Computational Arithmetic - Geometry for Algebraic Curves

Prof Nitin Saxena

Dept of Computer Science and Engineering

IIT Kanpur

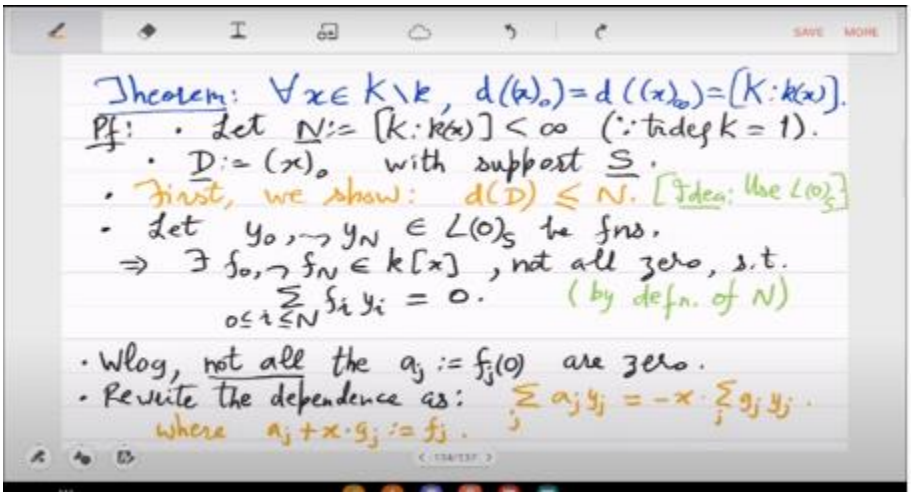
Week - 11

Lecture – 22

Z function of curves

Okay any questions? You want the valuation for 1 / f, 1 / x. So, 1 / x was special that was the point at infinity. 1 / f I do not remember, we did not have that. Yes, so 1 / x was the only one which was special. That was a proof, that proof we gave. So we characterize that this one.

Distinct DVRs are, yeah so Rf is clear that is like x-α basically. For algebraically closed field k it is just, you just look at the multiplicity of, I mean uniformizer is x-α. Yes. So, either that or now with in hindsight you can just think of this as z = 0, z = 0 is the point at ∞.

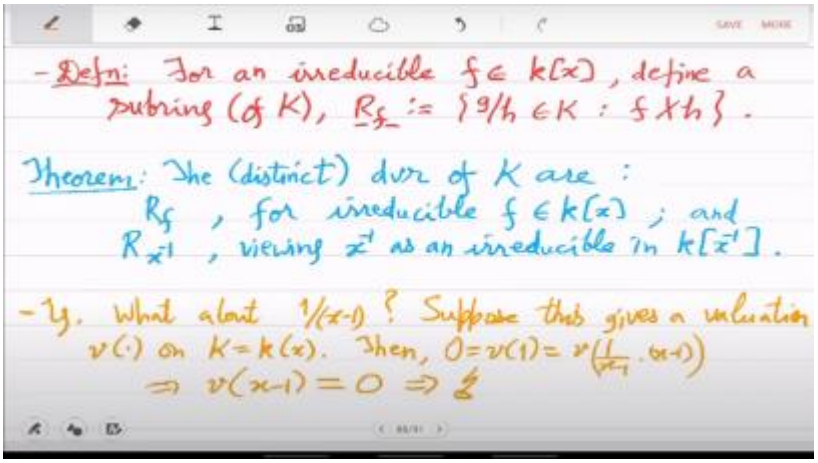


So, if you write down all the polynomials in x, y, z then you look at the multiplicity of z. oh this proof yeah so what okay suppose this gives a valuation then so valuation of 1 is 0

but valuation of 1 should also be the sum of the valuation but this is yeah this was nothing no I think it was later on that we got the correct one which was you write x as x - 1 + 1 / x - 1. Yes, yes. No, no basically you want to look at either whatever valuation of polynomial f you are taking either f or 1 / f whether x = 1 is a root. In this case.

In this case you showed first I said v (x) is 0. No, no, no because x = 1 is neither a root nor a pole. Yeah, so that will be the same, claim is that it will be the same as you want to count the x = 1 poles. Well x is a unit there in that DVR. So, if you call 1 / x - 1 t then x is what 1 + 1 / t and No, 0 would mean that it has to be a, it has, basically you have to show that it is outside the maximal ideal, yeah.

In other words, 1 / x - 1 should not divide this. no no so well what is x - 1 what is the what is the valuation of what is the valuation of 1 / x actually that also you have yeah you have to calculate that So in this case you have to collect, well when I wrote this Vx = 0, I just assume that you have to check the divisibility with X - 1 $^{-1}$. Divisibility by X - 1 $^{-1}$. It means the definition of that is how many powers of x - 1 divide each in the g / h representation. you have to go valuation has to be defined for every function, every function looks like g/h and the valuation is x - 1 $^{-1}$, how many times does it divide g/h which means that you look at let's say just simply you look at how many times x - 1 divides g, how many times it divides h.



No, no that is all, that may be fine but valuation has to work for every function. This is my definition for every function. For g/h, valuation of x - 1 $^{-1}$ is the highest power which divides g/h. So if g is 1 and h is x - 1, then the valuation will be 1. And if g = x - 1 and h = 1, then the valuation will be - 1.

That's all. You just take the, you just intuitively first define it for every function. Then

from there you build everything else. Yeah, valuation is a thing for the whole function field. You do not need to look at the DVR.

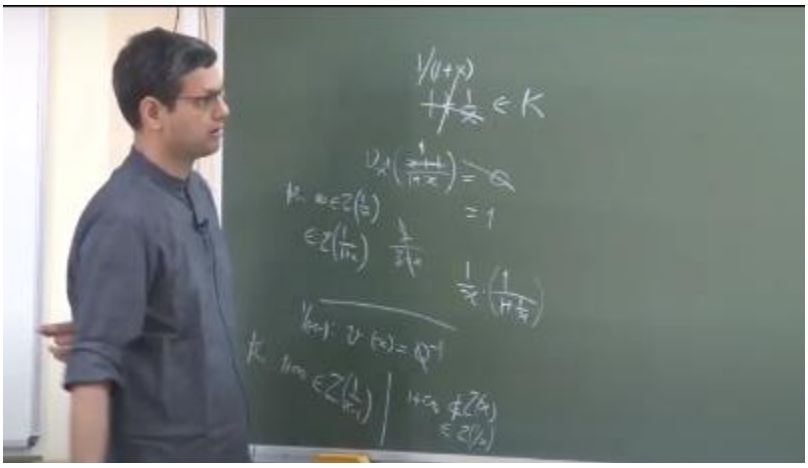
DVR actually gets automatic, once you define valuation on the functions, DVR will automatically be those elements in the, those functions whose valuation > = 0. That will give you the DVR and the complement is the functions where the valuation is negative. They sit outside the DVR. No, no, no, not power series, G and H are polynomials. G/h are polynomials and what is the valuation of X^{-1} there is just, just check polynomial division. This is not any different from valuation of X, this is the thing we did for X and since, I mean X is not something special, you can do the same thing with 1 / X. 1 + 1 / x and the valuation with respect to x. Sorry. 1 / 1 + x.

Okay so this in this case the valuation is 0. Sorry. Valuation is 1 because. in terms of pointed infinity, this is actually z / z + x. So, z = 0 is a root that is true.

So, valuation actually should be equal to 1. So, what you do, 1 / x you take out and then do this and this is a unit. I see yes 1 / x is a nice interpretation what is the interpretation of 1 / x - 1 then so you want to calculate the valuation of x with respect to 1 / x - 1. So it gives up at point level it is something like 1 + ∞ right. This is the point 1 + ∞ is the kind of the point.

So 1 + ∞ when you look at the function x that does not vanish. So this way this has to be 0 with respect to point interpretation. the point 1 + ∞ is the 0 of 1 / x - 1 that's the point x doesn't vanish at this point while here the point was infinity because I mean this is 1 / x so 1 / x ∞ is a point is a 0 of this 1 / x, right and it is also a 0 of 1 / 1 + x because 1 / 1 + ∞ will also vanish. So, clearly the evaluation of this function should be at least 1 and then for algebraic reasons it will be exactly 1, but here the valuation has to be 0 because So, it cannot be positive, it cannot be negative right. So, 1 + ∞, 1 + ∞ the point is neither a 0 (x) nor it is a 0 (1 / x).

1 / x it is actually a 0. that is true, so then it is actually - 1, so that reasoning is wrong then I have to correct that, yeah it is not 0, so then it is coming out to be - 1. So we have to actually then properly argue, why isn't 1 + ∞, I think the, it seems to be that this is the same, it will give you the same valuation as point at infinity, may be that would be the correct argument, so 1 + ∞ is the same as infinity. So I think the, I have to replace this orange argument by the argument that actually 1 / x - 1 will define a valuation but it is the same valuation as 1 / x. So the distinct valuation claim is still true.



Yeah, let me do that separately. That's a good point. Yeah, it's actually not ruling out valuation. It's just saying that valuations either come from an actual point or from point at infinity. Everything else gives you one of these.

Any other question? So then let's, so last time we started the Z function of smooth projective curves. So our interest is in point counting since day 1 which is that we want to count this big N sub n which is the number of points on the curve in a desired finite field which is of size q^n. So how many fq^n points are there which means that both the coordinates should be in this field. So I mean we know by algebraic closure that in fq bar. So, for any fixing of x you will get a you will get fixings of y possibly many that was the cover of the projective line, but then that does not tell you anything about finite fields, because in finite fields may be when you fix x usually you do not get y.

So we actually want that estimate to be made much more precise, the covering of the projective line, how good it is, is it for finite fields. That's our goal, so we will gradually move towards that by defining this Z function and studying it. So we proved some properties, that Z function version will be this. To begin with, it's just a formal power series in one variable t, integral coefficients.

and goes over all divisors. This is why we spend so much of time on divisors because actually Z function will be defined like this. Now why do we take t raise to degree of d? So for this you have to recall how the classical Riemann Z function, the first one was defined. It is sigma $1 / n^s$. So, and it goes over all the numbers. Now, in our curve world the numbers are somehow simulated by divisors, but then the divisor group is not a multiplicative group, it is an additive group.

So, we put it in the exponent. So, we change Riemann's original motivation slightly here,

but the spirit remains the same. So, we put t raised to the divisor. so that when you add divisors this someone multiplies, okay. So, this is the correct analog of numbers. Yeah and you can see that this is actually this, you can now try to recover classical theorems like this Euler formula can be recovered.

Z function factors into points. So that expression is the same as 1 - t raise to degree of a point inverse which expands this way. So just like numbers factor into primes, divisors factor into points. So Z function also has a corresponding factorization.

I do not think. So our base field k will be of choice. But so the point p may not be an actual point, it is just a cloud of points. These are point with their all conjugates. It is a prime ideal if the, I mean in general when k is finite field. Otherwise it is an actual point when k is algebraic closure.

Accordingly degree changes. In fact we will do this very systematically. Soon we will actually calculate how the Z function changes as k changes. So these things you will see explicitly. We introduced this δ. which is the image of degree map on the class group degree map we do not know whether it is subjective or not but we know that it is an ideal and since Z is a PID principle ideal domain so there is a generated δ.

So that number we will now keep track of. So we have the following exact sequence degree 0 class group arrow class group arrow δ. Δ multiples, this is exact. Okay so, next we started expanding the Z function.

So, we will do this even more today. We will keep expanding it into something we understand. So, we definition is sigma over all the divisors. So, you can write first you parameterize on the degree, pick a multiple of δ and then degree D class group you look at the classes that's fancy D. And then in fancy D you pick a divisor, right. So clearly in fancy D for whatever D you pick the degree is d, it does not change.

And now we study the two inner sums. So basically how many, what is the size of fancy D, that is lemma 1. And there you see that this L sheaf which we had defined already appears. So we showed that this is basically equal to Q raise to dimension of the L sheaf. So we get that formula and next we look at how many classes are there of degree D.

that is lemma 2. So, we showed that it is the same as degree 0 class and it is finite. So, those are the two lemmas and we can now collect that. So, that is the space of all devices, effective devices linearly equivalent to. Fancy D is just an element in CLD. It is a representative divisor, but it is not alone.

So, Fancy D will have many other divisors. Exactly. So, you go over all the degree D divisors. But then you classify them into classes where in every class if you take big D and big D prime their difference is a principal divisor, it comes from a function. So the number of classes is finite and also the size of a class is finite that is what we have shown lemma 1, lemma 2. So which means that now we can expand the Z function confidently.

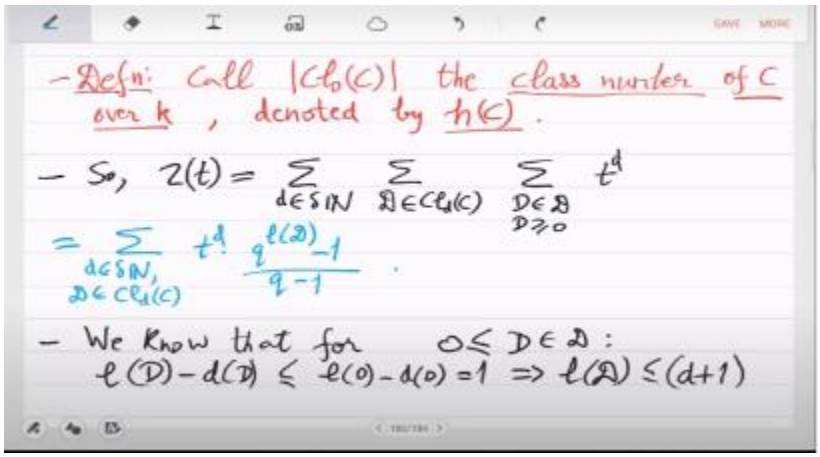
So let us do that. So, we will call this number since it is finite and it is equal to all CLDs a special name. So, this is called the class number, the class number of C over the field of choice k. and it is denoted by hc. So this number is of course originally motivated from algebraic number theory by the works of Drachley. So every transcendence degree one function field has a class number hc, call it hc.

So, what does Z function becomes? So, this is the triple summation your degrees are all non-negative. So, multiples of δ natural numbers then you have the class and then you have the elements in the class. oh and yeah the sum always goes over divisors that are non-negative, right. So, not all the elements in the class but only the non-negative ones, do not use negative ones that we have counted.

So, this is equal to we just count t^d. So, we have shown that it is this l dimension And now we have to recall Riemann-Trogue theorem to estimate L (d), what is L (d)? So, L (d) is related to the degree of d which is d, but then there is a difference is given by genus right. So, let us recall what that is. So, L d - d d < = l 0. So, basically yeah let us just say t > = 0. So, from that the l - d difference is smaller than that for 0 which you know is 1 meaning that l (d) < = d + 1.

So, we get at least an upper bound. We have still not used the full force of Riemann rock that we will do later. So, for now we just want to upper bound I guess. So, you will get the upper bound of this. So, Zt is less than equal to, maybe let us do next page. Okay so the class number we get because that is the count for fan CDs.

And the second thing we are approximating is this Q expression. So the Q expression basically is I mean you can just expand it out after division. So you have $Q^{L-1+L-2\ldots}Q^0$. So you have L many things which is upper bounded by D + 1. So you get definitely a lazy bound is $D + 1 . Q^D$.



So d + 1 . q^d and t^d sits there as the monomial. What do I mean by less than equal to? So this less than equal to just think of this as in comparing the coefficients of the monomials. It is Z of t is actually a polynomial and when I write this Z (t) < = another power series, I mean power series less than equal to another power series I basically mean that I am upper bounding the coefficients. I am not evaluating it, it is still a power series. So this upper bound we immediately get and so we can now write down a proposition.

about how this power series converges. So, Z (t) converges for which complex T's. What can you say now? Now in this power series if we start actually putting complex values to t, when will this infinite series converge? Yeah, so this hc is obviously a constant. is this Qt^d essentially which is growing very fast. I mean you can also ignore d + 1.

It is only Qt^d which is growing exponentially. So that is the thing which you have to kind of make sure that it keeps getting closer to 0. So for that it is equivalent that Qt should be < 1. So that is the condition. So, the convergence is equivalent to the absolute value of t or the radius of this t which is a complex number, it should be strictly smaller than 1 / q. Then qt < 1 and you can show by easy complex analysis that this will converge for all complex numbers.

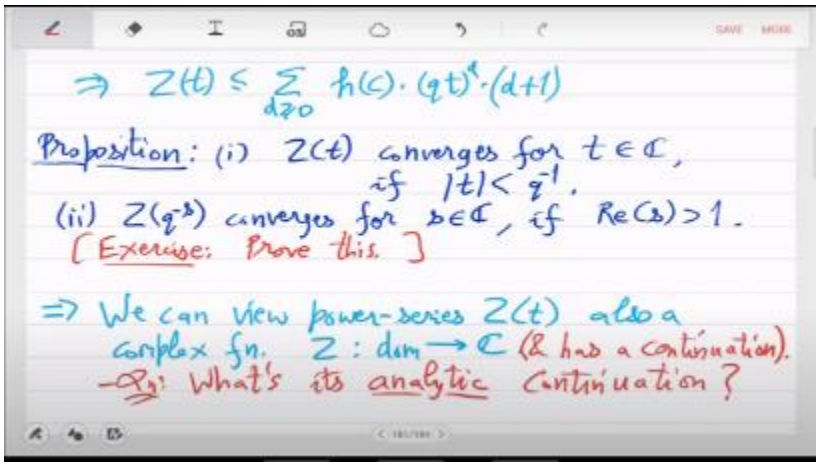
That is the radius of convergence. And, second is to compare with classical Z function of Riemann, we will sometimes substitute t / q^{-s}, where s is a parameter or s is a variable, it is a variable which you can think of taking complex values. So, when you put q^{-s}, then for what s will this converge? So now you have to look at basically q^{1-s}. So what does that give you? Q^{1-s} should be falling which means that the real part of s should be

greater than 1, right. So, if the real part of s is 1.1 then of 1 + ε then you get this 1 - s to be essentially – ε on a complex part.

but that is enough to let it fall and converge, the series will converge. So, the proof I leave as an exercise. and what this proposition tells you is that we can view the power series Z also as a complex function. So, if we wanted we can actually we started with a formal power series, but if we want we can also view it as a complex function. It takes complex values and converges to complex and under assumptions on the argument.

I guess it's not the domain is not everything of course, there is some domain. From that domain to complex. Yes, and it has a continuation, but that we will not discuss in this course. That is a good one. yeah so what's the continuation of this yeah good so it converges only for some part of complex but suppose you wanted to extend the Z function so that it converges for all complex, so that it truly becomes an analytic complex function.

So whether it has a continuation, yes it is an interesting point, we will come back to it again. Right now it is not clear whether these things will happen. So with this proposition let us define one more notation. So we denote this thing z of q^{-s} as actual Z.



So this is the notation we will use. that is where the name also comes from. So this will be the classical kind of notation for Z function. Now for a curve S taking complex values and Z (t) will be our power series version. yeah that's one thing and other thing is I want norms of a divisor so norm of a divisor will be defined as Remember you had this T raise to degree of divisor term.

So that is kind of the norm. Formally we define it like this. So norm of a divisor is

simply Q raise to degree. Why have we put Q? Well we have put Q because to match with the definition of this Z function. So instead of T I am using Q so it actually becomes a number. Sorry, Q is our old Q.

Yes, so why are we using that Q? There is a very good reason for it. using the same Q actually maybe you should already guess that. So this formula that we had on the top the approximation right upper bound that has Qt^{d}. So Q will be Q will actually be that which came originally from this lemma 2.

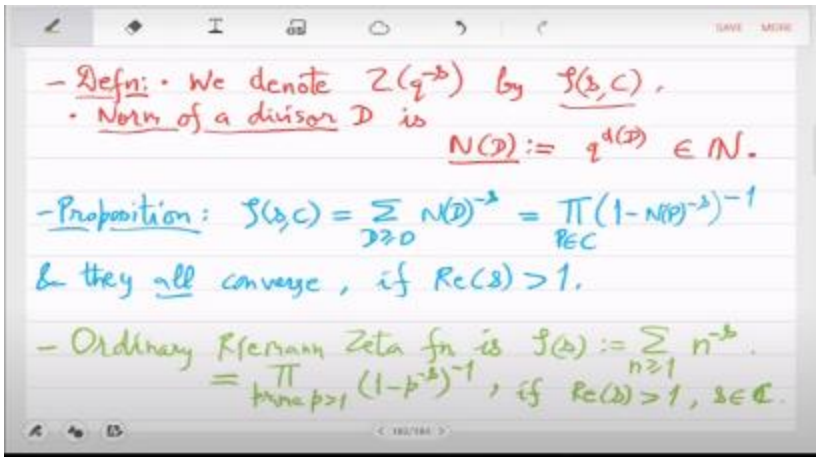
or lemma 1. So, in lemma 1 we had this estimate right. So, whatever q was here. So, that was the size of the base field k. So that is the queue which is hanging around everywhere. Its consequence will be pretty big. It will actually give you the kind of the analytic continuation of the Z function.

In other words we will show that Z (t) defined as a power series actually converges to a rational function for all t, I mean for the formal t. So that rational function is the analytic continuation. So this Q is important, only this Q will work, it is not formal. So this norm I have defined only to give you the comparison with Riemann's Z function So this Z function = $\Sigma\, d^{-s}$ and equal to by Euler's formula that holds here points on the curve and they are all convergent. So for these complexes they actually converge and for formal S you have this identity.

The first equality is just coming from the definitions. So why did we write it this way? Because now you can see that Riemann's original Z function is of this type exactly. So, there is an analogy. So, ordinary Riemann Z function is Z s Σ 1 / n to So, for numbers in the case of integer ring you go all the numbers these are kind of your divisors and the norm of that divisor is the number itself. So, this is n^{-s} let us just write in that exactly that form.

So, norm exponentiated with - s. So, it is exactly the same form. and by Euler's identity you can express it in terms of prime numbers, it factors. You can just match it term by term and see that this is actually an identity. So for primes two or more, you have the same analogous thing happening. Norm of the prime is prime itself in this case.

And it becomes convergent series if your s is. real part is greater than 1. So, you can recover the classical expressions and of course, you hope much more you want to recover all the classical theories as well. So, that is what we will do. So, the next thing that we want to recover is what is called the functional equation and the symmetries.



So I do not know whether you have seen because I have not seen the class, the ordinary Riemann Z function, the functional equation and the symmetries are not very easy because you have to first give the analytic continuation of this.

which does not assume real part of S greater than 1 and that is not explicit. However, in this our Z function Zt, we will actually, we get an explicit expression and that will be thanks to Riemann rock. So we now show that Z (t) is a rational function, further it has a symmetry. around S = 1/2. So the famous Riemann hypothesis that is basically this, it is conjectured by looking at this symmetry around s = 1/2.

So here the key idea will be of course Riemann rock. So because Riemann rock had also this symmetry, the divisor of speciality was basically w-d So, that symmetry at the level of Z function is what we want to now lift and what will we get? So, first is that Zt is in Qt, although there was no reason for this to happen because we define it as a power series. almost all power series are outside Q and in fact it's even worse almost all power series are even outside algebraic closure of Q right because they actually happen to be transcendental. So you can't really set up. algebraic equations.

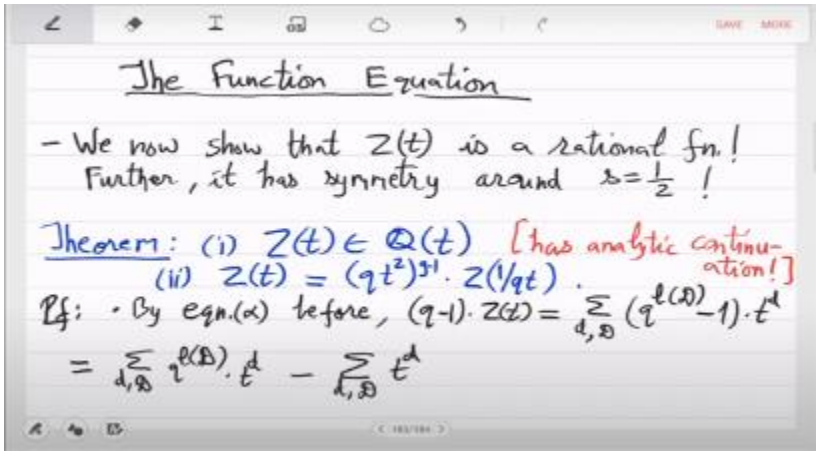
So, it is a very very special thing that this happens, this converges in Q (t). So, this is the answer to analytic continuation. So, answer here will be very explicit the analytic continuation, so you can forgo the power series and you can just focus on the rational function and then you can evaluate it wherever you want. It converges all the time except at the poles, poles also we will classify, so everything will be classified, it will just work always.

And second thing is very mysterious. that it satisfies this equation. So, what this is saying is you look at Z, you look at the transformation 1 / Qt. So, how does Zt compare with Z (1 / Qt) and there is a nice expression. which again there was no reason for this nice expression to exist, because even after you have rational functions the ratio of two

rational functions could be very complicated, but here it seems to be not it is highly elegant. So let us prove these things, it is surprising that you can actually see the proof of this now.

You have enough machinery for this. In fact the machinery that we have developed till now is built exactly for this. You will see that almost everything that we built goes in this proof. yeah from the previous not proposition but this place that we somewhere we had the expression, this blue expression, yeah let us recall this expression. we can write q - 1 times z of t equal to appropriate degree and appropriate class q l of the class - 1 . t^d.

Right that is what we have simplified at least the inner most sum we have simplified. And now what we want to do is study the first part which is the L dimension. So, let us break it up. I mean this will be nothing but just try to get this infinite sum to converge to a function, rational function. We want to sum up this series.



Now how do we further break it up to sum the components? It is basically guided by this L dimension. So we have a pretty good control. The L dimension is basically the degree when the, in the cases when the divisor is big. This we have seen many times because of Riemann's theorem. and then we made it even more quantifiable by Riemann-Roch, so we showed that essentially when the degree is at least 2g-2, in that case we have a formula for L dimension and when the degree is smaller than that then we do not have a formula, so we break the sum into two parts accordingly. Yes so first part is ft which is the good part, so that is degree > = 2g - 2 + δ, yeah degrees have to be multiples of δ, so it is that delta we are so Q of l d t raise to d - the other infinite part and the other part is g t.

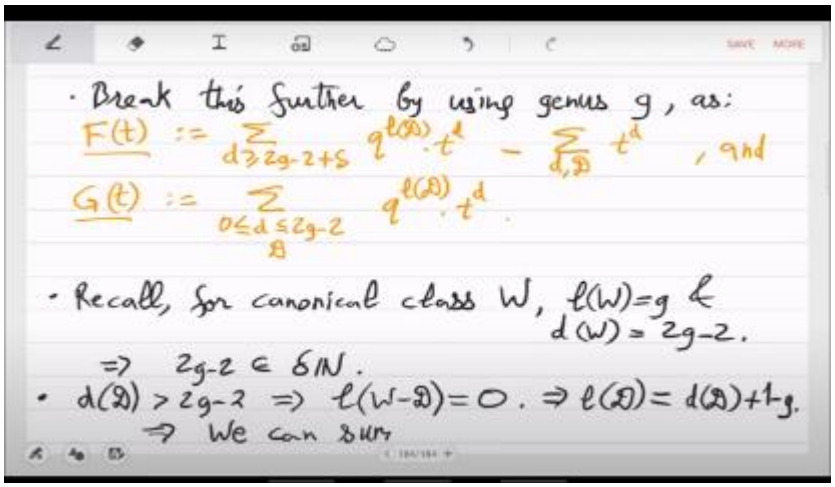
So, that is the finite part. So, this part is messy, but it is finite, so it is Yeah did we lose anything? So this gt goes up to 2g-2 and then ft goes starts from 2g-2 + δ. Did we lose anything in the middle? Well we did not lose anything in the middle because remember that 2g-2 is the degree of the canonical divisor right. So, in particular that was a multiple of delta because every degree happens to be a multiple of delta. So, 2g - 2 is some multiple and the next one will be + δ.

So, we are doing it in increments of delta. So, it is fine. So, the function can be partitioned into these two and yeah recall basically. that for canonical divisor the l dimension is g and the degree is 2g - 2 which means that 2g - 2 is a multiple of delta. Correct, yeah. So, degrees of all classes go in multiples of that. Right now there is no way to prove it because as I said base field k can be finite field and right now you have no idea whatsoever how the points are distributed in this finite field on the curve.

In fact your curve may have no point at all from there. So there is no way to say that there is a point of degree 1 for example. I mean degree 1 points are the real points in your base field but there may be no such because all the points they are in the algebraic closure which and you do not know where, so you are, so we are actually working in the blind right now and we will come out of this darkness only once we have proven the Riemann hypothesis, only then will we know that in every finite field essentially you have a lot of roots, so lot of degree one points. So yeah, but let us continue with this delta, formal delta, the unknown delta. Yeah, so when the degree is more than the canonical divisor, then you know that L (w – d) is nothing, because I mean w - d essentially is a negative degree divisor.

So, you cannot even have constant functions greater than equal to that. So, there is no function whatsoever in the L sheaf, which means that or may be use this fancy one. So, which means what about L (d)? So, L (d) is then simply given by the degree + 1 - g. So, this this what was that called degree of speciality is 0.

So, you get just difference is exactly 1 - genus. that is a good situation in our formula. So we just plug this in f of t and you will see that it will get very easy to calculate because what you will get essentially is I mean degree is just d, so you will get qt^d and qt^d you can sum up to d ∞ like that is geometric progression. So this case actually reduces to geometric progression and that is the magical part. So that was the hard part. What to do with the infinite sum? Infinite sum actually reduces to geometric progression and you have a rational function.



gt is the finite part, so it cannot disturb. So you have convergence that way. But we can't stop at this because we have to prove symmetry also, so we actually have do the calculations to get the symmetry. Symmetry is a more, is a deeper thing. So, let us do that. We can simplify or we can sum up f t like this.

So Ft is equal to, yeah let us, sorry there is always this d hanging around, fancy d. So we have to go over all the degrees and all the classes. So let us use the class number formula here. So we will get hc times this is from Riemann rock d + 1 - g t^d - hc / 1 - t^δ and the sum goes over large degrees and multiples of delta. So, we have removed the, we have counted the the classes by putting this hc and we have also used Riemann rock for high degree. So, we have replaced L by d + 1 - g and t^d stays and what have we done with the second sum and minus.

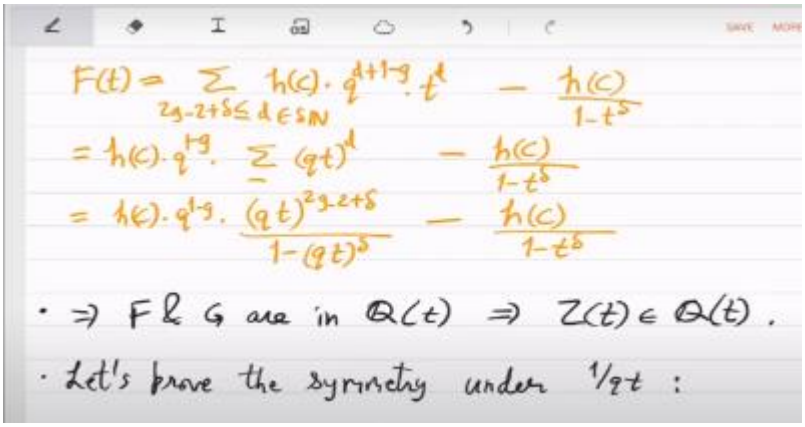
So, the - ∑ t^d we again have counted the by the class number and rest is just geometric progression. so it is happening in multiples of delta. So, the geometric progression will give you 1 / 1 - t^δ. Yeah and then we can just continue. So, let us take out h c q^{1-g} and get to qt^d that is the geometric progression part here same conditions as before which will sum up to by geometric progression formula.

So, qt to the starting point which is 2g - 2 + δ / 1 - qt^δ. So, that completes the proof that f of t is a rational function and you can see the poles. So, f and g are now in Qt. which means that we have shown Zt is in Qt.

This is the first major property. You can observe more interesting things here. For example, if you set t = 1, then the first part, then both f, the first part hc / $t^{\delta-1}$ right, it will go to infinity and it goes to infinity with residue the class number. So, you get the,

you can, we make this observation that the residue of the Z function at t = 1 is the class number. So, we will collect these properties later, but you can already see these things happening beautifully.

T = 1 and T = 1 / Q and many others, possibly others. Deltaire roots of unity in complex, yes. So the interesting thing is that this calculation is happening over integers while our curve was over finite fields. So it is a characteristic change. But anyways it is true that the residue of the Z function at t = 1 is highly important, it knows about the class number.



Let us go to the symmetry now. under 1 / Qt. So, for that we have to repeat this calculation with the big F of 1 / Qt, but also G (1 / Qt) and see that we get similar expressions. So, F (1 / Q t) is class number times this sits and Yeah, I will do that in the last expression. Yeah, because that would be easier. I do not want to start from the beginning. Yeah, so last expression when I put 1 / qt then essentially the base qt becomes now 1 / t and yes and there will be changes in the negative part.

So, let us do that. So, I get. T^{-1} raise to / 1 - $T^{-\delta}$ - the residue part and this becomes Q T - δ. Yeah, where? in the first part yeah so this is what i said that's the beauty of first part since there is already qt sitting so somebody great thought that why not just transform this by 1 / qt so the first term doesn't change by much so that should be a symmetry. Yes, so let us verify it, you will get now Q $t^{2\,1-g\,i}$ take out, let us check what remains. Yes, so what is happening is kind of these two summands they are flipping.

So, I will take $qt^{2\,1-g}$ and I think this should be fine. I have multiplied above and down by t^{δ} and same thing here with qt raise to δ I have multiplied. Yeah and I have taken a reciprocal of qt^{2} 1 - g, so that is g - 1 and this you can now check is simply qt^{2} 1 - g times f. So f already has this symmetry. Where? should be fine because in the denominator I have make it 1 - t raise to δ. So, the 2 terms here they have just actually

switched when I applied 1 / qt but then in the denominator also you have to switch them.

So, you will get back ft. So, big F is already behaving very well. This is just one half of the Z function. Let us check the other one. Is g of qt $^{-1}$. So, where is g? g we never studied. So G was the finite part, low degree so Riemann's theorem is inexact here.

So we do not really know how this L dimension behaves but we can still just substitute 1 / Qt and see what happens. So this is the d < = 2g - 2 part. So here actually since Riemann's theorem is inexact we will actually use the full force of Riemann shock. We will actually need this. the relationship between this degree of speciality with the L chief of the dual, which is canonical divisor - d, that is what will save the day, that is the reason for symmetry.

So, let us do that. So, these degrees and their classes fancy d. goes without saying that everything here is happening in multiples of δ. It is all implicit there and the new thing is that degree is at most 2g-2. So you have to be careful that when genus is 1 or 0 then this does not make sense.

So we have, these things are vacuous. But those can be checked separately, it is very easy. Just think of genus to be greater than 1 what happens then. So, let us write the Riemann rock in the exponent. So, that is d + 1 - g l w - d times Qt raise to - d. From here we can take out Qt ^{2} raise to 1 - g which we want to use in the symmetry and see what remains, so what remains is nice.

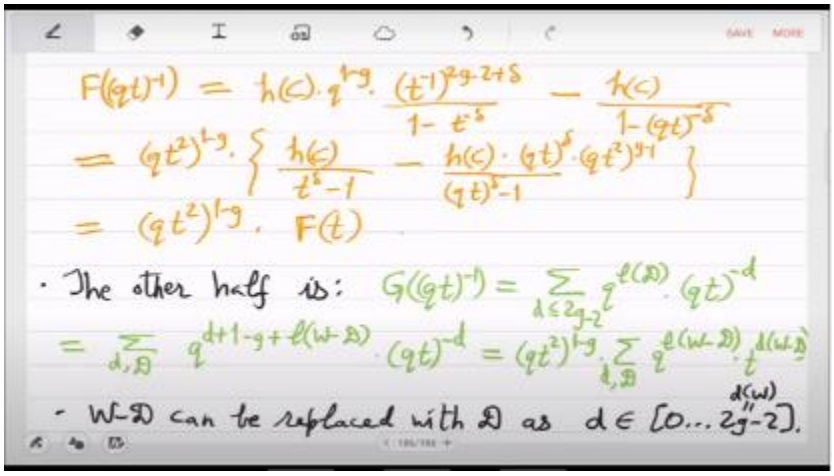
So let's check qt ^{2} raised to 1 - g. Are you convinced with this? So you have to use the formula that degree of w is 2g - 2. So T raised, what we have, there is T raised to 2G - 2 - D. Right? And I have taken out T raised to 2 - 2G. And given 2 raised to, T raised to 2G - 2 there.

And - D was already present because T raised to - D was there. So T monomial is correct. And now look at the Q monomial and you can check that it's fine too. because d and - d cancels and 1 - g remains which is out. So, this is just a rearrangement of q monomial and t monomial you can verify separately it is correct. And now what? So let us recall what g was, so g originally was q raise to ld times t raise to - small d - degree right. So this is equal to just let us just recall what this is, it is - of that is the exponent So Q raised to L dimension and T raised to minus degree of that divisor class.

That's the form here also. Wait, it's not confused with this. Let us go to the definition of G here. So here let us just keep this as like this. So G is Q raise to L and T raise to D. So that is the form we have now. Q raise to L and T raise to D and then as Madhavan said as

we are going over all the divisors Either you go over the divisor's d or you go over w - d, it's the same thing.

You have the same space. So that symmetry will help. as d runs 0 to 2g - 2, which is degree of the canonical divisor. So, this is the, so it is very important what the sum is over, since the sum is over 0 to degree of the canonical w - d behaves well. So, you can switch it back to d. So, this is all coming from Riemann rock. So, you we need everything that we did there which implies that g (qt^{-1}) = qt^{2} 1 - g times gt.



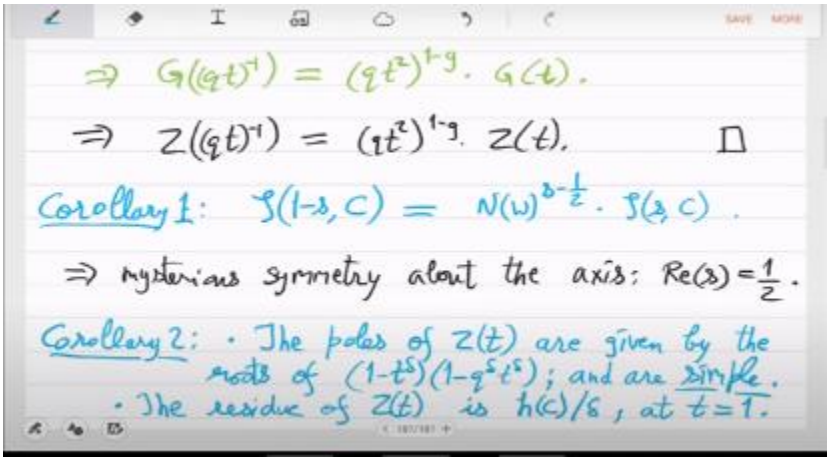
So both f and g independently have this symmetry, it's amazing. You didn't know when we partitioned the sum this way, which implies that Zt also has this symmetry. So that's the full proof. So Zt is a rational function which under 1 / Qt is changes very elegantly like this. Any questions? And what about the Z version of this Z? that also we can state.

So, Z version in the above you have to substitute t = q^{-s} and you can just easily verify that it becomes this. So, this is even better So you can check that instead of t if you use q^{-s}, you get this relationship where s goes to 1 - s, then what happens is you are just multiplying by the norm of the canonical divisor, canonical class raise to s - 1/2. So, at s = ½, these two things are obviously equal and then you can see that there is the symmetry around s = 1/2. So, there is a mysterious symmetry about the axis real part of S = 1/2. Yes, so here obviously we have a perfect explanation of this symmetry which is Riemann Rock. Do you know what is the reason for symmetry in ordinary Z function? Yeah, but I do not think it is known what is the relationship between these two things.

So, these two seem to be totally unconnected at the proof level, but this half is there, some syntactic comparison can be made. yeah the second corollary is the poles of Z t are by the zeros of 1 - t^{δ} 1 - q^{δ} t^{δ} = 0. And since we do not know whether delta is 1 or

bigger at this point we do not know how many poles there are, but they are of a simple type essentially t = 1 or t = 1 / q. definitely they are simple. So, this is an important thing to remember that we have shown that the poles of the Z function are simple because we are in characteristic 0 remember.

So, these polynomials they have only simple zeros. because these polynomials are not powers of anything, they are square free. These are square free polynomials. Even if delta is very big it is still square free. And something more we learnt which we can keep track of here which is that at t = 1 the residue that we are getting is something like H the class number divided by delta. This is the class number divided by delta, right. at as t tends to 1 what you are getting is obviously hc and then in the remaining thing you have denominator has $1 + t + t^2 \ldots t^{\delta - 1}$ which evaluates to delta.



So you get class number divided by delta that is the residue that is basically z of 1. may this may not be a good notation let us just say the residue of Zt at t = 1. So, when we know delta we will also know what the residue is exact I mean we will know that it will be exactly class number then. So, to finish that part what we need to do is something fundamental about the Z function that is to understand how it changes as we change the field.

So, how does Z t change as k changes? So that is called base change theorem. It will be relatively easy now. So let Cn be the curve obtained from C. by extending, previously it was q, size of the field was q, let us make it q^n. So, extend k to k'. Remember that the curve has coefficients from the field of constants fq. So, it defines a curve over whatever field extension you want up to fq'.

So, you can just go to fq^2 or fq^3 or whatever fq^n and you will get these Z functions

which will be very different, right. Morally speaking the divisors do not change, all that happens is the cloud becomes smaller. So previously there were many divisor or a point was actually representing a bigger cloud, as you go to bigger fields the cloud becomes smaller because now the conjugates will actually separate out. and once you reach fq‘, then the cloud is just a point, there are no conjugates, right.

So, we are moving in that direction. So, Z function will change a lot because it was actually counting these things. So, how does it change? So, it changes like this, Z function for the curve cn, if you substitute t^n then it factorizes. So, once this is written down you can see that it is quite natural expression. So, you have Z function for c n with t and you have Z function for c with t and the relationship is that in the bigger one if you substitute t^n.

then it factorizes into the smaller ones where you are scaling up t by an nth root of unity. So, it is kind of the factorization of t^{n-1}. So, t^{n-1} factorizes into or $1 - t^n$ factorizes into $1 - \epsilon t$ same thing. some version of that. So we will prove this next time.