Computational Arithmetic - Geometry for Algebraic Curves

Prof Nitin Saxena

Dept of Computer Science and Engineering

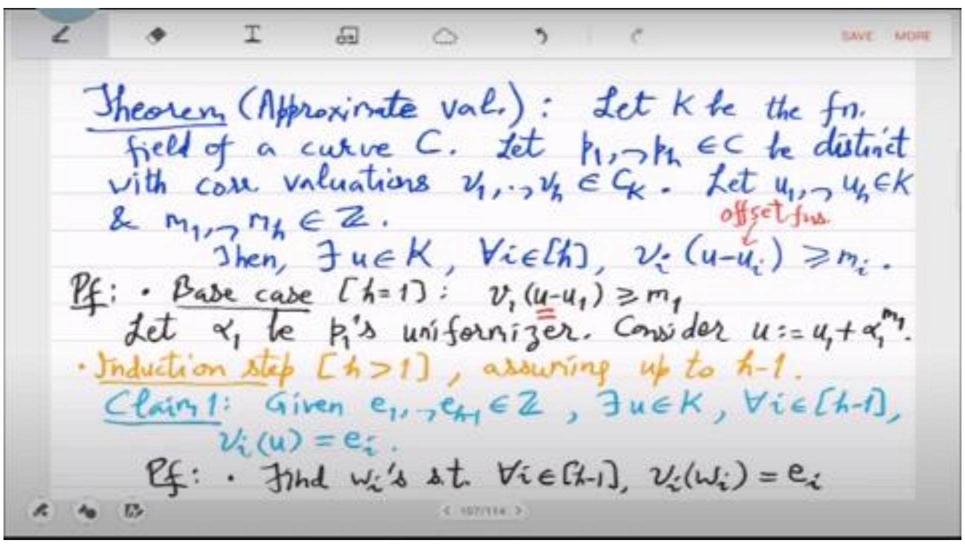
IIT Kanpur

Week - 07

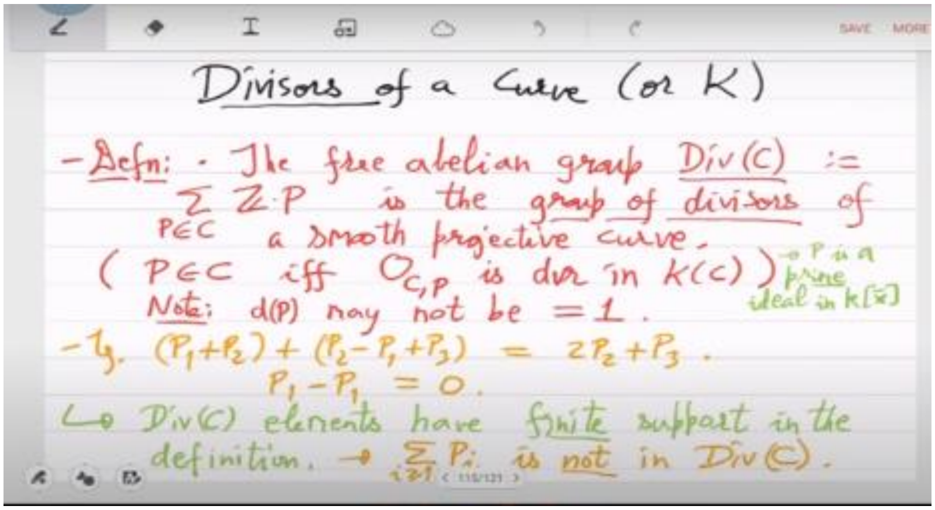
Lecture – 14

Riemann-Roch Spaces

So, last time we finish this theorem approximate valuation theorem, which tells you that for a set of valuations and multiplicities and offsets, you can find a common function u, since that valuation of u - ui is at least mi.



So this sets up a approximate correspondence of rational functions and zeros or poles with multiplicity. So to study that in a big way we define the divisors of a curve. So this is a new object. So this is basically the you take these primes. or these points on the curve.



So the point P remember will always refer to a DVR. In other words if you look at the unique maximal ideal of this DVR it will be a uniformizer. So we will think of the point, the uniformizer, the prime ideal all these things are the same for us. So this P is then a complicated object and we are actually taking combinations of these linear combinations but only integral.

So 2P1 for example this P1 + P2 and P2 - P1 these are things which are now available to you. And what is their physical interpretation is not clear but surprisingly this object will be highly useful in the analysis. any questions ok so this is called div c we have defined of course we have defined divisor which is an element of this div c we have defined order map which tells you what is the coefficient of the point in the divisor D, so this AP, so for D it gives AP, that is order, order is a group homomorphism, it respects addition, degree is the sum of all the orders, but also you have to weight by the degree of the point, so it is ∑AP times And the kernel of this is clearly those divisors whose degree is 0. They will be somehow special. We will call it div 0.

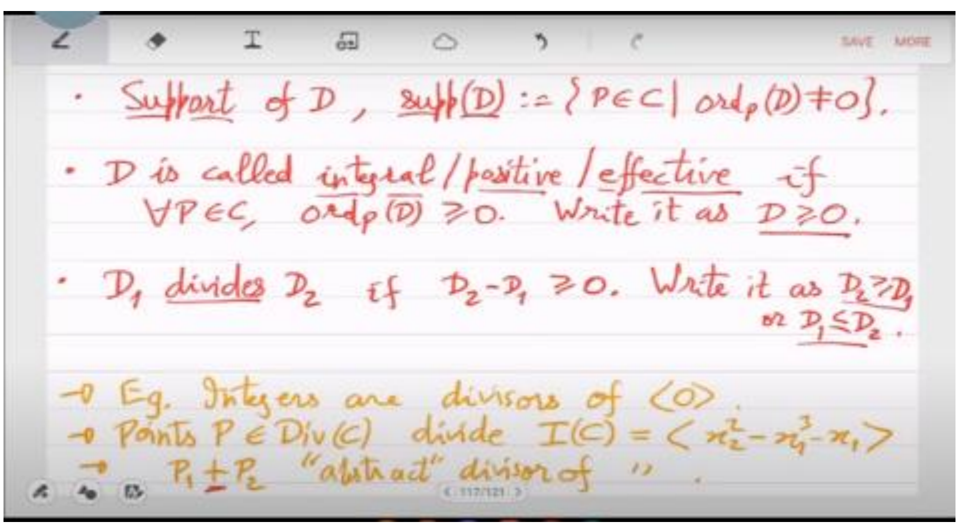
Support is the number of points that actually appear. So the multiplicity can be or the order can be positive or negative. integer then d is called integral or positive or effective if every order is non negative. So, essentially these kind of these poles you are avoiding d we say d >= 0 and then we define this notion of division. So, one divisor divides another divisor d 1 divides d 2.

if order wise orders of D2 are at least as big as that in D1. This division you can actually think of it also what it means physically. because if you are thinking of order as a multiplicity of that particular 0 of that particular root, then we can say d1 divides d2 if the multiplicity in d2 is at least as big as the multiplicity in d1. So, at the level of the function this is somehow saying that f1 divides f2. but it is not quite that, this is much more abstract than that simple thing.

So, just to give you some more analogies, so integers for example are divisors of 0. In fact the zero ideal if you think of the zero ideal in the ring of integers then 1 and 2 and 3 and all these they are actually dividing the zero ideal. So that is the thing we are also trying to simulate over a curve now in a more abstract setting. So these points the points P that are living in the divisor group, they divide the ideal of the curve which for example can be $x2^{2} - x1^{3} - x1$. So, these points are remember they are prime ideals.

So, these what we are saying is that these prime ideals in the divisor they divide the ideal which defines the curve. So, in that sense we can call it a divisor. So, at least the points which are primes they we can see this as the physical interpretation of the term divisor. But of course that interpretation fails when you start doing this additively. So, it is not clear if I take a prime p1 and I take another prime p2, why should this be called a diffuser.

So, at this point the physical interpretation fails, but at the level of point it is still true that points do divide. the prime ideals do divide they are actually divisors of the ideal. So, P 1 + P 2 is kind of an abstract divisor of this. And instead of, so in the case of integers we actually multiply integers and they remain divisors. In the case of divisors of a curve we will not multiply them, we will add them.



So these are actually written additively. But the physical interpretation is supposed to be coming from really the way integers behave and they give you a group. So when you add these two divisors, P1 and P2, you get the two prime ideals. So you add ideals and you get, when you are adding two prime ideals, you get the entire ring, right? No, no, no. Maybe it's a good example.

No, no. So now this example has completely confused you. This addition is not ideal addition. It was a free abelian group that we had defined. This addition has no meaning. in all your mathematics till now you have not seen any operation which corresponds to this addition.

It is a completely abstract addition. You are just taking kind of you take an animal like cow and you take an animal like goat and then you take a formal sum of that. There is no operation between cow and goats. So, you are just adding them. You are just saying that this is a new object.

So which is what is happening here, P1 is some point and P2 is some other point and we have just said that okay I will start looking at their sums without defining what a sum is. It is just formal addition. In other, in mathematical terms you are just saying that P1 is a basis element, P2 is a basis element and I can start taking formal sums and I will get infinitely many sums. There is no dependency between them. These are two independent objects.

So which is why this very soon the analogy breaks, but we continue using the term divisor and we write them additively. So these divisors written additively are actually new objects. and yeah so varieties or in this case curves they give you these new mathematical objects with no physical interpretation but we will soon see that actually it will we will be deriving some physical interpretation out of this object but that will take some time so after exam we will prove some theorems which will tell you that this new object actually carries fundamental geometric information about the curve ok, but that will take a lot of development of algebra. So, for now let us continue that development. So, divisors are interesting because each rational function x in k * has an associated principal divisor.

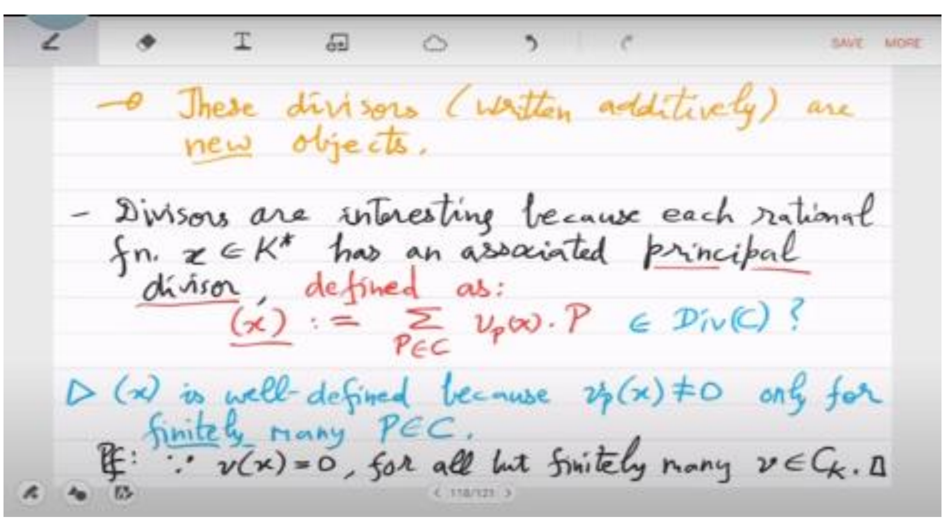
So we are defining principal divisor like this. So this is basically go over all the points of the curve, look at the valuation. This is one of the key objects which has inspired us to define the divisor group. For a rational function you can look at the zeros and their multiplicities. or poles and their multiplicity.

So it is because the point is actually, you can think about the DVR, the corresponding DVR and then the uniformizer will give you the valuation map and you can just put the valuation of the function x here. No, no, no, it means this is a definition. So the definition of principle divisor is this. This is the definition of principle divisor. So this again is a formal object but this has great physical interpretation because this is just saying I will take a formal sum of all the roots.

with multiplicity. Now one thing you have to show that this definition is actually, it makes sense because what you have to show is that this sum is not an infinite sum. If it's an infinite sum then this element will not live in div C. So why does it live in div C? because this sum actually has only finitely many non-zero summands. Can you show that? Only for finitely many p. How do you show this? By now this should be easy for you.

So, valuation positive means that you are looking at the zeros of the function x. How many zeros can a function have? That can only be finite. because you are on a curve, so dimension is 1, x puts another constraint, so dimension becomes 0. So, this system has only finitely many solutions. It cannot have, I mean over the algebraically closed field also, you have only finitely many points.

In other words, x only appears in finitely many MPs, the maximal ideals. we also saw that right so intersection of MP is 0 there is no element which appears in infinitely many MPs so just note that valuation of X is 0 for all, but finitely many valuations C sub k is our. is the abstract curve or equivalently the set of all valuations and if you go over all the valuations you will see that the valuation is always 0 except for finitely many cases and those are the ones that give you the p's. So, p's are actually only finitely many and so you have a finite sum. So, it is an element, it is a genuine element in the divisor group.



Is that clear? So, let us see an example of principal divisors. So, let us look at this curve. this is embedded in the projective space. So, it has three variables, x0 is the homogenizing variable. It is actually basically the curve is just $y^2 = x^3 - x$ I think.

Curve is simply that, it is an elliptic curve, happens to be an elliptic curve. Let us look at the function x_1 / x_2. So, what is the principal divisor of this function right. So, you have to basically find the 0s and the poles and their multiplicities, let us do that calculation. So, the well the first 0 is let us try $x_1 = 0$.

So, $x_1 = 0$ means that on the curve if x_1 is 0 then it means that $x_2^2 x_0$ is also 0. So, you have two possibilities you can take x_0 also 0 or x_2 also 0. So, there are let us take the first case. So, x_1, x_0. Because we are in the projective space, so you cannot set all the variables to 0, but you can set two of them to 0.

So x0 = 0 implies, sorry x1 = 0 implies that one of them have to be set 0, so we are setting x0 to 0 and x2 we are setting to 1. So that is the point. it is 0 , 0 , 1 that is P1, what is the uniformizer for this, because we want to think of the valuation that this defines. So, if you remember the calculations to find the uniformizer, what we do is we look at this curve equation.

and break it up into x0 and x1 parts. From that you can learn that either of these can be chosen as uniformizer. Let me pick just x1. So for the DVR, the unique maximal ideal is actually generated by X1 because you can see that X0 is multiple of X1 from the equation. X0 is just a unit times X1. So X1 I take as the uniformizer and that defines the valuation explicitly.

So let's now check the valuation of F. so which is the valuation of x1 - x2, what is the valuation of x1? Well uniformizer is x1 itself, so this is 1 and what is the valuation of x2? Well x2 is 1, So, valuation is a unit. So, valuation is 0 with respect to anything. So, for this point the valuation of the function is 1. No, functions can have only 0, some of the valuation should be 0. How do you know? We have not proved that in the class.

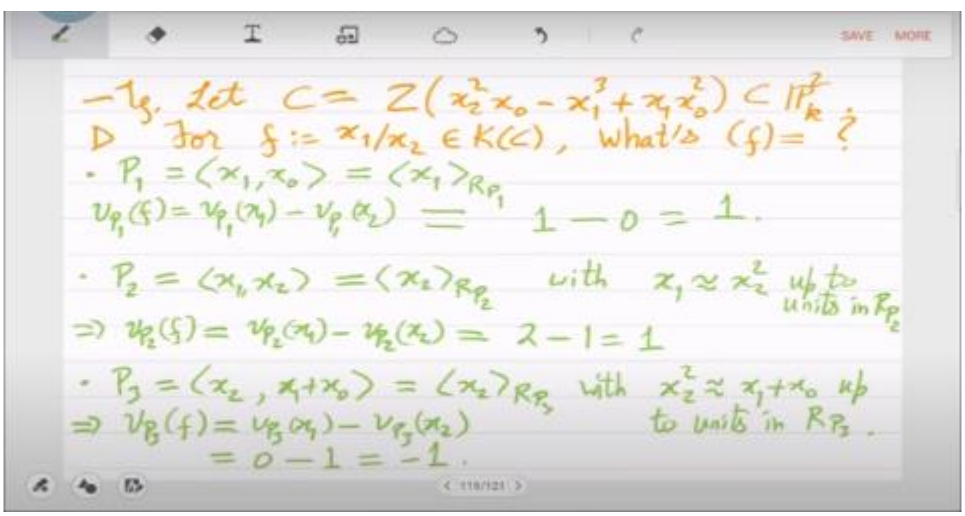
Let us go on. Let us look at the next point. So the next point is x1 I have already set to 0, I had an option, now I pick x2, so x1, x2. So the point now is 1, 0, 0. I have set x0 to 1 and I have set x1, x2 to 0. What is the uniformizer for this? This is more interesting, again in the equation you see that $x_2^2 = x_1$, to $x_2^2 = x_1$ up to units in the divisor ring for P2. So, the uniformizer you should you can only take it to be x2 now.

So it's just x2 and the DVR is RP2 with the valuation of, I mean basically this I can just write that x1 is like x2 ^{2}. in the DVR. This you can see from the equation of the curve. In other words valuation of x 1 is 2.

So, valuation of the function is. So, valuation of x 1 is 2. and valuation of x2 is 1, so you get 1. So, you can see that both p1 and p2 are genuine 0s multiplicity 1, they are simple 0s of the curve. What remains? Now, we have to move to poles, which means x2 has to be set 0. If I set x2 to then what do I get from the equation I have to now either set x1 to 0 which we have already seen that was p1.

Other options are I set x1 - x0 to 0 or x1 + x2 to 0. So x1 + x0 I set to 0. what is the uniformizer now. So, again similar calculation as for p 2 you look at the equation x 2 ^{2} is = x 1 + x 0 up to units. So, I again take x 2 as the uniformizer in r p 3 d v r.

Okay and what is valuation of the function now? It is again for x1 you will get what? What is this? Well x1 actually will be a unit, both x1 and x0 will be units, it's only their sum which is a 0, x2 is 0, x1 = - x0 but clearly x0 and x1 cannot be 0 because if they are 0 then you are out of projective space, so you have to pick x1 and x0 to be 1 and - 1. so both of them are units so this valuation first one is 0 what is the valuation of x2 that is 1 so you see that p3 is actually a simple pole of the function ok what is the other option that we have left so the only option now that we are left with is x2 , x 1 - x 0 which again like before is uniformizer will be x 2 in now in the DVR RP 4 with x 2 ^{2} like x 1 - x 0 up to units. in RP4 DVR which means that the valuation of F is exactly like before, you get 0 - 1 = - 1. So, what we have learnt is this is a very illustrative example. So, you have gotten all the 0s and the poles with their multiplicity.



So, p 1, p 2 are simple 0s and p 3, p 4 are simple poles and there are no other 0s or poles on this curve for this function. So, which means what? what is the divisor of f, it is p 1 + p 2 - p 3 - p 4, is that clear, that is the divisor in this abstract divisor group in DIPC. Yeah, so now coming back to what Deeptajeet was claiming in the very beginning without proof is that the sum of order should be zero. which in this case is true 1 + 1 - 1 - 1 is 0. So, we will prove after the exams that this actually is a property which is always true for principal divisors that degree of principal divisors is always 0.

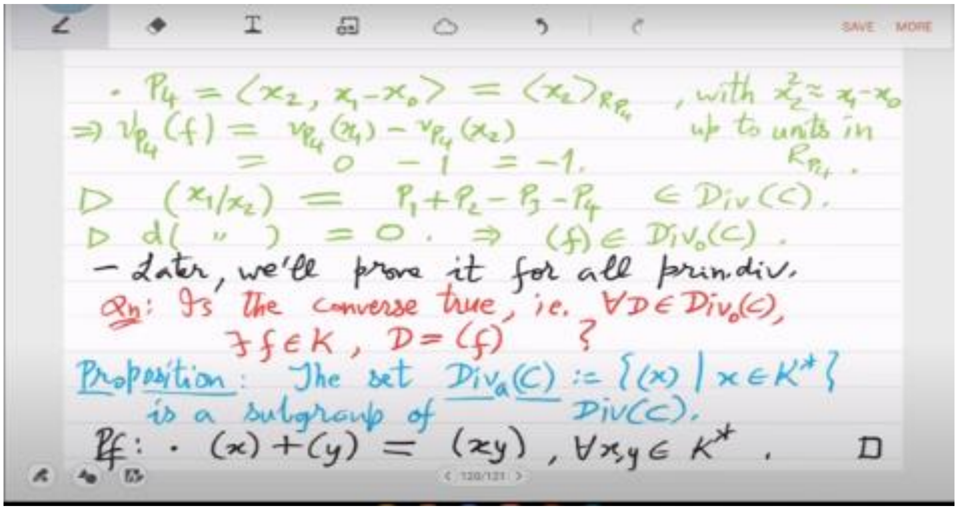
So, the number of zeros and poles they have to balance each other out. So, degree of this is 0. So, which also means that this principal divisor is in div 0 c. So we will actually prove that this is true for all principle divisors. Do you think that every divisor in div 0 is of this type? Is every divisor in div 0 coming from a rational function? So you have shown that every rational function lives in div 0.

Is the converse true? Is this, do you expect this? So, this question is what will ultimately we will formalize it and we will study this thing in great detail and depth. This question will lead to actually geometric pictures when or a geometric understanding when there is no geometry over finite fields. we will actually show that this is not true for no interesting curve actually this thing will be true except the projective line. So, it is only curves which are bitrational to the projective line that you will get div 0 equal to basically k. in all other cases div 0 will be bigger which means that there will be degree 0 divisors which will not correspond to any rational function.

It will be strictly bigger than k, big K, bigger than the function field. And how big it is that will tell you how many holes there are in the curve which we will call genus. We will measure those things. But it takes a lot of development, so do not get too excited.

So, let us just collect this what we have deduced now. So let's call these principal divisors. Let's collect them and call it div AC. This is a subgroup of div C. Why is that? So you look at the set of all these principal divisors, it is an additive subgroup. So you have suppose x and you add it to y, I am claiming that x + y is also in divac, why is that? What should I put here? in the blank space, what should you fill so that this divisor equation is correct? It's an identity.

Just think in terms of zeros and multiplicity, right? If there is a zero for x, p is a zero, so p appears in (x) and p appears in (y), then p will also appear in, and you are adding it, so p + p becomes 2p. So, 2p should appear where? What is the function where the multiplicity of p is 2? You can take x^2 or you can take y^2 or you can take their product x times y. So, just take x y, this is the identity. This is true for all functions. And you can check this by valuations for any point you look at VP both sides and you will see that it matches because we had this axiom in valuations that it is on multiplication it is on product it is additive.



So, it is just that. follows from the valuation action. Is that clear? So, immediately what we learn is we have now three groups. So we have a chain of subgroups, additive groups. This div A is a subgroup of div 0.

Sorry, this I have not shown. Yeah, let me not claim it here. Right now I just know that this is a subgroup of div C and div 0 is of course subgroup of div C. So these are the things we immediately know that the set of principal divisors give you a subgroup and of the divisor group and degree 0 also give you subgroup. So our long term goal is to compare these subgroups and measure them. So, we will actually want to develop a quantitative analysis or quantitative methods to say this properly that is div a contained in div 0, if it is contained how much smaller can it be and so on. What is the geometric interpretation of that? So, to do that study we have to define We have few more things, so let us move in that direction.

So we want to say that with respect to a divisor two functions are called equivalent. if yeah, so just take a q from principal divisors, when would you want to call x and y congruent to congruent modulo some principal divisor d, when x - y is a multiple of d. the function that d defines, if that divides x - y then, so here we will write it as x - y >= d or when d divides x - y. So, we are defining these things So with respect to divisor, we can actually compare rational functions. We say that they are equivalent if you look at the zeros and poles of x - y, each of the order should be at least that in D.

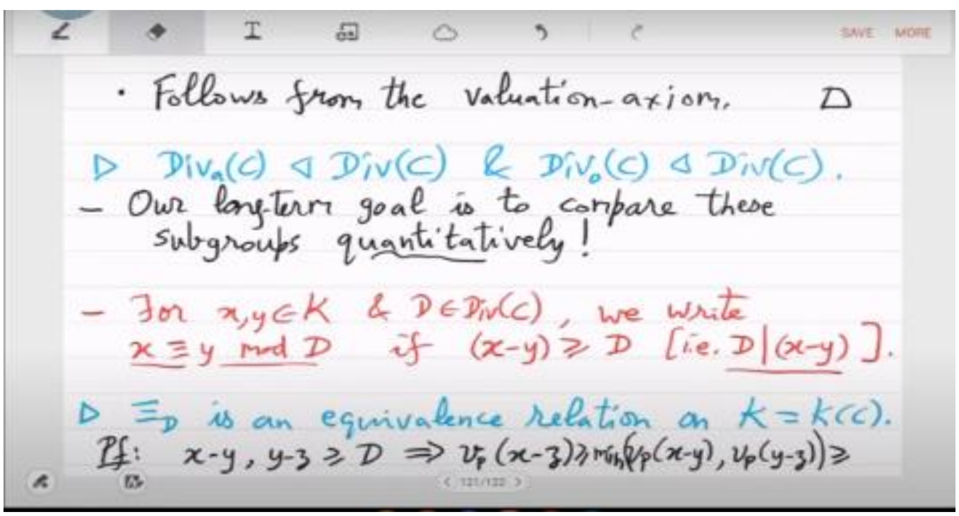
So in a sense, so when D is a principal divisor of f, then f should divide x - y. So we are trying to mirror that here in general. We can also write it as D dividing x - y. Where D is a divisor and x - y is a function.

This actually is a equivalence relation. on k on the function field that is because well x is congruent to x if x is congruent to y then phi is also congruent to x and if x is congruent to y, y is congruent to z then you basically have x - y >= d and y - z > = d you can sum this up and you will get X - Z > = 2D. Is that right? You don't want to do that.

Yeah, correct. So, yeah, you shouldn't do that. Let's just check it. So, x - y and y - z, they are > = d. This means what? So, you should actually do this properly by using valuation. You should. The sum will be > = d from the minimum, when you add two numbers, you get minimum of the valuation.

Correct. Yeah. So, the valuation, if you look with respect to p of x - z. So, now we are using the second axiom of valuation. which is on some right. So, x - y + y - z this is the this is > = both x - y and y - z. So, ultimately it > = d is that fine.

No the axiom was what, you take the minimum. Minimum. Yes, I should put minimum here actually, it is not this strong, it is only for minimum. Sorry, this is order of, yeah. so this will be > = order of P in D, that is the formal proof.



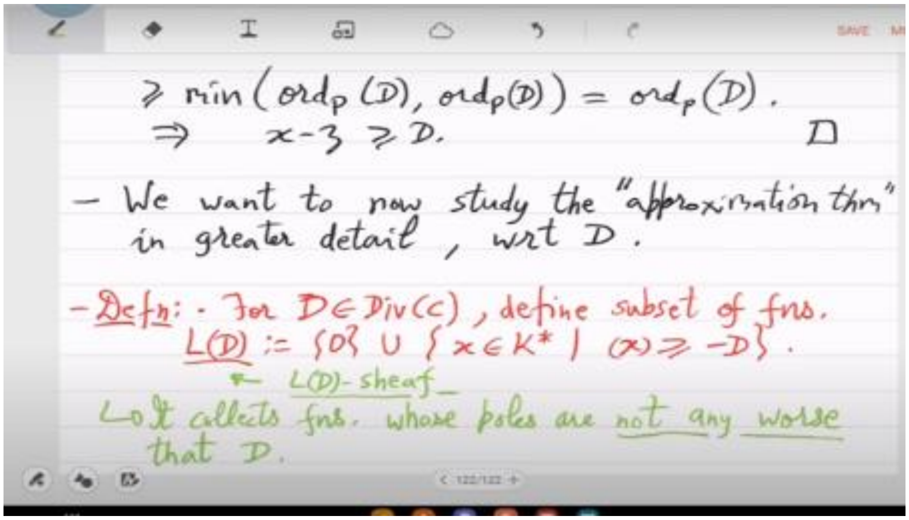
basically the valuation of x - y is lower bounded by the valuation by the order in the divisor D and the same thing is true also for y - z. So, hence the minimum will be equal to will be lower bounded by the order of D with respect to P, which then means since it is true for all the points it means that x - z > = d.

So, that is the second axiom of valuation. So, you can classify, I mean once you have a divisor in mind d, you can actually classify the functions into classes such that within a class all the functions they look the same mod d and across classes they look different ok yeah is that clear fine so we will now define a more important object So now what we will do is given a divisor D. we want to study this approximation theorem. So, remember the approximation theorem which we proved in the last class which gave you. So, approximation theorem said that if you specify points with the multiplicities then you can find a function which is lower bounded by that right. So, points with the multiplicities you can think of as the divisor that is the input given to you and approximation theorem says that there is a function which will be lower bounded by this.

function whose principal divisor will be lower bounded by this d. But now what we want to do is we want to understand how many such functions are there. We want to restrict to those functions which pass through the approximation theorem. And to do this properly we will define probably the most important object till now. which is this LD sheaf. So, for a divisor D L d to be all those functions and let me just skip this thing just normal L d to be the 0 function and all the non-zero functions.

whose principal divisor is at least - D. So, we will call it LD sheaf. without defining what a sheaf is, but if you already know what a sheaf is then it will hopefully guide you in the correct direction. So, this LDC for those who do not know what a sheaf is, is simply a subset of functions including 0, whose principal divisor > = - d. Now, I can as well have I mean I could as well have done this to be + d, I use - d because the theorems later will become nicer looking. This d - d is not important, we just go with - d. So, the in other words what this is doing is that it collects functions whose poles are not any worse than d.

So, think of D as just point P. So, what is the meaning of x > = - P? It just means that if you look at the poles of x, there is possibly only one pole and it can only be P with multiplicity 1. There cannot be any other pole because if x has some other pole q, then x will have - q, but - q cannot be > = 0, - q is strictly smaller than 0. So, what this is saying is that collect all those functions whose poles are not any worse than the 0s and the multiplicities that you see in D, this is what it is saying. So, this is our LD sheaf. and I can define one more version of this because that will be better for quantitative estimates for any subset of points define a restricted divisor ds and we are thinking of some divisor d.



So restriction of a divisor d with respect to s is just restricting to the points in s. So, instead of going over all the points which appear in the support of divisor D, you restrict to the ones which are in this set S. This is called a restriction of a divisor by a subset of points and I can define restriction of the LD sheaf now. So, this restriction of the LD sheaf is those functions which are correct on the s part. So, the difference here from the LD sheaf is that again of course, this is saying a similar thing that poles of x are not worse than d.

but only up to the points in S. This is only comparing the points which are in S. So if P is in S, then if P is a pole, its multiplicity should be at least - of the multiplicity of P in D. But if P is not in S, then we do not care.

Then this is not putting any constraint. So that is the difference. See that again. Yeah. D has to be same as the support of the principle devices that are in this space. So, that is why you are defining this LD underscore S. He did not understand.

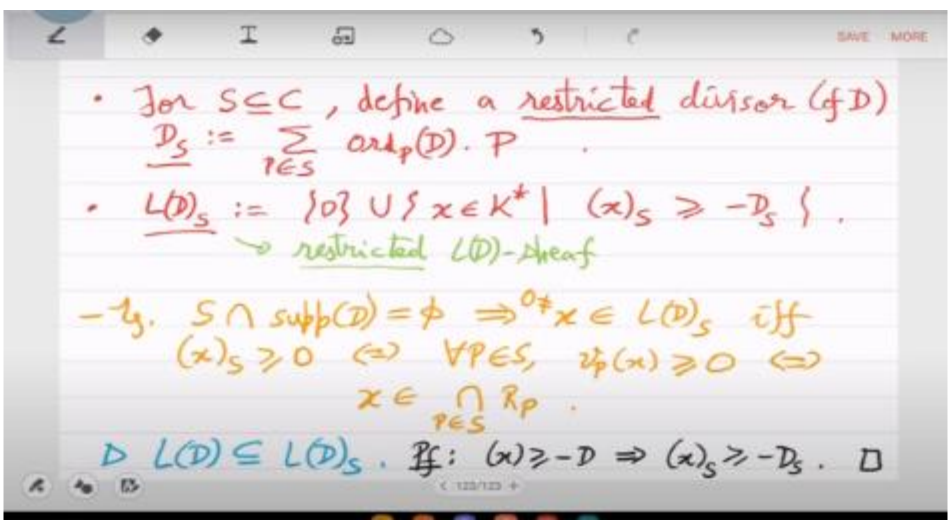
What do you mean? D is arbitrary and S is arbitrary. There is no requirement here. No, suppose D has a support subset S. Can be any support. So, if S is disjoint to the support of D, then D restricted to S is just 0. So, then this is just saying that collect all the functions x which on and so x sub s means that you are only looking at the points which are present in s those can only be zeros they cannot be poles maybe we should take this as an example it's a good example so example if you take s disjoint from the support of d then x is in LDS if and only if so non-zero x is if and only if this x sub s > = 0 right which is like saying I mean which is exactly saying that the points which are in s on them you want your rational function to either vanish so let us write that for all the points in S you want the valuation of X in those points to be > = 0. So either these I mean basically then

X has to be in the DVR that is what it is saying Let us just write this, x has to be then in the intersection of DVRs.

So, the points which are in S, you want x to be in that DVR. So, you take the intersection, that is the illuminating example you have. This is what LD restricted to S is doing if you take S disjoint from the support of D. If there is a point common between S and the support then you will have a different condition.

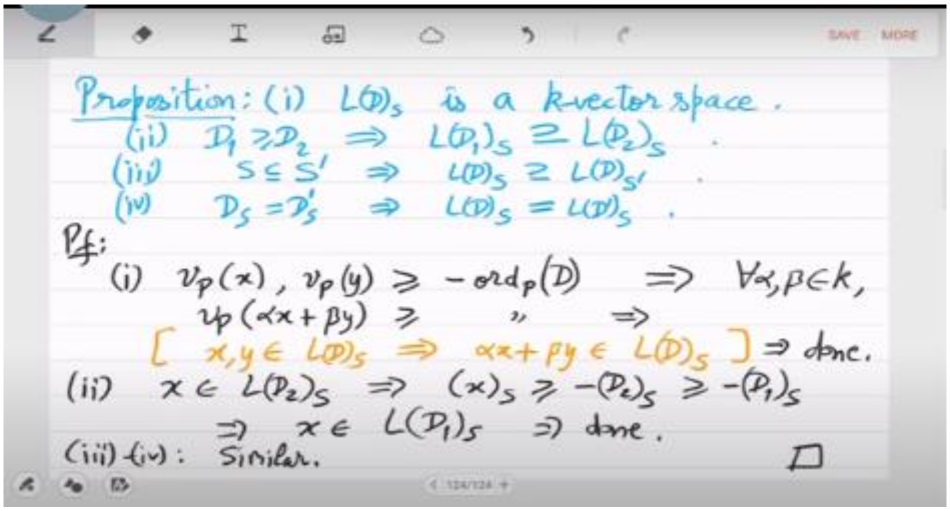
Then you will be talking about poles. Here you are avoiding poles. You are saying that poles are not allowed from the points in S. Greater than equal to 0 means that either P is a 0 or it is neither a 0 nor a pole right and. So, this is a big difference from L D the in the L D sheaf So, you will have more functions, because there you are not restricting to s, you are actually, sorry I am making a mistake.

Smaller. Yeah right, smaller. Let us write that down. So, ld will be smaller than lds. Why is that? So, if x > = - d, then it means that x restricted on S > = - dS. So, whatever x you have in L d that is trivially in L dS. but as you can see in some examples LDS will be bigger. So, although you are I mean I am saying it to be a restricted LDSheaf in terms of size it is actually bigger. Any questions? Okay, so let's see more properties because this already is actually, you will see many interesting properties which are easy to show.



So, LDS is a k vector space. So this is not just a subset of the function field. It's actually a vector space. It's a subspace of the function field. Why is that? If there is a function x, there is a function y in LDS. You have to show that (x) + (y) is also there, right? So again, it follows from the valuation axioms. If d1 > = d2, then what can you say about L and L ? How do you compare them? So, d1 may have more points and more multiplicities, bigger multiplicities.

So, it seems that you are putting more constraints on the functions. So, it seems that LD1S should be smaller, but that is not the case because you have to remember we have - sign. So, you are looking at functions which are > = - D1. So, it will be the opposite.



So, you will actually have LD1S bigger. So, - sign actually helps us in getting this. this property. So, d 1 > = d 2 means that functions which are in L d 2 s are already in L d 1 s. And similar thing for the subset how do this how will you compare these L d s and L d s prime. can use a similar intuition. So, s is s has fewer points, so fewer constraints. So, L d s should be bigger that is actually true and what if d s and d s prime are equal sorry d So, for D and D prime if they if for these arbitrary divisors the S part is the same, then clearly LDS and LD prime S they will also be the same.

Let us quickly prove these. Why is it a vector space? if for a point the valuation of functions x and y is at least - d, then you understand the valuation of their sum also. for any small k combination. If the valuation of functions x and y is at least some value then the valuation of the sum of these functions for any linear combination by the valuation axiom is also that.

which means that this if x and y are in LDS then alpha x + beta y is also in LDS right. So, you are done. So, you can sum up rational functions in LDS, you remain there. Second property, so if xs is at least - d2s. take any element in L d 2 s which means that x s is at least - d 2 s - d 2>= d 1 s which means that x is also in L d 1 s is that fine.

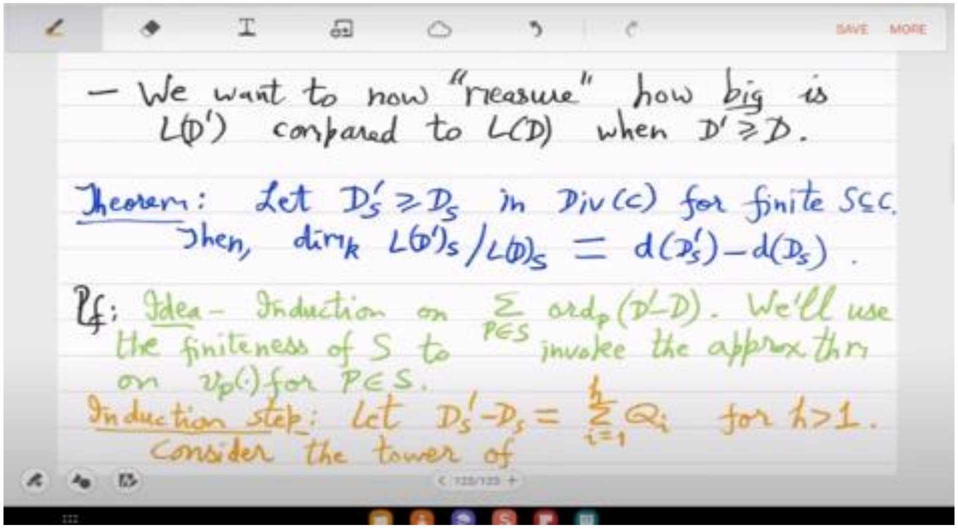
So here you use - sign that we have in the definition. I think others are easy. So that gives you all the properties. These are simple properties. Okay so next thing that we will do is remember we want to study we want to do a quantitative study which means that second property which is saying that if you take a bigger divisor than the restricted space the LD sheaf gets bigger we want to actually measure how much bigger will it get okay and we will do this now quite precisely. So, you want to measure how big is L D prime compared to L D now both are vector spaces.

So, we will of course, measure their dimensions. So, what is the oh in fact, L D is a subspace of L D prime right. So, we will just want to we basically want to compute the dimension of L D prime mod L D. that quotient vector space. So, that is a major theorem. So let us have this, so we have the setting S is finite, set of points on the curve and we have this d prime > = d on the restricted points S. Then this dimension of the quotient space can you guess what this is equal to ld prime s mod lds so this will be given by the degree so degree of ds prime - degree of ds So in a way the more points you add in D prime over D for every point the dimension grows by 1.

So per degree this LD sheaf is growing by dimension 1, this is what we want to show So, we will show this by induction on the degree essentially. we will induct on how many these points you see in d prime - d starting with one we will we are base case would be that we will use the finiteness of S to invoke the approximation theorem. Since these points are finite, the set S is finite, we can invoke the approximation theorem for finitely many points give you these finitely many valuations and that will give us the functions we want in the proof.

Approximation theorem on valuations for P in S. That is the plan. So, here actually the base case will be the hard case, induction step will be easy. So, base case is the case of a single point growth of D prime over D. so we will do that later the induction step will actually be easy which is let this growth be by many points q i's 1 to H, two or more points, we can actually reduce this to a single point growth which is H = 1. So, how do you do that? You basically look at these divisors which you are getting when you add Q1, then Q2, then Q3 ... QH.

So, you have a tower of space. which is L d s is contained in L d + q 1 s ... q 1 q h s which is L d prime. So we divide the vector spaces LD prime S and LDS into this tower of subspaces by the proposition. Is that correct? So when the divisor grows, the space also grows. The L sheaf, LD sheaf grows. And then we use the base case for every step here.



So what does that give you? so this means that dimension of L d prime S mod L d S over the base field k is equal to yeah. So, actually this is. This will just follow from linear algebra. You have a sequence of vector spaces strictly growing. If you know the dimension of each of these quotients in the middle, then the sum will be the total dimension.

Yet this is just like causal elimination or growth of a basis. You find a basis of LDS then you grow it by something to get to the next one and then you grow again to get to the next one and so on. Just grow the basis and you get the sum. and this is 1 less. So, i = 1 means l d + q 1 mod l and then i equal to you go up to i = h which is L d + q 1 to q h which is L d prime S mod the previous one. So, you that is the dimension that you have grown up to which by base case is just degree of q i which ultimately is equal to degree of this.

Is that clear? So induction step is pretty easy. Just growth of the basis one point at a time. So all we have to show is that in the first step when you go from D to D + Q1 the dimension growth is degree of Q1. If you show that then we are done with the theorem. So that's the claim. so dimension of L d + q s mod L d s = degree q always for any divisor d for any point q and for any subset of points finite subset of points s this is true on the curve.

Yeah, I think this will take longer, so maybe we have to stop now. The idea of this is not very hard, but there is some calculation to be done. So, idea is just that let your points in S be P1 to Pn. remember that in this setting Q is in S right Q is in S. So, p 1 is the Q and then you have more points p 2 to p n that is your finite set S.

and degree of q is d, let us say that is the setting you are in. So, when you add another constraint for the functions that you are looking for, basically the constraint is this - q that you are adding in the constraint. So, how much does the set of functions grow. So, you want to show that they grow by exactly d, the degree of that point. In particular think of degree being 1, you actually have a real point Q, in that case degree is 1.

So, you want to show that there is only one new function that you will add, that is what you want to show. When d, small d = 1 then just one new function appears. So, where does that function appear from? so it actually appears from the DVR of Q that is the idea so we will develop the basis the K basis by using that of the DVR, corresponding residue field actually. So you basically look at the DVR corresponding to that point.

Proof idea is that in that DVR, I will be able to find a function which will be new. That's all. But implementing this proof idea will take much longer. Because obviously, somewhere we have to use the approximation theorem and all that. So let's do that after the exam.