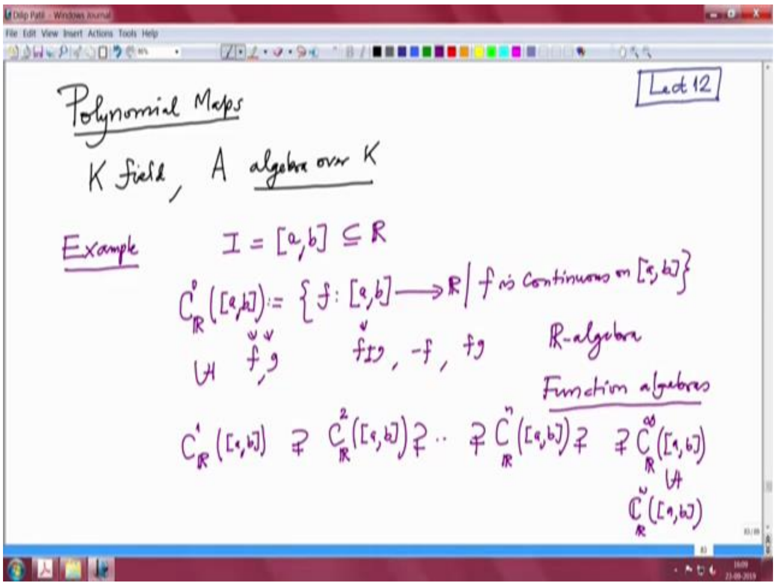
Introduction to Algebraic Geometry and Commutative Algebra.
Professor Dr. Dilip P. Patil.
Department of Mathematics.
Indian Institute of Science, Bengaluru.
Lectureminus12.
Identity Theorem for Polynomial Functions.

Welcome back to this second half of today's lecture. We have seen how within points as algebra homomorphisms and also how algebra homomorphism gives us a K spectrum of a finite type K algebra. Now, I want to spend a little bit time about polynomial maps, because like we have defined group homomorphisms, ring homomorphisms, K algebra homomorphisms, we also need to define sometime morphisms between affine algebraic sets and for that we need Polynomial maps.

(Refer Slide Time: 1:21)



So, I want to collect some basic informations about polynomial maps, not polynomials, but polynomial maps. Polynomial maps. So, this is also interesting topic because it gives geometry language. Sees whenever one thinks instead of a point a map, the maps will lead to geometry and the points will lead to sort of algebraic checking. So, let us see, so as usual I will fix a field K, K is a field and A algebra over K. For this definition, I will not even need it either find it is a type algebra or such assumption. So, arbitrary algebra.

So, what are the examples of arbitrary algebra which one might ask how many… So, we have seen very typical examples of polynomial algebra and residue class algebras of the polynomial algebra. These are the main objects for us to study in this course. But there are other interesting examples also, which actually come from analysis. So, just to give an example, let me give one example because I cannot, I do not want to give you so many because we will run out of the time.

So, this is what do you study in actually your first course on analysis. So, what is it? So, suppose I is a subset, let us take very specifically, I is the closed interval a b in real numbers and then what do we define, we define continuous functions on this close intervals, real value. So, that is C R, this suffix R is for real value, the values, the values go inside real numbers and this is a b.

So, this is by definition f, f is a function from a to b and real valued means image goes inside R and we have not studied arbitrary function but if f is continuous on a b. Then we studied various properties of the continuous functions. For example, we study that, if I have 2 continuous function, then this sum is also continuous function, the sum is point wise continuous. The sum is defined, sum of 2 functions is defined point wise. So, if f and g are continuous functions, f and g are here, then f plus g is also there, f plus g is also continuous.

Similarly, minus f minus g is also continuous, similarly, minus f is also continuous. Similarly, the product function, product function is defined by the value, multiply the product values, take the values and multiply their values. So, that is a product function, this is continuous. Identity function is, identity means inclusion function here is continuous. What does this mean? This simply means that this CR a b is in R Algebra. I just forgot to say that any constant function is continuous.

So, therefore, it forms and algebra and the first course analysis now, normally you study this algebra. So, that is R algebra, this is also called, all these algebras which I will give they are called function algebras, just because their elements are functions. Mow continuous, now we want to take differentiable function. So, this is, I should need a notation, so I will write a 0 here. So, that is 0 differentiable function. Now, CR 1 a comma b. Now, what should it be?

This should be 1 times the differentiable continuous functions on the closed interval. I will not write because this is really only a digression for a language purpose and not much. And also we prove that every differentiable function is continuous, so this is contained here. So, this actually sub-algebra of this, sub, R sub-algebra of this. And we can keep doing it.

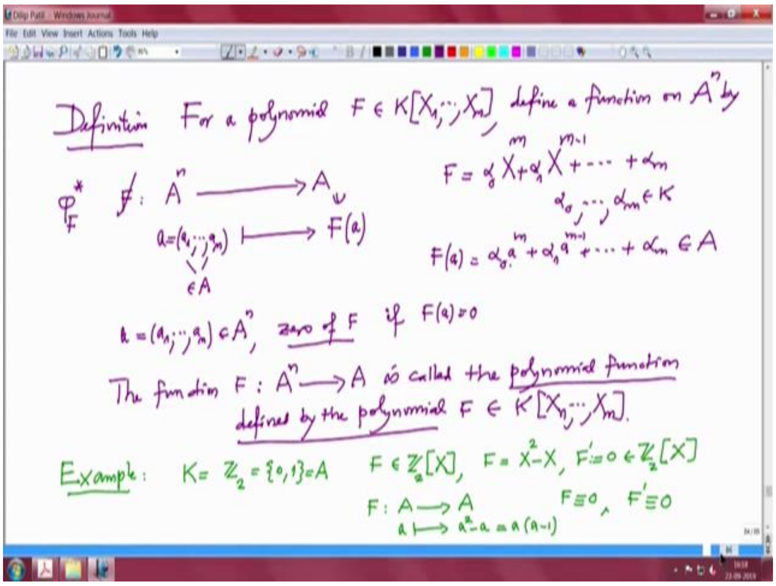
So, this is contained 2 times continuous differentiable functions on the closed interval and so on and n times. And then you ask whether if this is proper, is there a continuous function which is not differentiable, of course, we know that exists and so on. So, these inclusions are all proper. And also then you ask what is infinitely many. So, infinitely many times differentiable continuous function, that is denoted, that is also called C infinity function.

So, this is the notation. You can go on further, and this is also, all this stays proper and the last one is, they are called analytic functions. Analytic function means those function which have power series expansion at a point, locally they have A power series expansion. So, this is also called omega here a b. And also you can write down analytic function, there exists a C infinity function which is not an analytic function. So, this are proper inclusion.

And these functions are also use actually in probability theory and so on. So, all this examples, now I fix a field R here. Instead of R you could take complex numbers, then this whole is called real analysis. If I replace R by C, then it will be called complex analysis, but complex analysis is better than real analysis because in that case, all this will become equality. That is what is called Cauchy's integral theorem.

So, every complex differentiable function is also complex analytical. So these are, all these algebras are called function algebras and these algebras not finite type algebra, they are different from finite type of algebras. And therefore, whatever theory we will develop in this commutative algebra course that will not be directly applicable here. So, with this that I explained because there are examples of not finite type algebras over a field.

(Refer Slide Time: 9:29)



All right so, okay we go on. Now, what do I mean by polynomial maps? So, definition, for a polynomial capital F in K X1 to Xn, define a function on A power n by, A is a given a algebra. So, I am defining F, I will call it, I want to denote it with the same letter F, from A power into where A power n to A. What is the definition? Take any tuple A, which is a 1 to a n, that means all these ai's are in the algebra a. And map it where, map it to f of a.

And remember this is also in A because. See, let me just tell you in case of 1 variable, what it happens. If I have a polynomial F in 1 variable, it looks like this, a0 x power m plus a1 x power m minus 1, m, this is not n, m minus 1, m minus 1 plus 1 and so on plus am. This is not, I should not use a. So, I should use a different letter let me call it bs or alpha 0, alpha 1, alpha m where alpha 0 to alpha m, they are elements in the field K.

And when I plug it in now, what am I plugging it in. Capital X equal to small a, small a is an element in the algebra a. So, F of a is alpha naught a power m plus alpha 1 a power m minus 1 plus plus plus plus plus alpha m. But a is a K algebra, this was a K algebra. Therefore, this makes sense, I can multiply a by a, I can multiply a scalar, I can add these 2. So, this is indeed an element in a. And nothing special about 1 variable the same thing for many variables.

So, therefore, we do get a function on A power n where n is the number of variables here, we get a function from there to there. So, this function to distinguish I do not want to use a different notation really, but what I want to note is the following. When do I say that this a, a1 to an, this is where, this is in A power n, we say that this is a 0 of F, if F of a is 0. That means this function vanishes at a and remember this a is not on the field, a is not a tuple in the field, it is tuple in the given K algebra. So, then you call it a 0 of F.

And this F, if you look at it as a function, so the function F from A power n to A is called the polynomial function defined by the polynomial F in K X1 to Xn. Now, I just want to point out the danger in keeping the same notation. So, for that let me write an example. So, example, let us take very minimal example, Z mod, so my field I choose to be Z mod 2, then I know there are only 2 elements 0 and 1. And I take polynomial in 1 variable on Fx, F in Z mod to x, only 1 variable.

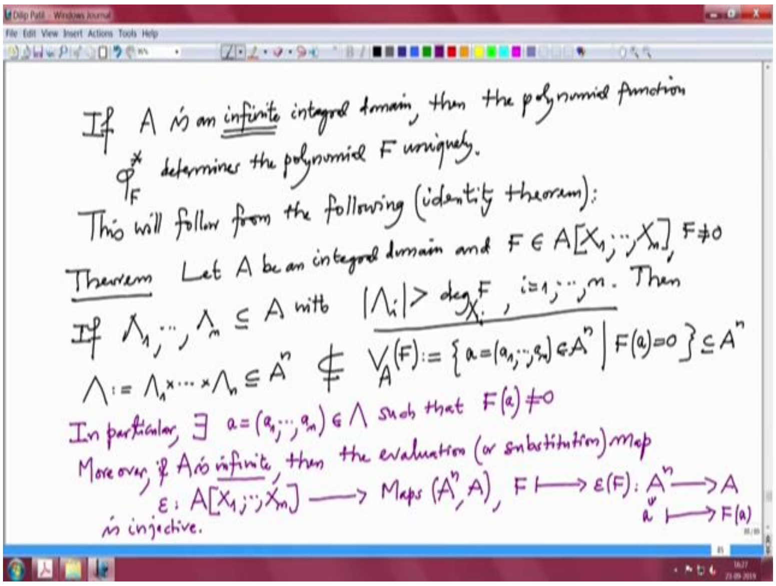
And let us take, first let us take F equal to x square plus x, x square minus x. And what is the polynomial function corresponding to this, what is my a, let us take a also equal to this, a also equal to take that, you can take any algebra. So, now, what is the function, the polynomial function F. This is from A power 1, n is 1 to A power 1 that is A to A what is the map, where do any A go?

Any A go to a square minus a. But a square minus a is a times a minus 1. And where is a varying, a is either 0 or 1. So this F is actually identical 0 function, F is 0 function. So, if I would have taken also, instead of F, 0 polynomial, so let us take a prime equal to 0 polynomial. And then by this then we will get F prime is also 0 function. So, what I am trying to say that this polynomial F is not uniquely determined by this given function and that will create a problem.

And this phenomena will happen especially in case of a finite field. Definitely it will happen because in a finite field, there are finitely many functions actually and they are infinitely many polynomials. So, many polynomials will give the same function. So, one remedy for that in the beginning, we should not denote by the same letter F, but then you should have some replacement also. So, what is the replacement one can do?

This we can do it by phi and suffix f and then I want to put a star here which I cannot explain now, but I will explain when time comes. So, this function is defined by phi star suffix f evaluated at a is F evaluated at 8, that is the definition. Now, let us do some interesting things about this this polynomial function.

(Refer Slide Time: 17:57)



For example, and this we will need it because we want to define functions on algebraic sets and not arbitrary function, but what called polynomial functions. Alright. So, what I want to prove is the following, if with the same notation earlier if A that A algebra K algebra a we have started with, if A is an integral domain, infinite integral not finite, infinite integral domain. Then the polynomial functions phi star F determines the polynomial F uniquely. This is what I want to prove.

So infinite is very important, because infinite integral domains are fields and in field case, finite field case we can always give functions, which are polynomial functions and polynomial is not uniquely determined. And how do we prove this? This is proved by, so this will follow, this will follow from the following identity theorem. So, I want to put this in a bracket. What is that?

This will remind you that you might have studied identity theorem in real analysis or complex analysis. And therefore, the following theorem is called identity theorem for the polynomial functions. This is the theorem. So, I will state it in more general setup. So, let A be an integral domain and if capital F is a polynomial in several variables over A X1 to Xn and this is nonzero point. If capital lambda 1, etc., capital lambda n, they are subsets of A with cardinality of A, not a, lambda i, capital lambda I is bigger than, strictly bigger than degree in xi of F for all I's from 1 to n.

Then I will digress you by giving you, before I prove this, I will digress you by giving a concrete examples in special situation. Then if I call this capital lambda to be the product of this sets which is each one of them is in A and therefore this is in A power m which is the set, product set is not contained in, now, I will use the notation VAF. What is this should mean? This means 0s of F in A

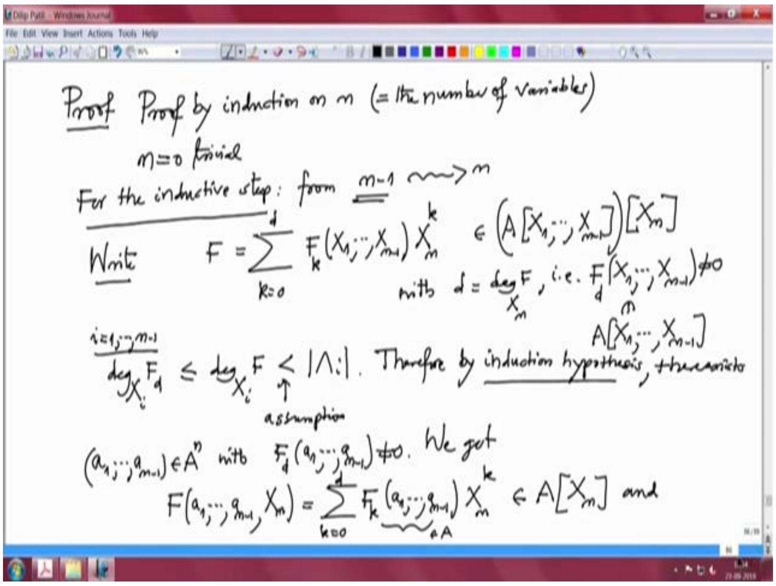
So, let us write it, this is all those tuples a which is a 1 to an in A power n, such that capital F substitute to a is 0. This one has a subset in, this one by definition has a subset in A power n see this its upset in A power n, this is also a subset in A power n. If this condition is given for all i's, then this set is not continuous. That means what do we have to produce, we have to produce a tuple in A power n which F does not vanish on that, that is a assertion in particular.

So, this is what we do? This is a more general statement and what is the consequence I am writing in particular. So, maybe I will write in a different color, in particular there exist there exist A equal to a 1 to a n in this capital lambda such that F of a is nonzero, an element here which is not here. In particular if a is infinite, moreover if A is infinite. Do not worry about the proof, proof will be very easy.

So, infinite, so far this is a general integral domain I wrote a statement. In particular if a is infinite then the evaluation map, evaluation or substitution also we are calling it now a substitution map, from where to where, that is denoted by epsilon, this is from the polynomial algebra over A infinitely many variables and this many. N is given here, to where, to maps from A power n to A. What is the map? What is this map? This is given by f, a polynomial F's with coefficients in A that is mapped to what do we call it, epsilon.

So, epsilon F, and epsilon f is by definition, this should be a map, this should be a map from A power n to A. And what did that map take any a here and evaluate at F, that is F of A. It is clear. So, polynomial goes to, Polynomial goes to a map from A power n to a this is F of a. What about this, the evaluation map is injective. That is what we wanted to prove, that 2 polynomials cannot go to the same Polynomial function. This map is injective means that polynomial F, the polynomial F here is uniquely determined by its function. So, this is what we want to prove. This is very easy, let us see it.

(Refer Slide Time: 27:15)



So proof. I am going to prove this assertion by induction on n, induction on the number of variables. So, proof by induction on n is a number of variables. For n equal to 0, it is trivial, n equal to 0 is trivial. Now, I have to prove, my induction started at n equal to 0, now I will prove the inductive step. For the inductive step, that means what, that means I will assume the step from n minus 1 variable case to n, we need to prove.

So, what is our assumption now, inductive hypothesis is given a polynomial over A in n minus 1 variables with the same assumption, that is the degree is smaller than the sets and then we want to prove for n, so, let us see. So, now what we have given a polynomial F. So, write polynomial F as a polynomial in the last variable. So, this you can write it as a summation, summation will be from K to D. This is a polynomial, think of this as a polynomial, in first n minus1, coefficients are in first n minus 1 variables.

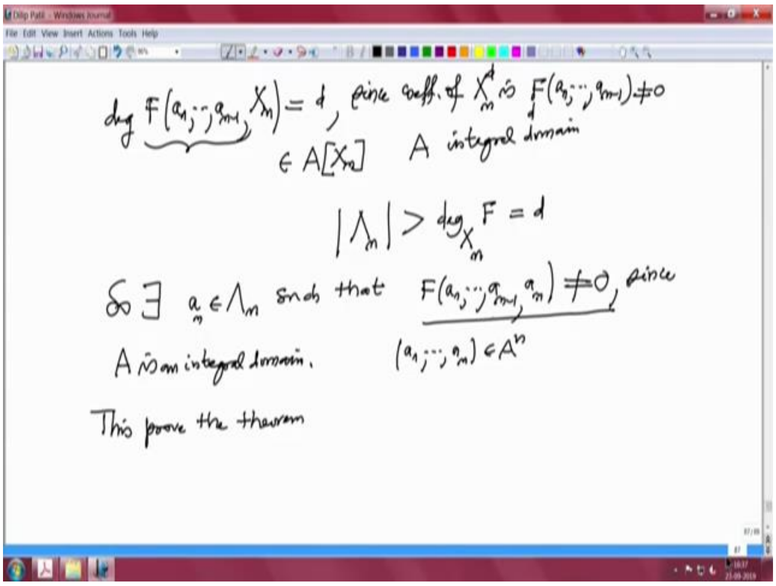
So, there will be some coefficients FKs, there will be polynomials in first n minus 1 variables Xn power K. You are thinking this is a polynomial in A X1 to Xn minus 1 and this is our new base ring and then to that this is Xn. So we have written in this way, with the degree D, with D equal to degree in Xn of F, that is the last question F suffix d, x1 to xn minus 1, this is nonzero. And this is nonzero polynomial in this polynomial ring. And obviously what is the assumption that we need to conclude, it is this one.

So, look at the degree in the variable Xi of the of the polynomial FD. So, I is from 1 to n minus 1, this is one here. So, the degree in ith variable cannot be more than the degree in ith variable in F because that term times this will definitely be degree. So, this is smaller equal to degree in Xi of the Polynomial, given polynomial F. But this is strictly less than the cardinality of the capital lambda I, this is the assumption.

So, I have a polynomial in n minus1 variable and I have this and this is true for I equal to 1 to n minus 1, I have the subsets whose cardinality is strictly bigger than this degree. So, what can I conclude by induction, I can conclude by induction that there exists an n minus 1 tuple. When I evaluate this every at that n minus 1 tuple, this is nonzero. Therefore, by induction hypothesis, because we are assuming the statement for n minus 1 variable, there exist a point a 1 to a n minus 1 in A power n minus 1 with when I evaluate Fd at a 1 to an minus 1, this is nonzero, this is induction hypothesis.

So, plug it in there. So, when I plug this here, that means, I am substituting x1 equal to a1, x2 equal to a 2, xn minus 1 equal to n minus 1 on this side. So, therefore, we get F of a1 to an minus 1, xn variable, I do not change this equal to summation k equal to 0 to d capital F K evaluated at a1 to a n minus 1 times x power n power K. We get this, this is a polynomial in with coefficients in a. So, this is a, this is a polynomial. These coefficients are in a. This is the polynomial over A in xn variable. And what is the degree of this polynomial? This is the last coefficient of X power d is precisely this, this is precisely this.

(Refer Slide Time: 34:04)

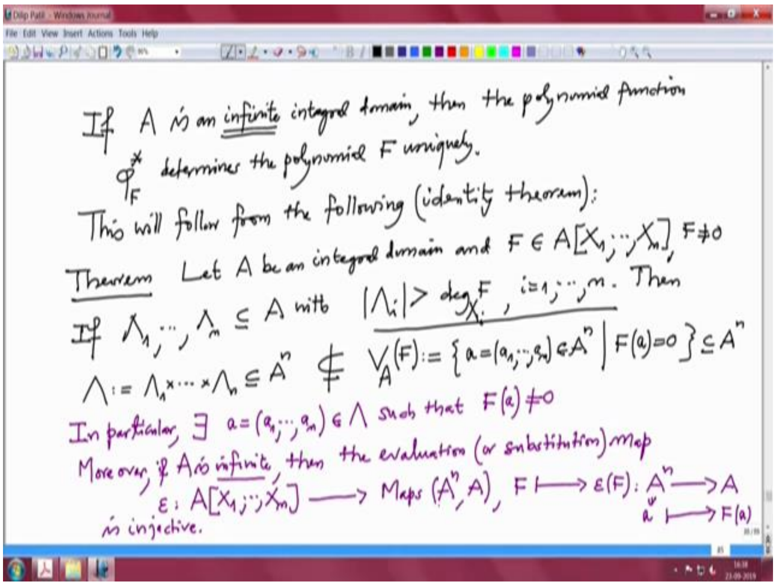


Therefore, and degree of F of a1 to a n minus 1, xn is still equal to D, since coefficient of degree Xn power d is F of a 1 to a n minus 1, Fd of this which is nonzero, that we have noted. So, the degree of this polynomial is D. Now it is a D degree polynomial. This is a polynomial in A Xn, A is an integral domain and remember A is an integral domain So, this polynomial cannot have more than d zeros. But cardinality of that capital alpha d, the capital gamma D, this cardinality is more than the degree of Xd degree of F, which is precisely, it is not Xd, this Xn this which is the degree d.

So, I have a polynomial in 1 variable, it coefficients in an integral domain whose degree is d and this subset has cardinality more than d. So, there will be at least 1 element where it is not 0. So, there exist point, there exist A n this is not d, sorry, this is n. There exist a in a n capital lambda, and let us call it a n, such that this polynomial. This one evaluated at Xn equal to this, it will not be 0.

Capital F of a 1 to a n minus 1, a n this is nonzero, since a is an integral domain. So, we proved it. We found a point a1 to An in A power n so that this polynomial is evaluated, that is nonzero. So we proved, so this proves the theorem. And reminder you, what I wrote later is the easy consequence of the earlier statement. One more step I have to go back.

(Refer Slide Time: 37:31)



Yeah, we wanted to prove there exists some element here, which is not in VAF. That means, if is not 0 there. In particular this follows immediately, if it is infinite, then it follows immediately because each polynomial will have at least 1 tuple which is nonzero there. So, that proves the thing. And with this, I will continue in the next lecture. And I will basically, I want to study more polynomial functions.

And then I will also come back to the properties of the, I will come back to affine algebra exercise and properties and using them I will define what is a topology that topology will be call Zariski topological. And then we will relate this Zariski topology to the maximum spectrum and spectrum. And that topology, with that topology, these 2 topological spaces, actually 3 topological spaces, one is a K spectrum, the other is a maximum spectrum and the other is a prime spectrum.

We will study the topologies on this set defined by these algebraic sets and that is precisely algebraic geometry. For K spectrum it is classical and for maximal spectrum it will still be a little bit more generalization of classical algebraic geometry. And for this spectrum it will become a full modern algebraic geometry. And in this course I will only stick to affine algebra geometry. Thank you.