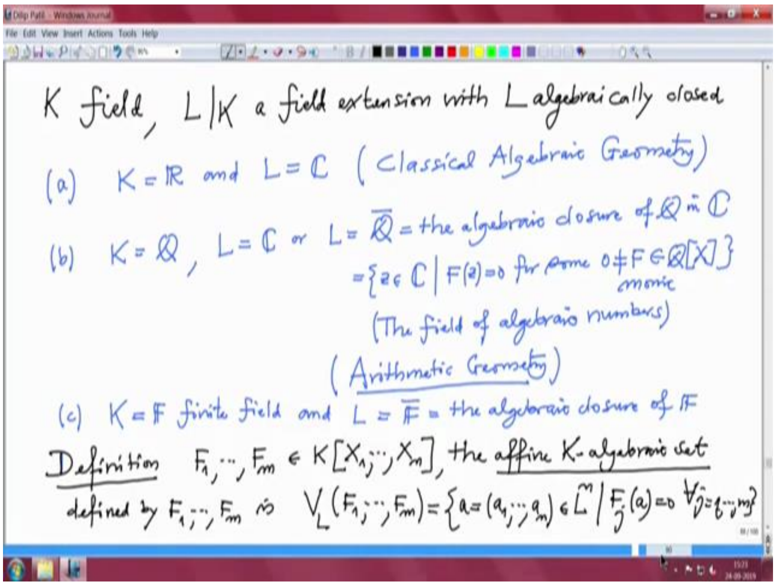
Introduction to Algebraic Geometry and Commutative Algebra.
Professor Dr. Dilip P. Patil.
Department of Mathematics.
Indian Institute of Science, Bengaluru.
Lecture-13.
Basic properties of K algebraic sets.

Welcome to this course on Algebraic Geometry and Commutative Algebra and now I go back, we have little bit competitive algebra background, so I will go back to the first lecture, where we have defined affine algebraic sets. So, let us recall what we have defined.

(Refer Slide Time: 0:49)



So K was our base field and L over K, a field extension with L algebraically closed, this is our setup. And just to recall a word about algebraically closed, that means every non-constant polynomial with coefficients in L in one variable has a zero in L. That is the definition of an algebraically closed field, all right. And typical examples I will, typical examples are the following 3 cases. So, where we apply these to the following 3 cases, number one K equal to R and L equal to C.

This is C, the algebra closure of R that we assume that you know that C is an algebraically closed field and C is an algebraic extension of R, therefore C is an algebraic closure of R and in fact, if there is a degree 2. And when we apply this special case, what we will get is classical algebraic geometry. This is said, this is a very old subject and it was lot of applications in a different fields, in the different real fields.

Alright, so second one is K equal to Q, Q is the field of rational numbers and either L you can take C or L you can take Q bar, Q bar is the algebraic closure of Q inside C. So that means what, that means is Q bar is set of all those complex numbers Z, such that this Z is a 0 of a monic polynomial. So, such that F of Z is 0 for some nonzero polynomial f with coefficients in the rational numbers.

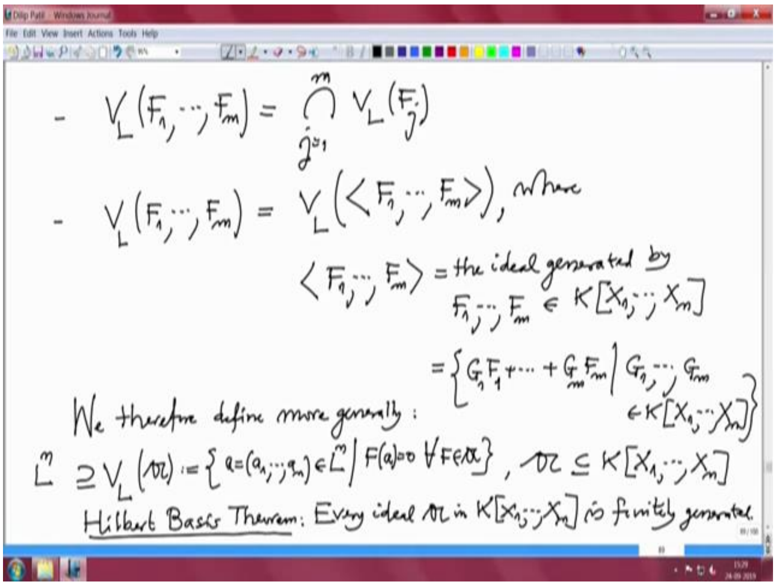
And so this is monic, this is also called as field of algebraic numbers, this is also known as the field of algebraic numbers. So, this way, if you take this K equal to Q and L equal to Q bar, this is a very famous now upcoming or very frontline research area in algebraic geometry, which is also known as arithmetic geometry. So, because it arose from the arithmetic, arithmetic is the numbers, the numbers which arose from rational numbers, integers and irrational numbers, there is no limiting process here.

Alright, the last one is, this is where, the C part is very useful for engineering purposes, that is K is F finite field and L is the algebraic closure of F bar, the algebraic closure of F. We have assumed that every field has an algebraic closure. So, it depends on what you want to do, it depends on the field, base field as well as the upper field that you choose. And what did we define last time, we have defined, so let me write a definition here. This is what we have defined last time, definition.

We have finitely many polynomials F1 to FM which coefficients in the base field with n variables. And they are affine algebraic sets, affine K algebraic set defined by these polynomials F1 to FM is V. Now, I put a suffix L here of F1 to FM, these are the common solutions or common 0s of the polynomials F1 to FM and the 0s has coordinates in L. So, this means these are all tuples A, A1 to An in L power n such that Fj at a is 0 for all ja from 1 to m.

This is what we have defined, affine K algebraic set. So, this is a subset of L power n, this is a subset of that finite dimensional vector space over L power n. But we are going to put more structure on that vector space actually. So, that will come final. But we are, our objects of study this common solution sets.

(Refer Slide Time: 8:18)



And we have noticed last time that this VL of F1 to Fm, this is intersection of all this V a lot of Fj, they are common zeros of this thing. So sometimes it is enough to study this particular one and look at their intersection. This is one thing we have notice. Another thing we have noticed that this VL of F1 to Fm does not depend on this polynomial but it depends only on the ideal generated by these polynomials, in now in a polynomial ring in K X1 to Xn.

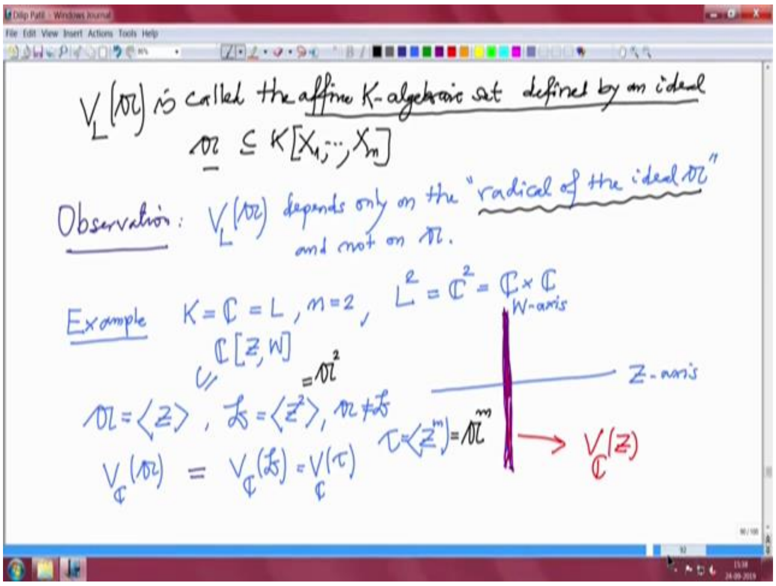
So this is same thing as BL ideal generated by F1 to Fm, so where this F1 to FM is the ideal generated by F1 to Fm in the polynomial bring over K, in this N variables. And we described these ideals, this is precisely the linear combination of these polynomials with coefficients in this polynomial ring. So, this is precisely G 1 F 1 plus Gm FM where this G1 to GM, they vary in the polynomials over K. This is precisely this ideal.

And it is clear actually from this description that if Fi vanish at some point in Ln then this combination also vanish, because we know that how do you evaluate the product and how do you evaluate the sum because evolution and substitution map is an algebra homomorphism. So, therefore, if Fi's vanish, this combination vanish, conversely, if combination vanish, obviously these Fi's are part here, then, therefore, vanishing depends only on the ideal.

So, we might as well have defined V L of any ideal. So, we therefore define more generally VL of any ideal A, where A is an ideal in the polynomial ring over K. But then here one might ask whether ideals are generated by finitely many polynomials. And the answer is yes and that will be proof a short while, where that is known as Hilbert's basis theorem. So, I will just quote it here and go on for some time and then when we come back to algebraic digression, we will prove Hilbert's basis theorem.

So Hilbert's basis theorem says, it says ‘every ideal A in the polynomial ring over a field K is finitely generated. So, we will assume this today and prove it in the next time when we switch to algebra. And what is VL of A formally, this is by definition then all those points a equal to a1 to an in L power n such that F of a is 0 for every F in ideal A. So this is, this VL A is a subset of L power n, all right. Now, one more observation I want to make this is called an affine. So I will write on the next page.

(Refer Slide Time: 13:35)



VL A is called the affine K algebraic set defined by an ideal A inside the polynomial ring K X1 to Xn. Now one might, I just want to make one comment here, why do I use keep adjusting, keep writing this adjective affine. There is also projective, but we may not do in this course. But that is also very interesting, because nowadays projective geometry is used in mobile applications. So, that has again revived interest from the engineering side.

But unfortunately our courses on linear algebra and algebra are not taught in the university setup. So, one should take up such courses. Alright, so, this is our affine algebraic set. Now, one more observation. So, observation and then we will, we this set, this algebraic set VL A depends only on the so called radical ideal, radical of the ideal A and not on A. So, before I go on, before I define the radical formulae I want to give one example.

So example, so let us take K equal to R or maybe K equal to C I want to take, K equal to C and L is also equal to C. Now, you see first of all drawing a picture is little bit tricky because

I want to take n equal to 2. So therefore, what is L power 2, this is C Power 2, so this is C cross C. So, one cannot draw this picture on the board because this is a 4 dimensional real space.

So, what convention we do it we, when I draw a picture of this, I do this is C and this is C. This is X axis is for C and Y axis is also for C, so our complex variables. And suppose now I take ideal A, so where, now what is the base, base field is also C and upper field is also L. So, now, what is the number of variables we are considering; the polynomial ring over C in 2 variables. Let me write it that Z and W, the variables just two, so this is a Z axis and this is a W axis.

And the points here are complex numbers and points in this C2 are precisely the pair of complex numbers. And now I take, we need an ideal, so I take an ideal A which is generated by Z. So, this is a principle ideal in this ring generated by Z. So, now what is VC of this ideal? So, let me indicate that, VC that means Z is 0. So, that means, this is W axis, the W axis is precisely this. This is precisely VC of Z, Z is 0 with a W axis.

Now, suppose I would have taken ideal B is ideal generated by Z square. Then what will it be pictures says, Z square equal to 0. So VB, VC of B, all 0s of this Z square. But if Z square is 0 then Z is also 0, because we are in a complex number field. So, therefore, if I want to draw the picture, it will be the same W, but it should be more thicker because it comes twice. But, as I said they are equal.

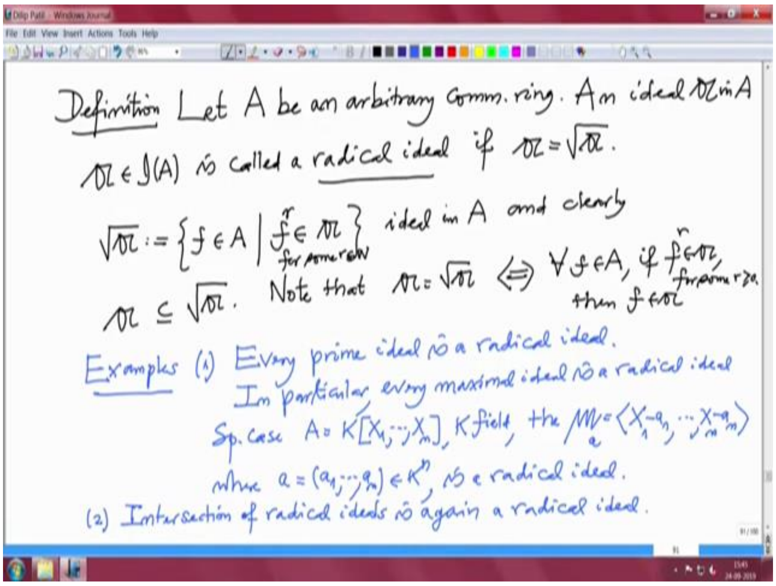
So, as I said there is no difference but so this equality means there is a set, but ideals are not equal, but A is not B. So, you see, when we go from algebra to geometry this information is lost, that the points are twice or we have to make a special efforts to say that we are counting this points twice and that effort is seen in algebra but not in geometry. So, sometimes geometry loses information, the precise information.

So, this we have to take care afterwards, when we become more serious geometry and how do you come back to algebra, that we have to make more and more clearer. And there is nothing special about Z square, if you would have taken Z power m. If I would have taken the ideal C equal to ideal generated by Z power m, then also this affine algebraic sets defined by Z power m is same as this, see.

And then it has to go more thicker, it has to go, this is very thick, this m. So, these examples shows that algebra gives more precise information, that is one of the reason why one has to study more competitive algebra and that is what we will do in this course. Alright. So, and how do you solve, how do you remain, I want to make some solution to this, so that this does not arise right now.

So, then I modify, not modify, I just define now, radical ideals, this one, it depends only on the radical. So, therefore, this ideal A, this B is also A square, B is also A square ideal, square of this ideal, which is A times A, that we defined operations on the ideal. This C is nothing but a power m alright. So, I want to define therefore first what is radical of an ideal. Now see this becomes algebra. So, let us go and define.

(Refer Slide Time: 22:31)



So, definition now this definition makes sense in a ring. So, I will not only the polynomial ring but arbitrary ring. So, let A be an arbitrary competitive ring. Of course, always with identity we do not consider other rings. And so an ideal A in A, gothic A in the ring A, also we have notation for the set of ideals. So let us use it, N a belonging to the I of A that means it is an ideal in A, it is called radical ideal, if so first I will define what is, when I say radical.

So, this root of a, this is what it is this by definition. This is by definition all those f in A, all those elements in f in A such that power of this f, f power R belongs to the ideal A. Then you call it a radical ideal. So, first of all one check that this is an ideal in A and also it is clear and clearly this radically is a bigger ideal, A is contained in the root of A. One calls it also root of the ideal A or a radical of A.

So, when do you call it a radical ideal if A equal to root of A. What does this mean? Let us fill out this. This means, see this inclusion is always true. So the other inclusion, so we are interested in when this inclusion happens. That means if f belongs here then it should belong here. So, that means if for so, note that A equal to root of A, if and only if for every F in A, if F power R belongs to A then already f belongs to A. This is for some R, for some natural number R, for some R bigger equal to 0, then A should already belong.

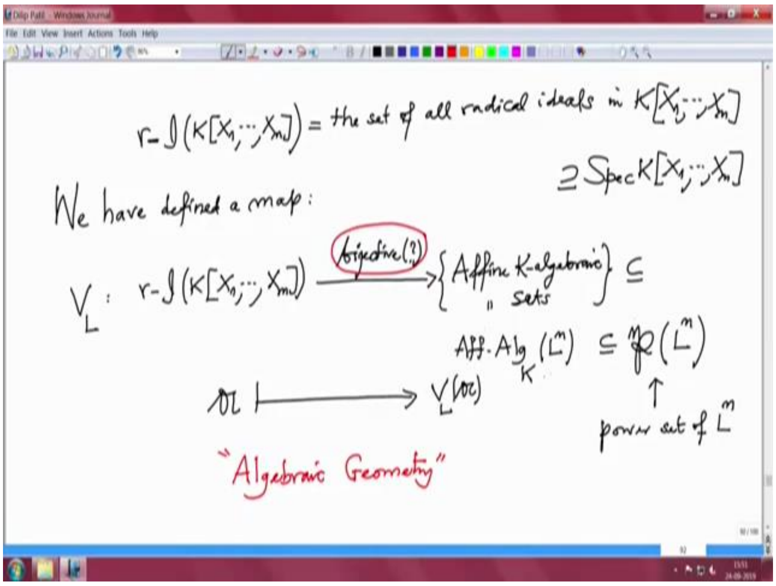
So, because this side, what is this, F belongs here means the power of F belongs to the ideal, then it should already belong to A. So, that means this what I wrote if and only if. Now, some example of radical ideals, so always whenever we have a concept, we should tell when is, what are the examples of that kind and not of that kind. So, some examples, every prime ideal is a radical ideal.

This is obvious, because the power of an element belongs to the prime ideal, then one of them means the element should belong to the ideal that means it is a, that is follows from the definition of a prime ideal. So, in particular every maximal ideal is a radical ideal So, in particular a special case, if you take A equal to K X1 to Xn, polynomial ring and K is a field, this is a case we are interested always. Then this ideal ma, which is ideal generated by x 1 minus a1, x n minus a n, this is where a equal to a1 equal to a is K power n, this ideal is a radical ideal.

We saw these ideals are maximal ideals and therefore they are prime ideals, therefore, they are radical ideals. All right. Now at least 1 example of a non-radical, so some more examples from this example we construct more examples, there is always the intersection of radical ideals is always radical. Intersection of radical ideals is again a radical ideal. Finite intersection definitely, all right.

Product is not a radical the ideal, for example, if I multiply A by A, that is A square and A square, that is no reason that A square equal to A. Like in earlier, for example, ideal generated by Z square is not a radical ideal. All right. So, we have examples and now, let us go on, so this is radical ideal. So, what did we do in this? So, let us see what we have achieved.

(Refer Slide Time: 29:42)



So, that means what, let us get back to our original setup. We are defining now a map from the set of radical ideals. So, radical I want to create a notation. So, r for radical ideals and I of K X1 to Xn, this is the set of all radical ideals in the polynomial ring with coefficients in capital K. And we saw this is nom-empty set.

In fact, this will contain all prime ideals, it will contain spec of K X1 to Xn, so there are many, many elements. In fact, also in particular, it will also contain Spm, also it will contain a K spectrum. Alright so, and then we have defined a map. So, we have defined from where to wear, VL, this is a map from letter r I K X1 to Xn set of all radical ideals from here to where to affine K algebraic sets.

And these are where, this is a subset of, so maybe I should put a bracket here, this is a subset of. So, this do I have a name for this, yes. Let us give a name for this also, A double f A lg suffix K of L power n and this is a subset of whom, each 1 of them. This is a subset of power set of L power n. So, we have defined this map, namely any ideal A goes to VL of A. So, this is by definition power set of L power n which is a huge set.

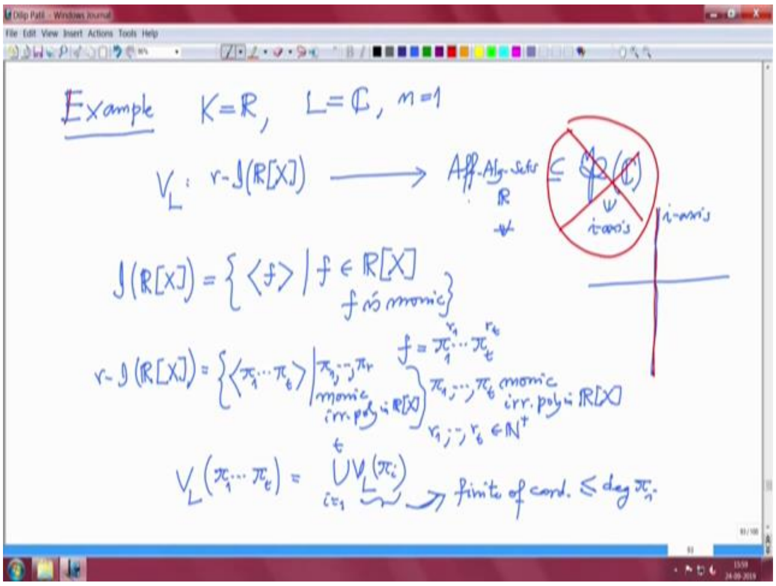
So, first of all, this map I want to study more, more intimately, because if you notice, this side is commutative algebra, studying radical ideals, maximal ideals and prime ideal this is, this argument except and this side are the geometry objects where I can draw pictures, also I am going to define a topology. So, I can talk about open sets, closed sets and so on. So, this will give first, so, if I could prove when can I prove that this map is bijective, that is where, I will concentrate.

I am looking for some assumptions. So that this will tell us this map is bijective, this is what we are looking, this is what we are looking for. So, because if you have bijective, then we can go from here to geometry and we can come back to algebra and that will become what is known as algebraic geometry. And one without the other will be incomplete in the sense we cannot really study geometry without algebra and algebra, if you study very algebra without any geometry it becomes a dry algebra, non interesting.

So, the motivation to study algebra will come from geometry and algebra will give you very technical support for geometry, to formulate statements correctly and prove them correctly and so on. So, our aim is to come to a situation where it is bijective, that is the best possibility, but obviously in life that best possibility does not happen. So, at least we should know when it is injective, surjective and so on.

So, this is what I will carry it on in the next couple of lectures and after the break first of all I want to give some examples. And so, for example, obvious examples are what, first of all, not affine algebra, not every subset is an affine algebraic case. Let me give that example right away. So, let us go to the next page.

(Refer Slide Time: 35:46)



So, let us see some examples. Let us take K to be R and L to be C, this is the classical situation. And now what we are looking at the power set of and I am taking n equal to 2 or even n equal to 1 let us say, even n equal to 1 we can take, n equal to 1. So that means, what is our map now V L, VL is a map from radical ideals of the polynomial ring over R in 1 variable RX to power set of L, which is a power set of C. Here are the affine A double F

ALG R sets, that means these are, this is subset here, this one I do not have to write the bracket no here because that is what we have denoted so.

So, all right. Now, let us see whether this map is surjective. So, what does that mean? Surjectivity means given any element in a power set, whether it is coming from some ideal here. So, for example, what is C, I will denote C now as a real plane and any subset here will be some subset here I can draw. Okay. Now, let us for example, take this set, this set this is a imaginary axis, I should draw better picture. This is a plane and let us take this one, this axis.

So, remember, we have all only 1 variable and a real polynomial and first of all remember that, what are the ideal, we know the description of ideals in a polynomial ring in 1 variable over a field. So, what are all ideals in RX? We know this, all ideals in RX are precisely the principal ideal generated by a polynomial. This statement follows from the fact that RX is a Euclidean domain because there is a Euclidean algorithm, you can divide arbitrary polynomial by monic polynomial and get remainder and so on.

So, every ideal, so the set of ideals is precisely ideal generated by a single polynomial f, where f is arbitrary polynomial in Rx. And if you want this to be a unique generator then one assume that f is monic, these are all ideals. And how do you write all radical ideals? All radical ideals are simply now, we have to look at the prime decomposition of f and then remove those multiplicities.

That means what you write f as product of pi 1 power r1, pi t depower rt, where this pi 1 to pi t are monic irreducible polynomials in Rx. And this R1 want to Rt are positive natural numbers. Every polynomial you can write uniquely like this, this pi 1 to pi t are called the prime factors of f and R1 to RT are called the multiplicities of f pi i's. So, what is radical ideal corresponding to this, we just have to forget these powers.

So, this is precisely ideals generated by the different primes, product of different primes. Please pick are also called square free polynomials where pi1 to pi t are monic irreducible polynomials, monic irreducible polynomials in RX. So, we know radical ideals in terms of the generators. And where does it go? It goes to 0 set of this, complex 0 set, they do not have real 0, so we have to look for the complex 0s.

So, where do they go? Some of them may be linear also. The linear will correspond to the real 0 and the nonlinear will correspond to the complex conjugates 0s because… So, then any case pi1 to pi t have finitely many complex 0s. Therefore, this product will have finally many complex 0s. And therefore, this, where will this set go, under VL. So VL of pi 1 to pi t is precisely union of VL of pi i's, i is from 1 to t and each 1 of this is finite set.

In fact of cardinality less equal to the degree of pi i's because any polynomial of degree d cannot have more than degree 0. So, therefore, this is finite set, finite union, so all together it is a finite set. But this red line what we have taken are taken that is infinite set, therefore, this one cannot come from any polynomial, any radical ideal therefore, map is surjective.

This, what do you call it real, this is imaginary axis, this is y axis, I should actually not call y axis, let me just call it i axis. So, what we have checked is i axis which is a subset here, which belongs here, but which does not belong here. Or for that matter any infinite subset, any infinite, there are lots of infinite subsets of complex numbers, they cannot be affine algebraic sets. And so, therefore, this map cannot be surjective in general.

So, we have to ignore outside this, we have to ignore this. So, now we can at least ask whether every, now it is by definition surjective, any affine algebraic set is coming from some radical ideal. So, we will continue this with more examples in the latter half of this one so that we can get acquainted with what is going on. Okay, thank you. We will continue after the break.