Computational Arithmetic - Geometry for Algebraic Curves

Prof Nitin Saxena

Dept of Computer Science and Engineering

IIT Kanpur

Week - 03

Lecture - 06

Local Rings

So last time what we defined is, we have to go back quite a bit, so we have defined many things, we have defined these, the notion of continuous functions now algebraically, which is regular function. So we have defined it via this, I mean at a point it should be regular which means that around open neighborhood U it should be F = G / H where G and H are coming from the coordinate ring which is you can think of it as the polynomial ring. So G and H are just polynomials. So neighborhood by neighborhood you have to define this. And then we showed actually that in this proof sketch we showed that once you define it locally it's also true globally, so everywhere it's the same G / H. That's a special property of Zariski topology for affine varieties, for affine or projective varieties.

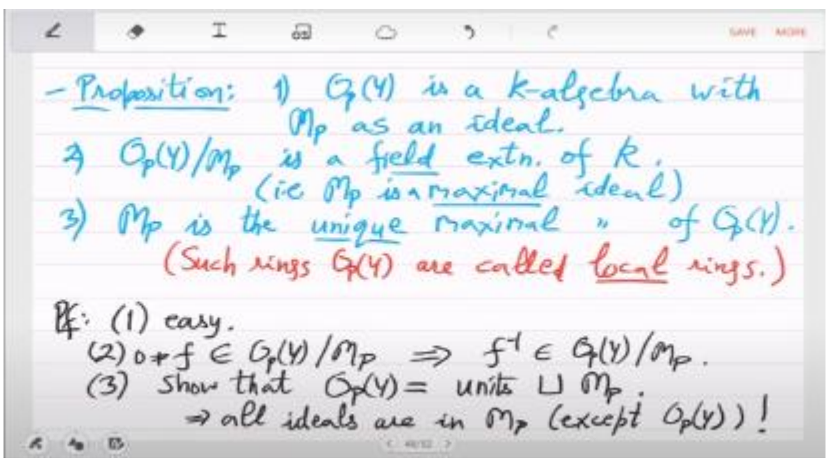
Then based on that we define morphism. which will allow you to compare two different varieties. So this was defined so that it not only takes care of continuity but it also takes care of regular functions. So for any open set V ϵ Y, φ '(V) should be should also be open and the function should all any regular function defined on v should translate back I mean there should be a way to pull it back on x on φ '(V) and then we defined this notion of oh yeah so we defined o y which is the ring of regular functions and we defined k y.

which is the field of rational functions and it will be strictly bigger than o y. So you should think of o y as the polynomial ring and k y as a function field over the polynomial ring, right. And then we define this for a point also which is germs on y near p. that is O sub py, okay. So, let us look at these properties quickly.

So, we have this these three basic properties, so O P Y is a, it is obviously a ring, it is a K algebra, it also contains the field K. So it is a K algebra with M P as an ideal, so remember M P are those germs at P which are 0 at P, it is they are defined around P and at P they are 0, right, they will not be 0 everywhere, so that is an ideal. So one is easy, second property you have to show that opy by mp is | mp| is a field and this we had shown by simply claiming that or simply observing that if f is in this then f^{-1} is also there as long as f was not 0. no no no I want to show that op y | mp| is a field. So, take a field take a element there f it is not 0 means that at p it is not around p it is defined and at p it is not 0.

So, hence 1 / f is also defined in the same quotient ring right. So, this is essentially shows you that Opy mod mp is a field and which then also implies that mp has to be a maximal ideal. So, all that is implied. Why is it unique? Why cannot there be some other maximal ideal also? if you started in a different direction inside Op(Y) maybe you will get to some MP prime. So, here it is not possible because what you can show is Op(Y) has only 2 parts, there is the units elements which are units and if you remove the units then what remains is just mp, which means that the functions thus so the germs around p either they are vanishing at p or they are invertible, then it is easy to see.

So, so either the either any element is a unit or it is in MP, which means that if you take any element outside MP then the ideal generated by that will be everything, okay. So, this implies that MP is unique, basically all ideals are inside MP. except the complete one which is Op(Y), right. So, this shows the uniqueness of this maximal ideal and when that happens then we say that the ring is a local ring and this is really a definition or term coming from the geometric intuition. Any questions? So, let us prove one more proposition.



So, for a fine variety y and we always assume algebraically closed k of course. the natural map from Ay → Oy is a ring isomorphism. I mean so we have defined this new object O (y) which is the ring of regular functions defined on the affine variety y. It will be good if we can realize this algebraically right. So I think I probably mentioned this before we even proved that it will be equal to a y but let us quickly see the steps of the proof.

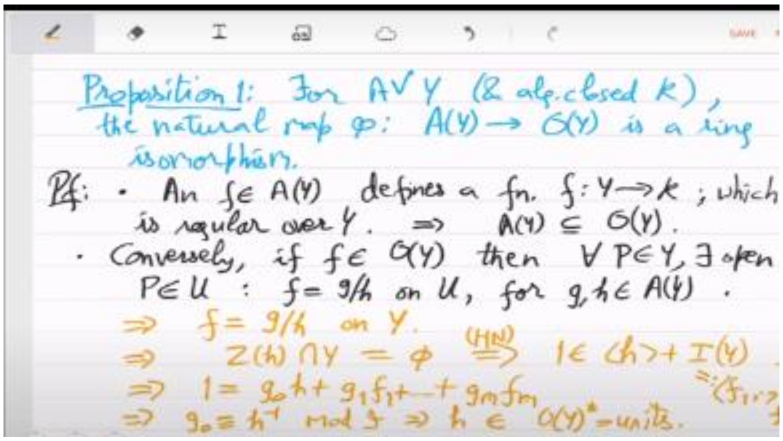
so that you know that O(y) is not really a new object, it is only an interpretation, it is just an interpretation of Ay, the coordinate ring which you can think of as the polynomial ring mod the defining ideal Iy. So, the way you prove this is any f in Ay So any polynomial defines a function y → k, right because clearly if f is a polynomial you can evaluate it at whatever point you want, there is no issue of division by 0. So that is the function and which is regular over y. So this means that, we can just think of Ay as contained inside O(y), right. So the map φ, the natural map is simply containment, you can think of explicitly.

Now why is the converse true, why don't you have anything else, something else other than So conversely if you take an element in O(y), then for every open U or how did I define it, I think I defined via point, so then for every point and its neighborhood U, or let us do it properly. So, for every point in Y there exists an open U around P such that f = g / h on U for g and h ϵ Ay. Okay so this is the meaning of f an element in Oy it is a regular function so any point you pick there is a neighborhood open neighborhood where it is basically a fraction of two polynomials and then we had this proof sketch that the same g and h you can use everywhere so this means that f = g / h on the whole y. Basically we showed this by taking two different open sets u1 and u2 and then this representation has to match on the intersection and the intersection is again an open set which is very big. So if the two representations match if two polynomials are the same on a very big set, then it means they are exactly the same, that was the intuition and so you get the same representation everywhere, which means what.

So, this means that 0 of h and y is, there cannot be any 0 (h) right, so this is empty But if H has no 0 then it means that, it means that by Hilbert's Nullschallensatz, 1 has to be in the ideal H plus Iy, right. So, now you come to algebra. So, if you look at the ideal which is defining Y and H that ideal has to have 1. because this is the only obstruction to having a common 0, because we are over an algebraically closed field right. So, 1 is in h + iy which actually means that you have equation of this type g0 h + g1 some f1 … fm, where this ideal is let us say generated by F1 →Fm and we know that every ideal has a finite set of generators.

So, from that we get this equation and from this equation you get that G0 is $H^{-1}|I|$.

So, H is a unit. H is a unit in O(Y). So, units we denote by star. So, H is in O(Y) *, is that clear.



So, since H is a unit, so you can just think of G, so then G / H is basically a polynomial. so g / h is in ay that is what you reduce, okay that finishes the proof, is that clear. So we have shown that any element of OY is actually in AY and AY is contained in OY, so you have equality and formally there is this isomorphism between these two objects, that is an important thing to remember. So that gives you a complete understanding of OY. Now look, let us look at the germs around the point.

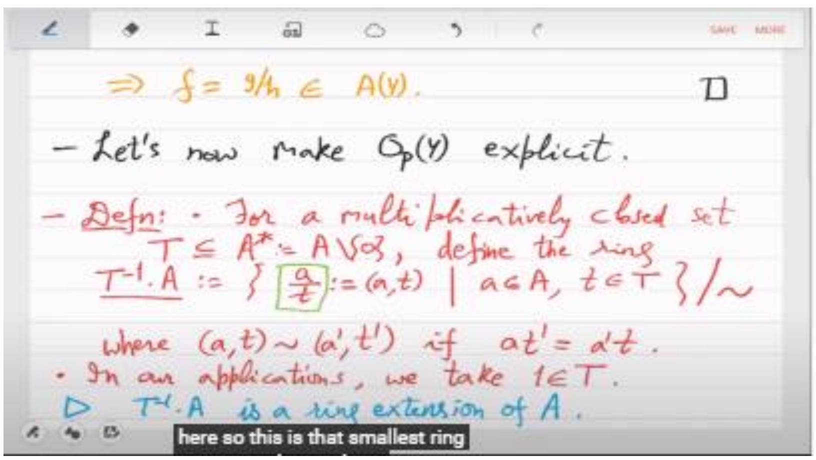
What does that mean algebraically? Okay, so now we have to look at this, the germs around P. So for this we will need as I mentioned last time we will need the idea of localization in algebra, which again is directly motivated from this situation we are in. So what is localization? So for a multiplicatively closed set T. of A star where A is again the polynomial ring and star is removing 0. So maybe I should write here by this I mean A-0.

So for a multiplicatively closed set we define a new ring T^{-1} times A. So, the ring where elements in T are have fractions have reciprocals. So, to make it a ring we have to introduce everything. So, we basically introduce something like A by T or you can think of it simply as a where A is in A and T is in T. And since I want to think of this A, T pair as the fraction A / T, so I also have a, I should have defined when two fractions are equal.

So I go modulo a relation where A T is the same as A ' T ', if what should happen, A T ' should be equal to A ' T, okay. So, this is the symbolism, by itself it does not make, I mean it is not defined by itself, The interpretation is that we are looking at these A x T pairs up to an equivalence relation and any two of them can be added where the addition formula will be A / T + A ' / T '. So, the addition formula for two fractions, so you will get a third fraction and any two can be multiplied and so on. So, it is a ring, it is forced to be a ring. No, but when A is the polynomial ring it is fine and also polynomial ring modulo and ideal no no the ideal will always apply on prime ideals, we will only use it for varieties, so it is okay do not make it more complicated.

So what Madhavan is worried about is that what if A is a general ring, so in that case the equivalence relation has to be generalized a bit but let us not worry about that because it would not apply to our case. So, is that clear that this is a ring T ‘ A, especially because in our applications we will put 1 in T. we will always have 1 in t. So, when 1 is in t then 1 is available in T‘ A. So, it is a ring it has 0 it has 1 and it has for the fractions it has these addition and multiplication rules naturally.

So, the immediate property is that t^{-1} a is a ring extension of A. And this is a kind of a unique ring extension or minimal ring extension where all the inverses which you wanted are present. You wanted to append 1 / T for every 1 / small t for every small t element. So, all of them are present here. So, this is that smallest ring extension that we have built.



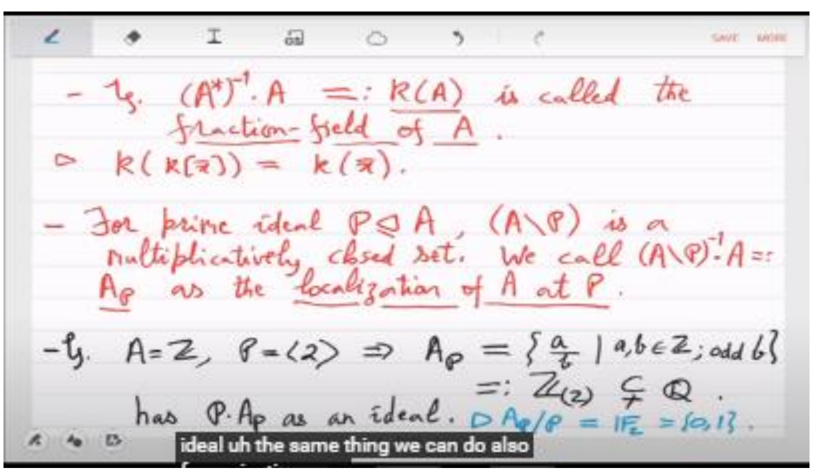
here is a key example. So, what happens if you invert everything possible, what is this? So, everything except 0 you want to invert. then from polynomial ring you go to the function field and we call this k small a, small k of a, this is called the field of fractions or fraction field of a, fraction field of a. So for the polynomial ring k of the polynomial ring is equal to this. So previously 1 / x1 was not there now you have 1 / x1 that is the thing you wanted all the rational functions are there.

Another thing we want is. take a prime ideal of the polynomial ring A, what can you say about A minus P. So, if you take two elements in A - P is the product also there, the product has to be there because if it is not there then it will be in P. but it cannot be in P because P is a prime ideal right, so one of the factors has to be in a prime ideal. So basically this is a multiplicative set, so multiplicatively closed set So we can actually we can localize by this, we can introduce inverses of this and that we will give it a special name. So we call A - P $^{-1}$ times A, we call this A sub P.

as the localization of A at P, okay. So the algebraic operation it is completely new, I mean it is basically the instead of including all the fractions to get the fraction field you only introduce some of them. Okay so you get kind of infinitely many new objects. So what you do is that you take any prime ideal and then you introduce you invert everything except prime ideal. Okay so that is called the localization of A at P.

So let us test you what will happen if you take A to be integers and P to be the prime ideal P. So what is a localized at p, what is the object? So you want to invert everything except multiples of the prime p, let us make it even more specific, the prime 2, right. So all the odd integers you want to invert, not even ones. So you get what? you will get numbers like A over B, A, B are integers and B is odd. So, this is called Z2, ok, not to be confused with 2-adic integers, this is.

it is related but a different object. So, here I mean clearly this is a proper subset of rationals right. So, instead of going all the way to fractions you have stopped in the middle somewhere in the middle where you only invert odds not evens and do you know a special ideal of this ring so multiples of 2 here are it is again an ideal right, this has P x AP as an ideal so within this you can only you can focus on multiples of 2 so basically then you also say that A is even so even A divided by odd B right so that is an ideal and what is AP | PAP| so if I call that ideal again P AP | PAP | is, no so then you, so what was A | P|, that was just the finite field with two elements. So, you get the same thing here, you get the Galois field F2, just 0 1. So you can do the same thing but now it is kind of buffed up to this infinite object which is very different, it is basically these fractions and you can, yeah it is a way to embed the finite field in different kind of fractional rings. And yeah so we have defined till now this localization and localization by T and by a prime ideal.



The same thing we can do also for projective case where you have to take care of homogeneity So what will you say is T^{-1} now we call it S right because S was the graded polynomial ring where we only look at I mean where we look at the homogenous parts of your polynomial. this I mean here again you want to look at fractions but then you want to use the grading. So you will say that the numerator and denominator has the same degree that is an extra condition. So you look at s, t pairs again thinking of this as s by t such that S is in S, T is in T and so these have to be homogenous or homogenous of the same degree and modulo this understanding that 2 fractions are equal if this cross product is the same, Is that clear, so it is just a modification to the homogeneous condition and similarly we can define for a homogeneous prime ideal P or I (s). we have the localization SI right which will which is a special case of the thing above right.

So now we have some good properties. or in fact, we now have good objects, this using this A sub p the localization, we can now understand the germs at p. So, what you can show is that, for affine variety y, for all the points in that variety, is the same object, the same ring as the coordinate ring. So, well clearly it is not the full coordinate ring, it is a sub ring of that which are defined in a neighborhood of P, right. and sorry it is not yeah it is an extension.

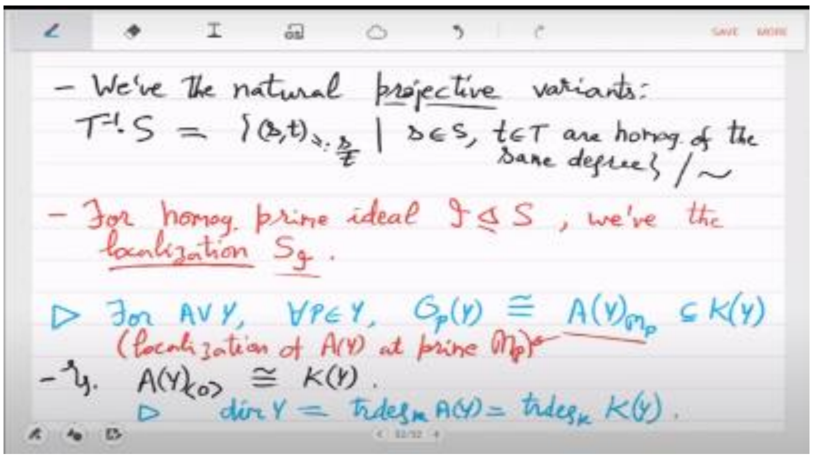
So, let me write that and then explain. So, Op(Y) is clearly a subset of KY. right because ky are the rational functions which are defined on y, somewhere in particular if you look at those rational functions which are defined around p, then you will get opy, but algebraically we have identified which ones are those. So, these are the ones which come from fractions G by H where G, H is in Ay in the coordinate ring and all you want, all you need to be careful about is that H should not be in MP, right. H should not be a germ which is vanishing at the point P because then G / H will be undefined. So, with that care you have identified what Op(Y) is and with localization.

So, this is the localization of Ay at the prime mp is that clear. Remember that MP is a maximal ideal, so it is clearly a prime ideal. So, we are localizing Ay at this specific prime ideal which happens to be in fact maximal and that is what Opy is. So, what happens if you localize Ay at the prime ideal 0. what is this? So, if you invert everything except 0 then you should get you should get the maximum which is k y big k y.

So, only at 0 localizing at 0 you will get all the rational functions defined on y, for everything else you will get a proper subset which is this ring. Why is it called localizes? Sorry. Why is it called localizes? Because of the picture, these are the functions which are defined only around p. in arbitrarily small neighborhood. So, the global I mean the functions that are defined everywhere globally are a y and if you only want to look at those functions which are defined in an extreme vicinity of p that is a y sub m p.

So, localization is the precise exact term that you want that is exactly what the definition of Op(Y) was and it also follows by our earlier results that the geometric dimension that we define for a subset of the affine n space in particular here for the affine variety y. So, dimension that dimension is equal to transcendence degree of Ay and also transcendence degree of this field Ky, big Ky. So, all these three things are the same, because when you localize you do not increase the dimension, though you do not increase the transcendence degree. So, Ay sub 0 is has the same transcendence degree as Ky.

So, from that you can see three things are equal. Any questions? Okay. So, Let us see a quick example.



So, in the affine plane, let us look at the affine variety $x2^{2} - x3 - x1^{3}$. So what is the function field of this k big K y, what are the functions maximum possible which are defined somewhere on y, we do not care about everywhere but somewhere. So this will be you can unfold the definition and just check that it is actually this.

Okay so look at the rational functions over k in x1 variable and then so that is a field and over that field you basically are introducing square root of x1 is the same thing. So this is the same as in x1 you are introducing √x1. Is that clear? You are actually introducing $x1^{3/2}$, but which is the same as x1 to the half that you are introducing. So, that is the set of maximum, the biggest set of functions which are defined somewhere. Note that there are many many things here which are not defined everywhere, right.

Even if you look at 1 / x1, it is not defined everywhere. For example it is undefined at 0, 0 but that does not stop us from calling it a function of y because it at least it is defined in a large chunk which is an open set. So most of y these things are defined but somewhere there are these undefined zones and so let us look at that. So the point is 0, 0 in y.

what are the functions defined at that place. So, what is O P Y, right. So, O P Y is the coordinate ring localized at M P, what is, so what is M P now. So MP is this ideal x1, x2. It is the ideal which should be maximal, so it should actually correspond to a point, the point is 0, 0.

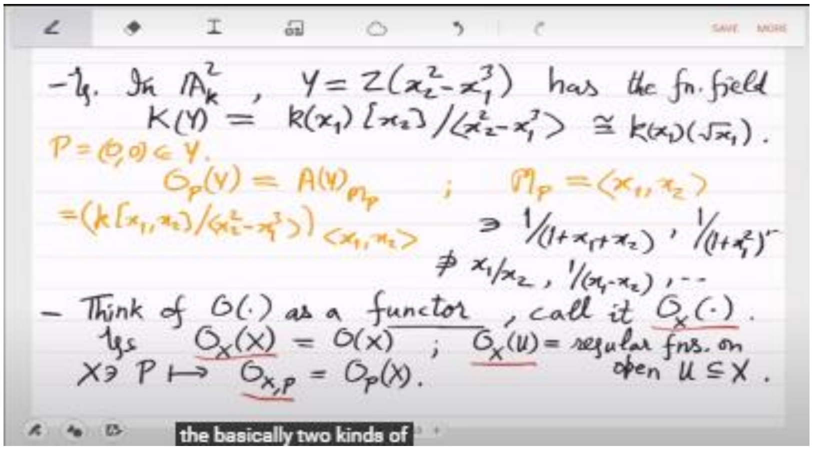
So the ideal can only be x1, x2. It sets both the variables to 0 and clearly that is a point on y. So that is the ideal and you just have to look at the fractions by the definition. So this will come out to be k the polynomial ring modulo this ideal and then you localize it at the ideal x1, x2, okay. So it looks complicated but I mean slowly if you unfold that definition it would not be so complicated. You should just think of the thing inside the bracket to be just polynomials in x1 and x2 and you are allowed those polynomials to be divided by polynomials which are not in x1, x2 ideal.

So they should not be constant free the denominator should not be constant free that is all it is saying. So for example it has this object has 1 / 1 + x1 + x2 but it does not have x1 over because the problem with 1 / x2 or x1 / x2 is that the denominator x2 is in the ideal. So, that clearly geometrically also you can see that it is something which is undefined at the point p, while the first function is defined, is that clear. Similarly, 1 / x1 - x2 is also not defined.

and here 1 / 1 + $x1^2$ is defined and so on. So, you create a good idea of you create a complete understanding of what these functions are and explicitly work with them. So, what we will do now is we will think of this O as think of O as a functor which is taking you from geometry to algebra right, you get you are going from these the affine n space to the function field. So, we will call it O x acting on something, then this functor we will use and generalize You can think of this O x as the functor of ordinary functions. You can think of O as standing for ordinary functions over x in a neighborhood. So, that dot will be for example, you can if you apply it on the whole.

of your affine variety then what you will recover is what we have defined before ox or you can look at it on a open set. So, these will be regular functions defined on u. on open U. So, we will think of O as something more general instead of just the ring object that we have defined. We will think of this as a functor, it is taking something from geometry and landing in a very different area which is algebra.

And then if you take a limit of these open neighborhoods around the point P, then you will get the germs. So, it takes a point which is in $X \to O_X P$, these are the germs.



Is that clear, so I am changing the notation of bit here, I am changing it to ox dot, so you can apply ox on a either you can apply it on everything or you can apply it on a open subset or you can apply it on a point, these are the basically two kinds of applications. So this functor is key in algebraic geometry.

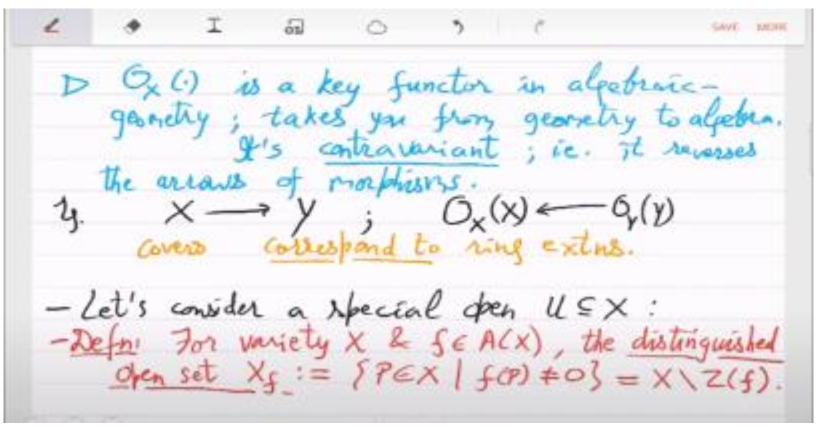
So it takes you from geometry to algebra. and there is a fancy property it has which is that it is contravariant, so contravariant means that it reverses the morphisms. So, for example, if you have a morphism from some affine variety X to affine variety Y, then what can you say about OX or let us say there is a, say we first apply it on the whole thing. So, what can you say about OXX and OYY. So when the arrow goes from X → y, then after applying OX, the arrow will be reversed, okay.

So the arrow will go from here to here. So in geometry, basically if you are trying to cover Y by X, then in algebra you are going to a ring extension of OYY, okay. So covers are like ring extensions. So covers correspond to, any questions? So this we had seen also happening when we defined morphism, but now it is more precise in terms of this OX functor, so we will frequently be reversing the arrows and doing the analysis in proofs, right. So if you defined OXU, okay.

So then let us look at an example of OXU for an open set. Let us consider a special open set. So this will be called a distinguished open set for a variety X and an element of the coordinate ring. x sub f you want to define x sub f. So, the distinguished open set xf is defined as follows.

So, it is basically the set of those points in x at which f will not vanish. it is as simple as that. So, this is the points on the variety at which fp is non-zero, okay. So, that part of the variety x it is clearly open because in Zariski topology we have defined open as complement of closed. So, the closed subset will be f of I mean those points p such that f (p) = 0 and this is the complement of that.

So, this is the same as x - z (f), right. So, that is close this is open, this is called the distinguished open set because if you understand these open sets then you understand all other kinds of open sets, okay. These are the only open sets you need to study.



So why is that? Any open U is a union of distinguished ones. So what is the proof of that? So, u is open which means that it is complement of some 0 set right. So, u defines a j such that this happens and you also know that any ideal J has finitely many generators, so we write it as f1 … fm.

So any open set is basically just complement of the 0 set of some roots of polynomial system. And so another way to write this is, see the 0 set is an intersection, so the complement is a union. So you write it like that, so it is the union of x – zfi, which is union of x sub fi. Is that clear? Because complement means that one of the Fi's will be non-zero, right. So, any point in the complement will be available in some Zfi complement for some i.

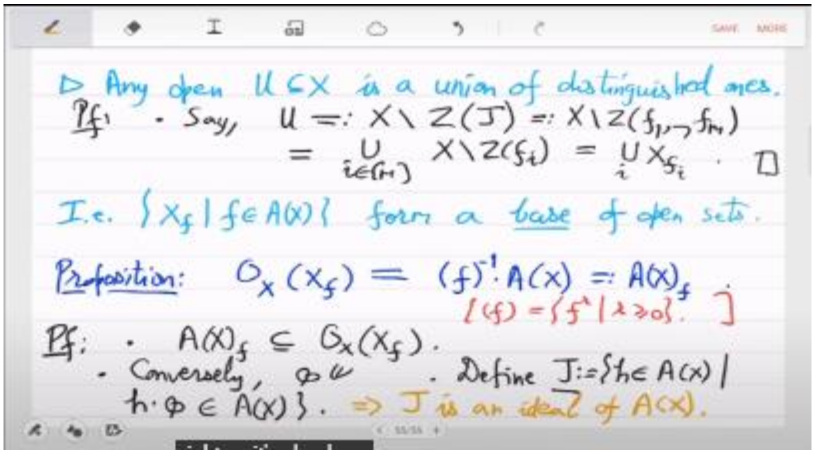
So, in other words open sets are union of finitely many distinguished ones. So, distinguished open sets you should think of as giving you a basis. It is of course an infinite basis but any open set you have in mind can be represented by using finitely many of these, okay. So this contains a lot of structure from algebra, so these they actually form a base. of open set open sets this instead of basis we call it a base right. So, I have defined this just to test you on what is the O functor on this xf can you give me that what is O x functor on this open set.

xf is distinguished open set. So, what are the regular functions that are defined on this part, which is the part of which are the points of x that do not vanish, do not annihilate the polynomial f. It is very simple right, the functions g by h all you want is h should not be divisible by f right. basically. So, we will show that it is actually this.

It is the multiplicative set generated by f and then you make these things invertible. So, you introduce. So, all the functions which are defined everywhere on x. was Ax and when you are looking at this neighborhood xf then or this open set xf then you are also allowed to invert by powers of f essentially. So you can divide by f, you can divide by f^2, f^3 these will also be defined on xf because the denominator does not vanish and we will call this we will denote this by Ax sub f that is the proposition and the definition is that clear. So, let me write it may be that f is just powers So, by bracket f I mean the multiplicative closed set generated by this single element.

So, it you get only powers what is the proof of this well. So, what we just defined clearly Ax sub f anything here is defined I mean it is a it is regular on xf. right because g over f or g over f square these things are defined on xf, so that part is clear. We have to show the converse that is the non-trivial part, so conversely you take let us say φ in O in this and we have to show that this φ is just like g / f →r. So, let us look at the possible denominators this h that I am talking about.

So, these h such that h times φ is in Ax. So, let us consider all these possible denominators h. such that h x φ is a polynomial in the coordinate ring. And what we have to show is that these h are essentially coming from bracket f, it is like f → r, right, nothing else, okay. So, first thing you observe is that j is an ideal. Is that clear? Because any outside element of Ax if you multiply it with h, then you can then h φ continues to be in Ax right.

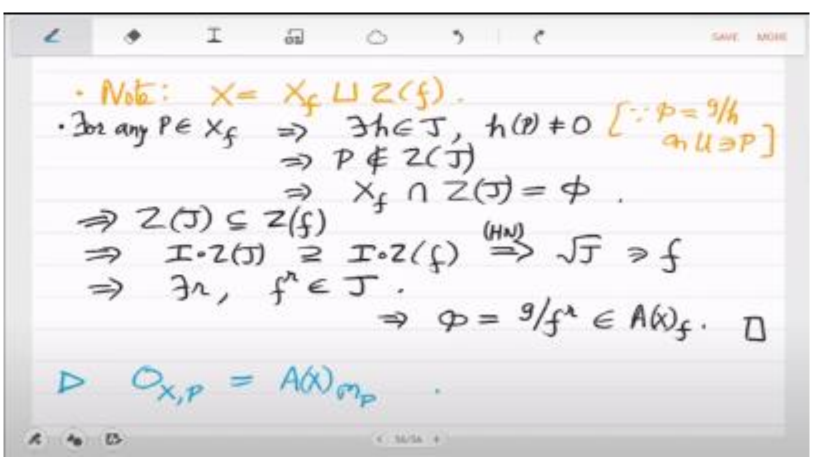


So, it is clearly an ideal and yeah I think one another thing which will be useful to remember is that x has the following decomposition. because any point in X either it annihilates F or it has not right, so there is a clear coverage these two things cover X. The question you have to ask is whether these two components are disjoint or can there be a common point, so let us analyze that. let p be a point in xf oh and ok this j is also connected here let me write that. If p is in xf then, oh this is trivial sorry, this is trivially disjoint because if fp ≠ 0 then clearly p cannot be z (f), so this is by definition, so this is a disjoint union covers x, the question that you have to ask is if I take a point p which does not annihilate F, then there exists an H in that ideal J, says that H at P is non-zero, is that clear.

That is just from the definition I think. Because the ϕ, yeah so here you are using the fact that ϕ is regular over xf, right. So ϕ over xf already has, I mean at the point P, it has a representation like g by and if you use that particular H it happens to be in J and it clearly wouldn't vanish at P. So, this just follows from since this $\phi = G / H$ on a neighborhood containing P. So, for any point P in XF there is a polynomial in J, in the ideal J which is not annihilated by that point, this is just parsing through the definition, through the hypothesis, which means that the point is not in Z (J), which means that xf and z (j) are disjoint, is that clear. So any point P that you pick for any P You will find an H at which is such that H at P is non-zero and so that means that basically XF cannot have a common point with Z (J)and when that happens then you should invoke Hilbert's null-challenges.

So is that what I want? and sorry okay there is one more conclusion so now you look at the orange note so since z (j) is disjoint with xf you deduce what it is a subset of z (f) yeah and on this you can apply the ideal functor so you I(ZJ) is then, it then contains I (ZF), which will give you what, so by Hilbert's Nullschleinsatz, you get that radical of J contains F, which means that there exists an R, such that F^r is in J, is that clear. And yeah that is also g was the collection of all possible denominators and we have shown that f^r is 1. This means that φ is equal to some g / f^r which is an element in Axf that is what you wanted to show. Is that clear? So it is a simple argument but you have to get familiar with how to keep switching between points and rings and ideals. So but you have learnt ultimately a basic geometric fact that the functions which are defined on points which do not annihilate f.

their denominator is a power of f, that is all, that is what you learn and of course, this is our algebraically closed field that we are always assuming. What else? I think the stock, the germs thing I have done right, yeah Op(Y) we have studied, so fine. Yes now we have a good handle on the Ox functor, we understand what it is, how does it act on the distinguished open sets, so Ox (xf) is just localization by this powers of f and we understand how it acts on everything, so Ox (x) is just A (x). and finally how it acts on a point that also we understand. So, Ox, p is the localization of Ax / mp, yes so that gives a complete understanding of the Ox functor.

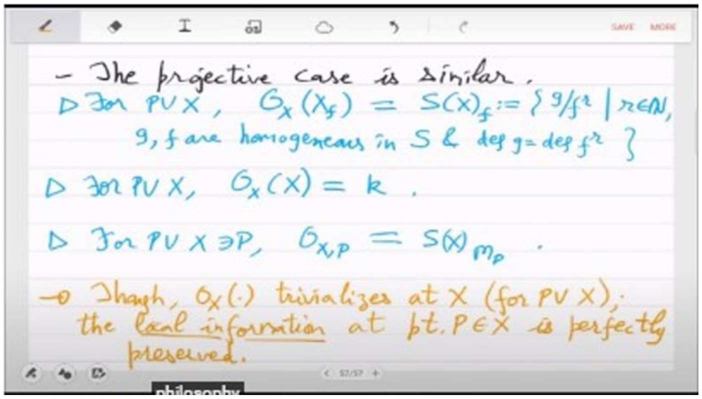


fine I think this is all done, correspondingly, so analogously you can define for the projective case also, so for the projective case, for a projective variety X, the regular functions defined on x of f, the definition of x of f will be similar, like these are the points of the projective variety x which do not annihilate f, the polynomial f. So this will be what? So analogously you can show that this will be the homogeneous functions I mean homogeneous g over f^r where degree of g and degree of f^r is the same. So, this is the this is basically the set of those g / f^r such that G and F are in some SD sorry not the same SD, GF are homogenous in S and degree of G is equal to degree of F^r and R is. a natural number, okay is that clear. Yeah, so that would be the definition of Sx localized at powers of f, you always have to take numerator and denominator equal degree and then again you will have to say this again the Ox for functor will be clear.

what is Ox of x. So, this we had argued before right that this will be the only thing that remains that works everywhere is constants right, Ox of x is just constants. And finally the germs, what was that? So, for projective variety X containing a point P, what is O_XP? So, this again is like before SX localized at MP. So, MP is the maximal ideal that defines the point P and you just localize by that it is also a prime ideal of S.

So, that will be the same thing. So, there is a nice thing that is happening here. So, this OX functor if you look at it on the whole of X. then it seems that all information is lost because all only the functions which are the only functions which now remain are the constant ones right. So, they then it is not giving you any information about the projective variety x itself while if you look at the germs that has perfect information as you go over different points you will get different parts of Sx. localized. So, what you should learn from these two results is that, though O x x, so O x functor is trivialized at x, for a projective variety x.

the local information at point P is perfectly preserved. So, which is why these functors so they did so you if you look at it globally then it will have fewer information but if you look at it locally which is specially around the point it will have all the information which you will want okay so we will also use this philosophy often the local information is the true information so next time we will Next we define more local kind of morphism.



We have already defined a morphism, next time we will define what is called a rational map. so we can write it may be to differ to make the arrow different rational on top. So we will define how to compare x → y in a more local sense without asking for definition everywhere.