Computational Arithmetic - Geometry for Algebraic Curves

Prof Nitin Saxena

Dept of Computer Science and Engineering

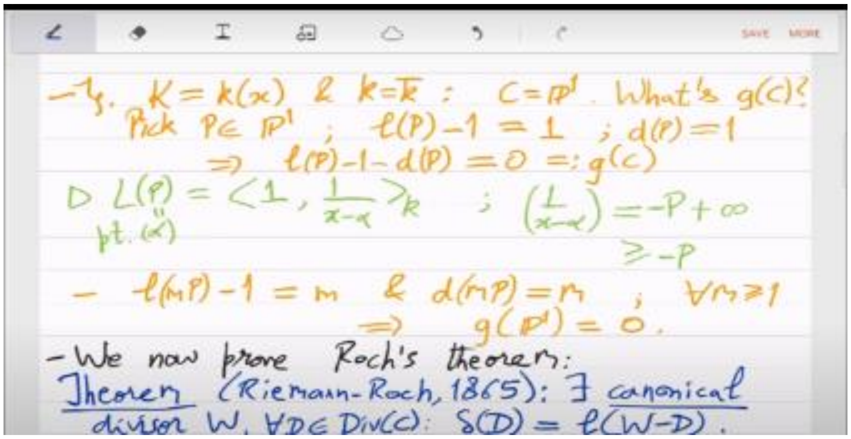
IIT Kanpur

Week - 10

Lecture – 19

Differentials and Riemann-Roch

So we want to prove this theorem Riemann-Roch theorem which says that for any divisor it will give you this equality. The difference of L D with degree of D + 1 - genus is exactly equal to this some other L of some other divisor. Key thing is that this theorem is saying that there is a magical divisor w such that w - d is what you are getting. So this w will be called a canonical divisor in the divisor class group. So there is no reason why this thing should exist. So for that we go via this new object called Adele.



- Eg. $K = k(x)$ & $k = \bar{k}$: $C = \mathbb{P}^1$. What's $g(C)$?

Pick $P \in \mathbb{P}^1$; $\ell(P) - 1 = 1$; $d(P) = 1$

$\Rightarrow \ell(P) - 1 - d(P) = 0 =: g(C)$

▷ $L(\underset{\text{pt.}(\alpha)}{\overset{\shortparallel}{P}}) = \langle 1, \frac{1}{x-\alpha} \rangle_k$; $\left(\frac{1}{x-\alpha}\right) = -P + \infty$

$\geq -P$

- $\ell(mP) - 1 = m$ & $d(mP) = m$; $\forall m \geq 1$

$\Rightarrow g(\mathbb{P}^1) = 0$.

- We now prove Roch's theorem:

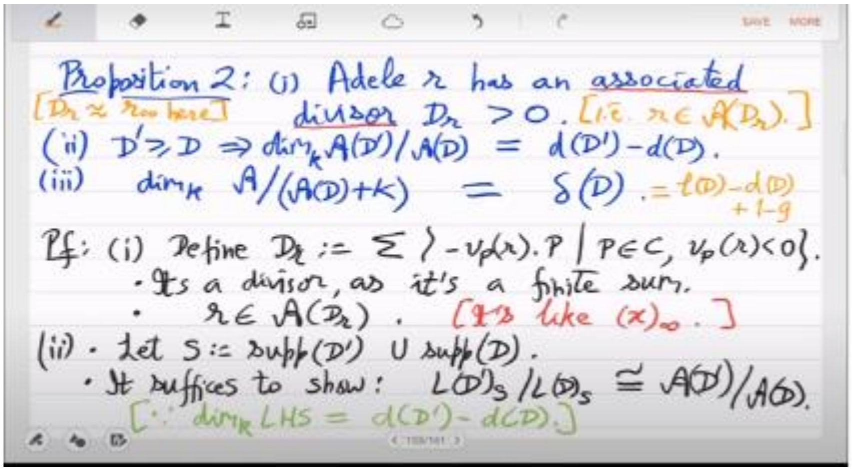
Theorem (Riemann-Roch, 1865): $\exists$ canonical divisor W, $\forall D \in Div(C)$: $\delta(D) = \ell(W - D)$.

So which is just define as a tuple of infinitely many rational functions. Yeah so instead of a single rational function now we are looking at kind of function field raised to ∞. all kinds of tuples and we can define everything that we did with functions. So, we can define valuation with respect to a point, we can define addition, multiplication and hence we can also define the LD sheaf idea and now this is called AD where A is an Adele.

is the ideal and we can look at, so this again will be a vector space and we can talk about its dimension which turns out to be ∞. So, this by itself is not very useful. So, what will be useful is the dual of this which is a modulo ad, this will turn out to be a finite vector space and that so we want to now show that. So, before that we had said that every Adele R has an associated divisor which is kind of this ∞ that we had for functions the poles such that R is in the EDR, ED Basically this r + dr >= 0. So you should be looking at dr as the poles.

 Yes, so think of dr as ∞. So, if r was instead of an adele it was if it was a rational function I think you weren't there for the adele class do you want a. So, if r was a rational function then you just look at the poles and that gives you dr. So, it was we called it r ∞ same thing you can do for adeles also. that is the associated divisor dr, it will be positive, key thing you want is it should be positive and r should be in adr.

 Second property which we have shown is that the dimension is actually degree difference, dimension of the quotient is degree difference. So this is much better than ld ‘ over ld because there you only got an upper bound And third is the most important property which is that AD and A of course these are infinite dimensional vector spaces, but their quotient is finite and it is exactly equal to the degree of speciality. So, this is recall that this is equal to LD - DD + 1 - G. So, for every divisor this thing will be true that is what we are saying. So, let us go to the proof of third property, we had started this.



Proposition 2: (i) Adele r has an associated divisor $D_r > 0$. [i.e. $r \in \mathbb{A}(D_r)$.]

[$D_r \approx r_\infty$ here]

(ii) $D' \geq D \Rightarrow \dim_k \mathbb{A}(D')/\mathbb{A}(D) = d(D') - d(D)$.

(iii) $\dim_k \mathbb{A}/(\mathbb{A}(D)+k) = \delta(D) .= \ell(D) - d(D) + 1 - g$

Pf: (i) Define $D_r := \sum \{-v_P(r).P \mid P \in C, v_P(r) < 0\}$.

- It's a divisor, as it's a finite sum.
- $r \in \mathbb{A}(D_r)$. [It's like $(x)_\infty$.]

(ii) • Let $S := supp(D') \cup supp(D)$.

- It suffices to show: $L(D')_S / L(D)_S \cong \mathbb{A}(D')/\mathbb{A}(D)$.

[$\because \dim_k LHS = d(D') - d(D)$.]

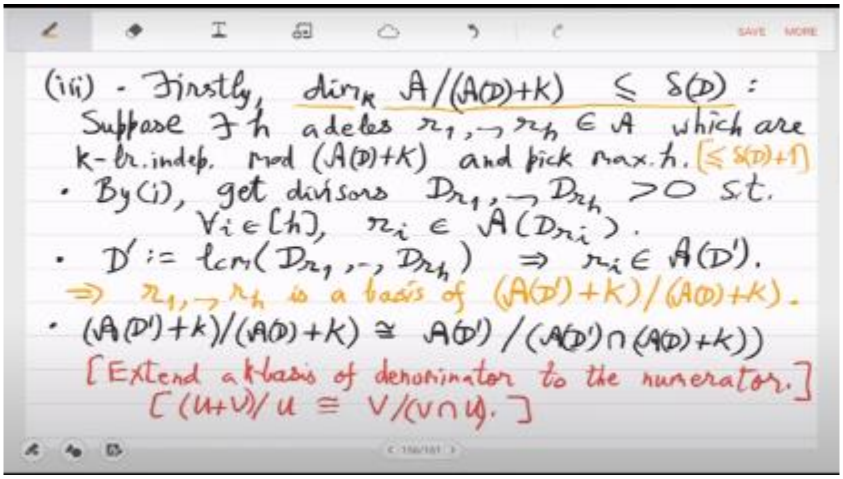
 So, first we show that the dimension of this quotient vector space is at most δ D. How did we show that? Well, I do not think we have shown it. So, we are in the middle of the proof. take a basis R1 to Rh of a mod ad + k and this is each is the maximum possible integer so by the first property you have these associated divisors dr1 to drh ri is in 8 dri take the lcm of this which basically means that these are divisors right so you have for every point there is a order you just pick the maximum and define d ‘ so now every ri is also present in ad ‘ so you have this common divisor d ‘ now associated this continues to be a basis of ad ‘ mod ad because it was a basis of the bigger thing so of course it is a basis of the smaller thing also and it is there, it is present in ad ‘ + k. So we will just do some vector space calculations, some dimension arguments it is nothing to do with complicated algebra.

So here we will just look at Ed ‘ + k mod Ad + k is isomorphic to Ad ‘ modulo this subspace. So what is this? This is just a basically you take a basis of Ad + k Ad + big K take a small k basis And similarly you can take a basis of Ad ‘ + big K, the two there might be basis elements which are common. So the common part is the intersection. So you are removing them. So if you remove the common part what remains is the difference.

So by that you can show this in general for vector spaces. So a mod ad is again infinite, that is the problem here. You can study a, you can study ad and you can study a mod ad but you will still not get close to δ d because they are all infinite. No, no, no, no. So, for example, you can just, yeah, there could be an infinite basis.

So, why do not you just take H to be δ D + 1? Yeah, yeah, but maximum can be maybe, yeah. Once we finish this proof you will see that it won't matter, it will be correct. So let me give this proof, it's a very simple proof. Then you can come back and say that take H to be either the maximum or if it is infinite then you take it to be δ D + 1 say. So maybe I can just write here maximum H < = δ D + 1.

okay so this can be the definition of h maximum you can go up to δ d + 1 and we will show that actually it you cannot you will you can only go up to δ d so you will show two things at once you will show that basis is finite dimension is finite and δ d is an upper bound this proof will prove the things two things simultaneously So let us continue with this right hand side.



(iii) - Firstly, $\dim_k \mathbb{A}/(\mathbb{A}(D)+k) \leq \delta(D)$:

Suppose $\exists h$ adeles $r_1, \ldots, r_h \in \mathbb{A}$ which are k-lin.indep. mod $(\mathbb{A}(D)+k)$ and pick max. h. $[\leq \delta(D)+1]$

- By (i), get divisors $D_{r_1}, \ldots, D_{r_h} > 0$ s.t. $\forall i \in [h]$, $r_i \in \mathbb{A}(D_{r_i})$.
- $D' := \mathrm{lcm}(D_{r_1}, \ldots, D_{r_h}) \Rightarrow r_i \in \mathbb{A}(D')$.

$\Rightarrow r_1, \ldots, r_h$ is a basis of $(\mathbb{A}(D')+k)/(\mathbb{A}(D)+k)$.

- $(\mathbb{A}(D')+k)/(\mathbb{A}(D)+k) \cong \mathbb{A}(D')/(\mathbb{A}(D') \cap (\mathbb{A}(D)+k))$

[Extend a k-basis of denominator to the numerator.]
[$(U+V)/U \cong V/(V \cap U)$.]

So this is isomorphic to or maybe I should copy that. yeah so we are here now what is this, this is ad ‘ mod ld ‘ + ad why is that well so in both these objects so AD is clearly contained in AD ‘ so AD is common beyond AD you only have rational functions in big K right so what are the things which are functions and present in AD ‘ that is by definition LD ‘ fine So from here, from k you get ld ‘. Yes. It is basically u is already present in both numerator and denominator, so u is kind of 0.

So, you have to use V modulo something, but something should be what, it should be essentially the elements of V which are already present in you, because they are to be killed. So, this is true also for infinite dimensional vector spaces, it is a completely qualitative property, you can just think of this a proof as a construction of basis and then finishing the argument, it does not require finite dimensional. Yeah, so now we are reaching, now we have introduced L, L chief and we will just keep doing this, keep improving on this. So, AD ‘ mod LD ‘ gives you what? So basically we want to reach property 2, property 2 is something that we know exactly. So we want to reach ad ‘ mod ad, that is the goal in this calculation.

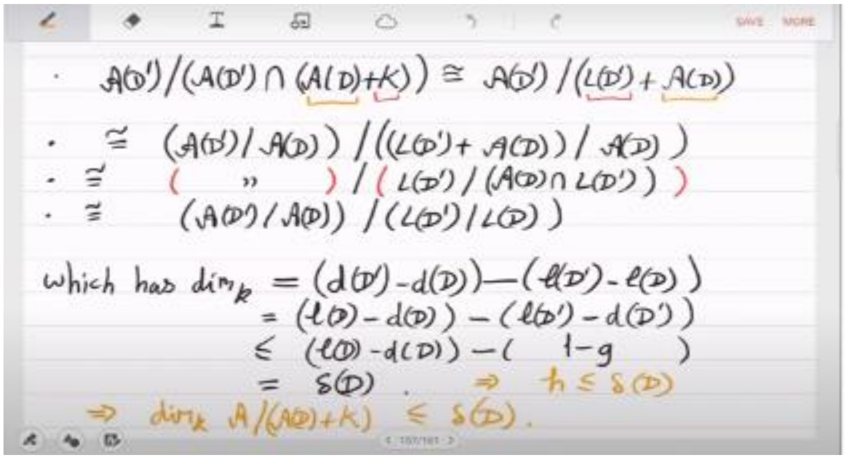
So let us just jump to that, so ad ‘ mod ad, mod ld ‘ + ad mod ad. Now, in this quotient we can all you see that AD is present in the numerator and in the denominator. So, we can take mod both sides and the quotient will not change its isomorphic and which is isomorphic to this thing mod, here again you can do that trick, so intersection trick, right, this is clear. In the modulus you can again do Ld ‘ mod intersection with AD and yes so now you are looking at functions in LD ‘ which are of the type AD which is so you are not looking at ADL you are actually looking at functions which are > = I mean + D ‘ and + D > = 0 which in which basically means that this is just LD. this is something which we now understand better than what the thing that we started with so from here now you can get deduce that the dimension = degree d ‘ - degree d - L d ‘ - L d right.

We know all the I mean we know the first quotient and we know L d ‘ and we know L d. So, we get this by property 2 and properties of L d sheaf and Now we can turn to genus so this is equal to Ld - dd - Ld ‘ - degree d ‘. So, I do not change the first thing and the second one I can say ld ‘ - dd ‘ is the bottom threshold is lower bound is 1 - g. So, we can put that here right and this is the degree of speciality of d by definition. Is there a mistake in this? I think I made a mistake in this comment, it is not 1 - g, g - 1.

Yeah, so ld - dd + g - 1, so that is the degree of speciality by definition. So you have an upper bound. So you have shown that a mod ad + k < = δ I mean this implies that h < = δ d which implies this right. So, I mean your question was that what if what happens in the infinite case. So, in the infinite case you can go up to δ d + 1, h will be that and then you will do this argument, but this argument will actually say that h cannot be δ d + 1, you will get a contradiction.

So, it is h has to be finite. and then this also tells you that each has to be δ d or less. So, it is fine with also maximum with infinite dimensional case. So, we have this first thing we have identified first time we have identified an Adele object which is finite dimensional. So, this is a fundamental construction Yes, so for such a d the degree of speciality will be 0, δ d will be 0.

d ‘ from, yes so but it is not clear how you will do this in an algorithm because these adels are infinite objects. So, it is not clear this how do you work with ∞, a is infinite, ad is infinite. So, this is I mean in the algorithm you have to analyze more which I have not done. But you are correct that, I mean in the end after I have proved more properties, this will give you far more than just genus. You can actually compute, you will actually be able to compute this thing that Riemann-Roch says the canonical divisor W.



$$\mathbb{A}(D')/(\mathbb{A}(D')\cap(\underline{\mathbb{A}(D)}+\underline{K})) \cong \mathbb{A}(D')/(\underline{L(D')}+\underline{\mathbb{A}(D)})$$

$$\cong (\mathbb{A}(D')/\mathbb{A}(D))/((L(D')+\mathbb{A}(D))/\mathbb{A}(D))$$

$$\cong (\quad " \quad)/(L(D')/(\mathbb{A}(D)\cap L(D')))$$

$$\cong (\mathbb{A}(D')/\mathbb{A}(D))/(L(D')/L(D))$$

which has $\dim_k = (d(D')-d(D)) - (\ell(D')-\ell(D))$

$$= (\ell(D)-d(D)) - (\ell(D')-d(D'))$$

$$\leq (\ell(D)-d(D)) - (\quad 1-g \quad)$$

$$= \delta(D) \,. \quad \Rightarrow \quad h \leq \delta(D)$$

$$\Rightarrow \dim_k \mathbb{A}/(\mathbb{A}(D)+K) \leq \delta(D).$$

so for the computation of that which is basically related to a mod ad + k that object you will be able to compute yeah but that's jumping far ahead so we have to right now we actually have to prove now equality with δ d so let's first do that that the dimension of this dual object is at least δ D. So, this is this object is clearly a dual right, LD was the primary object that we had studied and this is kind of A modulo LD. So, it is a dual thing. and we want to show that it is actually an equality. So, all we have to show is that it is at least δ D.

This will be actually much easier to show. So, you know that by Riemann's theorem there exist a D0 such that L D0 - degree exactly equals 1 - g. So consider the LCM of D and this D0, right. So there is a D0 which is given by Riemann, you do not know what it is but you know that it exists. because the place where the it meets the threshold that is called the genus that is what we call 1 - g.

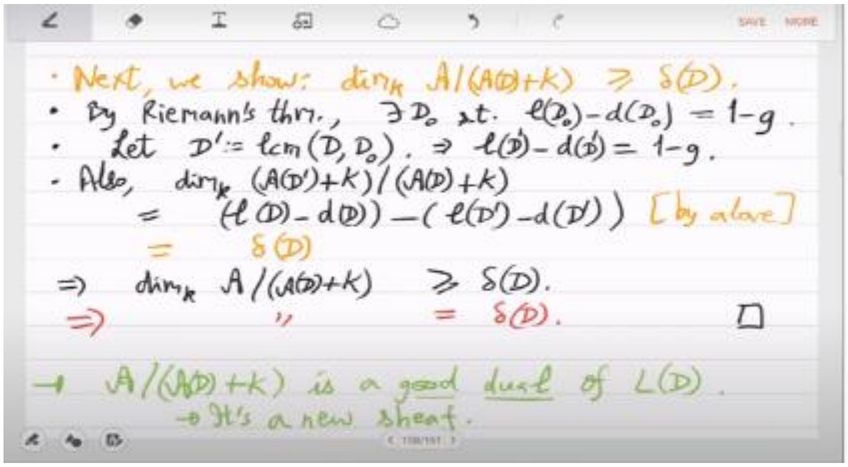
So, by definition d 0 exists by definition of genus d 0 exists. So, if you take the LCM with the input divisor which was d that will you will get a bigger divisor right and the bigger divisor will again satisfy the equality. So, Ld - dd is also equal to 1 - g, because you we have this basic property from Ld sheave that when you increase the divisor the difference reduces, but it cannot reduce below 1 - g, so it will remain 1 - g. So now let us look at the previous calculation which is ad ‘ + k mod ad + k. We had shown that this is the same dimension as the dimension you are interested in a mod ad + k.

no no sorry not it is not the same this is something else but anyways I can calculate this dimension this dimension is is this which is sorry this was d ‘, d ‘ is the bigger one. And which gives me what, no no we have to use this formula that we showed, yeah let us do it in steps, jumping too fast. So, what we had shown is that this equals degree of I mean in the end we got this L - D of big D and L - D - L - D of D ‘, so let us continue using that, so first for D then for D ‘. Yeah, that is what we had proved. We had proved it for any d ‘ actually, any d ‘ > = d.

So, we are using that part of the proof and we know that l d ‘ - e d ‘ is 1 - g. So, this is then equal to δ d. because it is ld - dd - of 1 - g. So, that is the degree of specialities which is the lower bound right, which gives a lower bound for a mod ad + k. So, a mod E d + k is clearly a subspace which is at least as big as the one above.

So, it has dimension > = δ d and the two together mean that this is equal to δ d. Is that clear? Yeah, so this is really a consequence of what you saw in Riemann's theorem and correcting the LD sheaf to AD sheaf gives you equalities. So, use that use genus as the threshold and the proof is not very difficult with all those tools. So this A mod AD + K is a good dual of LD. okay because it tells you about the about the remaining part which was the degree of speciality of the divisor and so ld we were calling the l sheaf ld sheaf similarly this new object is also a you can also call it a sheaf it is the a mod ad + k sheaf.

So it gives a new sheaf. I mean we have not defined what a sheaf is but it is basically it is a vector space that we have now defined and it is a dual of the first vector space we have defined. So we will use this to now prove Riemann-Roch theorem, but we have to finish that proof. What we will do is now we look at the maps, linear maps from this new sheaf to base field k. So we look at the home from this to homomorphism from this to small k. So that will be the beginning of differentials.



- Next, we show: $\dim_k A/(A(D)+k) \geqslant \delta(D)$.
- By Riemann's thm., $\exists D_0$ s.t. $\ell(D_0)-d(D_0) = 1-g$.
- Let $D' := \operatorname{lcm}(D, D_0)$. $\Rightarrow \ell(D')-d(D') = 1-g$.
- Also, $\dim_k (A(D')+k)/(A(D)+k)$

$$= (\ell(D)-d(D)) - (\ell(D')-d(D')) \quad [\text{by above}]$$
$$= \delta(D)$$

$\Rightarrow \quad \dim_k A/(A(D)+k) \geqslant \delta(D).$

$\Rightarrow \quad$ " $\quad = \delta(D).$ $\quad \square$

$\rightarrow$ $A/(A(D)+k)$ is a good dual of $L(D)$.

$\rightarrow$ It's a new sheaf.

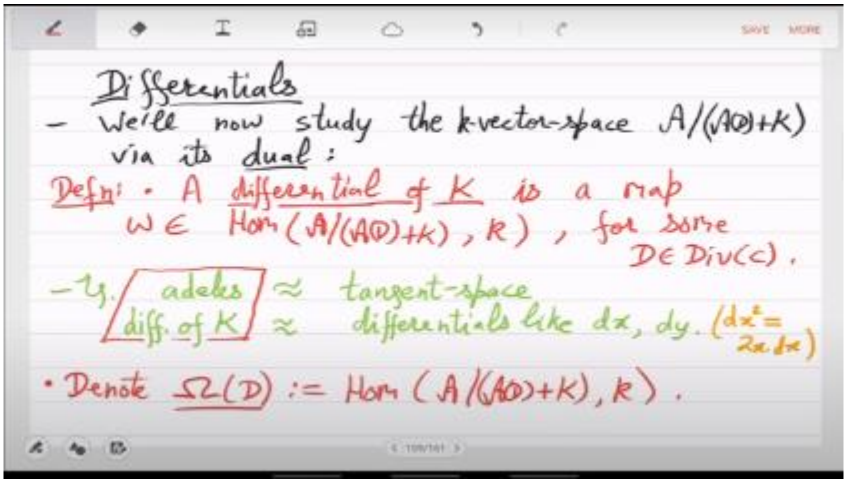
Yeah, so we will now study this object a mod a d + k via its homomorphisms. The k vector a mod ad + k because this is finite dimensional via its dual and what is the dual of a vector Yeah so this kind of we are using dual also in two ways. First we said that we want to have a dual of LD sheaf which is this a mod ad + k and now we will study it, we want to study this so we will study this via its vector space dual which is basically homomorphisms that send elements from here to the base field small k. So that we define as a differential of the function field. So, a differential of the function field k or equivalently of a curve is a map Ω that sends this object to base field small k for some divisor D.

So, for a function field we can define differentials these are basically maps which these are linear maps over the base field small k they send this a mod ad + k big K, these functions are mapped to field values, base field values. These adels in fact, it maps the adels actually into the base field in a linear way. This may be conflicting in your minds with the notion of differential as in derivatives, So, for that you have to recall that a differential in the sense of derivative for example, dx or dy those things are also seen as linear maps on the tangent space. So, tangent space is also kind of a basic sheaf. So, it is a similar idea, but here it is much more algebraic.

and generalized. So, we have actually gone from functions to adels and now at the level of adels we are talking about linear maps. So, basically you have to associate adels with tangent spaces and linear maps on adels as differentials. So Adel is kind of roughly like a tangent space. Then in that vocabulary or in that dictionary, here you have the differentials. like dx and dy that is what now we have defined as differential of k.

So these are the more complicated things. So this is why the name differential is not out of place but of course In the course when we say differential we will mean this, we will not mean the usual engineering dx or dy or d of x ^{2}. So, differentials are these objects which satisfy these identities, d of x ^{2} = 2x dx. So, these are differentials, I mean the key property of differential, Leibnitz rule. But in like even to begin with the differential what you want is you want some linear map on a vector space. So, that vector space in our case is this Adele thing and we are looking at homomorphisms of it to the base field.

So, this must have been the motivation to define it in the times of rock and what good is this for. So that you will see very soon. So we will denote it like this. So Ω of big, so we will actually skip the subscript.



Differentials

- We'll now study the k-vector-space $\mathbb{A}/(\mathbb{A}(D)+K)$ via its dual:

Defn: • A differential of K is a map $\omega \in \mathrm{Hom}(\mathbb{A}/(\mathbb{A}(D)+K), k)$, for some $D \in \mathrm{Div}(C)$.

- Eg. $\boxed{\frac{\text{adeles}}{\text{diff. of } K}}$ ≈ tangent-space ≈ differentials like dx, dy. $(dx^2 = 2x.dx)$

• Denote $\Omega(D) := \mathrm{Hom}(\mathbb{A}/(\mathbb{A}(D)+K), k)$.

Let us just call this Ω d. So this is the home. So, big Ω d is for a divisor are these linear transformations from a del quotient to the base field. This is a set of differentials and now we will study properties of this. So, the first property what can you say about Ω d ‘ and Ω d what is the relationship between them if d ‘ is a divisor at least divisor d so one thing to remember I mean which will help in all our future properties is that you are interested in homomorphisms or maps which have to annihilate ad + k right because you have this mod ad + k so maybe this should be remembered. So any Ω here has to annihilate the modulus which is ad + k. So you are interested in those linear maps on adels that have to annihilate all the functions and they also have to annihilate all the adels which are > = - d right that is what essentially you want.

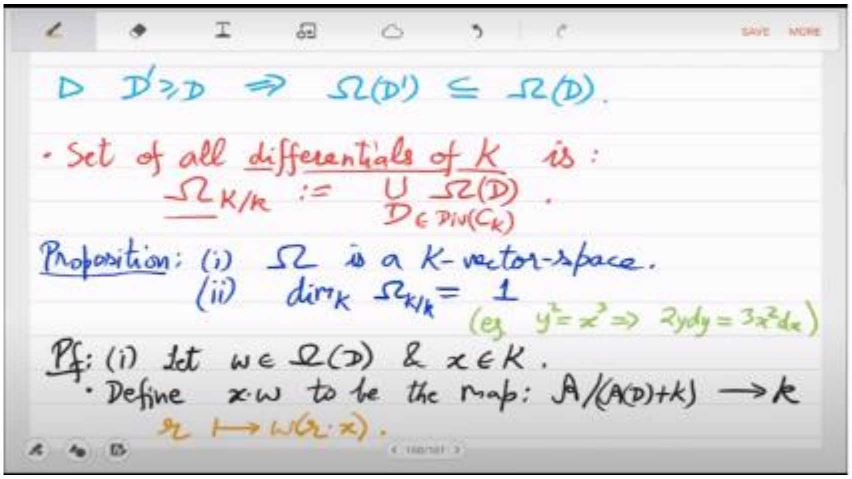
So, if an adel is annihilating d ‘ its I mean ad ‘ its clearly also annihilating ad. So, which means that this is a subset. So, when you increase the divisor you go to a subset. So, it is the opposite direction. So set of all differentials of K is denoted by just Ω and if you want we can put the subscript here K, big K mod small k which is the union of all these.

So, if you go over all the divisors in the in where in the in diff C right. So, big function field of transcendence degree 1 big k over a base field small k defines a smooth projective curve that C k go over all the divisors look at all these differentials that is the big Ω set of all differentials. So that is going to be a very useful object as you will soon see. So the first property is that Ω is a big K vector space. Clearly it is a small k vector space because these are linear maps over small k.

So you add 2 things you get a third differential, but over the function field also it is a vector space and in fact it is a rank 1 vector space. Okay so all the set of all differentials actually is rank 1 over the function field, that is a surprising fact. Although you could have predicted it by the dictionary we had between the engineering differentials and these adele based differentials, because in engineering differential if you remember you have this. So, if $y^2 = x^3$ it means that $2y\ dy = 3x^2\ dx$. So, you can see that there are two differentials dy and dx, but they are dependent Because one you can multiply by a function and get the second one right.

So, because those engineering differentials are dependent you could have predicted that these abstract differentials are also dependent. There is only one which is needed, but the proof is not so easy. Proof has to be more abstract at the level of Adel's because this is a different object So let us do it. First of all why is it a big K vector space, so you have to define what happens when you multiply by a function.

So Ω is a differential and x is a function. so define x times Ω to be so what do you want to do you want to map adels to the base field and you are given Ω right. which is an element of Adele I mean it is a map from Adeles to constants. What should you do with x to define x times Ω? Well the natural thing so Ω when you apply it on an Adele you first multiply the Adele with x and then apply Ω. so an adele r you first multiply r with x this you can do because of function is also an adele, adele can be multiplied so rx is that adele and then you apply Ω. So, that is the obvious thing you should do that gives you another differential from Ω you can get x Ω.



$D \quad D' \geq D \Rightarrow \Omega(D') \subseteq \Omega(D)$.

- Set of all differentials of K is :
  $\underline{\Omega_{K/k}} := \bigcup_{D \in Div(C_K)} \Omega(D)$.

Proposition: (i) Ω is a K-vector-space.
(ii) $\dim_K \Omega_{K/k} = 1$
(eg $y^2 = x^3 \Rightarrow 2y\,dy = 3x^2 dx$)

Pf: (i) let $w \in \Omega(D)$ & $x \in K$.
- Define $x \cdot w$ to be the map: $\mathbb{A}/(\mathbb{A}(D)+K) \longrightarrow k$
  $r \longmapsto w(r \cdot x)$.

So, you know how to multiply by functions now you have to also show. Actually the two things can always be added, so that I think is easy. Oh no, there is one thing, so this big Ω is all the differentials, so they may be for different divisors. So let us also check that.

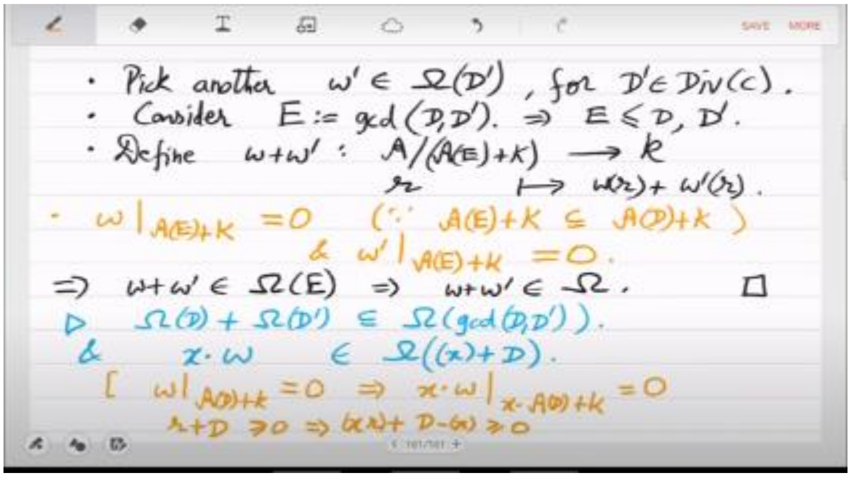
So pick another Ω ‘ which is coming from Ω d ‘. So Ω is in big Ω d and Ω ‘ is in big Ω d ‘ and these d and d ‘ are independent. So now what is the way to add them? This also we have to specify and show that it is again a differential. So, for that we use the usual trick we consider a bigger divisor E which is LCM of D and D ‘ which means that E is at least D and it is at least D ‘. So, pick a bigger one and then what is Ω + Ω ‘.

So, Ω + Ω ‘ I will see it as a map in adele this. So, what it does is that it on r it just goes to Ω r + Ω ‘ r. Well clearly Ω or Ω ‘ are constant you can add them. So, this is a linear map, but you have to check whether Ω + Ω ‘ is annihilating AE that you have to check. So, what is Ω on AE + k. See yeah, so why do not we write that first or maybe the claim is that this is 0, why is it 0 because ae + k is, this is true right.

function adels + e > = 0 implies that yeah correct okay and same thing with Ω ‘. Yes Ω and Ω ‘ in other words are actually differentials over this Ω e. They are differentials in Ω e and you can add them and you will get another differential in Ω e and hence you can add any two differentials. That's all. So I have shown you how to multiply a differential with a function and I have shown you how to add arbitrary differentials over different divisors.

So that is a big K vector space. Now comes this abstraction of the engineering fact that for a curve the differentials are actually there is only one generator. I think I have something I have messed up it should not be like this E < = D should be opposite should be GCD. what was the property for Adele comparison yeah let's check that proposition I think I am using it opposite yeah when the divisor is bigger AD' is bigger sure that was the degree yeah yeah so it's opposite so actually Now it is correct, so since E < = D, AE is actually a subspace of AD, you have to take GCD, you have to go smaller, there Ω + Ω ‘ lives and so it will be good to remember that. so we can remember two things from this proof first is that when you add something in Ω d ‘ where you go is gcd. So sum of two different divisor based differentials is actually contained in the GCD.

 That is what we saw and for a function x when you multiply with differential where you go x + d this is the setting of the proof x was the function Ω was in Ω d small Ω was in big Ω d then where is x times Ω it is here this was in the previous proof first property because we did this R times x. So, you can recover from there. Any questions? not sure about the second property. How do you show this? So, let us say Ω annihilates well Ω we know annihilates ad + k. So, what does x Ω annihilate? x Ω annihilates functions which are here and what where is x times ad flow of function f + d > = 0 then xf is where.



- Pick another $\omega' \in \Omega(D')$, for $D' \in Div(C)$.
- Consider $E := gcd(D,D')$. $\Rightarrow E \leqslant D, D'$.
- Define $\omega+\omega' : \mathbb{A}/(\mathbb{A}(E)+K) \longrightarrow k$

  $r \longmapsto \omega(r)+\omega'(r)$.
- $\omega|_{\mathbb{A}(E)+K} = 0$ $(\because \mathbb{A}(E)+K \subseteq \mathbb{A}(D)+K)$

  $\&\ \omega'|_{\mathbb{A}(E)+K} = 0$.

$\Rightarrow \omega+\omega' \in \Omega(E) \Rightarrow \omega+\omega' \in \Omega$. □

▷ $\Omega(D)+\Omega(D') \subseteq \Omega(gcd(D,D'))$.

& $x\cdot\omega \in \Omega((x)+D)$.

[$\omega|_{\mathbb{A}(D)+k} = 0 \Rightarrow x\cdot\omega|_{x\cdot\mathbb{A}(D)+k} = 0$

$r+D \geqslant 0 \Rightarrow (xr)+D-(x) \geqslant 0$

this implies that xr + d - x > = 0, isn't it? Yeah, so I think it was a mistake, so it should be d - x not x d + x. because these functions x are I mean these adels are greater than equal to x - d so you have to use d - x here fine. These are typos from earlier lecture notes. So, this will be now important in the next part of the proof which is dimension 1.

 Let us start that. So let us pick two differentials from two different I mean two arbitrary divisors dd in Ω big K over small k. We want to show that they are related one is a multiple of the other by a function that is a very powerful claim we are making. So, how will you So it is not as easy as the engineering proof where you just look at the equation of the curve and applied the differential or differentiated the pi variate polynomial. Not just that, you have to use arrows.

You basically have to construct these maps. It has to be a more abstract proof. So, let us what we will do is let us pick a positive divisor E. the thing with positive divisors is that LE is, what is the L dimension of a positive is bounded by the degree right. I think this is also not very important probably to see, but yeah anyways this for a positive divisor the L you can see is at most the degree + 1. and now the abstract proof will be, so consider two k linear maps.

So, one from L D + E and the other from D ‘ + E. So, this map is how do you map a function to a differential so you are given Ω right you have to use Ω so basically that function you should just multiply with Ω that's the plan and here just multiply function with Ω ‘, x ‘ goes to x ‘ Ω ‘. Let us check whether this makes sense, if I take an x in L d + c I multiply by Ω which was in Ω d, what happens where do you end up, x Ω is a new differential and yeah so d - the previous thing we had was d - x right when you multiply by x then you get to d - x Ω d - x so that will be d - d - e so you get to - e and same thing with the second one so you are getting this because d - d + e So you can map functions to this differential. We are doing this because we want to compare Ω with Ω ‘ up to functions.

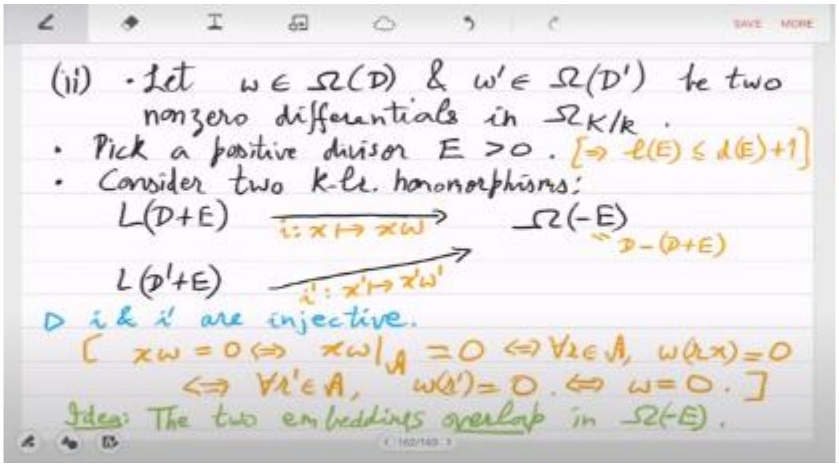
So xx ‘ will help. This map, this picture will help. So first property is that i and i ‘ are injective. Well what will happen if x Ω = 0, the 0 map. See if x Ω goes to the 0 map, so on every adele it is annihilating every adele, then it means that Ω itself must have been annihilating every adele. because x is just a function. So, x Ω equal to 0 implies that it is 0 on every adel actually on every ideal it is mapping it to ad + k, a sorry a - e + k because that is the concept of 0 in Ω - e.

So yeah I think that no that was correct sorry x Ω no no no wait Yeah a - e + k it anyways has to vanish and it anyways has to annihilate and actually it is annihilating now everything. So, it is annihilating all the Adels, right x Ω is a transformation annihilating every Adel which means that for every Adel you are saying that x Ω on R is 0. which is basically saying that Ω on every Rx is 0, but I mean if you multiply an Adele by x this is a kind of a it is an automorphism of Adele's right. So, it actually means that Ω r is 0. When you want to show that Ω r ‘ is 0 you just when you want to show that Ω r ‘ is 0 you just use here r to be r ‘ over x.

r ‘ over x is also an adel. So, from the first property you get the second property. So, these two are equivalent properties. So, which means that Ω is 0, right. So, you have these equivalences.

So, which means that this these two are injective maps. okay. right so but how will this help so injective is almost a trivial result basically you have an embedding of ld + c in Ω -

c and you also have an embedding of ld ‘ + c in Ω - c you have some information about their dimensions so let us compare Suppose you can show that these two embeddings they overlap, they are not disjoint. So, if they overlap then it means that x Ω = x ‘ Ω ‘ for some x and x ‘ which will finish the proof. So, we just have to show that these two embeddings the range is too small. So, these two embeddings actually overlap. the overlap in Ω - e and then we will be done because that will give us x and x ‘ such that Ω x Ω = x ‘ Ω ‘ is that clear.



(ii) • Let $\omega \in \Omega(D)$ & $\omega' \in \Omega(D')$ be two nonzero differentials in $\Omega_{K/k}$.

• Pick a positive divisor $E > 0$. [$\Rightarrow \ell(E) \leq d(E)+1$]

• Consider two k-lt. homomorphisms:

$$\begin{tikzcd} L(D+E) \arrow[r, "i : x \mapsto x\omega"'] & \Omega(-E) \\ L(D'+E) \arrow[ur, "i' : x' \mapsto x'\omega'"'] & \end{tikzcd}$$

$D-(D+E)$

▷ i & i' are injective.

[$x\omega = 0 \Leftrightarrow x\omega|_{\mathbb{A}} = 0 \Leftrightarrow \forall \lambda \in \mathbb{A}, \ \omega(\lambda x) = 0 \Leftrightarrow \forall \lambda' \in \mathbb{A}, \ \omega(\lambda') = 0. \Leftrightarrow \omega = 0.$]

Idea: The two embeddings overlap in $\Omega(-E)$.

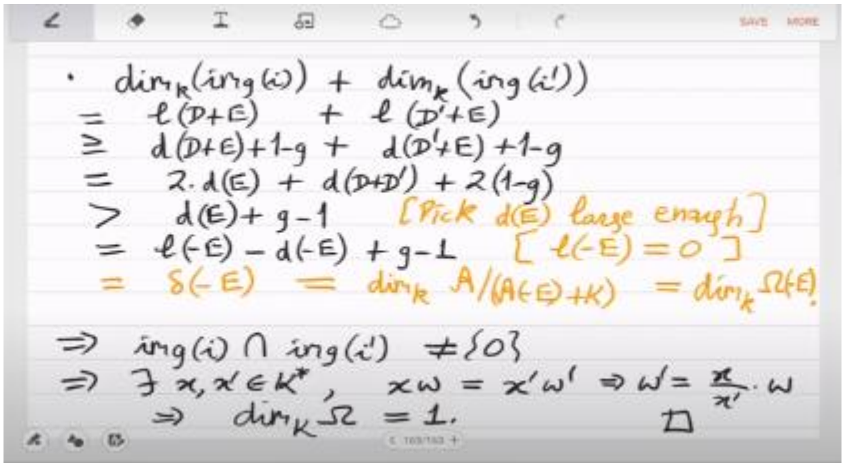
So, let us check that by looking at the dimension of the image of i. and the dimension of the image of i ‘. So, this is equal to image of i is just the l d + e image of i ‘ is just l d ‘ + e. so we have good information about these two so let us write that so this is equal to that this is by Riemann's theorem l cannot be too small I mean l - d cannot be too small it is given by genus. So, these are the lower bounds now degree is very well behaved it is just you can sum these things up. So, you get degree of twice the degree of e + degree of d + d ‘ + twice of 1 - g.

So, it is here that I will make E bigger, I will make it so big that this quantity is at least this. I am allowed to do this because big D and big D ‘ are fixed divisors, we fixed them in the proof E is free. So, I can just pick a very big positive divisor. So, that DE compensates for this negative contributions of 2 1 - G and the whole sum is at least degree of E + G - 1. Okay and what is that, so this is equal to L of - E - D of - E + G - 1, why is that? Essentially I have added only L of - E right, I am claiming that it is 0, why is that 0? Well, E was a positive divisor.

So, you basically are saying that functions which are greater than equal to E. So, there should be no poles and there has to be a 0, but there is no such function which has no poles, but has a 0 except So only functions will actually satisfy, there is no non-constant function. Yeah I think this is the important thing, it is not this le business, it is actually l-e that I want. This is what I wanted in the end, so positive is important for that purpose. so it gives me this in the end this l - d + g - 1 so that is δ - e and by a major proposition δ - e happens to be the Ω e dimension of Ω e. may be one step I write because this we know by proposition is the dimension of a mod - e + k.

Now when you look at the homomorphisms of this two constants you will get as many as the dimension of this so that means it is also the dimension of Ω - e. So what have we shown? We have shown that the two images sum up to more than the dimension of the range.

So we are done. This actually means that the images overlap. It is not 0. They cannot just have 0 as common, they have to have something more because some of the dimension is bigger than the range. So you pick, so this means that there exist xx ‘. such that image of Ω image of x and image of x ‘ are equal and that is that means that means nothing but that the dimension of Ω over the function field is one. So, it is a cyclic vector space rank one. So, note that this we use two things two kinds of dimensions here we used dimension over constant field we also use dimension over using that we got the dimension over the function field.



$$
\begin{aligned}
\cdot\ & \dim_k(\operatorname{img}(i)) + \dim_k(\operatorname{img}(i')) \\
= \ & \ell(D+E) + \ell(D'+E) \\
\geq \ & d(D+E)+1-g + d(D'+E)+1-g \\
= \ & 2\cdot d(E) + d(D+D') + 2(1-g) \\
> \ & d(E)+g-1 \qquad [\text{Pick } d(E) \text{ large enough}] \\
= \ & \ell(-E) - d(-E) + g-1 \qquad [\ \ell(-E)=0\ ] \\
= \ & \delta(-E) = \dim_k A/(A(-E)+K) = \dim_k \Omega(-E)
\end{aligned}
$$

$$
\begin{aligned}
\Rightarrow\ & \operatorname{img}(i) \cap \operatorname{img}(i') \neq \{0\} \\
\Rightarrow\ & \exists\, x, x' \in K^*, \quad x\omega = x'\omega' \Rightarrow \omega' = \frac{x}{x'}\cdot\omega \\
& \Rightarrow \dim_K \Omega = 1. \qquad \square
\end{aligned}
$$

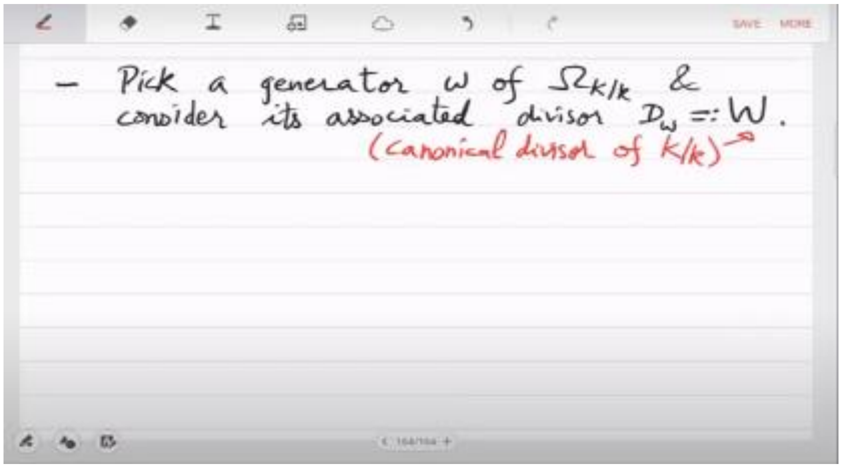
And yeah, so this is a obviously far more abstract proof than what you are used to in engineering by just differentiating. So, this is the proof by arrows. which can be generalized to I mean even more abstract levels, for example in cohomology theories. So, yeah once it is rank, once we have shown that it is rank 1, dimension of Ω is 1, You can talk about a unique differential right and that unique differential in the next class I will say that look for the unique differential look at the associated divisor and that is the canonical divisor and that will finish the proof of Riemann rock.

So, now we are very close to the end of Riemann rock. So, pick and consider its associated divisor. d Ω that is what we will call W right. So, we will formally define this next time it will need some more some more care. because the thing is that it is not unique you can pick a generator multiplied by a function x. So, x times Ω that will have a that can give you a different associated divisor. So, there is actually infinitely many ways to get this associated divisor d Ω neither Ω nor w are unique, there are infinite possibilities.

So, I have to just I have to give a proposition that although there are infinitely many ways they are somehow all equivalent. So, I have to then I can say that canonical divisor is a unique object. So, once we do that we will just prove Riemann rock using this L of w - d, w is a unique divisor. it of course it will know about genus, but it will know much more, it is a very special thing, it knows almost everything about the curve and the function field.

So, this basis a by n + k can this be explicitly reconstructed, can one provide a basis for it. Yeah, that is what Rishabh was. also asking see the thing is once I have defined this canonical divisor I think from that point on I can give an algorithm. So, some more work is needed.

It has many nice properties. Yeah, once you know that it exists and how it exists, then you can use it too. No, no, no, but that is infinite. A is just a infinite tuple of functions. Functions themselves were infinite and now this a mod ad + k, you are not just looking at a mod a d + k right, you are looking at linear maps from these two constants which is like it is very complicated because this the way we have defined this Ω d, the two quotients the two things which appear in the quotient they are infinite dimensional and from there now you are looking at these matrices. This home is actually not matrix sorry it is a vector you are taking a vector inner product with the adele to get a constant so you are looking at vectors over this over adeles so adeles were bad enough now you are looking at vectors over adeles which is even worse yeah so right now it is not clear how will you make this into an algorithm but very soon it will become an algorithm because of the canonical divisor that you will get essentially these although Ω ds are such big there are so many Ωs still ultimately they come from a unique one so instead of working with these things I will just try to compute the unique one and that will know about all of this machinery



- Pick a generator ω of $\Omega_{K/k}$ & consider its associated divisor $D_\omega =: W$.

  (canonical divisor of K/k)