Computational Arithmetic - Geometry for Algebraic Curves

Prof Nitin Saxena

Dept of Computer Science and Engineering

IIT Kanpur

Week - 05

Lecture – 10

Discreet Valuation Rings

Any questions still now? We looked at this curve $x_2^2 = x_1^3$. It has a point of singularity at the origin and we resolved it by changing it to the curve $y^2 = x_1$. The transformation is $y = x_2 / x_1$. So, we are introducing a third variable and then you see that clearly the similarity at the origin is gone. right now the curvature is just right, but of course we in algebra we do not have any concept of curvature or we cannot draw this picture, so we are doing this algebraically and for that we have to develop more algebra, so we have developed tangent space and rank of that. we want that rank to be 1 in the non singular case and for resolution we have defined these discrete valuation rings.

So, resolving a singularity is a blowing up process. So, we increase the variable and we basically we want the ring of germs to be bigger. And yesterday we showed what we mean by bigger is integrally closed. We actually showed three properties.

So we want first property is we want the maximal ideal to be principal. This we take as the definition of DVR. But there are many equivalent properties in even definitions of DVR. Second property is that there should be a valuation on the function field. So, valuation means basically a metric, it is a map that sends every field element to an integer such that it should respect the multiplication and it should respect the addition.

The axioms are in orange. So, for multiplication it should be additive. V should be additive and for addition it should be at least the minimum. So, $V(\alpha + \beta)$ should be at least $V(\alpha)$ and $V(\beta)$. And third property was integral closure.

So, integrally closed means this thing that if for a monic polynomial you have a root in the field then you actually have a root in the ring. in that case you call the ring integrally closed and then we showed that all three properties are equivalent. So, we showed that this for transcendence degree one field big K, R is a DVR if and only if there is a valuation on the field if and only if R is integrally closed. So, any questions till now. Okay so now we will see the what are the valuations of field of the affine line, before that let us pick a more unusual example or a more basic example actually that of rationals So in this case DVR within rationals will be you are looking for a ring R which is inside rationals and which should have a maximal ideal that is principle.

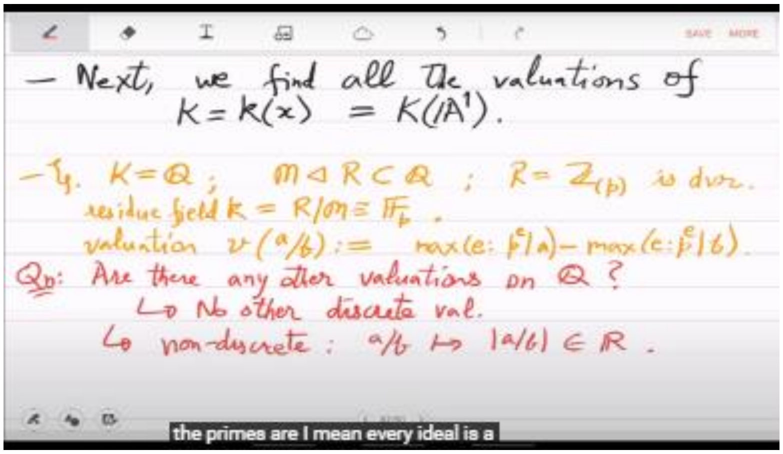
So one example is you take a prime and localize integers at the prime. So, these are not all the fractions, these are those fractions where p does not divide the denominator. And this is a DVR, it is a DVR because you can see that the maximal ideal is p times So, it is a principle unique maximal ideal and the quotient the residue field is r over m which is fp right. What is the valuation? that it gives on fractions. So, valuation v on a fraction a over b, a and b are integers is defined to be, yeah the highest prime power of p that divides a divided by that for b right.

So, this is also called the valuation with respect to p of integer a. So, calculate that for integer a-. calculate that for the numerator and the denominator and the difference is what gives you the valuation. So, this is something you might have seen, what it tightly relates to is the DVR. So, this gives you infinitely many DVRs and infinitely many valuations on the fractions, on the rational numbers.

Are there any other options? What do you think? Is there any other way to define this metric V on rationals? So, as an exercise show that these are the only valuations. For rational numbers there are no other valuations possible. So, they are tightly related to prime numbers. No, that is not a valuation. Yeah, maybe discrete, yes you want a map to integers, you want a map to integers, yes so I should say discrete, that is important, it is a good point.

This is a trivial one, you just map everything to 1. Yeah, so no other discrete valuation, there is this non-discrete one, which sends the a / b to the norm of a / b, but this is a real number. So, we do not count that amongst the discrete ones the way we have defined, yeah you can show that they all come from prime numbers. Second one is called R d value. Yeah, that is what he said.

but in this course we are I mean we have defined it to be discrete valuation, so that does not exist and what we now want to do is we want to look at kx, right. So, let us say you have this field of rationals and you introduce a new variable x, in that case what are the valuations that you get, you want to study that question. And after that of course, we will repeat that argument, we will invoke that argument for the case of curves, for the case of curves it will be similar, all the valuations will actually come from the type that we will describe here. Yeah, so the primes in the ring kx, the polynomial ring kx right they are the primes are I mean every ideal is a principle ideal, so primes will be irreducible polynomials right that will be your first guess. So, let us define that as a ring, so for an irreducible f in the polynomial ring, define a sub ring of K, we will call it RF.



It is basically like the case of primes, we will look at fractions, rational functions where the denominator is not divisible by f. Everything else you can use in the denominator, which is the same thing as does it reduce to localization probably yeah I think we are you are just localizing by the prime ideal f is the same thing yeah. So, we will call this R sub f we are redefining localization basically and we will prove that these are essentially the DVRs for the function field, transcendence degree one function field. so the distinct discrete valuation rings of K are, this Rf for irreducible f in Kx and one more. So, you get one more over on top of what you had in the case of fractions can you case what.

So, it has to involve x right because now you have a new element x. So, f = x already appears in this example. but there is another thing you can do, you can look at 1 / x, so you can look at R x^{-1}, viewing x^{-1} as an irreducible in this ring. in the ring in again the polynomial ring, but instead of x you are using x^{-1}. So, r sub x appears in the first type and r sub x - r sub 1 /x appears in the second type, but this is new it is a different DVR than the above.

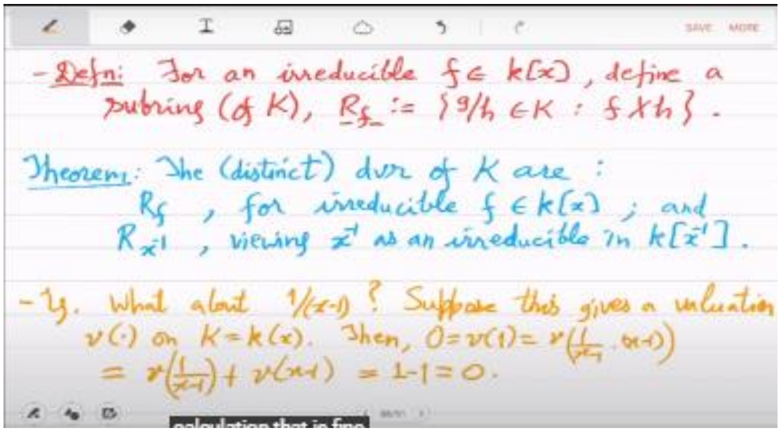
You can ask here why cannot we use 1 /x - 1. right if instead of the valuation with respect to x^{-1} can we true this for any f inverted right which is I mean the valuation seems to be defined but will it work suppose this gives a valuation v on k x, then what you can look at is v of 1 right. So, 1 is or maybe no not this think Let us do this, which implies that 0 has to be at least V of x and V of x - 1. Is that giving the contradiction? The valuation of 0 is defined to be infinite or 0? Infinite.

Infinite. The contradiction will be that here it will be 0. this x - 1 is measuring the order of the 0 at x equals 1, but then the constant polynomial 0 does not have any 0. Say that again, what is the proof? So this valuation with 1 /x - 1 is kind of measuring the order of the 0 or pole at 1, but then the constant polynomial as no 0 or full at the point 1. At the point 1 it has a 0.

Yes, that is right. At the point 1 it has a 0. Which means it has some non-trivial value. So, you want to look at valuation of 0. No, if I substitute 0 in 1 /x - 1. then I'm not getting zero, right? It doesn't have a zero, right? Oh, but we have one equals zero.

Yeah. That should be . Yeah units are of course 0, which means so valuation of x - 1 should be 0. Yeah, no but why can't you do the same thing with x^{-1}, yeah I thought I had a simple contradiction but. we have to think about this, let me leave this for now, but this is getting weird, so valuation of 1 has to be 0, which means this has to be 0, which is a contradiction, but why is this thing not Why can't we do the same thing with 1 / x? No, we are the big field is the function field. So clearly x - 1 is there and reciprocal is also there.

Oh the DVR is this. Yeah that you can deduce, you will X^{-1} here, it becomes a symbol. No, I mean it is also an element in the function field, so it is that symbol, it is not a new symbol. But what is the valuation on R sub X^{-1}? so valuation is always given by the uniformizer in this case the uniformizer is 1 /x so okay let's let's check that yeah let's check that so valuation of X^{-1} will be 1 and valuation of x will be - 1 then right, because you can write x as 1 /x^{-1} and that gives you - 1. No, no I think I am. No, no, no, no, I think I have messed it up, no, no, no, no, this is the axiom I am using wrong, wait, so this is 1 / x - 1 . x - 1 on and the product it is additive, so what you will get is actually sum. and valuation here was with respect to 1 / x - 1, so this is equal to 1 +, yes something we don't know, but anyways, this is - 1, yeah that is true, okay, this will not give a contradiction, yeah fine so for contradiction we have to use something else this won't give a contradiction for x 1 /x - 1 or for anything this is just a example calculation that is fine okay so then i go to a different calculation i use the added the axiom on sum, I think that was my original plan, so consider Vx = x - 1 + 1 which then has to be at least V of 1 which is 0, that also is not very good, v of x I know is 0 and v of x-1 I know is what else can we try. The valuation of x-1 is - 1 right. Yes. So, when you expand that valuation of x-1 + 1 you will get minimum of valuation of x-1 or valuation of 1. No yeah which is true 0 is at least - 1 or 0 that is not a contradiction, so that is fine.



Yeah I hope that here it will be enough some contradiction will come but it is not happening. But V of x equals 0 implies x is a unit which is not. No this is the 1 /x - 1 valuation we are trying, we are trying to get a contradiction there. No there is no ring, we work with the function field. Any element in the function field valuation should work.

No I just wanted to check why is 1 /x - 1 not falling in these types. So 1 /x, what you can do with 1 /x, you can also do with 1 /x - 1. think maybe this is the part which we should look at, maybe this is the contradiction. So, valuation of x - 1 will be - 1 and valuation of 1 of course will be 0. So, these two valuations are different.

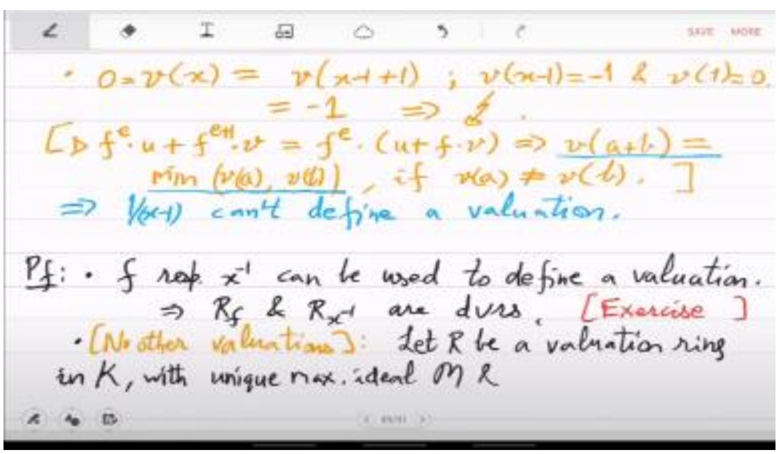
So, when you add x - 1 and actually the valuation should come out to be - 1 shouldn't it yeah it should be the minimum of the two summands yeah when these two are when the valuations of the summands are different then you should have an equality so actually this should come out to be - 1 that's the contradiction well this is because the way we define valuation once we have picked generator of the maximal ideal, we define it by the divisibility. So think about it like this, if you have a multiple of f to the e and you have a multiple of f^{e+1} and u and v are not they are co-co-prime to f. So, the valuation always picks the minimum right because you can take out f^{e}. So, which so this actually this property actually tells you that valuation of a + b actually is minimum if the valuations were different. So this property you have to show first, we have not shown it before but we are showing it now that actually valuation of sum is equal to the minimum as long as the two summands are different valuations.

Yeah, so now this is being contradicted above, okay you have - 1 and 0, so you will pick - 1 but LHS is 0, so yeah that needed more proof. so thus 1 /x - 1 can't define a valuation. So, there is a significant difference between 1 over f and this 1 /x, 1 /x is somehow very special is that clear. How is this relation of x is 0? I mean as you said x = 1 is not a pole is not a 0 or you just have to see is x - 1 dividing it or is 1 /x - 1 dividing it and that is not. I mean at x = |x| - 1 it is just 1 so you see that it is a unit there units have valuation 0.

So, I think you are now ready to see the proof. Key property there was basically that there is always some f that you can write every valuation of the form $f_{2\,e}$ = u that then right that is why it just happened you always had a valuation in that form. That is the yeah, so this you have to pick the uniformizer of the unique maximal ideal. So, because of that you get this property, this property that we have shown, valuation is equal to minimum. So, it is in the lower bound, it is actually exactly equal.

unless the valuations of A and B are different then what can happen is what happens is they cancel out and you go you can get something bigger, but not here. Any questions? So, we have to prove this, proof is similar to the prime case. so f respectively x^{-1} can be used to define a valuation so basically rf and rx^{-1} they are DVRs. So this how to define it this you check, I mean you have to be a bit careful with x^{-1} because as we saw bad things can happen like 1 /x - 1 this bad thing happens but that will not happen with 1 /x. So with 1 /x the usual thing check the multiplicity of x will give you a genuine valuation.

for rational functions in x and we have to now show that there is nothing else. So let us show that. So let r be some other of k or in k, it's contained in k with maximal ideal m and valuation v. So we will divide into two cases there is this distinguish element x either it is in R or not in R. So let us look at the case when x is in this valuation ring R.



So since x is in R the whole polynomial ring is in R. generated by x, because k ϵ R, x ϵR, so the whole thing is in R. So, we can actually look at the ∩ of the maximal ideal with this, the univariate polynomial ring. The claim is that this is non-zero. it has a non-zero element, why is that? So, maximal ideal in terms of valuation represents the positive values, if this was empty then it means that there is no positive value.

So, what will happen? Let us prove this. if the ∩ is 0 then every element in kx is invertible. So, it is in which means I mean it is a unit, everything here is a unit, so it is outside M, but it is inside R, which will mean, I think it means that the valuation is 0, the 0 map. Is that clear? yeah because we are in the function field of this one variable x and if you are saying that every polynomial is a unit, so valuation is essentially 0. So just by the non degeneracy you know that there is some element here, so this is then an ideal of kx. This basically reduces to the prime case which we did for integers.

So, it is a non-zero prime ideal and kx obviously has only principal ideals. So, what you get is that this ideal is generated by a irreducible polynomial, which means that m itself is generated by this And yeah, so you have identified the uniformizer and that is type 1, so we are done. Okay, let us go to case 2. Yes, how did you go there? No, but f is an element in kx, right.

So, it transfers to m. I mean all you wanted was some polynomial inside m. Sir, f power is subset of m, that will imply. No, no if you find an element common to m and kx, then you have found the generator. So, the what is changing is here it is kx and that changes here to R, but the generator is the same. Oh no also you are assuming the fact that m anyways was principal, obviously from this you cannot show that m is principal that was given to you.

So, already m was like generated by u and you have shown that u ∩ kx is f from there you deduce. Yeah, so something strong was known about m, we are not doing it in general and case 2, so here x ≠ nr. So, we have again assume that R is a DVR right. So, if x the field element is not in R then its inverse will be in R.

So, use the previous case. we get some polynomial which is irreducible generating the maximal ideal and the only thing which will be different which is not covered in case one will be x^{-1}. any polynomial if you substitute their x^{-1} then the new thing that you have is actually 1 /x, all the other examples are covered in case 1. So, this is the only new one, so that characterizes. Is that fine? Yes, so we have shown we have classified the DVRs, the valuations on the univariate function field.

From here now when you want to go to the two curves. For some irreducible f. Yeah, so say f was x - 1. So, no, no, no.

So, this is x^{-1} - 1. So, you simplify it. So, it becomes x - 1 /x. But yeah, the x - 1 part cannot give you anything.

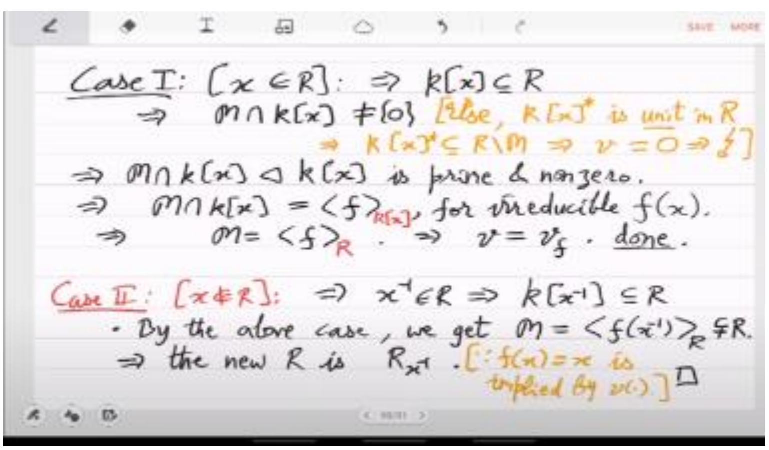
It is only the 1 /x. 1 by x only. Only 1 by x. I have to prove that x 1 and 1 belongs to R. x - 1, no x - 1 will be a unit. Well, so you have to look at that case, how to remove x - 1 and reduce to x^{-1}. I think you can show that x - 1 in this case will be a it will be a unit, right, you can show that.

So the only new thing you will get is this. If $x^{-1} \in R$, then x is in the field, it is not in R. Sorry, if, so we are looking at, let us say $x^{-1} - 1$, so this is $x - 1\ x^{-1}$ and we are looking at this ideal. Now what? No, x^{-1} is not in R. So, $x^{-1} \in R$, so x is not in R, but you are claiming that x - 1 is a unit in R.

x - 1 should be a unit. Why is that happening? If x is not in R, then x has to have a negative Now, when you are doing x - 1, you are getting valuation 0. So, how is that happening? So, x is not enough.

So, x has a negative valuation. Yes. Yes. So, what will be the valuation of x - 1? x - 1 you are claiming that. So, it has to be 0. So, now. No, so then f itself I think gets classified because of that, this cannot happen because $x^{-1} - 1$ is a unit because x was negative, x^{-1} is positive. So, since x^{-1} has positive valuation and 1 has 0 valuation, you again know that this object has 0 valuation.

So, $x^{-1} - 1$ is a. yeah so actually what you deduce is that f has to be 0, I mean f has to be x, yeah that lemma is needed, yeah that detail is needed, yeah I think now it's integrated with this case well because in any other case other than fx = x you will get the problem of this maximal ideal actually generating everything when this is actually a proper maximal ideal. So you want to ensure that.



So, once we have done this we want to now extend it to curves. So, we want to do extension of valuation rings to the function field of curves. so any field k of transcendence degree 1 which is coming from curve can be written as base field small k and transcendence degree 1 field containing this element x such that this is a finite algebraic.

and this is the transcendental extension. So, for the pure transcendental extension we have already classified the valuations. which means what we have classified is all these rings contained in small kx in the function field that are integrally closed. So, we have classified all the integral closures, we want to extend those integral closures now to big K and we will see that that extends quite naturally and what we will prove is this theorem. that if R is a, be a local domain in K and MR be its unique maximal ideal.

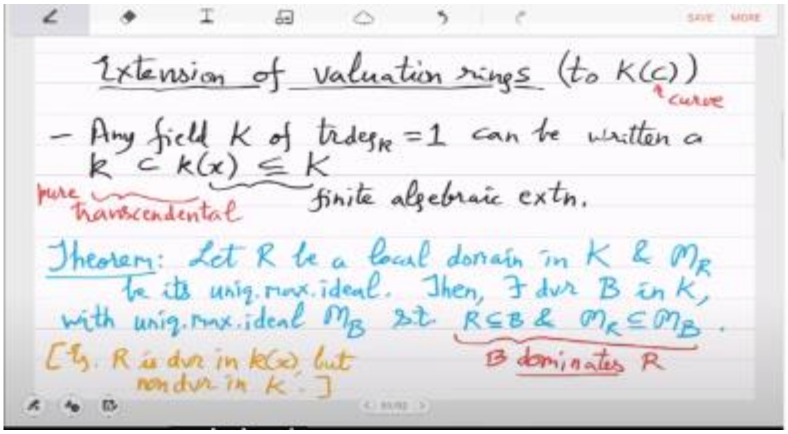
then there is a DVRB in K with the unique max ideal MB. So, I want to extend R right. So, I should write R contained in B maybe here. So, such that two things will happen R is contained in B and MR is contained in MB. So, basically the DVR that we got for small k x that is what we are calling R here and any such R we can extend it to B which is a DVR for big K and it will be extending R in both for the ring and for the unique maximal ideal.

So, this condition is also called domination. so we say that B dominates R. So, when I say a DVR dominates another DVR what is meant is that, sorry a local domain B dominates another local domain R. when the unique maximal ideal and the ring satisfies this containment property. So, you can compare two local domains by this termination relation. No, r could have been I mean r can also be b, we have just said that r and b are local domains and we have defined termination and now we are seeing that and in fact B is DVR. Sir, then we can always make B = R, this theorem will be true, that is what I am saying.

No, R is in the input, R is in the input, you cannot choose it. Whatever Rs somebody gives you, you can convert it into a bigger local domain which is a DVR. What I am just saying is that there is just some DVR such that R is a .

Yes. No, but R is not a DVR. R is not a DVR. It is just a local domain. See because it was a DVR for kx, it is not a DVR for big K. In our application that is what you have to remember that. example R is DVR in kx, but not DVR in the bigger in the function field of the curve it is not a DVR. So, how to find a DVR then? So, this is basically the I mean this is exactly the case of non singular points, when a point is singular its germs is a non DVR. So, from that non DVR, how do you smoothen it out? So, what this theorem is saying that there will always be an integral, basically you take the integral closure.

So, we are basically just extending our evaluation, the evaluation that we have on the extend that. Exactly. So, you will also extend the evaluation here. Yes, all these things I think you can think of the proof just as finding an integral closure.



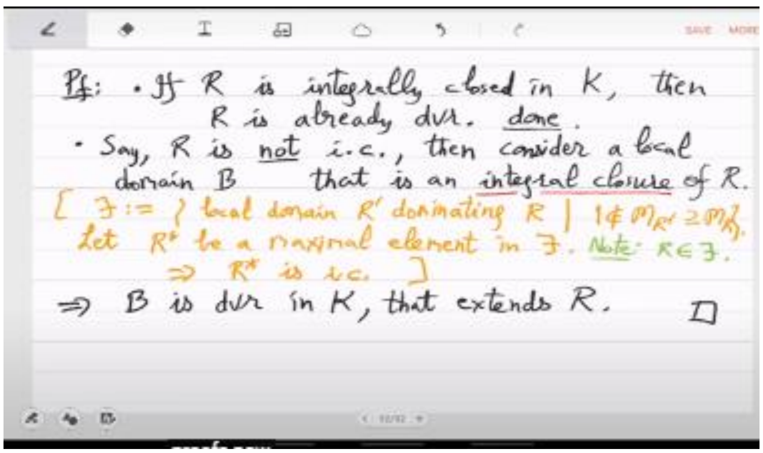
There are several ways this is proved. Theorem is saying that and I am giving you the proof, the proof is just in one line you find the integral closure that is all, that is just a one line proof. So, if R is integrally closed in K, then you know that it is already, then R is already DVR, so you are done. The only interesting case is when R is not integrally closed. so it's not integral closed means that there are these some monic polynomials are there with roots in the big field but not in the ring so you just keep adding those roots keep growing your field not integral yeah then consider a local domain B containing R such that, that is an integral closure of R, so I do not need to say this containment, just keep adding these points which are missing in R, so ultimately you will get very close to big K and you will have an integral closure of the ring. So, there may be infinity issues, why will this thing converge and so on, why will you stop at some integral closure.

So, formally what you do is, formally you just define this set F which is local domain R prime. collect all of them local domain R prime dominating R such that one is not in the maximal ideal of R prime. So, essentially R prime should have a non-trivial unique maximal ideal. So, collect all such R primes right this is the set It's dominating so it's also contains MR.

So let's define this set and say that, pick a maximal element in the set. Let r star be a maximal element. in F maximal with the relation of termination right. So, take the maximal element that maximal element has to be integrally closed otherwise you will get a bigger one.

So, formally you prove it like this. Sorry. How do you show that this set is this collection is not empty? No, it already has R. But R is not. Yeah, it already has R good point. So, it already has a local domain which dominates itself and MR was non-trivial and from that you just collect everything and then take a maximal element and that will be integrally closed.

So, that algorithmic proof you can just do it formally with the set. and that is your B right. So, the maximal element this gives you the formal construction of B, but it is also an algorithm you can think of this as growing the integral I mean growing by the integral elements. So, that is all it was just this in the proof just have to interpret properly. So, this is a DVR then by the proposition this implies that B is a DVR that extends Yeah, so the proof is simply whatever local domain you have, you keep dominating it by another by bigger local domains and you take the maximal one that is integrally closed it is a DVR and everything. So, some people actually use this also as a definition of DVR, it is the maximal dominating local domain, but we have started in a different with a different definition. these things are all equivalent, maximal dominating, integral closure, valuation, DVR these all these four things are equivalent.



So, you have seen all the proofs now. So, again the same old example you can interpret the case of this curve. and R is the germs at 0. So, problem was that this R is not DVR in its function field and that was because it was not integrally closed and the example was this x 2 /x 1, this function x 2 /x 1 is not in R, so this function y was not in R.

although you had this integral equation y^2 = x1 right. So, you have to introduce this. So, when you introduce y you get 2 DVR to get b which is just a y which is a DVR. in the function field. So, this was the trick we had done in those two diagrams, but algebraically the motivation is now here in terms of DVR is very clear and clearer is in terms of integral closure.

You just need to introduce these integral roots which is DVR in kx that extends extends R. So, in this case as I have said many times this in this curve there was only one point of singularity and we have resolved it. So, now we have a birational curve that is non singular. Now our ambition is to do this in all the cases. So, even if you have 100 singular points you want to do this. and so the idea will be quite algorithmic you just keep repeating this trick so that the first singular point gets resolved and the second one gets resolved and third one and so on of course what you have to take care of is that there are no conflicts so when you resolve the first one and the second one resolving the third one, you should not introduce any new singular points or you should not make the first one singular, so you have to do this systematically.

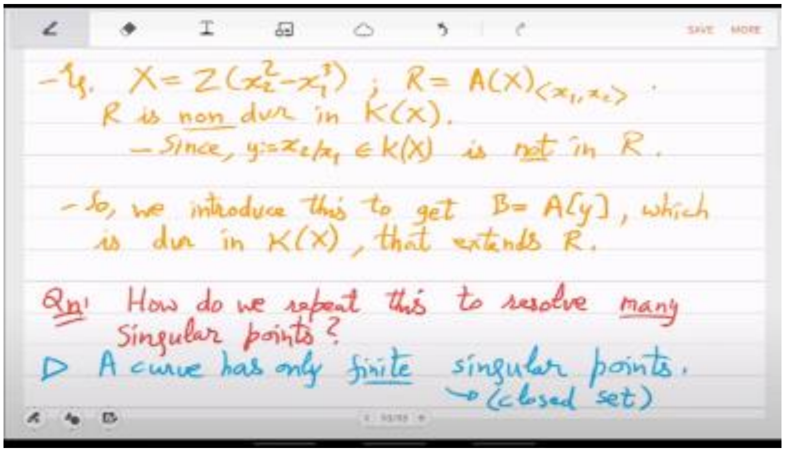
So, that will be our next goal, how to repeat this, to resolve many singular points. So, one helpful condition here is that a curve has how many singular points, can it be infinite? A curve was a dimension one object, singular points give you this constraint. So, if you intersect the curve with another constraint, you get dimension 0. right so intuitively you can see that there will only be finitely many singular points yes so what what is this constraint that gives you singular point. So, for that you have to go to the comparison results we had we called comparing tangent space with the rank of the partial derivative matrix right. So, that the first order derivative matrix of the generators of your curve So, that is the constraint the determinant of that I mean the rank of the that should be how much should be should not be full basically.

So, the that matrix of derivatives should not be a full rank matrix. So, you can write that down as a set of determinants vanishing. So, that is an extra constraint which intersected with the curve gives you 0 dimension. So, using that you can show it is not very difficult that singular points they actually form a closed set in your curve and these points are finitely many, it is a closed set.

So now you will work on the generator of the ideal of that flow set. No, we will not work with that. No, this is just a statement. We are just saying that singular points are on a curve, they are only finitely many. So we have handled the case of one singular point.

We just have to increase one to let us say 100. It is not finitely many. So it will still be a finite process. So you want to remove the singular points one by one. If we give this, I mean if we give this kind of inductive algorithm then you are done because it is a finite algorithm, it will converge. So we have to do this a bit systematically which will need some more geometric concepts.

So let us start that. Most probably, yeah he must have needed, I mean yeah if he wants to, if you want to show Riemann hypothesis for all the curves then you have to show that somehow very bad curves also relate to good curves which is this non-singular curves.



Otherwise those curves you would not be able to study. If you cannot remove singularity then you cannot come to non-singular curves. So, it is I mean for the Riemann hypothesis and other things it is needed that you have a good curve which is the non-singular curve where tangent spaces have all the information, information is not lost at every point. So, the systematic way to do this is the following, consider any transcendence degree 1 field K, we want to think of it as a curve which we will call an abstract curve via valuations.

so the idea is that we got two valuation because we were looking at a point on a curve, the point defines the uniformizer and the uniformizer defines the valuation in the DVR or for the DVR. So, let us reverse that and make it more abstract. So, you can take any function in any field, transcendence degree 1 is important, look at all the valuations of it and think of the valuations as points and the field as a curve. So how do you do this formally, so formally let CK as promised let this be the set of all valuations, valuation V on K with respect to DVR RV.

and unique maximal ideal MV. So, think of the points on the curve as these valuations all of them think. So, what should be closed points closed sets So, you have we have the potential points. So, once you have points you have to consider closed sets and open sets to give a polar logical structure to this making geometric. So, closed set should be see in the case of curve remember that closed sets were finite right on the curve, because the closed set is a 0 of some ideal. So, if you have another constraint beyond the curve then you get only finitely many points. So, closed sets we should define as finite subsets of CK be defined as those subsets of Ck that are finite or Ck itself.

Ck is also a closed set of course and everything else only pick finite ones. So, that will be a good choice from our experience of curves, open set will then be complement okay and so once you have points closed sets open sets what remains what remains is what are the functions on top of this on an open patch what are the regular functions right which we took many classes to define for curves so with that experience now we can say that for an open u define the regular functions ring as OU, the thing we defined for curves also. So, this O applied on an open path should be what? So remember U has valuations, so you have to define a function which is evaluated on a valuation, so this becomes crazily abstract, it's not an actual point, so this should be actually ∩ of the rings, the DVRs. So, what is the intuition for this, basically pick an element f in RV in the DVR RV, how can you evaluate it on V, what is the interpretation that an f in RV is evaluated on V.

So, you want a base field result. So, what you should do is that you should think of that f |mv|. so f |mv| will be in the residue field which is small k. This is the insight you think of these elements as functions on the curve because at a valuation you can just go mod that max id and they which so it becomes a constant. So, hence this is a genuine function definition on an open patch.

So, you are saying that that is how we should evaluate. That is how you should interpret these as being functions. Yeah, the a function f, I mean an element f here is when you want to evaluate it on v, you want to map it to a field element. What will that field element be? f |mv|, f |mv| is a field element. So you are kind of looking at the constant part of the function or the element. We will develop this on Tuesday. This will need one more lecture to prove the theorem.