Computational Arithmetic - Geometry for Algebraic Curves

Prof Nitin Saxena

Dept of Computer Science and Engineering

IIT Kanpur

Week - 10

Lecture – 20

Canonical divisor and proof of Riemann-Roch

Yes so we have done properties of Adele's, the main property you have to remember is this proposition 2.3 that Adele's mod this Adele sheaf ad + k, this is a finite dimensional object and this is exactly what we want to study, the degree of speciality of this divisor d. So l - d how bad is it compared to the genus. so it can be bigger basically δd can be positive and then when it is positive it gives you these new objects which is adels mod ad that we showed and so once these objects arise we have to give it a name so we call them differentials. So, in particular we do not call a |ad+K| differentials but we call the linear maps on this. to be differential.

a |ad+K| we can continue calling adels, but the linear maps from basically the vector space dual of this, this is a vector space. So, the dual of this we call that, that is again a finite dimensional object we call this differential space. So, if you think of adels or functions as non-linear analog of tangents then differential should be thought of as the engineering differentials right when you differentiate a polynomial what happens so dx dy so this this differential is a non-linear version of your engineering operators so these are generally new objects we call this now Ω d big Ω d this is the space of linear space of differentials. And what we have shown is a major result that over the function field this is actually just one element.

There is a single element which is the canonical differential, all other differentials are just multiples of that. Again the analog of this is in engineering you have d x or dy as the canonical differential, everything else is a multiple of y functions. So, this is a, there are two vector spaces here right, one is over the base field of constant small k, there it is a infinite dimensional of, it is not infinite dimensional sorry, its dimension is δ d. So, over the constants its dimension is what we wanted to study δ d. no wait a minute, that's Ω d, Ω d is finite dimensional, this Ω is union of all Ω d's, this I don't know, probably this is infinite dimensional.

So, over constants it's infinite dimensional vector space, but over function field it's dimension 1. so those are the nuances here we have covered all this. So, all this was towards the proof of Riemann rock right. So, let us now continue and finish it in this class. So, we will pick this canonical differential Ω and we consider its associated divisor.

So, that requires a proposition. So, in fact for any Ω in the differential space the set m Ω we define it to be all the associated divisors which means that Ω is in Ω d. So, for a differential there may be many associated divisors infinitely many that set is m Ω. and this has a the properties that this has a unique maximal denoted by bracket Ω notation. we are overloading the notation here.

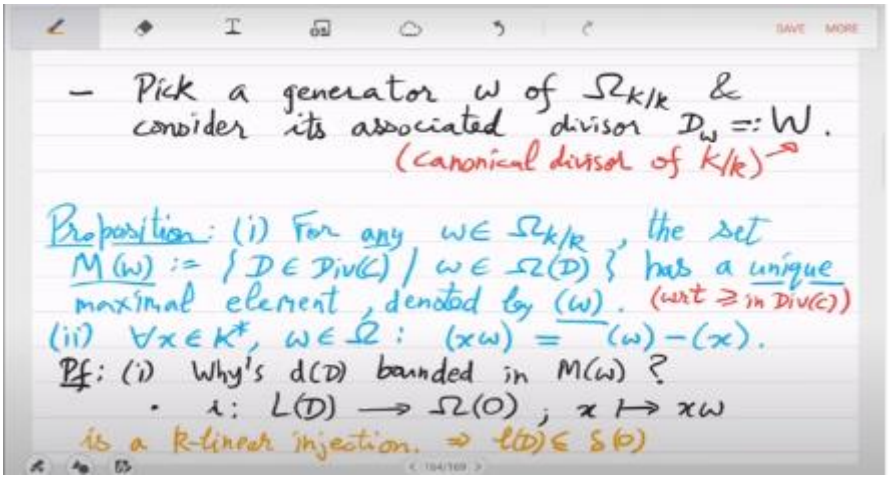
So, bracket Ω was also for when Ω is a function we were calling it the principal divisor. Now, Ω is not a function it is a differential. So, for differential bracket Ω would mean the divisor which is associated to Ω and is maximal. Now, the only problem is that this may be I mean there since there are infinitely many associated divisors how do you say that there is a maximum one. so what we will show that is that the upper bound is a degree I mean there is a degree upper bound so we can define maximal.

Second property is that for all rational functions and for all differentials the following holds so if you look at x Ω this is another differential, the maximal associated divisor of this which is defined above has to be related with Ω right. So, what do you think is the relationship? The maximal divisor for differential x Ω and the one for Ω the relationship is this. So now we are mixing the two things, so bracket Ω is maximal divisor for the differential Ω, bracket x is the principal divisor of the rational function x and the three things are related like this. Then where is the x Ω? function in fact vector space of dimension 1 over the function field. So, x Ω is also an element there, it is again a differential just like x times dx is again a differential.

I mean in engineering. Similarly, here also multiplication by functions is a differential. In fact, how did we define it? Do you remember the definition? Because now we will need it. So, x times Ω is defined to be on an adele its action is first multiply the adele with x and then apply the map Ω rx, this is what we will now use. to prove the proposition.

So, for first property I need to show that the divisors associated to a differential are bounded in degree. What is maximal element mean? So, it is not clear what it means and whether it exists. So the proposition will define all this in the proof. First we will show is that the set m Ω degree is bounded. Once I have shown that the degree is bounded then in that bounded degree I can pick anything I want that's a maximal element.

oh yeah actually i can define maximal also properly here this maximal is with respect to divisor greater than equal to that also works that is correct so in this ordering which we defined in divisors in that ordering there is a unique maximal element But this chain could have been infinite, so I have to first bound the degree. So let's do that first. So that is through this map. That you saw last time. So, consider the map \(I \) which is from \(L_d \) to \(\Ω_0 \) that sends a function \(x \) such that \(x + d >= 0 \).



Right, that is the function x, and what we did was multiply this by the differential Ω. Of course, the hypothesis is that Ω is in big Ω, and d small Ω is in big Ω d, which is just saying that small Ω vanishes on ad + k. It seems that "right" is not a complete sentence. If you meant to convey agreement or correctness, you could say "That's right." If you meant something else, please provide more context! So, if small Ω vanishes on ad + k, what does x Ω vanish on? It vanishes on Ω 0; just check that.

This diagram was there last time in a different mode of generality; actually, these arrows were there as well. So, what I am doing now is taking \(e \) to be 0. So, LD maps to Ω e; it is an injection. These are both small key vector spaces, and this is an injection that we used last time as well. Which means what?

The last time, we also used the dimension of the left-hand side (LHS) as less than or equal to the dimension on the right-hand side (RHS). So, this will mean that \(L_d \) is less than or equal to \(\δ_0 \), because \(\Ω_d \) has dimensions of \(\δ_d \) over the field of constant small \(k \). Let us continue; this means that \(L_d \) is less than or equal to \(\δ_0 \), which is equal to \(L_0 - d_0 + g - 1 \). That is the definition of \(\δ \), which is simply \(g \). We are interested in the degree of the divisor, right? So, let us do this again for big D.

Again, by the definition of δ D, you have this, in which you plug in L D, and you get degrees. So, wait, this is at least g - 1. So, that means the degree is at most LD - g + 1. Wait, something is wrong. This means that the degree <= g - 1 and is upper bounded by ldi, so I get 2g - 1; I just need it to be less than ∞.

So, the degree of all these is true for all divisors associated with the differential Ω; the degree is finite, right? So, with respect to the ordering, you will have a defined maximum element. So that completes one part of Property 1: there is a maximal element that is defined; let us call it d sub Ω. Why is it unique? We could have taken two different paths and two different chains. So the second could be D ‘ Ω. So, what should we do now? We should try to get a bigger element than these two.

So, for that, you take the LCM. So, take the LCM, which means differentials here. Okay, if d Ω and d ‘ Ω are different, then there will be some curve point at which the order of one is greater, so the LCM will strictly increase. If you want to contradict that, how do you do it? You basically show this property: you demonstrate that the Ω of LCM is equal to the intersection of Ωs.

Basically, you have to take a differential of the LHS, show that it is an RHS, and so on. You just have to use the definition of Ω D, which is maps that highlight ad + k. However, if you're looking for a more formal option, you could say, "Yes." So, this is an identity that is unconditional.

I mean, there is no special case. Once you prove this property, let me make a remark: leave it as an exercise. Use the fact that AD + AD ‘; I mean, even this identity is true over LCM. So, you can show that Adele's, I mean, essentially a differential that annihilates D and D ‘ will also annihilate AD + AD ‘, and thus it will also annihilate A of the LCM of D and D ‘.

So, this means that it is also a differential for the LCM of DD ‘, which demonstrates the sequence of simple identities they follow, almost by definition. So, once you have this, you can continue the proof. So, what this means is that since Ω is small, Ω is both in big Ω D and big Ω D ‘.

Oh, any day. No, no Ω is fixed here, right? In the entire proof, proposition Ω is fixed. Yeah, I am saying to just take any divisor. Yes. And I can find some Ω such that I will belong to Ω d then.

No, no, no. But why are you changing Ω? I do not understand, small Ω. No, no, no, small Ω I have given you; I have given you a differential. Now tell me how you will show that \(m \) and \(\Ω \) are bounded and that the degree is bounded. I have shown that for any Ω, it holds true.

No, no, no. Why do you keep saying "any Ω"? The proposition is given for any Ω in this context. Yes. If \(d \) belongs to this \(m \) Ω, then the degree of \(d \) < \(2g - 1 \). So, for any divisor d, does there exist an Ω such that d belongs to m Ω? Oh, you are saying that there is a problem with the proof. That is in relation to every point where I have 2g - 1.

You are saying that this means every element in the class group, or even in the divisor group, has a degree. No, this—yeah, that is an interesting point. So you have already jumped to the

proof of the Riemann rock. So what is happening is that if you take very high-degree divisors, these objects just evaporate. No, because you will see very soon in this class that for high-degree divisors, the domain we are working in does not exist.

I mean this Ω d will be zero-dimensional. Because it seems you already have the intuition, I guess. So, at the beginning of the class, I reminded you that Ω big Ω d has dimension δ d. Δ d is the difference of l d -, I mean, the difference, basically, in the Riemann theorem for high divisors; that difference will not be there.

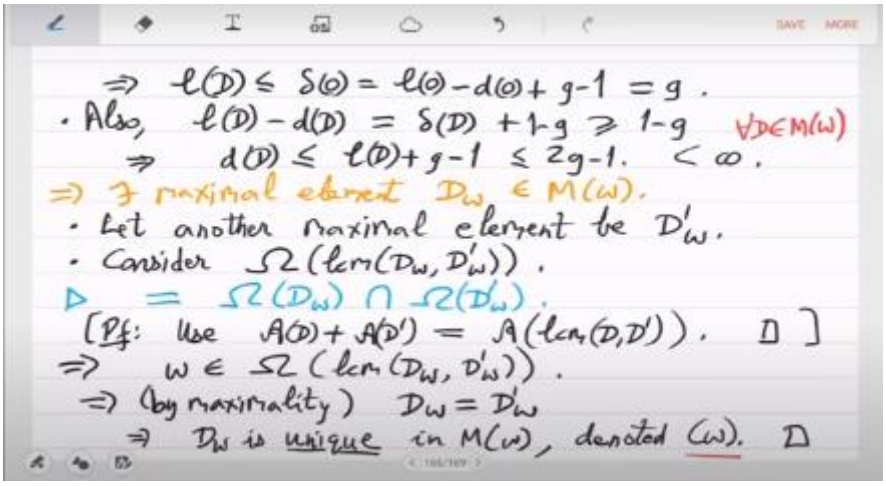
So, everything we are doing will evaporate. So, that is what we have realized. However, if you want to enhance it slightly, you could say: "That is true." That's a fundamental concept we'll see very soon in quantitative terms. It's not a contradiction, although it may seem that way.

So, yeah, now "intersection" means that Ω is in both, so Ω is in the LCM. As was pointed out in the beginning, the LCM strictly grows; however, it also contains small Ω. So, it cannot grow, which means that both divisors are equal. So, this means that by maximality, the only way out is \(d\Ω = d' \Ω \), and that is the uniqueness, which we will denote with this notation.

This will be the same notation as the principal divisor, but now for differentials. Sorry. We can just put this Ω in the hypothesis.

Correct that is correct, yeah. Yeah, so these objects that we are building and working with are actually all trivial in the limit. So, this degree of specialty is really a very small case in the grand scheme of things. But that is what Riemann Rock intends to study; it aims to examine the places where the Riemann theorem is not exact.

But generally, it is accurate. You will see that. Okay, the second property that we have to show is this X Ω. Now we have defined this range of differential. So I want to understand the bracket of \(X\) and the Ω differential in terms of Ω.



So, what is that? So we start with this small Ω being contained in big Ω, bracket Ω small Ω.That is just in one line. According to maximality, what you learn is that suppose d Ω and d ‘ Ω have different orders at some point, which means that in the LCM, the order has actually grown and increased. So, once it increases, the LCM will essentially be strictly greater than both the d Ω chain and the d ‘ Ω chain, which will contradict the maximality of d Ω. So, it contradicts the maximality of d Ω if it is not equal; fine. So, now with this new notation, little Ω is in big Ω of this unique divisor, and where is x Ω? So, x Ω is in this divisor - the principal divisor, which is almost by the definition of x Ω, because first you multiply the Adele by x and then you apply the differential Ω.

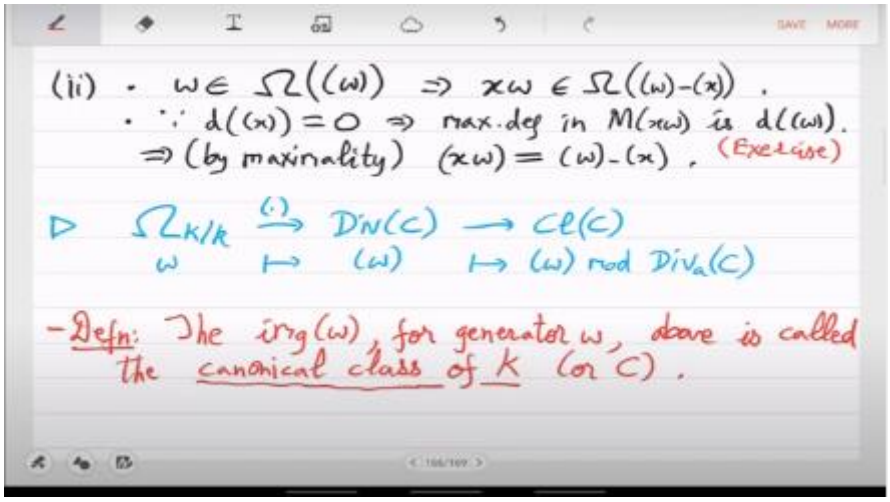
So, you have a loss here that is negative x. From here, I want to claim that the maximal associated divisor for X Ω is this; it cannot be anything more. This is simply due to the fact that the degree of the principal divisor \(X \) is 0. So, whatever chain of divisors you follow, the maximum degree of \(m \) in \(x \Omega \) will be equal to the degree of \(\Omega \). You have to show this, and this is a divisor whose degree is also the same, so it is maximal and unique. I feel there is one more step here, but you can treat it as an exercise; this part you can simply complete.

Yeah, so the identity for the maximal divisor of the x Ω differential is the previous one - the principal divisor. So, what is the advantage of this? So, now you actually know that this maximal divisor of a differential, I mean, if you consider going modulo principal divisors, it does not change. So, let us write that down or perhaps state it as a property.

So, here are your differentials. This bracket notation provides you with a divisor that can be mapped to the class group. So, little Ω is mapped to bracket Ω, which is mapped to bracket Ω modulo the principal. That's the sequence of maps; these are all vector spaces and at least abelian groups. Therefore, you have these morphisms, and essentially, if you multiply on the left by scaling up Ω with a function x, the image doesn't change. That's all I wanted to say, and from this, you can derive a definition.

The image of Ω above is for the generator, Ω. I mean that big Ω, which we have shown, is a one-dimensional vector space over the function field. So, for the generator, the image is unique. Although you can choose many generators, they will all simply multiply by functions. The sentence "That will not affect the image.

It is indeed grammatically correct. No changes are needed. So, the image above is called the canonical class of the function field of the curve. So, for all transcendence degree one function fields, we have this new object: a new invariant we call the canonical class, which is simply a divisor. It is unique.



Yes, I don't have an algorithm. No, but you want a fast algorithm. I do not know a fast algorithm because, right now, big Ω is just this adel mod adels, mod sub adels, and that calculation is infinite. So, I mean, sure, you can try brute force, but I do not know how you will verify everything. I cannot do it immediately, but at least we can finish Riemann Rock for now.

Let us state it again. So, let \(D \) be an arbitrary divisor that we want to study, and let \(W \) be this new entity we have defined as a divisor in the canonical class. So, what we will show is that, structurally, we will prove an amazing result: that these differentials are, in some sense, isomorphic to the L sheaf; in particular, it is W - D. That is the kind of weak intuition we started with: we wanted to understand δ D through some dual of the divisor D, which is L - D. So, it is L W - D, and this means that δ D, which is L D - D D, + g - 1, is equal to L of W - T.

In places where the Riemann theorem is inexact, it actually introduces new objects; it seems that these differentials are new objects, but now we see that they are actually old objects because they are just the LC for some other divisor. So, this ties all the threads together, and its proof is now actually obvious after so much development. So, we will just give you the maps. So, consider phi, which sends a function to, as before, x Ω, where Ω is, actually, I want to say

Ω. Thus, W is the divisor; the canonical class is, yes, Ω is simply the generator of big Ω—that's all.

You can now choose any generator of big Ω, and you know that its bracket, the maximal divisor associated with Ω, is a canonical divisor. I mean, it is a divisor that will not change except for multiplication by functions. So it is equal to this big W in the class group. If you would like a slight rephrasing for clarity, you could say: "Thus, it is equal to this big W in the class group.

" So, it may absolutely change; however, with respect to principal divisors, it is not changing. That is all you need to take care of. And yes, you already know that φ is a k-linear injection. What we need to show is that φ is also a k-linear surjection; then it will be an isomorphism of vector spaces. So, this means that we should take a differential element, Ω ‘, and find its preimage.

So, you know that Ω ‘ and Ω will be related by a function, up to a multiple, right? So, there exists a function such that Ω ‘ is x times Ω, which is correct, and I think this should also be remembered. Perhaps I should not mix these two up. So, x is present.) Also, you know that the maximal divisor associated with Ω ‘ will be at least d because d is one of the associated divisors; Ω ‘ is in big Ω d, right? So, by definition, you also have this, which is now a condition on x Ω.

And what does this provide me? Yes, maybe I should use a different one. So, what I need is a y in the pre-image. So I should just take it as it is. Yeah, so what is this? See, this is just \(w \), so this tells you that \(w - x - d \) is greater than or equal to 0. Right? So what? Do I have a function in \(L(w - d) \)? That is the inverse of x.

So this implies that \(\frac{1}{x} \) is in \(L \set- d \). Does it work? For Ω ‘, I needed a y, but this x is not materializing. You just have to show that there is something that approaches ω. To Ω ‘. Not Ω ‘, just Ω; the rest will follow because everything else is related.

Formally, you have to do this because differentials are the product of a generator and functions. Whatever you do must follow this principle. But do I already have this or not? I need to find a function such that when multiplied by Ω, it equals Ω ‘. We have to divide it into cases: if W - d is less than 0, then no function will exist, right? The sentence "Yeah.

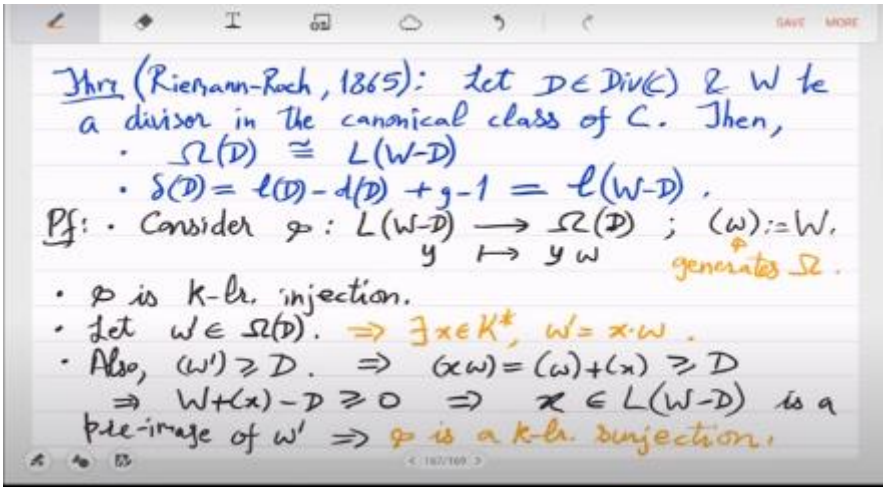
If you would like to make it more formal, you could say "Yes." No, but suppose that it is not the case, then. I mean, my plan was to use just 1 over x as y, but the problem is that 1 over x is mapping to Ω over x.

No, but that should be okay. So give me a y that will work and give me x Ω. I don't see that. Can I just change the association?

No, no, no. Yes, this is... y - y + y - t is greater than or equal to 0. I want to check now what Ω is on AD. On AD, there is an R, and there is an ADEL, which is like this.

No, I am worried that it should be Ω + x. I think this - sign is incorrect. I may have to make corrections to the previous proof. It should be w + x - d; otherwise, this will not make sense.

So let us check that. Why should it be Ω + x? Oh, this is... Yes, that needs to be corrected because other things are fundamental. You can't change anything here, so the only mistake I think I made is that this should be + x; Ω should be Ω + x. Therefore, w - x - d is what you get, which actually gives you x, doesn't it? Lw-d, so that is the preimage of Ω ‘, which means that phi is a surjection. So, it's an injection, it's a surjection, it's an isomorphism; however, it's not consistent.



This has to be addressed, and yes, we need to check this by definition. Let's denote it as \(\Ω_d \). If \(\Ω \) is annihilating \(A_d \), we are claiming that \(x \Ω \) is annihilating \(A_d + x \), which should be correct. Know what I have written here. So, if Ω is annihilating and I want to show that x Ω annihilates d + x. So, any r here is of the type r + d + x, and x Ω will multiply this, and then it will apply Ω to that.

Yeah, this part I have to check. Yeah, if there is a heavy inconsistency, I will correct everything, but let's do this. So, with \(x \Ω \) equal to \(\Ω + x \), you actually get a preimage, and then

it is an isomorphism, and the second thing follows. So, δ d is equal to G - 1. So, basically, this proof is hardly anything; we just have to consider the development we have done before this.

So, it follows from that that the differentials over this divisor D are actually this old object. The sheaf on W-D is the statement of Freeman rock. There is a sequence of corollaries that is very useful to know. The first corollary, as Rishabh pointed out earlier, is that if a divisor has a high degree, this becomes quantitative now. If you take a divisor of degree greater than 2g - 1, then Riemann's estimate is exact.

So for larger divisors, Riemann is already exact; rock is needed in that case. So, why is that? Yeah, so look at the line above the Riemann rock statement. So, look at L - D of W. The degree of D being greater than 2g - 2 is what you are given. Sorry, let us do something simpler first. Understanding the canonical divisor, the degree of the canonical divisor is 2g - 2, and L of the canonical divisor is g.

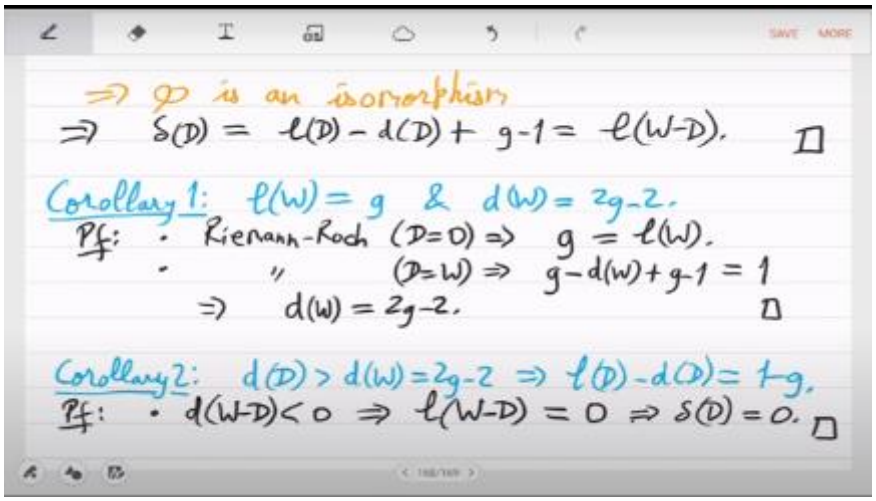
From the Riemann-Roch identity, we will actually gain information about this abstract canonical divisor. How do you demonstrate this? Yes, we can do two things. Since it's true for all divisors, we can try divisor 0 and divisor w. So for \(d \) equal to 0, you will find that \(L(0) \) is 1.

Therefore, the left-hand side is \(g \cdot L(w) \). That is the first property. The second is Riemann's rock: for \(d \) equal to \(w \), this will give you \(L(w) \), which is \(g - \text{degree}(w) \) (that is unknown) + \(g - 1 \), equal to \(L(0) \), which is 1. So, what gives you that degree is 2g - 2. So, for the canonical divisor, you know that the degree is not too large. So, as Madhavan was saying, you can try to brute force this, but I still do not know what the algorithm would be because you do not know the points. You know that somehow 2g - 2 should suffice, but then there are all these positive and negative orders; you do not know the orders, and you do not know the points.

So, this alone is not enough; you actually have to go into the structure we have developed thus far and devise an algorithm. Okay, now for the next thing regarding Collori 2: if the degree of a divisor is greater than the degree of the canonical divisor, which is now \(2g - 2\), then Riemann's theorem is exact. The proof of this is simply that since your divisor has a higher degree than W, W - D becomes negative, indicating a negative degree, which informs you about its L dimension. A negative divisor means that you are looking for functions that are greater than or equal to positive values. Therefore, those functions won't exist; in this case, not even constant functions will work, so you will actually get a zero-dimensional space.

Because even for constants, the principal divisor is greater than or equal to 0. So, nothing will exist if there are no functions. You can now use this in the formula that provides you with the

exact result. So, the degree of specialization is 0. So, Riemann's expression, \(ld - dd = 1 - g \); that is true.



The third corollary is especially nice; it is used in algorithms. It states that for these high-degree divisors, the degree of the divisor is high; however, both positive and negative orders will still be present. You may have 10 times P1 - 5 times P2; that kind of thing will be present. What this corollary states is that you can make all the orders positive in the class group. Okay, so for any high-degree divisor with negative orders, the negative ones can be replaced by positive ones if you are only interested in principal divisors modulo. This means that d ‘ - d is a rational function, where d has negative orders, d ‘ has only positive orders, and their difference is a function.

How do you demonstrate this?) So, for this high degree, you know this by Corollary 2. So, LD is equal to what is dw 2g del 2g - 2? So, LD is equal to what is dw 2g, del 2g, - 2? So, that is 2g - 2 + 1 - g, which equals g - 1. I guess I need \(g \) to be positive; actually, \(g \) equal to 0 will also be covered because if \(g \) is equal to 0, you are just saying that the class group is 0, which is fine.

So, when this is greater than or equal to 0... What happens in genus 1 is then 0, but it is strictly greater than that, correct? So, this is essentially greater than or equal to 0, which means that LD is positive, indicating that a function exists, right? So, there is actually a function; this LD space is not empty, and when that happens, by definition, you have d + x greater than or equal to 0. You choose this as your divisor. So, there is a function that you can find explicitly.

So, this, by the way, is an algorithm. You are given a high-degree divisor, and you can compute the LD vector space. Then, you can find a function x. In fact, you can take any function x, so you only need to find one function. You just pick the first function you find in the LD.

And if you add it to your divisor, you get D ‘. So, this is a fast algorithm. So, this basically tells you that in the class group, the only divisors you need to study are the sums of points on the curve. You do not need to worry about the negative order, as it is a powerful concept. It was not anticipated when we defined it a priori, and it was not clear that this would occur. However, this is true in the class group, and you know that.

It's efficient because you will never need more than a certain number of points. Whatever divisor you take, that many points will sum to be equivalent to this divisor, so it's all fast. Yes, every divisor has a small positive representation; this ∑ pi is the positive representation. So, the other thing is just a small observation: did we not formalize this algorithm to compute genus correctly because Riemann's theorem was imprecise? Sure! "Yes, we can now clarify that algorithm a bit because you can start with the high-degree divisor, which is 2g - 1.

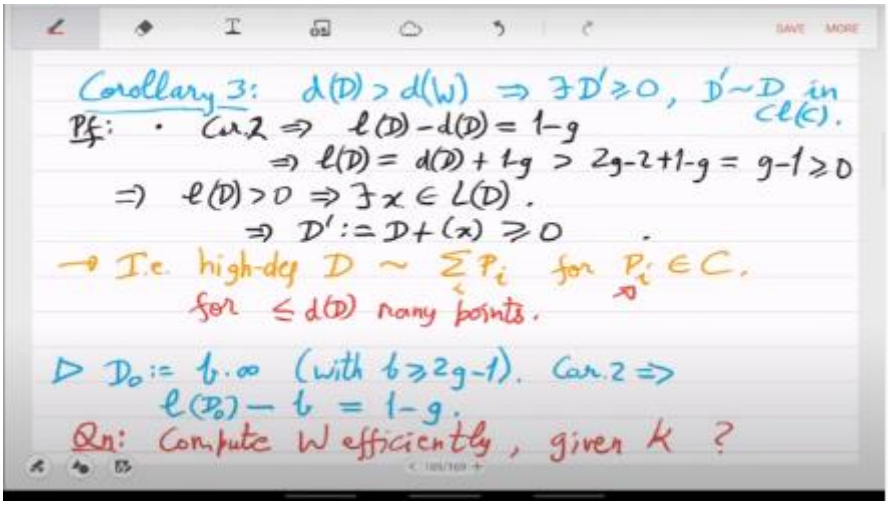
So, let's begin with this." So, it is a single point: the point at ∞ with order \(2G - 1\). Start with this divisor; this is the high-degree divisor. You may ask why we do not know the genus, but we have established an upper bound of D ^{2}. So, there is an upper bound that you know; let us use the bound \(B \). So, start with a divisor, which is simply ∞ multiplied by a sufficiently large number that can be the square of the degree for your curve, and compute \(L_d(0) - d(0) \); this will give you a genus.

So, L D 0 space - B, which is the degree, is equal to 1 minus the genus. So, this is a clear algorithm to compute the genus; it is fast, and you only need to compute this L D. However, I believe B should be the only consideration. We had estimated D ^{2}, which comes from Riemann's proof.

It is D ^{2}. Yes. What is d? The degree of the curve is... So, just from the point at ∞, you can compute the genus using the L-D shift.

You have a very precise bound when it functions. No, but if you know the degree of the curve, there are even more precise formulas that you can compute directly. Sure, if you work hard, you will achieve more; I don't doubt that. So, the last question is one that I have not answered; sometime later, we can discuss this given algorithm to compute w. So, given a transcendence degree one function field, how do we compute the canonical divisor that should follow from this theory? However, I am not sure about the details.

Yes, the last thing is that we do not have much time today. We will meet again tomorrow. The last thing is this: the motivation, I mean, this ∑ pi representation of positive divisors, actually motivates a very important object related to curves, which is this abelian variety—a higher-dimensional object that represents a new property of the class group.



So, let us quickly sketch it out. So, consider the subset of degree zero. Divisors like these exist. So, go over all the subsets of g points on the curve, sum them up, and calculate the degree minus the genus times the point at ∞. So, this is the subset that we call the Jacobian, and it has amazing properties. For example, you can demonstrate that any two points are related. So, it is not just a subset; it is actually an abelian group that is isomorphic to the class group.

So, this is just an explicit representation of Cl_0. So, that is the property for which I think we should at least outline the proof. We can't cover this in detail in this course.

We haven't developed the machinery because it is a higher-dimensional object. It's no longer a curve. So, we want to show that this is, in a way, isomorphic to the class group. This also means that for any two elements in this set, you can add them to obtain a unique third element. I mean, we define the divisor group so that there is a enforced group structure, but that was not very interesting because it was a free group.

So, you were cutting this at these infinitely many points; here, it will be more interesting. Here, it will also be infinite; however, I should say that it is better to think of k as equal to k bar. So, the points p1 to pg represent an infinite number of possibilities. So, of course, this also has infinitely many elements, but the representation is nicer, and there are many more things you can actually do that you cannot do in just the divisor group. So, the first property is this:

However, if you're looking for a slight variation, you could say, "Why should such a thing occur?" So, let us outline the idea. For any divisor, we will call it \(d \) and consider \(\gamma \) as an index parameter for non-negative divisors of degree \(g-1 \). Collect these degree 0 divisors such that the L-dimension of \(d + 2g - 1 - \∞ - d \γ\) is 2. So, I will call this mysterious divisor \(d' \).

The degree of d ‘ is 2g - 1 - g - 1, which gives you g, and the degree of d is 0. So, this is degree g. What is this a subset of? It is a subset of "Well, I guess, yeah, I do not want to see anything more; div 0 is where it lives." Sure! Yeah, so think of a fixed divisor \(d\) and a non-negative divisor of degree \(g - 1\). What is this statement saying. So, being equal to 2 means that there are always these constant functions, but there is a more interesting non-constant function in this L space, right?

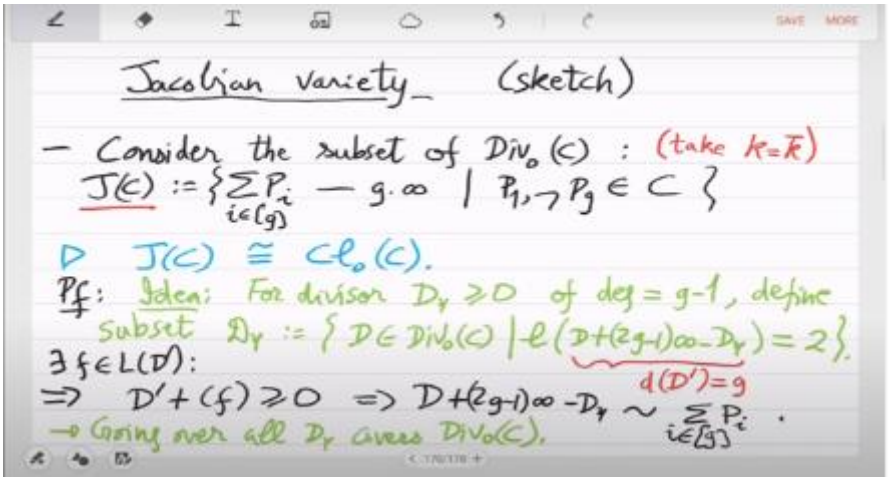
) So, you can add it to this D ‘, and you will get a positive representation; that is what we actually want to use. In this context, there exists a function in the L space of D ‘ such that D ‘ + f is greater than or equal to 0, which means it is a sum of points; D ‘ + f is a sum of points. So, you have essentially written this as \(d + 2g - 1 \∞- d \γ\) and rewritten it as \(\∑ \pi \). However, if you're looking for an alternative phrasing, you could say: "How many points are there?" So, consider \(k \) to be equal to \(\bar{k} \); therefore, the degree of all the points is 1.

The degree of the left-hand side is \(g \), and the degree of \(d' \) is \(g \), resulting in \(g \) points. So this is what the subset is doing: it is collecting all these degree zero divisors, along with something that is fixed, right? This 2G - 1 ∞ - D γ is a fixed divisor. So, don't worry too much about it.

So D + this fixed value is simply the sum of G points. So, what are such D's? You collect them, and then you keep changing the γ. So what you can show is that in the union of these D γs, you will have all div zero C's. That is not very difficult to show, but it will require notation that we cannot develop here. So, going over all D γ covers divides by zero. So, all the divisors \(D \) will be taken into account.

So, basically, you have these patches; as γ varies, these d γ are the patches in which you have partitioned div 0. The thing is that this L d + the fixed term equal to 2 is a linear polynomial system that you obtain in terms of the unknown d.

Yes, that polynomial system will yield a variety, so D will be the solution set of a variety of an algebraic system. Let us express this more elegantly. So, now we can define a nicer-looking set \(C_\γ \), which is the ∑ of these points that we obtained - \(g_\∞ \). \(D \) is in \(D_\γ \), and \(\∑ \pi \) is the result we obtained from the LD function. So, these are the points that the divisors you get from D γ actually correspond to. So, this is a nice object because you can demonstrate that it is a quasi-projective variety.



So, these degree 0 divisors that you have there actually form an algebraic system whose solution they represent. It is still an infinite set because we are in an algebraically closed field. In fact, it is always infinite; the way we have defined points makes it an infinite object, but it is more than just a simple sum. The sum of points is correct; it has now actually become a projective variety. So, C γ is a projective variety, and if you look at the union of all these parts as you go over all the γs, this encompasses everything in C L 0.

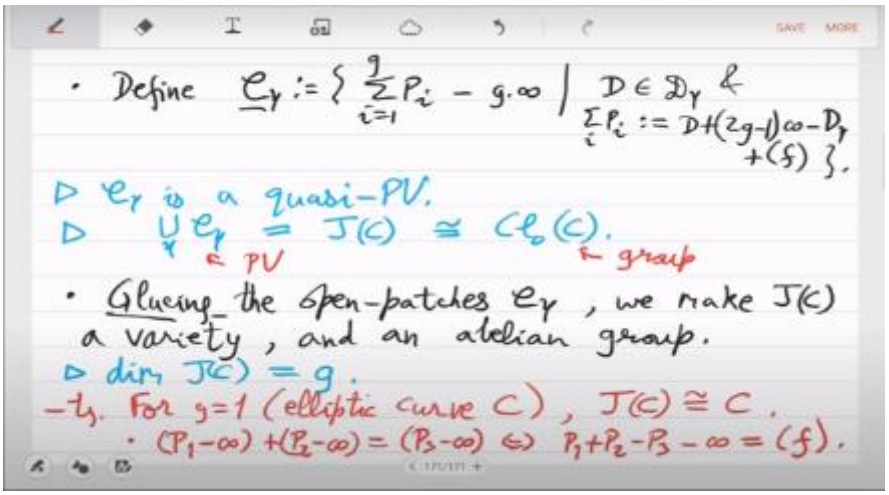
Yeah, that was actually our original definition of JC as well. So this set, JC, is now complete. We have found its patches, which are varieties, and you can glue them together to obtain a single variety. So this JC set is now a variety that is also a group.

By gluing the open patches \(C \) and \(\γ \), we obtain \(J \) as a variety. And an Abelian group. So, there are two parts, two facets of J.C. So, this is the group part, and this is the variety part. So, JC has both these facets: it's a projective variety and also a group; it's called an abelian variety. It has a relatively high dimension, which we can already infer from the fact that you are summing up g generic points, and each point comes from a curve.

Therefore, it is expected to have dimension g, and that's true. For higher genus, this object becomes more complicated. It's a higher-dimensional variety. And yeah, so what happens for genus 1? For genus 1, this is just a single point, - ∞. That's the case of an elliptic curve. So for a genus equal to 1, which is an elliptic curve C, J(C) is actually the curve itself.

In the case of genus 1, the curve is its own Jacobian, which makes this curve an abelian group. That is the reason why the elliptic curve forms an abelian group. It comes from here: how do you add points? So, \(p_1 - \∞ + p_2 - \∞ \) results in \(p_3 - \∞ \), right? This means that you want \(p_1 + p_2 - p_3 - \∞ \) to be a rational function, right? So, you are on an elliptic curve. If I give you two points, p1 and p2, what is this third point, p3? So, essentially, what is done is that you draw a line through P1 and P2, and the reflection of the third point under ∞ will give you P3 because of this minus sign. So, there is a negative P3 here. So, what I mean is, are you

aware of elliptic curve addition? So, for P1 and P2, you can draw a line that may be drawn here.



So, if p1 is here and p2 is here, maybe there is a point here. When you draw the line, the third point that you get makes the line essentially the function. And this is the curve; maybe I should call it L. So, a line is the function that contains points P1 and P2. So, it uniquely defines L, and this point is then in the formula, setting it to - p. This is why a reflection is needed, and that reflection is essentially guided by the point at ∞ in your embedding. The reflection will give you the P3, which is the addition; first of all, it is the Jacobian group addition. The elliptic curve just inherits it—that is the picture.