Computational Arithmetic - Geometry for Algebraic Curves

Prof Nitin Saxena

Dept of Computer Science and Engineering

IIT Kanpur

Week - 06

Lecture – 12

Non Singular curves

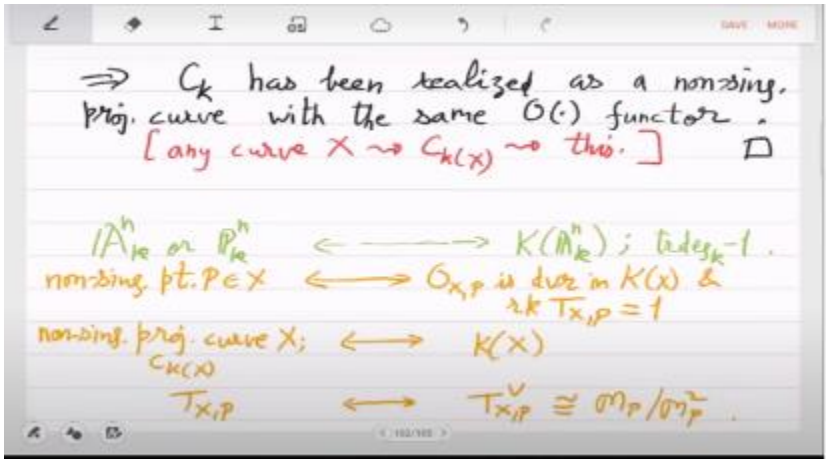
So, last time we showed that for any transcendence degree one field, there is an abstract curve which can also be realized as a non-singular projective curve. It is an if and only if condition. So, from now on we can just focus on smooth curves or non-singular projective curves or quasi-projective curves. that I think well motivates now the point of all this abstraction. Any question? So at this point we can again take stock of the situation in terms of what is the dictionary that we have built between algebra and geometry. so the geometric space, affine space or projective space in fact versus the function fields.

k and K, which is the function field on n variables, transcendence degree n. In fact, I should say here transcendence degree 1 maybe. We did not do anything with higher dimension, we stayed in curves, so basically affine projective curves versus transcendence degree 1 fields. So what we have seen is non singular points So, non singular points you can go from a non singular point to a DVR.

So, this O is a DVR in the corresponding function field and also the rank of the tangent space is 1 and you can go back also so whenever you have a DVR then how do you go back to a point on the curve so look at the DVR look at its maximal ideal it has a uniformizer it's a principal ideal so uniformizer solution gives you a unique point that's the point P so you can go back and forth via the uniformizer essentially and non singular projective curves and equivalently abstract curves based on a function field from here you can go to function field and back. So, actually function fields or transcendence degree one fields are in one to one correspondence with non singular projective curves respectively abstract curves that also we have shown and for a tangent space. from a tangent space you can go to the functions on the tangent space which was the dual which is also the same as the linear part of the germs that are vanishing at the point and you can go back from here also. so in geometry you have tangent space in algebra you have the germs which are vanishing their linear part or the dual of the tangent space these are the functions defined on the tangent space in the curve case both of them will have

dimension 1 I mean in the non singular point case when p is non singular then the tangent space will be of dimension 1 if and only if and similarly the dual space the functions defined on this vector space they will also be dimension 1 if they happen to be dimension 2 then your information is lost so dimension 2 tangent space means that there is no connection with the point so the point is actually a singular point right so we have done all this till now is that clear no no no no yeah it's that is not what I mean I mean it means that n = 1 I mean these are two different things we are looking at the function field of the affine space in fact subspace of the affine space in particular curve Yeah, but till now whatever we have done only holds for transcendence degree 1 such objects. We haven't even begun studying transcendence degree 2 and this course we won't be able to do that.

For that you need multiple courses after this course. So, this is only about transcendence degree 1. But it's an object that lives in this key of the affine space. Okay, any other questions? So, we will interchangeably use non singular or simple or smooth. These things will mean the same now on.



So, non singular curve or point, simple curve or point and smooth curve or point. So, points on a smooth curve. So, I want to sketch this geometric picture, you have some curve and you have the projective line and this is the curve so the curve is smooth we want to we can see the curve as a cover of the projective line so we want to describe what it means what we want to say is that say look at a point P1 here so this is related to some point Q1 in fact we will show that it is a unique point so P1 actually covers some point on the projective line for every P1 but sometimes it may happen that So every point on the curve corresponds to a unique point on the projective line. But it can happen that a point on the projective line corresponds to many points on the curve. So this is called ramification of Q2.

So I will not define it except in this picture that basically points on the affine line they can have multiple associated points on the curve. This happens because for example in

the case of $y^2 = x^3$ for a single x you have two y's. okay because you have two variables on the curve instead of single variable so when you fix a variable the other variable may take many values so that is why this cover it's actually a ramified in general it's a ramified cover of the line but this picture is typical this is what happens and so the so this thing is called a cover if K is algebraically closed. So, let us see a proof sketch of this. So, any point P that you take on the curve, how do you show that it corresponds, I mean what is the point you should associate to on the projective line.

So formally what you should do is since P is a smooth point you look at its DVR and look at the uniformizer and the solution of that is the point on the projective line that this should correspond to. So we set up that mapping. So point P has a DVR. cp this o of cp and in fact I can just assume the setting here. So, setting I should have written.

So, k is contained in kx is contained in the function field. of the curve. So the projective line is coming from this Kx and the K is giving you the curve and k is the base field which is algebraically closed. So this is the setting. So in this setting actually when you get the germs OCP around the point P, you should take intersection with Kx.

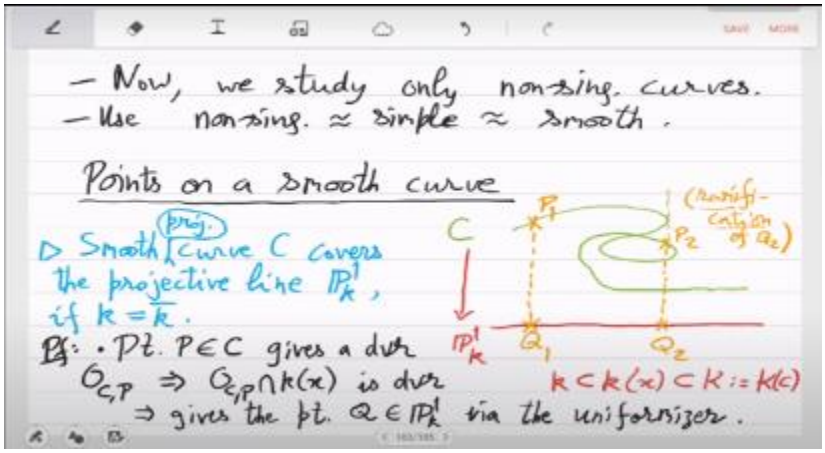
that will work smooth curve is projective yeah sure but if you remember the projective is needed only because there is a one extra valuation this valuation because of 1 /x Yeah, sure and that was only because we went via the abstract curve, in the abstract curve there was one extra valuation. So, all the infinitely many valuations except this one valuation is what we cannot realize in affine because it is it corresponds to this fraction, it does not correspond to polynomial, the fraction being 1 /x. So, that requires I mean its solution is basically 1 /x = 0 which means x = infinity. So that is called the point at infinity. So which is why you need a projective curve because it will have a point at infinity concept.

Otherwise all the discussion will be the same as affine curves. So when I say point P you can think of it just as an actual point on an affine curve. Basically you take the affine open. in the affine open patch, so you get this DVR and you look at the elements which are in KX, take the intersection. So, let us take the intersection with KX, this also is a DVR.

it is a DVR in kx now which gives you the unique point via the uniformizer. So this projective line its field which is contained in your curves function field kx. When you take the intersection with this field you get a DVR which gives you the unique maximal ideal which is principal and the generator gives you the point. So this is the association in one direction. Curve point gives you a point on the projective line.

and the converse of this will be will be similar so now let's take a point Q on the

projective line this gives a DVR inside the function field of the line which is kx, then extend it to R tilde inside the big field. So, a DVR can be extended to the full function field, we had seen this. So, basically the integral closure inside the big field and this may not be unique. So, there may be many R tildas. So, you pick one R tilde and its maximal ideal gives you the point on the curve.



So, in this case r tilde and p are not unique. So, this is the reason we have this now both ways. So, when you go from curve to the projective line you get a unique point. but when you go from the projective line to the curve, since there are many possibilities of extending DVR, you get multiple points and that is called ramification. So, it is a cover that possibly ramifies.

So, possibly multiple points on the curve are covering a point on the projective line, but every point on the projective line gives a point on the curve. This as you can see the proof is not very trivial, it needed all this machinery. But in the end what this is telling you is something very important that these smooth projective curves, they are actually very tightly related to the projective line. And since in the end of the course we want to count points on the curve, somehow that counting will be done, will be inspired from the count on the projective line. So, projective line has how many points? It has p actual points and one point at infinity p + 1.

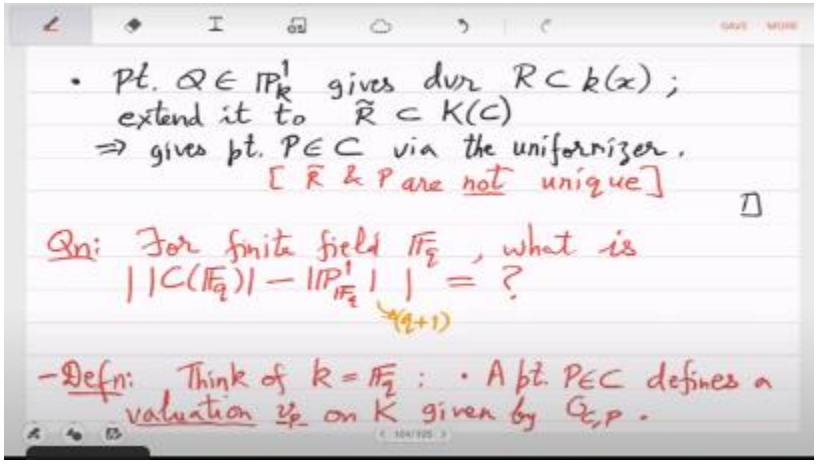
So, in the end of the course we will show that the any curve, any smooth projective curve has points almost p + 1. It will have points p + 1 + - square root p. So, the whole course is to show this square root p error that is called Riemann hypothesis. So we ask this question and we will answer it before the course ends. So this finishes the proof and the question now from now on is this, for finite field FQ what is size of the curve restricted to FQ points coordinates should come from FQ - the projective line on that space.

So, what is this? That's the question and this of course = q + 1. So the motivating

question of this whole course and in fact much of modern math is how far away can the points on a smooth projective curve be from Q + 1, the points on the lines. So, the picture does not give you a very good idea because every point on the curve may have many possibilities of PIs. So, it seems that the curve may have 2 times Q or 3 times Q or 100 times Q many points. but we will actually show that that's not true.

It has almost as many points as the line. So that's a very surprising thing and very difficult to actually conjecture. So that will prove in generality for curve case. If you are interested in higher dimensional objects, surfaces, et cetera, then that, as I said, is a much harder topic it requires many courses that we won't be able to sketch here but even that is inspired from what we will do in this course this was done first by veil okay yes so i need some definitions now So think of K as FQ for this definition. It is definitely not algebraically closed.

So in this case, we need some more definitions because things are not that nice. At least what is true, what still holds is that a point defines a valuation P on the curve defines a valuation VP on the function field given by OCP. This continues to be true because this fact was just based on this ideal that is defining the point and the point of course always is in some finite field. even if your k was k was algebraically closed still when you look at a point the coordinates are finite so they are always in some finite field so the valuation is the same as we worked with before but there is another thing which might change which is the residue field so residue field at p will be called Kp, it is the quotient of this germs modulo the germs which are vanishing. We have seen that this is a field but in the algebraically closed case this was itself k.



Because I mean from an algebraically closed field there is nowhere else to go. If you want to go to a algebraic extension you will stay in k because it is algebraically closed. But here since now our k is a finite field this thing may be bigger. There is no reason why it will be = k.

So it may be bigger. This is the different thing that can happen when your field is not algebraically closed, when it is a finite field that at a point although the point is coming from the same finite field, but the functions around may take you further away. So, from GFQ you may go to GFQ ^{2} or Q ^{3} or wherever bigger field. and hence we should take care of the degree. So, the degree of a point is dp, sorry not this p, how far is this field from the base field, so that is the degree. Is this clear? So, if you go from GFQ to GFQ square then the degree for example is 2 and if you go from GFQ to itself then the degree is 1.

So, in the algebraic closed field case degree is always 1, now it may not be 1. So, that is the big change that can happen. So first is degree of a point is always finite. That's an easy property. Second property is if you take intersection of all possible powers of these maximal ideals, you get what can there be a function which is present in all these powers mp to the i will show that the only thing that is present is 0 third property is so MP gives a uniformizer U then the relationship between the uniformizer and the valuation that the point defines, the relationship as you can guess it is the highest power of U that divides α.

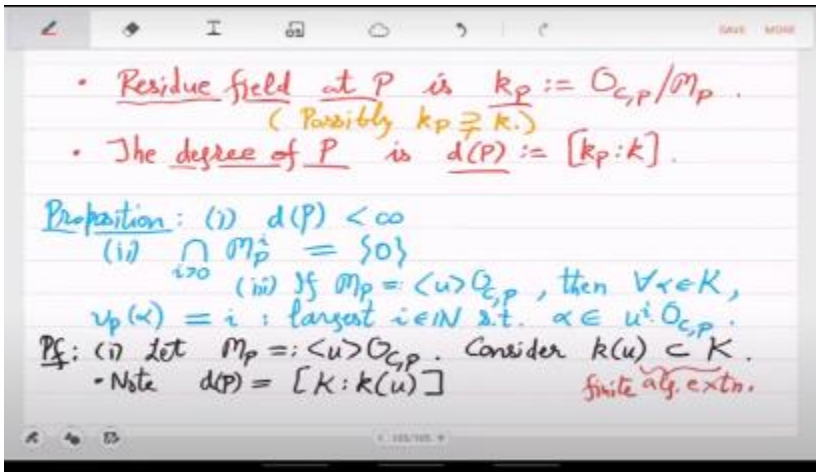
So, I can write it formally as α contained u raise to i OCP. So, the third property is saying that for the generator of this principle ideal and the valuation the connection is that for all field elements Vp α is equal to the largest power of u that divides α. so these things continue to hold for what is the first property proof of the first property so how do you show that the residue field is finite degree so let u be the generator let MP be generated by this uniformizer U, consider all the rational functions in U. So they are clearly contained in the big field, transcendence degree 1 field. Now what is the connection between the degree, the dp and ku? So the claim is that the degree is equal to the degree of this.

This is an algebraic extension. finite it's a finite algebraic extension simply because u is transcendental over the base field and K has transcendence degree 1 so once you have introduced the transcendental element u what remains is a finite algebraic extension so that degree is actually equal to the degree of the point do you believe that No, no, no, so yeah that is a good question because the functions I am looking at are also coming from k, they are not coming from the algebraic closure of k, then it would have been infinite. So the K is actually the functions from the same field. Like if it was a finite field FQ, we are looking at functions from FQ. So the constants are the same.

Think about that example. In the example, can we see this easily? So U essentially comes from the definition, the ideal that defines the point P. No, I think I maybe misspoke. I think the point on the curve here is arbitrary point. It's not coming from GFQ.

Yeah, this, I think this should just, this can be anything.

So the curve here is actually coming from K '. yeah and then these objects ocp mpp mp are actually coming from k ' but let me clarify this next time i will not need the degree thing anyways today so let me skip these details for now let's move to the second property So let Y be an element in the intersection. So this means that the uniformizer raised to I divides Y for all I. So essentially infinitely many powers are dividing y, but y is a, ultimately it's just a element in the function field, right? So it's a finite object. So infinitely many powers, I mean it is impossible to be divisible by u raised to infinity.



At some point the division will stop happening and after that it will never happen. So basically there are finitely many i's for which this can happen. So that's a contradiction. This is the only thing, well or in other words this means that y is zero. is the only number function for which this is possible otherwise it is not possible.

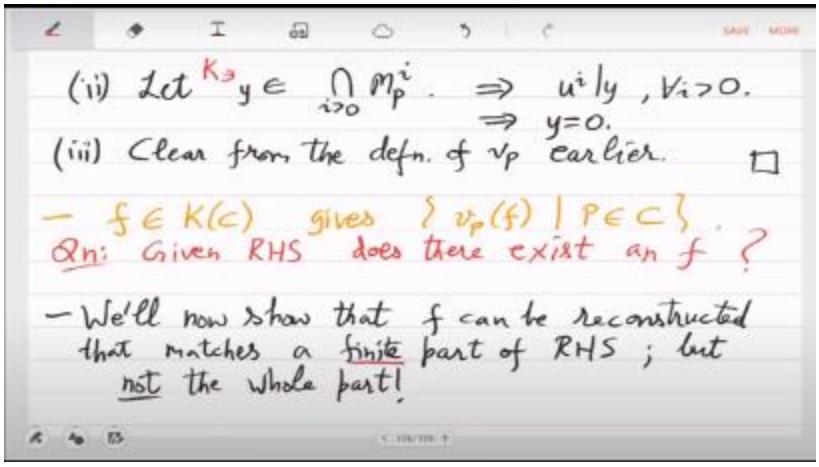
And third property which is generator of the principal maximal ideal MP is related to the valuation that way this is clear from the way we had defined valuation anyways. yeah so this degree thing is the only property which is messed up I have to clear this proof next time because next time we will start a new topic where this will be useful which is the divisor class so today we will not do that what we want to finish today is so any f in the function field of a curve gives you these numbers. So, a function corresponds to this infinite array of integers, this can be negative, positive or 0. So, the question we want to answer can we go back. if I give you an array of infinitely many, I mean VP values for every point P, is there a function which corresponds to this infinite array? Given RHS, does there exist NF? okay so given the value given the like candidate valuations is there a candidate F that matches matches them so we will show that For this, yeah, you can assume any k.

So you can assume algebraically closed. Yeah, we'll not work with degree yet. So you

can just assume k to be algebraically closed. And it's not an algorithmic question yet. I mean, it is still, even the mathematical part is currently not clear whether an f exists. Does every array on the right-hand side corresponds to a function in the left-hand side? Or are there holes? So there are these arrays which actually don't correspond to a function.

So these are holes. Now what I am getting at is that actually there will be holes and based on the dimension of the holes we will define genus. So that we will do after a month. But this is the starting point of understanding what holes are in a curve and how can we measure them. How many holes are there? We are doing this work in the direction of genus definition. We will now show that F can be reconstructed from well not from matching reconstructed that matches a finite part of RHS but not all.

So, we will show that if you care about certain points, certain valuations finitely many, then those values can be matched by a function, but if you care about all the values simultaneously then it may not be possible and f may not exist. So, we will prove this approximation theorem. approximate valuations theorem. So, let K be the function field of a curve and whenever we will say curve we will mean smooth curve.



So, I will not mention it from now on. let p1 to ph be the points that you care about with corresponding valuations v1 to vh. so remember that the field is algebraically close could be algebraically close so the point number of points is infinite but in this hypothesis we only care about finitely many points h many points so let us call them p1 to ph and the valuations they define are v1 to vh in the abstract curve the abstract curve has all the valuations and let u1 to uh be some functions given to you and some numbers given to you. That's the hypothesis, the premise of the theorem. What we will show is there exists a function such that for all these i's 1 to h, the ith valuation of u - ui is at least mi. So, this is the approximation theorem of valuations finitely many valuations.

It has some extra data like these ui's are also there given to you and mi's are given and you want a single function u such that the difference of u with ui, that valuation is at least mi. It is phrased a bit differently than the question that I had asked. But actually the question will be answered from here also. We will see that very soon.

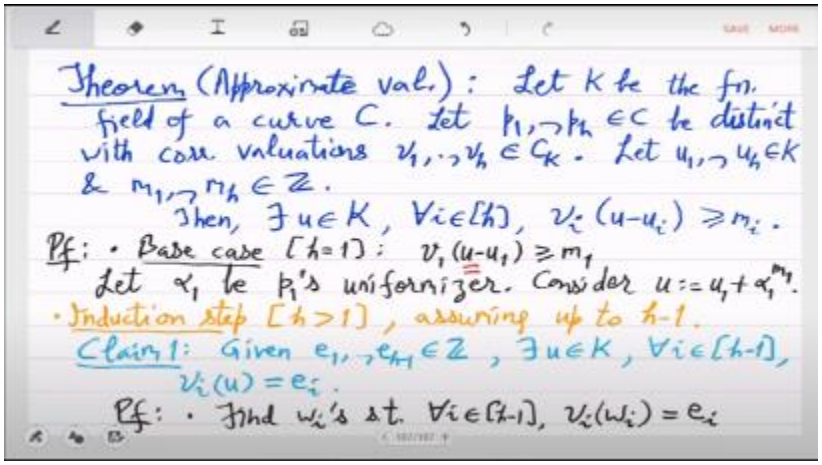
Is the statement clear? It's a highly non-trivial statement. It may as well be false because the numbers, MIs are arbitrary. The points are arbitrary, the valuations are arbitrary and you want a function that matches all these things. There is no reason why that should happen because the curve is also arbitrary. This is a very general statement.

You cannot really see this from geometry. It is a purely algebraic fact. So, we will prove this in steps. So, we will prove this by induction on H. What is the base case? H = 1. so you are given a point there is only v1 so you want v1 u - u1 to be at least m1 how do you do that you want to solve for u1 can you solve it you want to solve for u everything else is known point is given u1 is given m1 is given can you find a function f such that v1 f is at least m1 i mean of course you can take the uniformizer of the point p1 and raise it to m1 so uniformizer need something else let us call it α 1 may be.

Consider u to be u 1 + α 1 $^{m\,1}$, this is simple because now u - u 1's valuation is exactly m 1. So, you have matched it exactly. So, base case is easy. What is not easy is the induction step.

So, now we will assume that the theorem holds for h - 1. and we are trying now H that is the induction step we want to prove it for H using H - 1. So, for example, when H is 2 what the problem is that you have two constraints v1 u - u1 at least m1 and v2 u - u2 at least m2. So, this solution which we found before it's not clear how do you modify it so I mean even if you forget u1 and u2 we set them to 0 what we have done is u = α1 ^{m1} so next time you should try α1 ^{m1} times α2 ^{m2} right that kind of thing you should try but it's not a it will not work generally because when you compute the valuation maybe α2 contributes something to v1 and α1 contributes something to v2. So you have to do this more systematically.

Plus there is this additional thing of u1 being present. So this is not so simple as the base case. So now we are in the induction step and here I can prove a claim, actually many claims. that given integers e1 to eh - 1 there exists a u such that. for all i 1 to h - 1, vi u = ei, that is the thing I had promised in the question that if you are given numbers, potential valuations then I can give you a rational function which will match them.



So, viu = ei. I will get this basically from this theorem which we are assuming in the induction hypothesis. I mean in the induction hypothesis at least we have answered the question and then we will use this to complete the induction step. So, again read the theorem statement for H - 1 can you deduce claim 1. So, here is the proof find W i's such that for these i's H - 1 i's V i W i = ei this is easy because wi depends on i right so this is just the thing we did in the base case so wi you can simply take uniformizer α i ^{ei} right so wi you can construct really So, consider those w i's and now set up the system for the theorem. Consider the system 1 to h - 1, you have vi u - wi >= ei + 1.

So, by induction hypothesis of the theorem we get u in the function field. So, the induction hypothesis of the theorem will tell will give you a u such that the difference of u and wi is at least ei + 1 that is the theorem statement which means what which means that the valuation of what was claim 1 you want to look at valuation of u. So what is valuation of u? Valuation of u is valuation of u - wi + wi and now you use the additive nature of the valuation. So u - wi has a valuation ei + 1 or more while wi has valuation only ei.

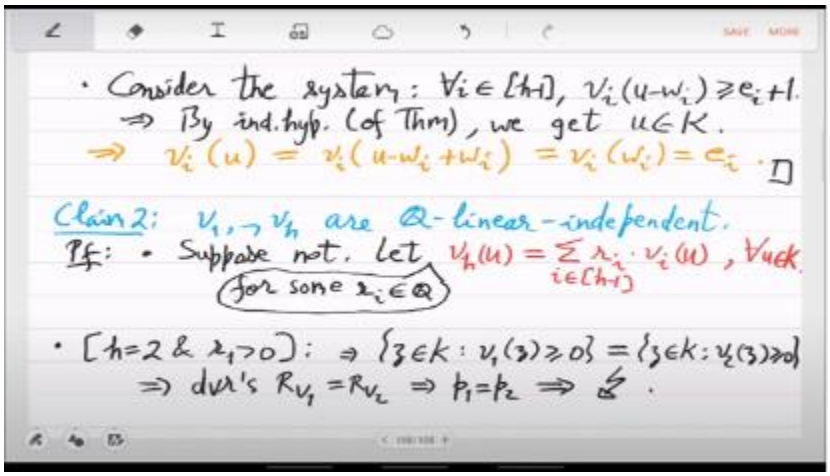
So this valuation is ei. The theorem immediately gives you this U which we asked in the question. So for H - 1 valuations, they will be matched if the theorem is true. The theorem for H - 1 is true. That was the claim, so we have proven the claim now.

So now we move to the next claim. which is that v1 to vh are Q linearly independent. Now this is a statement interesting on its own because we are saying that if you take distinct points then the corresponding valuations are somehow they are very different in particular there is no linear combination of these functions which vanishes globally on the function field. So, suppose not. So, then let a linear combination vanish. So, what you

can write is this equation v h let us say v hu = σ ri vi u for all u and k for some R ‘ in rationals.

So, let R1 to Rh - 1 be some rational numbers such that this identity holds for all u ok the valuations are basically linearly dependent we are assuming that so we want to get a contradiction from here do you see an easy contradiction yeah we don't see an easy contradiction because everything here is arbitrary we don't know anything about the valuations or the curve so we have to do this in a bit deeper way. So, let us look at the case of H = 2 and R1 positive. So, we are saying that V2 is dependent on is a multiple R1 times V1 and R1 is positive What this means is that the DVR for V1 and V2 are the same because DVR comes from positive non-negative valuations. So, this means that if you look at the Zs for which V1 is non-negative, V2 is also non-negative. right is that clear because V1 is just let us say V1 is 2 times V2 or 3 times V2 so in that case you can see that if one is non-negative the other is also so you get DVRs to be equal And what happens when the DVRs are equal? Yeah, so DVRs give you the uniformizer, uniformizer are the same, so points are the same, which is not the case.

Points were different, valuations are different, so DVRs are different. So, now you get some handle. on this thing, at least you have understood that why are V2 and V1 very different. But only when R1 was positive, R1 can also be negative. Then what do you do? So then we have to give a different proof.



So let's take R1 to be negative. And H can be anything, I will not need H to be two. so that the other cases are one negative in that what you have to do is find z z ‘ two functions says that for all i 1 to h - 1 the following happens so v i z should be 1 while Vi z ‘ should be 0 if Ri is non-negative and opposite otherwise. Now just looking at one point would not be enough, so we want to construct two points, which should somehow contradict the linear dependency that we had before. And this system is basically dependent on the coefficients, these R i's.

So, for the non-negative R i's, Z Z ‘ has that valuation 1 0. I mean essentially Z is identifying with non-negative RIs while Z' is identifying with negative RIs and this should give a contradiction. But why will they exist? That we have shown in claim 1. So just look at the system for Z. you want valuations to be 1 and all 0, the rest 0. So, you know that such as z exists and similarly z ‘ exists where it is 0, 1 in this distribution.

So, they exist that is from clean 1. because we are asking only for 1 to H - 1 so that was the induction hypothesis based claim 1 once you have this what can you deduce now you look at the red equation and check VH (z) what is that so VH (z) is So Z identifies with non-negative. So hence VH will be greater than = 0. And VH (Z ‘) identifies with negative.

So this will be negative. So, we are using the additive nature, property of valuation. This is how we had designed Z and Z ‘. Now, what is the contradiction? Where will that come from? So for the contradiction you have to look at Z + Z ‘, that's where the contradiction will come from. So Vi(Z + Z ‘) is what? See Z is non-negative, Z ‘ is negative valuations and the valuation of some will be then the least, sorry will be. oh yeah actually they are different so since they are different it will be the least one so that will be negative no wait something is wrong it will be then the minimum one or some it will be zero and it will be 0 here, sorry I should have said what i is, I am thinking of i = h, no I want i 1 to h - 1, I am looking at this.

So for example, v1. So the above part, in the above part, you know that vi of. If you look at the z valuations, they are. I guess you just have to compare 1 and 0 and pick the smaller one. So that will be 0.

So you get 0. Is that clear? Because Z and Z ‘, the valuation is always different. So you just pick the minimum one. That will be 0. And which means what? Yeah, so 1 to H - 1, valuation is 0.

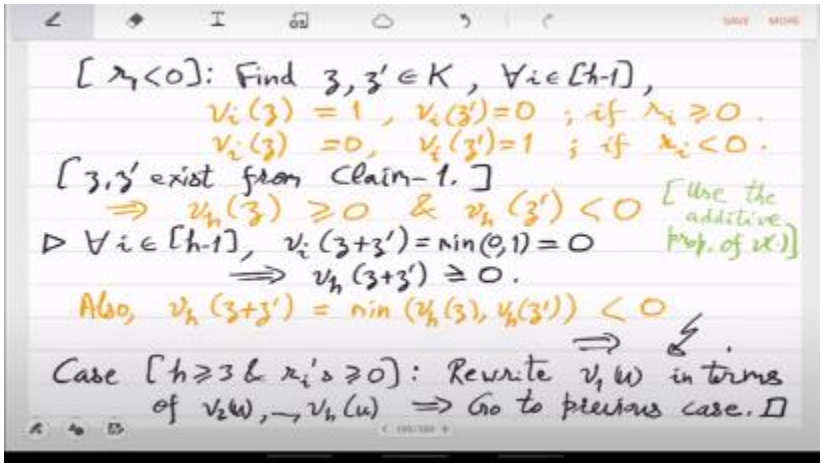
So you get for VH by the red identity, also 0. Do you actually get 0? No. or greater than = 0 and then what it is they are all equal right so for example 1 - 1 valuation jumps from 0 to infinity so I only get >= 0 but now what yeah so I did not deduce anything from there now I use that also vh z + z ‘ is the minimum of VHZ because they are different and the minimum one is negative. That's the contradiction. The orange part tells you that it should be negative, the black part tells you that it should be non-negative, so you get the contradiction. So after all these calculations you have shown almost independence, is there any case remaining? For H2 I have handled positive and I have handled negative in all the cases, so what remains is let's say H = 3.

and both R1, R2 are positive. Those kind of cases still remain. That's the last case. No, no, no, we must have. No, no, we did, right, because this orange premise is non-vacuous. See, we are using that to get the negative sign you have to have yeah exactly the middle orange one you actually want negative sign so that's where you use the non-vacuous nature exactly b is a 0 z ≠ 0 because b1 (z) = 0 and there is negative and positive terms both Sorry, where, what? VH (z). VH (z), yes.

So, VH (z), only look at the Z values, VIZ is 1 when RI is non-negative, otherwise it is 0. So, what it does is that it kills all the negative coefficients, only the non-negative, in fact the positive ones survive and from the positive ones you get. Yeah, so just one case remains, which is H = 3 and all the RIs positive. This is the case remaining.

So basically, this V3 is dependent on V1, V2. But both of them are positive. That's the case we are left with. In that case, you just rearrange. rearrange the equation so there is a negative sign that's all so for example you rewrite yeah yeah you just rewrite v1 u in terms of v2 v3 so in fact the rest so vh So this implies that you are in the previous case.

So that's all. So all the cases are there. Hardest case was this one, where your R1 was negative. There you really need the full power of the induction hypothesis. Is that clear? So, we cannot finish the theorem I guess, let us do it next time. So, after this claim what we will do is, we want to do the induction step. So, we want to construct this U and we will construct it in the following form.



σ xi ui for rational functions xi. So, you in the conclusion of the theorem what you want is you want to study, you want the valuations u - vi (u – ui). So for that we will instead find these x i's. So the thing that we will study is actually this. So for example if you look at V1.

what this is x 1 - u 1, x 1 - 1 u 1 + x i u i i = 2 to h. So, we will control these valuations, this valuation and this valuation. will design Xi so that this Xi's and Xi - 1's their valuations are in control and then from that we will get the, we will finish the induction step. What we want is this thing to be > = Mi, so we will take care of that next time.