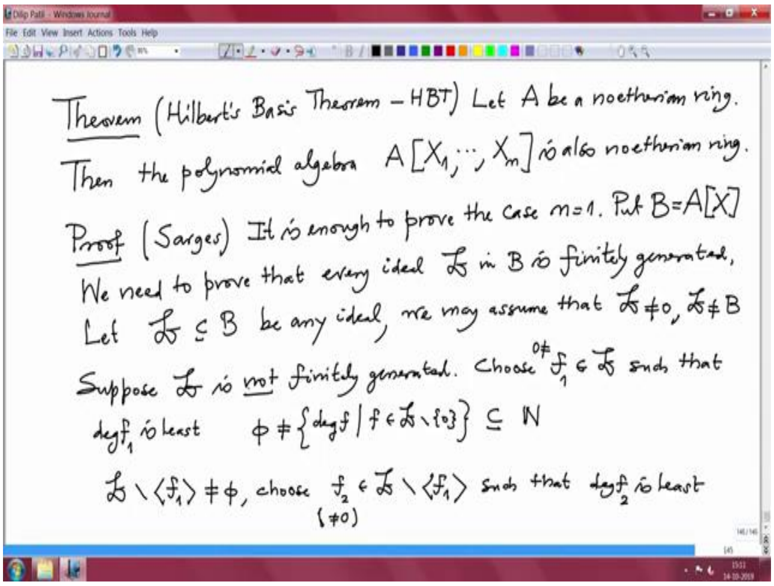
Algebra Geometry and Commutative Algebra
Professor Dilip.P. Patil
Department of Mathematics
Indian Institute of Science, Bengaluru
Lec 23
Hilbert's Basis Theorem HBT

Welcome to this course on Algebraic Geometry and Commutative Algebra. Last time I have left to prove Hilbert's Basis Theorem. Today, I will prove Hilbert's Basis Theorem and some of its applications.

(Refer Slide Time: 0:48)



So, for today we will prove this is the theorem. This is called as Hilbert's Basis Theorem. I will also abbreviate by saying HBT. Say that let AB a Noetherian ring, then the polynomial ring, the polynomial algebra infinitely many variables were A X1 to Xn is also Noetherian. Proof: Proof is very simple. There are several proofs available for this theorem and I am going to give the shortest proof that is due to Sarges.

So, first of all note that it is enough to prove the case m equal to 1 because then you can by induction you can keep going for arbitrary many finitely many variables. In this case, I will put B the polynomial ring in one variable. So, I will just write the variable as x and we want to prove that be is a Noetherian ring that means we shall prove that, we need to prove that every ideal B, in B is finitely generated this is one of the characterization of Noetherian ring that to prove a ring is Noetherian equivalent to bring every ideal is finitely generated.

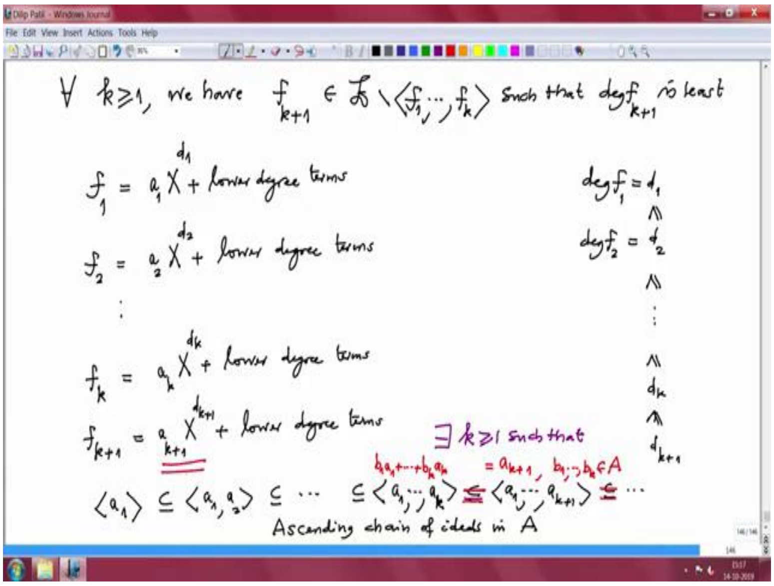
So, let B be in any ideal in B. We may assume that this B is nonzero and B is also not the whole ring B, B is not a unit ideal, because in this case it is regenerated by the element 0, in this case he degenerated by the element 1, so we can in both the cases it is finitely generated therefore, we can assume this. Now suppose, B is not finitely generated then we should look for a contradiction. And contradiction to what?

Contradiction to our assumption that base ring is Noetherian. That is what we will get a contradiction for. So, B is not finitely generated, then what do we do? In B so, in this case choose a polynomial f1 in B such that degree of f1 is least. So, note that I am choosing f1 nonzero, nonzero in B such that the degree of f1 is least. Why is it possible? Because we look at all the degrees. So, look at all the degrees of any f where f varies in p minus 0.

And this one is a subset of natural numbers and this is a nonempty subset because B is nonzero B is not in it so B have to have some polynomial which is nonzero. So, this set is non empty and therefore, we use well ordering principle of n that any nonempty subset of natural numbers have the least element, so I choose that. And now, look at B minus ideal generated by f1. Seems we are assuming be is not finitely generated, B cannot be generated just by this polynomial f1 because otherwise B will be finitely generated.

So, this is definitely nonempty. And again choose, choose f2 in B minus ideal generated by f1, such that degree f2 is least among the elements from here, this is again note that f1 has to, f2 has to be non-zero, because B zero but the ideal also zero so, that is gone, so B f2 is non zero. Note f2 cannot be zero. And we want to repeat this process. Now, next step will be take the ideal generated by f1 and f2 and remove that ideal from B and continue this process and every time we will be able to choose a new element with the least, degree least that is because we are assuming B is not finitely generated.

(Refer Slide Time: 8:27)



So, let us note what happened at the k stage? so that means for every k because equal to 1 we have chosen, we have f2, fk, fk plus 1 in ideal generated by B (mino), in B minus ideal generated by the polynomial, earlier polynomial f1 to fk such that degree of fk plus 1 is least among all the polynomial from here, so, this is what we have chosen. So, let us see what, what how do the f1, f2 et cetera look like.

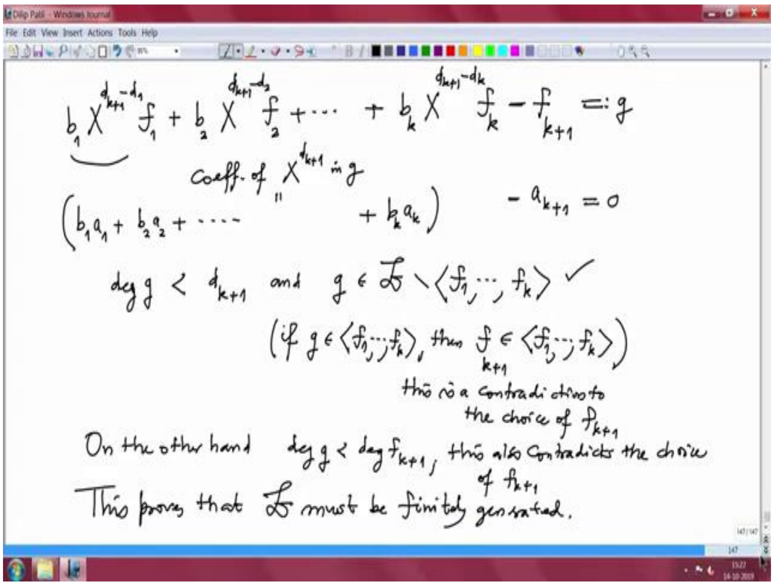
So, f1 will look like degree of, let us call degree of f1 to be d1, degree f1 to be d1. So, this one will look like some coefficient a1 f not f, x, x power d1 plus lower degree terms and f2 will look like a2, x power d2 plus lower degree terms and what is the relation between f1 and rather d1 and d2. So, degree of f2 which is d2, d2 has to be bigger equal to d1 that is obvious because f2 is also in b and so on.

So fk similarly this is ak X power dK plus lower degree terms and fk plus 1 equal to ak plus 1 X power dk plus one plus lower degree term. Now, I want to cancel this term. So, d1 this is increasing sequence dK less equal to dk plus 1 and if I have to cancel this term I will supply the correct power of x to earlier polynomials and then try to cancel this. How do I do that? So, first of all note that, if I look at now somehow we have to use the assumption on the base that it is Noetherian.

So, look at the ideals in a, ideal generated by this quotient a1, ideal generated by the next one will be ideal generated by a1, a2 and so on and ideal generated by a1 to ak containing ideal generated by a1 to ak plus 1 and so on. This is an increasing sequence, increasing chain or ascending chain of ideals in the base ring a. Ascending chain of ideals in a but a is Noetherian, so therefore, there exists a stage k from that onwards it will be quality.

So, we will write here there exist k bigger equal to 1 such that it will be equality onwards equality here, equality here and all the way it is equality that is because a is Noetherian. But now, what is more important is ak these ideals equality is important in the ak plus 1 is here. So, this ak plus one should be linear combination of the earlier one. So, that is b1, a1 plus bk ak for some b1 to bk in the base ring a your (())(13:42). Now, I will use this b1 to bk and f1 to fk to cancel this, this term. So, how do you do that?

(Refer Slide Time: 14:10)



Let us go. So, now, what you do is you multiply f1 by b1 look at b1 f1 plus bk fk, no we have to supply some power of x. So, let us write more precisely, b1 X power, I have to make power to be dk plus 1. So, I have to make here d k plus 1 minus d1 that is f1 plus b2 X power dk plus 1 minus d2 f2 and so on, consider this polynomial, bk X power dk plus 1 minus dk fk. Look at this, let us call this polynomial g.

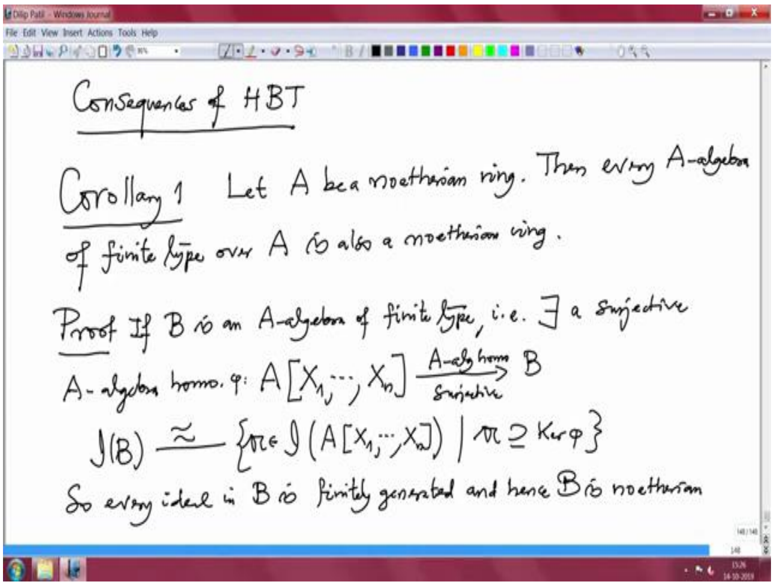
So, first of all note that the, no I have to subtract it from here you subtract fk plus 1. Or from fk plus 1 subtract that does not matter call this as g. Then what is the leading term of fk plus 1? That is ak plus 1. And what is the leading term here b1. So, now, all of all these terms have become degree dk plus 1 because in f1 has degree dk, d1. So, the leading term will be b1 times leading coefficient of f1 that is this.

Similarly b2a2 plus bk ak and minus this, but we have written ak plus 1 as this so this is 0. So that means this is coefficient of this is precisely, the coefficient of X power dk plus 1 in this that is precisely this, this is 0 in g. Therefore, degree of g is, degree of g strictly smaller than dk plus 1 and where is g and g I claimed first of all that belongs to B that is no problem, because all these fi's belong to g and it cannot belong to ideal generated by f1 to fk.

Because if it does this side is already belong to this. So, if g belong, so, let us right explanation for this. If g belongs to ideal generated by f1 to fk then f will also belong to ideal generated by a f1 to fk, not fk plus 1 because these belongs already, if these belong this also, this will also belong, but that is a contradiction to the choice of. So, this is a contradiction to the choice of fk plus 1. So, therefore, we have checked this b cannot g.

On the other hand degree of g is strictly smaller. On the other hand degree of g is strictly smaller than degree of fk plus 1. These also contradicts the choice of fk plus 1, this also contradicts the choice of fk plus 1. So, either statement contradict the choice of fk plus 1 that means something wrong with our original assumption that B is not finitely generated. So, this proves that the ideal B must be finitely generated. And hence, the, conclude the proof of the theorem, this is really very-very simple.

(Refer Slide Time: 19:27)

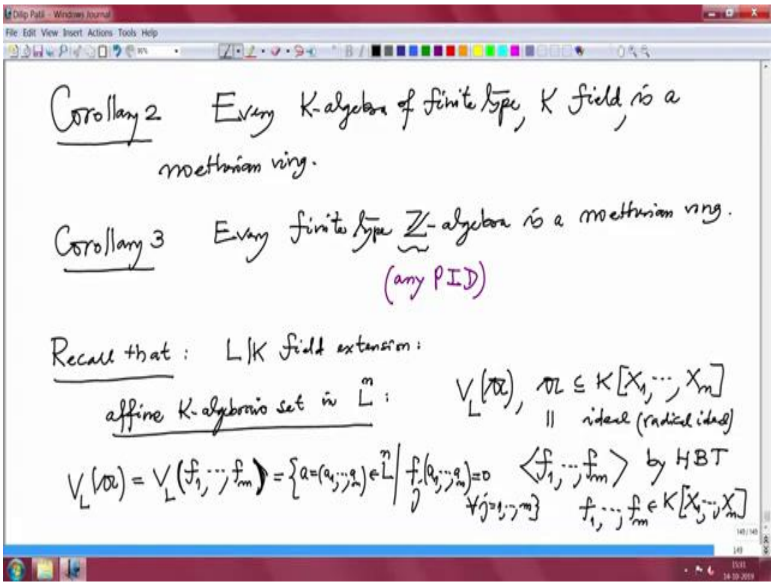


So, now, I will write few corollaries to this, few consequences. So, consequences HBT. There are many, many consequences of these HBT as I was saying in the last lecture, that Hilbert proved this theorem to prove some existence of some invariants and this was much easier than the existing proof then. So, first of all some corollaries, corollary 1 – Let A be a Noetherian ring then every A algebra of finite type over A is also a Noetherian ring.

Proof: If B is a finite type, if B is an A algebra of finite type what does that mean? That means, so that is B is, there exists a surjective A algebra homomorphism. From the polynomial ring infinitely many variables to B, this is A algebra homomorphism hence surjective. And now, we know, you have noted these earlier that mean this B is the quotient of the polynomial ring infinitely many variables and we know therefore, there is a one to one correspondence between the ideals of B and the ideals of the polynomial ring which contain the kernel of this map.

So, if I call it phi, if I call this as phi then the ideals of B and ideals of the polynomial ring in these n variables which contain a, a contains kernel of phi this said and these ideals that is a bijective correspondence, but these ideals are finitely, in fact, all ideals here are finitely generate these ideals are finitely generated therefore ideals of B are finitely generated and therefore B is Noetherian. Though so, every ideal in B is finitely generated and hence, B is Noetherian.

(Refer Slide Time: 23:24)



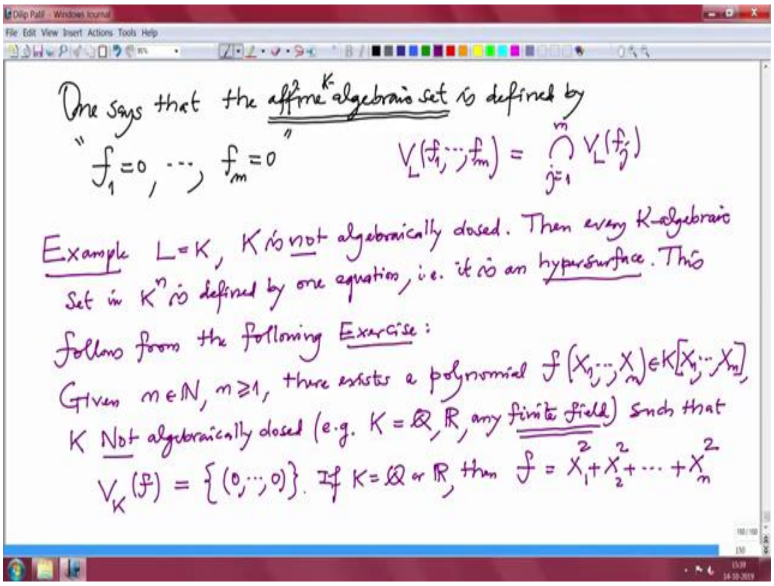
Okay, so also, so corollary 2 – Every K algebra of finite type where K is a field or, I will write that separately, is a Noetherian ring. So, another corollary which I, it will be very important. See this corollary is very important for, you remember when we introduced affine algebraic sets and then we say that every affine algebraic set is defined by finitely many equations.

So, this is very important. I will note that also later, but let me note another one which is also very important. Every finite type Z algebra is a Noetherian ring, because Z is Noetherian we in fact Z is a principal ideal domain. So, therefore, this corollary actually one should write instead of Z replace it by any PID, any PID. Every type algebra over a PID is also Noetherian ring, okay. So that is these two, okay. Now. All right.

Now, this is for the recall that what we have in this setup when you have a field extension a lower k field extension then what was affine K-algebraic set in L power m, this was precisely VL of an ideal a where a is an ideal in the polynomial ring in n variables over K ideal, that is affine algebraic, that is what this k algebraic means, the equations the ideals are in the polynomial ring over k and also we have noted that actually we may assume even a is a radical ideal.

That is not so important right now, what is more important what I am saying that because this a is an ideal in a polynomial ring over a field which is Noetherian by HBT therefore this a regenerated by finitely many polynomials so that is f1 to Fm by HBT where f1 to fm are polynomials with coefficients in k what does that mean? So, let us write down this over this. What does it mean? Means that means, V of a, VL of a is same thing as VL of these finitely many polynomials, you have noted that this depends only on the ideal generated by f1 to fm and what is this? This is all those points a equal to a1 to an in L power n such that fj of a1 to an is zero for all j from 1 to m.

(Refer Slide Time: 28:48)



So, sometimes you will also see in a classical algebraic geometry books that one says, one say that the affine algebraic set, K-algebraic set is defined by this equation f1 equals 0, et cetera fm equals zero, this is not very good notation, but that is how classically it was written because vanishing common zeros of these polynomials are precisely the points in the fine algebraic set defined by ideal generated by f1 to fm.

So, see this one, one cannot write because one side the polynomial I said it is 0, what it means? Abuse of notation means, this is the common set of zeros of these polynomials. So, this was what long proved. So, henceforth, whenever we want to study a fine k algebraic sets, we can always assume that it is defined by finitely many equations. Now, the next question will crop up how many equations are really needed to define? And that is more serious questions. And even till today, it is not completely settled, there are some partial answers. When time comes, I will keep commenting on this.

But right now, I will make one example to show you that. So, let us make an example. Example. So, in other words, this VL of f1 to fm is intersection of m hyper surfaces as I have been saying it. So, now the question becomes given an algebraic k set how many hyper services are needed to get the given algebraic set? And these example showed that even the ground field is not algebraically close ban this question is not so interesting.

For example, so let me write what I want to write. So let, okay I am in the case, the classical case, classical means, L equal to k. So, we are only considering K-algebraic sets in the affine space over k and I am assuming K is not algebraically closed. Then let us see what happens. Then every K-algebraic set in K power n is defined by one equation that is, it is an hyper surface.

So, I am not going to prove it here completely, but I am going to give you a sequence of arguments in the assignments. And one of the crux of that assigned is the following statement. So, this follows from the following, let me say following exercise. So given any natural number m, N bigger or equal to 1, there exist polynomial f of, let me write now X1 to Xn in K X1 to Xn and again stress here, K not algebraically closed.

For example, K equal to Q or R or any finite field such that VK of f, there is only one 0, namely 0, 0, 0. Originally the only zero of this polynomial f. So, and let me also say that in case of real numbers or rational numbers, it is really very easy because can simply, if K equal to Q or R, then you can simply take f equal to X1 square plus X2 square plus Xn square. The only zero of these polynomial is 0 0 0 0 no other 0, which is very clear for Q and R that is because of the order.

The squares are positive always for any, if you have any n real numbers, then the squares of, some of the squares of these real numbers is always positive, so it cannot become zero. All right. So, for finite field one has to work out little bit, it is not so difficult, I will say do it by induction and n, and more hints I will write in the exercises. So, with this, I will end this half, first half of this lecture, and we will continue after the break. What some more consequences of HBT for modules and so, we will meet after the break. Thank you.