube plus x 2 power 4, this is degree 4 component, this is f 4, this is f 2. I collect all the terms of same degree and write this as f i.

So, if we have to you know tweak the polynomial and get a Monique polynomial we only have to worry about this one right? Once we tweak that the highest degree term and make one of the coefficients, one of the leading the coefficients of one of them Monique then we can take that polynomial, it if we can make a linear change. So, let me. So, the question is where we can deal with this homogeneous polynomial, and make corresponding change.

So, consider the polynomial. So, let us write this as summation C k 1 up to k n, x 1 power k 1 to x n power k n, summation k I to the equal to d. And I am just representing the polynomial they are all of degree d. What happens to this polynomial if I make a linear change? For example, suppose let x i be equal to y i plus a i y n.

Let me just write this as y i times x i equal to y i times a i plus n. Y i is are you know again I am just you know say I am taking y i. So, that this is this for some a is you know a m a n minus 1 for and x n equal to y n. Let us substitute like this; what do you get f d y

1 up to y n. So, each one bill will become x 1 will be y 1 plus a 1 y n whole power k 1 and so on. Suppose I write this as a polynomial in y n with coefficients coming from other as a polynomial in y n with coefficients coming from K y 1 up to y n minus 1. What would be the highest degree? Highest degree will be K 1 I mean the summation the degree is d right. So, the highest degree will be y n power d.

Now what would be the y n power d plus I would just write the coefficients as I will just write this O y n power d minus 1. Something less than or equal to I mean with coefficients coming from y 1 k y 1 up to y n, now what would be the leading coefficient here? There would be see I am substituting x 1 by this one. So, see from each of them see I am writing y 1 plus a 1 y n whole power k 1, y n minus 1 plus a n minus 1 y n whole power k n minus 1 y n whole power k n. I am looking at k 1 see the this is one term right this is c k 1 up to k n term in each term I will have a 1 power k 1 up to a n minus 1 power k n minus 1 times 1 multiplied by y n power k I mean y n power d.

So, the leading term and this will come from each C1 I mean each term like this. So, the leading coefficient will be of the form C k 1 up to k n, a 1 power k 1 a 2 power k 2 up to a n minus 1 power k n minus 1 and 1 coming from here. From each term that will be there and y n power d will be common to each of them.

Therefore, this is nothing but. So, let me just write it like this a 1 power k 1 up to a n minus 1 power k n minus 1, 1 power k n. I will write it like this will be the coefficient of y n power d, but now what is this? This nothing but f d of a 1 to a n minus 1, 1 y n power d terms which are less than. So, the question here can be make change, see here I have obtained a polynomial such that this is 0, I have obtained the relation whose f is 0. Now this is 0 means if I multiply by any lambda, lambda in k this will also be 0. So, if I can get a polynomial whose leading coefficient is an element from k I can always scale it.

So, here I have a an element from k, but now what is that I need to say here, see if I can choose a 1 up to a n minus 1, so, that given this homogeneous polynomial I can always choose a 1 up to a n minus 1 so that this becomes nonzero. There exists a 1 up to a n minus 1 so that this is nonzero. If I can say that then this transformation will give me a new polynomial. So, I make this transformation the entire thing and this will be a degree, this will have y n power d with some coefficients in k which I can always scale it, and some I mean other terms whose degree is as a power of n it will as a polynomial in y n

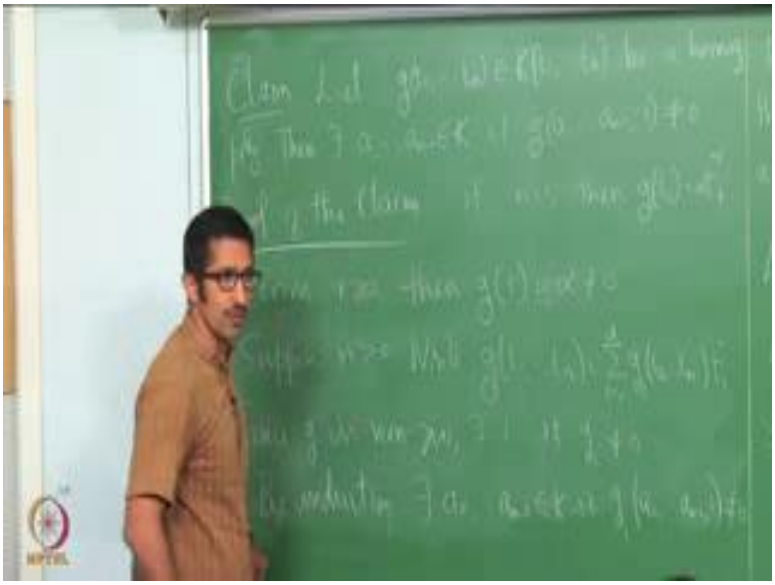
they will have smaller degrees, and that will imply that and this if you put f of x 1 up to x n again this will become 0, this new polynomial will again become 0, because they are all x 1 I mean coming from this itself. So, that will become 0 that will imply that y n is integral over k y 1 up to y n minus 1. Now you can apply induction on k y 1 up to y n minus 1, get a polynomial ring which injects into y 1 up to y n minus 1; this is integral will imply that this is finite, this is by induction this is finite therefore, this is finite that is the idea.

So, the question is whether given a homogeneous polynomial, can we always find some a 1 up to a n minus 1 so that this becomes nonzero. See in the case of infinite fields this is know at least intuitively you can say that it should be possible, I mean you can. If you look at a polynomial and look at its solutions in; I mean n space, that should be a close set which is you know. So, we should always be able to pick a point outside the given close set, but we have to prove that. But when your field is finite it is much more difficult for example, there can exists polynomials which is as a polynomial it is nonzero, but you put any value of the field it becomes 0 for example.

Student: X power.

X power p power n minus , x power p power n minus 1 minus 1 or x power p minus 1 minus 1 that becomes that is a nonzero polynomial such that for every a in the in f p this is 0 right.

(Refer Slide Time: 43:18)



So therefore, when the field is finite, its little tricky 1 has to deal it separately. But when your field is infinite, what I claim is the following let g x 1 up to x n in. So, let me use a different notation g t 1 up to t n in the polynomial ring is be a homogeneous polynomial then there exists a 1 up to a n minus 1 in K such that g a 1 up to a n minus 1, 1 is nonzero I precisely what we want to prove here.

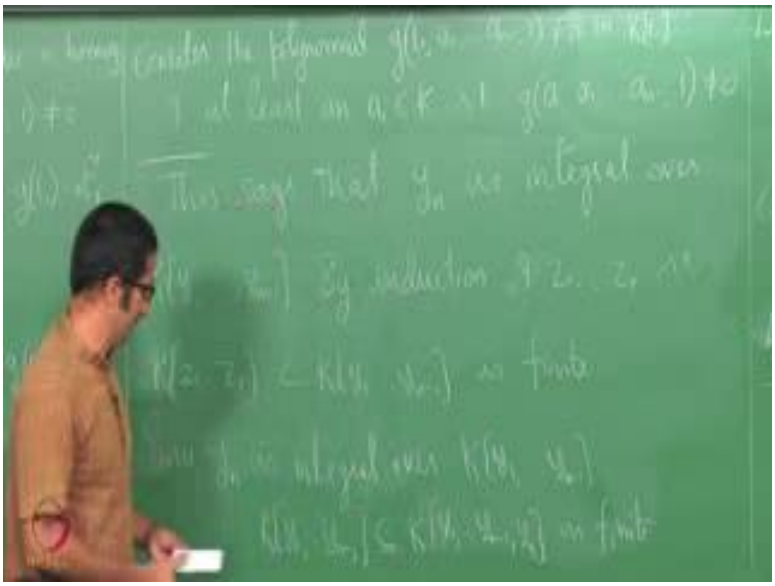
So, again we prove this by induction if n is equal to 1, we are through take any nonzero. So, this is g is a degree 1 sorry degree some this x power n. So, if n is 1 then g t 1 is some alpha t 1 power r for some r, because it is homogeneous polynomial, then take a 1 to be any nonzero element in k. So, the claim is through if n is 1, now suppose assume that I mean assume the induction hypothesis that if I have a homogeneous polynomial of degree n minus 1, then it has the nonzero root like this sorry n minus 1 elements we serve with is being nonzero. So, let f sorry. So, 1 it is sorry a 1 take a 1 there is no a 1 that is true then g of 1 is nonzero, g of 1 is alpha which is nonzero.

So, let now assume that suppose n is positive, write g t 1 up to t n as summation g i t 1 up to t n minus 1 t sorry to t 2 up to t n, t 1 power i, i from 1 to d. So, write this as a polynomial in t 1 power I mean polynomial in t 1 with coefficients coming from t 2 up to t n. S g is nonzero there exists 1 I such that at least 1 I such that g i is nonzero; g i is a nonzero polynomial by induction there exists a 2 up to a n minus 1 in k such that. So, let us say g i a 2 up to a n minus 1, 1 is nonzero for this.

Student: (Refer Time: 48:03) 0 p (Refer Time: 48:06).

Of course it will be homogeneous; because this is if I take a term of degree I mean the g is homogeneous. So, if I take t 1 power i the rest of the terms each of the terms will have you know degree i minus 1, g i will be of degree you know the rest d minus i, degree of g i will precisely be d minus i, if I assume degree of this is d.

(Refer Slide Time: 48:53)

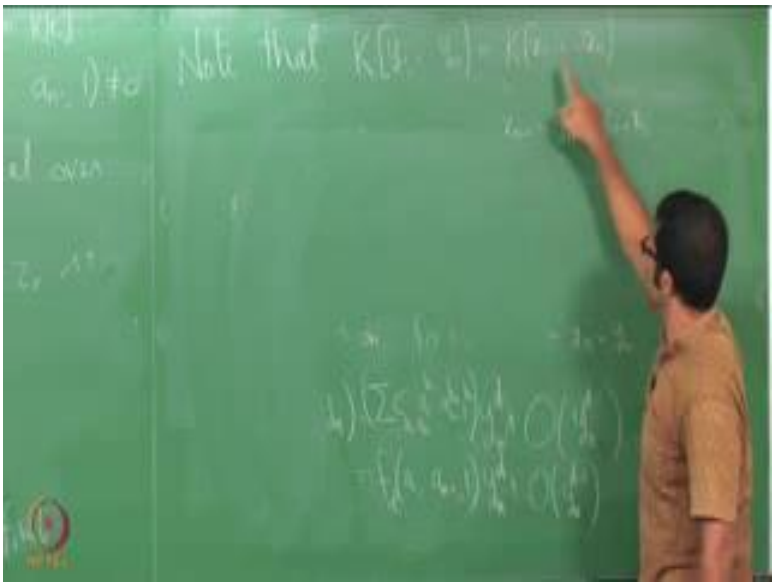


So, for this corresponding i I have g i is nonzero; now what I do is I look at consider the polynomial g of t 1 a 2 up to a n minus 1, 1 this is a polynomial nonzero polynomial in K t 1 sorry K t 1 because this, this term is nonzero.

Now, this is a nonzero polynomial here therefore, there exists at least k is infinite there exists at least an a 1 in k such that g, a 1 a 2 a n minus 1, 1 is nonzero and that is precisely what we want to prove. So, once we obtain this what we have is let us go back. I take this f this is 0, now if I substitute x 1 instead of x 1 I just put take this a 1 up to a n minus 1 and put x i equal to this equation that will give me this will give me I mean if I put x i equal to this, that will give me another say g y 1 up to y n, but g y 1 up to y n will again be 0, but then it will have a y n will have a leading coefficient coming from the field which I can always scale it; that will say that Y n is integral this says that y n is integral over K Y 1 up to Y n minus 1 by induction K there exists Z 1 up to Z r such that K z 1 up to z r, this is y 1 up to y n minus 1, this is finite and this is since y n is integral y 1 up to y n minus 1 this is also finite is finite.

Now, this is finite this to this is finite therefore, this to this is finite, but what are the substitutions that we had made x 1 equal to y 1 plus a 1 y n, x 2 equal to y 2 plus a 2 y n and so on up to y n. So therefore, this ring is same as note that k y 1 up to y n is same as k x 1 up to x n. So, that finishes the proof.

(Refer Slide Time: 53:21)



X n is y n; therefore now, x n minus 1 is y n minus 1 plus a n minus 1 y n. So, this is x n right. So, x n is here therefore, y n minus 1 is here I mean y n minus 1 is here. So, therefore, x 1 minus 1 is here. Now keep going back what you get is this is certainly contained here, but this is also contained here, therefore, they are equal. That means, I have obtained z 1 up to z r such that this contained in k x 1 up to x n is a finite extension that is precisely what the Noether normalization lemma says.

We will do some applications of Noether Normalization in the next class.