Computational Arithmetic - Geometry for Algebraic Curves

Prof Nitin Saxena

Dept of Computer Science and Engineering

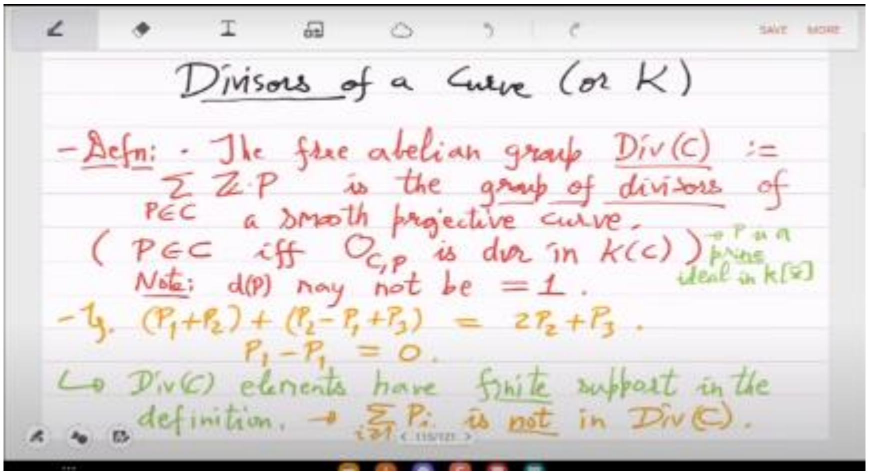
IIT Kanpur

Week - 08

Lecture – 16

Divisor Class Group

So we started long time back divisors of a curve div C, this is the sum of basically a integral combination of linear combination of the points, where points has to be thought of as more general than just an actual point, it is a prime ideal actually. in the let us say bivariate polynomial ring over the base field small k and the function field of the curve is big K. So, these p's are actually you can think of them as just DVR's these are the discrete valuation rings because it is a smooth projective curve. a point, we will always think of it as a DVR or a valuation, defining a valuation. So, we did define a lot of things regarding this. So, div C is the, div C is the, this biggest group, it collects all these points.



Divisors of a Curve (or K)

- Defn: · The free abelian group Div(C) := $\sum_{P\in C} \mathbb{Z}\cdot P$ is the group of divisors of a smooth projective curve.
($P\in C$ iff $O_{C,P}$ is dvr in $k(C)$) → P is a prime ideal in $k[\bar{x}]$
Note: $d(P)$ may not be $=1$.
- Eg. $(P_1+P_2)+(P_2-P_1+P_3) = 2P_2+P_3$.
$P_1-P_1 = 0$.
↳ Div(C) elements have finite support in the definition. → $\sum_{i\geq 1} P_i$ is not in Div(C).

Div 0 is that subgroup which has only degree 0 divisors and div a are those divisors which come from a rational function from the function field. So, there are actually it is not very hard to see that most of the divisors will not correspond to any function, they will just be abstract. sum of points. For example, if you just look at two points p 1 and p 2 and look at p 1 + p 2.

So, p 1 + p 2 there may not be, in fact if you just take a point p, p may not correspond to any function, because if it did say if p was equal to the principal divisor of a function f, then there should also be a pole. but there is no pole p you are only talking about p so single points will actually never correspond to functions you need minimum two points one with one or zero other the pole so we have three things div c div 0 div a div a is for principle divisors and yeah then we had this we defined this l sheaf So this ld sheaf for a divisor is those functions which are not any worse than - d. So the poles are not any worse than the divisor d. It is a way to specify not exactly but approximately you are specifying the poles. You are interested in those functions x.

whose poles have multiplicity no worse than - d. If d had already negative order points then minus of that will become plus. So, you can specify both zeros and poles to some extent it is not an exact. description of x, but it is only approximate. So we are interested, so there will be many x's actually which will satisfy this condition.

So if we collect all of those and this is a very good object, we call it the LDC, we showed that it is actually a vector space. So we showed that LD is a vector space over the base field k. This is simply because if you have an x and y that have poles or that basically the valuation is not any worse than this d, then for the sum also you can prove the same thing because of valuation property. So it is a vector space and more interestingly we can actually compare LD prime with LD. So when d’ >= d, then the L sheaf we can actually compare the dimension of these two vector spaces and it happens to be the degree of the difference.

We proved this theorem and from this actually we showed. Okay we showed two things first thing is important we showed that if divisor D' >=D then the dimension of LD' | LD| is upper bounded by the degree difference. So we have an upper bound on the dimension of any LD that's second corollary and hence we showed that dimension of LD is always finite and we will call it ld. So, ld is the dimension of the ld sheaf it is always finite. So, we prove the finiteness finite dimension of the sheaf ld sheaf.

So, at this point what we have is. we have this ld, small ld which is the dimension and we have the degree of d which is d (D), d (D) and we want to understand their difference, how far or close are they. So that is the question that we will focus on this whole week, that this ld - dd How much can it fluctuate? For example, it can become as small as possible. Can it become arbitrarily negative? You can also ask the same question for positive. Can it become arbitrarily large? So, these are the two questions.

Can it become arbitrarily large and can it become arbitrarily small? Okay, we will focus on the small question first because Riemann studied it and completely solved it. Why do you want to study this question? I do not. So, Riemann was the one who studied this question. So, in 1800s Riemann gave a.

.. What is the... Well, how small can the L sheaf be compared to the degree of the divisor how few functions can LD sheaf have. So, can the LD sheaf be very small or can it be very large.

So, Riemann focused on the small question first, can the LD sheaf be arbitrarily small compared. So, when we say small we are comparing with the degree, because we have these upper bounds which we showed before that LD sheaf is kind of upper bounded by degree. So, which is why the fluctuation on the upper side is kind of already understood. It is only the fluctuation on the lower side which we have to understand. So, Riemann studied that question and showed that actually it cannot fluctuate too much.

There is a range in which it fluctuates and the bottom range will be called genus. okay that is the algebraic definition or arithmetic definition of genus that we will. d (D) is the degree. D yeah d (D) is the degree, where you have to account for not only the order of a point, but also degree of a point. So, it is sigma order of a point multiplied by degree of a point.

So, actual points are degree 1. and these cloud of points are higher degree, you have to collect the conjugates. If you are not in an algebraically close field otherwise everything is degree 1, every point is degree 1 I mean. Any quick questions? So, we will prove some technical results. which are quite important to move to Riemann's proof for genus, in fact Riemann's invention of genus even.

So, we first try to understand how many zeros or poles can a function have. So, degree of principle divisors, let us define that. So, for a rational function x in the function field big K non-zero x, define the divisor of zeros as x 0. So, these are the zeros that the function has with the multiplicity.

So, it is just this. So, it is the sum of valuation times p for positive valuation which means that p is a of X with multiplicity VP, VPX, right. So, that is an element in the divisor group, in the absolute divisor group and similarly divisor of poles. So these are the poles which means the valuation is negative. We will call this x ∞ . So it is the - of negative valuation.

Why do I put - because I want these two to be positive divisors. So, x sub 0 every order is positive and x sub ∞ every order is positive because Vp was negative I make it positive. So, these are both positive divisors. It is in div C and it is a positive divisor. So divisor of zeros and poles.

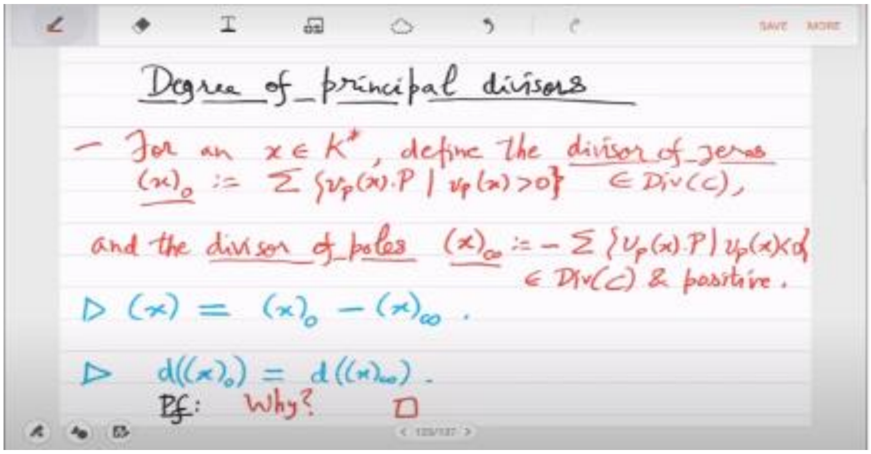
Oh, but that we have seen since the first month. Any rational function, how many zeros can it have with multiplicity? So even in the algebraic closure case the zeros can only be finitely many with the multiplicity. So the sigma that I am doing is actually always finite. I mean in div C you can only add finitely many things.

It's a free abelian group. So this sigma has to be finite and that you can just use our results which we have been proving since first month. that a rational function has only finitely many zeros and also analogously or symmetrically finitely many poles counting multiplicity. So, the points p for which valuation is non-zero or overall it is finite. So, finite sum and what is the relationship between the principal divisor of the function. How is it related to divisor of zeros and divisors of poles? So, zeros are given by this part and poles are given by this part.

So, this is the relationship. It is an obvious thing. You sum up the zeros and take the difference with poles, subtract the poles so okay why did we do this so the goal is to prove that or to understand what is the degree of either of these what is the degree of x0 and what is the degree of x $_\infty$ right how are they related can you show that what is the relationship between degree of x0 and degree of x ∞ yeah what is the proof how do you prove this yeah so formally you look at 1 / x So degree of 1 / x, zeros of 1 / x are the poles of x. That is the key thing, 1 over x is again a well defined function on the curve. in the function field of the curve. So, if you look at the 0s those are actually are the poles.

So, I mean even without the degree 1 / x 0 = x ∞ , these two divisors are the same, their degrees are the same and how does that relate to x 0? Yeah, so maybe we prove the more fundamental thing. So, - x0 is 1 / x0, wait what But how do I convert this into x ∞ ? Yeah, I think that part is wrong. so degree of x 1 / x is degree of x ∞ and I want to say that it's the same as degree of x0, but why is that or maybe let's put it in the middle. I do not know how to prove it right now. Let us just continue with a bigger theorem.

This will follow. For now it is just a curiosity. Let us leave it at this. We will actually prove something much stronger about the magnitude of degree of x0 and degree of x ∞ in the next theorem. Let us do that first. what we will show is that for every rational function these 2 degrees are equal to the field extension.



Degree of principal divisors

- For an $x \in K^*$, define the divisor of zeros $(x)_0 := \sum \{v_P(x) \cdot P \mid v_P(x) > 0\} \in Div(C)$,

and the divisor of poles $(x)_\infty := -\sum \{v_P(x) \cdot P \mid v_P(x) < 0\} \in Div(C)$ & positive.

▷ $(x) = (x)_0 - (x)_\infty$.

▷ $d((x)_0) = d((x)_\infty)$.

Pf: Why? □

Okay so what is this field extension this is the function field of the curve that is we call it big K and small k is the base field you can also think of it as finite field or algebraically closed field whatever attached with x so since x is a non-constant function small kx to big K is actually a finite, it is an algebraic extension, it is a finite extension because small x is a transcendental element and this is a transcendence degree 1 field. So, this is a finite number and degree of this function field is exactly equal to the degree of the poles and the zeros. So, this is a major result, it tells you a lot about the divisor, the principal divisors. and this will also actually subsume the proof of Riemann's theorem for genus.

So, let us do this in detail. So, let n be this degree. which we know is finite because of transcendence degree 1. So, we are only looking at function fields of transcendence degree 1 which is why this is a given and D be the zero divisors of zero x zero with support s. Informally you can see that first the degree of x zero is the number of points.

Number of zeros yeah. So, it should give the extension degree of x. No it is not, it is not at all, I mean may be people guessed it like that, but it is very far from a proof. The problem is that there is no easy way to tell or to interpret the extension degree, big K over small kx. I mean because if you think of a planar curve, it is given by a bivariate polynomial f (x) , y = 0. So, your big K is just Kx |f (x , y)|.

It is just this quotient ring. What is its degree? You do not have any interpretation. Its degree over Kx. Also x is an arbitrary function and you are the curve is given in some other variables let us say u , v. So, f of (u , v)= 0.

So, from that it is not so easy to do this. This is a fairly general statement about transcendence degree one fields, but you are right that in very special cases you can guess it. because I mean if you just look at a univariate, trivially the zeros over algebraically close field at least, the number of zeros is equal to the degree right, I mean with multiplicity I mean even for x to the 10, the number of zeros with multiplicity is 10 and the degree is also 10. So, what Deepthujit is saying is we are trying to achieve that. but in a very general case, nothing here is univariate, this is all a very complicated situation. So, you will see the proof will be quite long and very indirect.

So, and it will use the LD sheaf, we will actually work with the LD sheaf that will be utilized here. So, big N is basically the, it will give you the number of basis elements, right. Big K you can think of it as a vector space over small kx and you get that vector space as dimension N. So, we will use that. that the degree of the divisor, the divisor of zeros is upper bounded by big N and then will lower bounded by big N.

So, there are two parts in the proof both are quite long. So, let . Yeah, you can take up primitive element y, yes and so then you can think of y as satisfying f (x , y) = 0 equation. Now, you will be talking about the degree of y then.

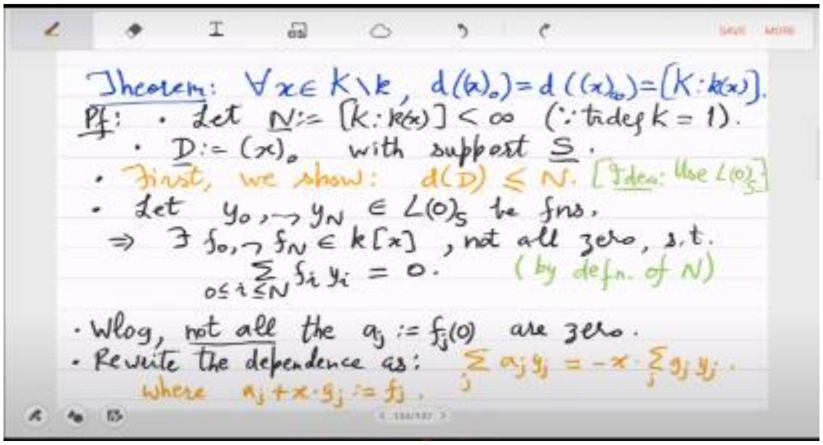
This extension degree is the degree of y. How will you relate it to zeros of x? That is not clear. No, if the primitive element of big K is y, there is a single polynomial f(x,y) equal there is this planar curve description, but we are only talking about the degree of the extension, there is no Galois, we never talk about Galois anywhere in the course, may be only in April we will talk about Galois, here it is just a general field extension. So, it is not clear that degree of y, what is degree of y to do with zeros of x or poles Yeah I mean maybe once you see the full proof you will have some interpretation but I can't start with that because this really needs a proper proof. So here the idea will be to use the L0 sheaf.

for some reason using L0 sheaf here will be helpful. So, what we will do is collect n + 1 functions y0 to yn from the L0 sheaf. and since I mean obviously they live in the function field big K and since they are n + 1 many they are linearly dependent. So this means that there exist f0 to fn polynomials in one variable x not all 0. such that sigma f i y i is 0. So, this is just by the definition of n wait sorry I made a mistake l 0 s these things are tricky.

So this is by definition of S, by definition of N. So L0 sub S recall it is saying that when you look at the valuation of these functions with respect to points that are in S, they are all non-negative, they are not poles. This is all we are saying, I mean for now it is not important, what is important is that for n + 1 functions, any n + 1 functions there is a dependence by F i's being univariate in X and from this dependence now we will conclude some interesting things. No, no, no for any n + 1 functions there is a dependence because dimension is begin that is all. I mean as I do more calculation L0s will be used.

right now we are not using it. You will see how it will be used. So, we can assume here that not all the fj0 are 0. Because if all these fi0s are 0, I mean fi remember is a univariate in x. So, if all these are 0, then it means all of them are divisible by x, then I can as well divide by x and recalculate. So, after a while since f i's are finite degree you will get to a situation where you have a dependence, but let us say f 1 at 0 is not 0.

This is easy just by division by x both sides. So, we can rewrite this. as sigma aj yj equal to - x times gj yj, where aj + x times gj. is fj. So, I can break fi into the constant part and the non-constant part with respect to x. Constant part is aj and the non-constant part is multiple of x, x times gj and not all the ajs are 0.



Theorem: $\forall x \in K \setminus k$, $d((x)_0) = d((x)_\infty) = [K : k(x)]$.

Pf: • Let $N := [K : k(x)] < \infty$ ($\because$ trdeg $K = 1$).

• $D := (x)_0$ with support S.

• First, we show: $d(D) \leq N$. [Idea: Use $L(0)_S$]

• Let $y_0, \ldots, y_N \in L(0)_S$ be fns.

$\Rightarrow \exists f_0, \ldots, f_N \in k[x]$, not all zero, s.t. $\sum_{0 \leq i \leq N} f_i y_i = 0$. (by defn. of N)

• Wlog, not all the $a_j := f_j(0)$ are zero.

• Rewrite the dependence as: $\sum_j a_j y_j = -x \cdot \sum_j g_j y_j$.

where $a_j + x \cdot g_j := f_j$.

So, this left hand side is non-zero. I should not say the whole thing is non-zero, but one of the edges is non-zero just remember that. So, this implies that for all the points in S, the valuation of left hand side which is sigma aj yj is equal to valuation of x + the valuation of sigma g j y j. This is just the, just severely apply valuation both sides. Since you have x times something, valuation will become additive, will be additive on that. And what do I want from here? So, this is at least minimum over all the j's, valuation of g j and valuation of y j.

So, first thing is valuation of x, second is it is a sum, valuation of sum. So, it will be +. So, valuation of summoned is valuation of g j + valuation of y j and over all the j's the minimum can be used, that is just valuation axiom. Yes, so what can you say about valuation of g j and valuation of y j with respect to the point, g j is a univariate.

in X. So, I claim that both of them are greater than equal to 0. Do you believe this? So, valuation of yj >= 0 because of the assumption that we have not used that all the y's are in L0 S. So, because of that it is >= 0, P is a point in S. Why is valuation of g j non negative? That is because g j is a polynomial in x, if valuation of p is negative then p has to be a pole. The only pole of a polynomial is can be point at ∞ , but point at ∞ is not in So, pole of g j can only be infinity , point at inifinity , but that is not in S, because what was S? S was the 0 of x.

and we are using x in g j correct. So, because of that. So, now we can continue the calculations. So, this is then at least v p x which is the order of d at p. So, this means what? So, this actually this whole calculation tells me something about the function sigma aj yj. So, this tells me that sigma aj yj j0 to n is in an l sheaf which is l - d s. Okay, because I went over all the points in S and I have compared the valuation and it is at least, it is at least - of - of d, that is d.

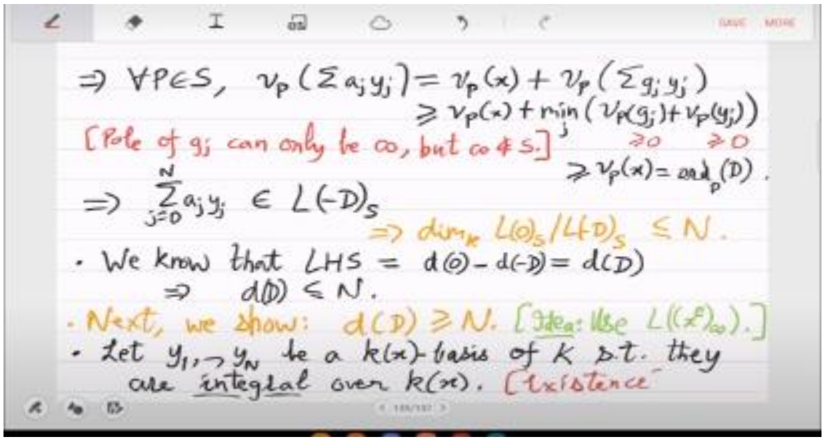
Right, so we started with y's which were in L 0 S and we have ended up with this combination of y's which is in L - d S. So, what have we deduced? So, we have deduced that the dimension of the quotient space is less than equal to n, because If you take any n + 1 functions in L0 S mod L - dS, there is a linear combination that kills it and the linear combination only uses constants a j's which is in the base field small k. So, we have shown that dimension of this quotient of L sheaf is at most n and Now we are done because we know that the left hand side here, this was a lemma we showed for any finite s, we exactly know the dimension of the quotient. It is the degree of 0 - the degree of - d which is degree of d. So, which means we have shown that degree of d is less than equal to n that was the goal.

So, we have upper bounded the degree of the divisor of 0s of x. Is that clear? So, this is not a trivial proof, not a direct proof. You are actually looking at a basis of functions of the function field. It is not, there is no good interpretation of this. It is really an algebraic proof of the field extension.

So, next we will show that degree of D is lower bounded by n. Here the idea will be the opposite. Again L sheaf, but the L sheaf that we will use here is very different, we will use x ∞ . So, instead of l 0, we will actually look at this x ∞ and we will use some very large exponent e, from this we will get the lower bound of degree. So, previously we started with n + 1 functions, now we will use, we will again start with a basis. let y 1 to y n be a k x basis of the function field such that these y i's are integral over k x.

So we need a basis, but we also need them to be integral. What is the meaning of integral? We have seen it before when we were doing geometric interpretation, the geometric part of first month. So integral basically means that, see every element in big K is algebraic over small kx.

So there is a min poly. for Y1. So, I want that main poly to be monic. So, why will such a basis exist with monic main poly. So suppose you got a y1 whose minpoly is this. So over the univariate polynomial ring, the main poly is this. The problem is that this leading monomial y1 ^{2} has coefficient x.



$\Rightarrow \forall P \in S, \quad \nu_P(\Sigma a_j y_j) = \nu_P(x) + \nu_P(\Sigma g_j y_j)$

$\geqslant \nu_P(x) + \min_j(\nu_P(g_j) + \nu_P(y_j))$

[Pole of g_j can only be ∞, but $\infty \notin S$.] $\quad \geqslant 0 \quad \geqslant 0$

$\geqslant \nu_P(x) = \mathrm{ord}_P(D)$.

$\Rightarrow \sum_{j=0}^{N} a_j y_j \in L(-D)_S$

$\Rightarrow \dim_k L(0)_S / L(-D)_S \leq N$.

- We know that $LHS = d(0) - d(-D) = d(D)$

$\Rightarrow \quad d(D) \leq N$.

- Next, we show: $d(D) \geqslant N$. [Idea: Use $L((x^{\ell})_\infty)$.]
- Let $y_1, \to y_N$ be a $k(x)$-basis of K s.t. they are integral over $k(x)$. [Existence

We want it to be 1. How do you make it 1? I mean if you divide by x then the problem is that you will get 1 over x times y1. You do not want that. So what do you do? So the simple trick is you instead of y1 ^{2} y1 you should look at x times y1 that will be integral because you multiply this by x. So you have x ^{2} y1 ^{2} xy1 + x ^{3} equal to 0 which means that xy1 whole So in terms of xy1 if I see it has a monic min poly, so xy1 is integral. So, use this transformation whatever is stopping you from integrality which is the leading coefficient you multiply by that I mean some power of that and then use y1 multiplied by 8, y will still be a basis, it will still be a basis element because you have only multiplied by univariate in x which in your word is a constant.

right small kx is your base kind of the base field in this extension. So, you can multiply by whatever constant you want basis will not change. So, from a basis you can go to an integral basis. So, we have that and So notice that x i y j when you multiply by x is to this basis you get this set let us call it b. these functions are k linearly independent for any t. I have changed the linear independence here, I am talking about now small k, the field of constants.

y1 to yn was the basis over kx. So, it obviously means that if you multiply by x powers these functions xi, yj they will be independent over the base field of constants small k. Small k is think of it as a finite field. There cannot be a dependence of these xi, yj because if there was a dependence then the ys will be dependent over kx. which will contradict the definition of the basis, is that clear.

So, I can change the kx to k and I can multiply by xi's as many as I want. So, I multiply up to t, this t is a parameter you will see that it will give an interesting proof, will take t to be ∞ . So this is clear. The other property I want you to see is if y is integral over kx and has negative valuation. then x has negative valuation.

This is not very difficult to see, let us quickly check this. Sir. Yes. Sir, earlier the k e n dependent on periodic Yeah, some very big number t. No, no y is given, y is fixed, y is this, sorry where was that, yeah the last line y1 to yn they form a kx basis of the function field. I mean just read this line what this is also saying what it implies is that if you multiply yi's by x to the j's then they are independent over the field of constants. oh whether y can y1 be 1 over x you are saying. No, no, but such a thing can only be 1, I mean it only y1 can be 1 over x, others then also have to involve, see 1 over x in kx is kind of 1 right, it is a unit.

So, it will only be a scaling. So, 1 over x if you multiply by x to the i. No, you do not need to remove it. Oh, you are no see. So, let us take y 1 to be even simple just 1. When you multiply it with x to the i, you get x, x^2, x^3, dot, dot.

These are independent functions over constants. You get them independent over constants because x is a non-constant. No, no see it says k linear. No, first of all algebraic independence is nowhere being used. Yeah, we never, we started in the theorem premise just a non-constant x, big K - small k.

why is this big k over kx finite degree extension, because of the transcendence degree one. So, that is the only place where I said anything about algebraic dependence or independence. I am thinking like the example like 1 by x.

Everywhere else it is linear dependence. x is to m, this is linear independence. Exactly. This is algebraic independent over. Exactly. Yeah. that is algebraically independent. So, I see should I say that small k is algebraically close then because otherwise it may be a problem.

No, I think since you have mentioned this is now important that I call this, this. See I want my results at least in this part of the month to work also for k to be a finite field. So, in that case I do not want you to take x to be just a element in bigger finite field. I want you to take x to be a genuine function. So, I should subtract out k bar.

It is only then that I can claim algebraic like a transcendental function. x is a transcendental function. It is important to have this actually. This is a very simple property, again let us just see it in an example. Suppose the integral dependence that you have or min poly you have is $y^2 + xy + x^2 + 1$ equal to 0. The key thing is that the leading monomial y^2 comes with coefficient 1 and then you have univariate in x.

First is x, the other is $x^2 + 1$ and so on. Sorry, it is not ∞ , it is 0. So, if the valuation of y is negative, what does it mean? I want to deduce that x is also negative valuation. This simply follows from the fact that, see you see 4 monomials y^2, xy, x^2 and 1 and their sum is 0. So, y^2 valuation has to be equal to one of the other 3 valuations is equal to Vp of one of the other three. So, let us do it case by case. So, if the valuation of y^2 and xy is the same, then clearly you get that valuation of x is negative.

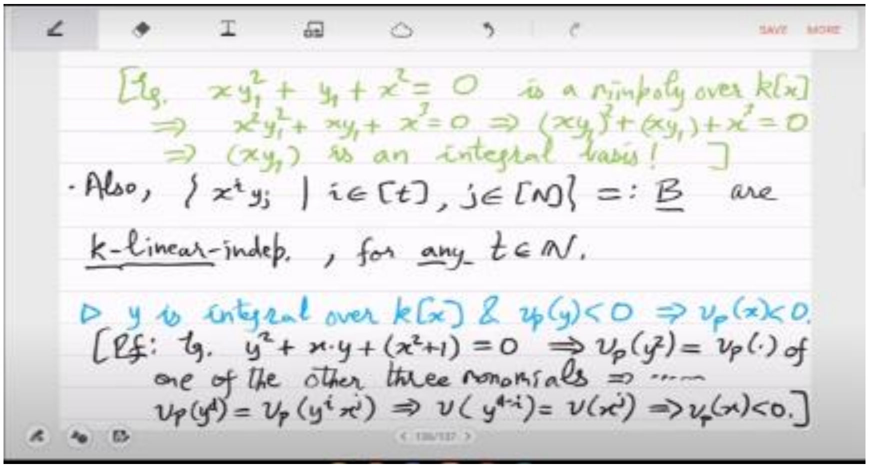
If valuation of y^2 is the same as valuation of x^2, then again you get that x is negative. and if valuation of y^2 is equal to valuation of 1 then you get a contradiction. No, no, no, I am not making an exclusive statement I am saying that valuation of y^2 is overlapping with something and whichever thing it overlaps with gives you the same result which is that valuation of x is negative. Is this clear? You can look at the three cases here and you can see that everything works. Even simpler, just focus on y^2 and look at the cases, valuation of y^2 equal to valuation of xy or x^2 or 1.

So, some of these cases are impossible other cases give you x negative. Same thing. No, no it is same thing you look at y to the d and when you compare with some other monomial either that monomial is an absolute constant like 1. That is a contradiction. Non-constant monomials either already have a y to the i. or its y to the i times x to the j, x to the j will give you negative x valuation.

Not clear, then we have to do it the painful way. So, essentially what you learn is that valuation of y to the d is valuation of y to the i x to the j, which means that valuation of y to the d - i is equal to valuation of x to the j. No, this is the exact proof. You compare y to the d with y to the xj, i is less than d. We are using integrality here very critically, it is an integral dependence.

So, i is less than d and d - i is positive. So, LHS is negative, valuation of y power is negative, while on the RHS you have valuation of x to the j. Now, j cannot be 0, it has to be positive.

When it is positive, valuation of x is negative. That is all. So, that is a general proof as well. So, this is just a technical result. Now, how will we use it? So, what this tells you is, since the y j's that we have picked they were integral. their poles, their poles are shared by x, that is all it is telling you.



[Eg. $xy_1^2 + y_1 + x^2 = 0$ is a minpoly over $k[x]$
$\Rightarrow x^2y_1^2 + xy_1 + x^3 = 0 \Rightarrow (xy_1)^2 + (xy_1) + x^3 = 0$
$\Rightarrow (xy_1)$ is an integral basis!]

· Also, $\{x^i y_j \mid i \in [t], j \in [N]\} =: \underline{B}$ are <u>k-linear</u>-indep., for <u>any</u> $t \in \mathbb{N}$.

▷ y is integral over $k[x]$ & $v_p(y) < 0 \Rightarrow v_p(x) < 0$.
[Pf: Eg. $y^2 + x \cdot y + (x^2+1) = 0 \Rightarrow v_p(y^2) = v_p(\cdot)$ of one of the other three monomials ⇒ ……
$v_p(y^d) = v_p(y^i x^j) \Rightarrow v(y^{d-i}) = v(x^j) \Rightarrow v_p(x) < 0$.]

So, poles of yj are shared by x, you should read the previous probability like this and from that it follows then that for large enough s the divisors x to the s + t poles of this + the poles of that basis x i y j for all i's and t's.

for all i's and j's are all positive. So, let us read this in the following way. So, x to the i yj is what I am interested in. the only thing that stops it from being positive are the poles. Now, the poles come either from x to the i or from yj, the ones which come from x to the i they will be made positive by x to the t, x to the t the divisor of poles of that will make the poles that come from x to the i, make them positive and for yj we have shown whatever is a pole, it is also a pole of x. So, x to the s, s is big enough, it will make yj poles positive.

Otherwise, what would happen is that the y^2 in the example may be sitting with an x^3 for example. So, when you compare x^3 y^2 with other monomials, you do not get a property on valuation of x. Integrality is given as like 1 x like y raise to t. Yeah, because y^2 is free of x. When we say integral means that all the roots of this are in.

Let us go to the place where I talked about integrality. the existence of an integral basis. What did I say here? Maybe I should have redefined it. I just want the minpoly of y1 to be monic over the polynomial ring kx. I want it to be monic that is all. It is not about integral closure or anything. So, tell me this, is ^{2} root 2 integral or not? No, no, obviously you know, I am asking them, because they are confused about this.

So, ^{2} root 2 is integral right, because it is min poly is x^2 - 2. But what, but is 1 over ^{2} root 2 integral? 1 over ^{2} root 2 is not integral because it is min poly is 2x ^{2} - 1. So, integrality is a concept of eternity. I mean this always, integrality always means that somehow when you look at the min poly it is monic.

There is no fractions involved. So, it is the same concept. And now you see why it is important, in this proof it is important because y^2 has to come with 1. If it came with x multiplied by x then you get some, then the last line you get into trouble. Min poly over the, I mean the polynomial in x and y1.

polynomial in x and y, y1 I do not want fractions here. You want the minpoly of y1 right. Minpoly of y1 yeah. So, a priori these other coefficients they could be stuff like 1 / 2. No, no, no, no in the integral definition I want a polynomial in x and y1 that is what I mean by minpoly, it is a polynomial in everything.

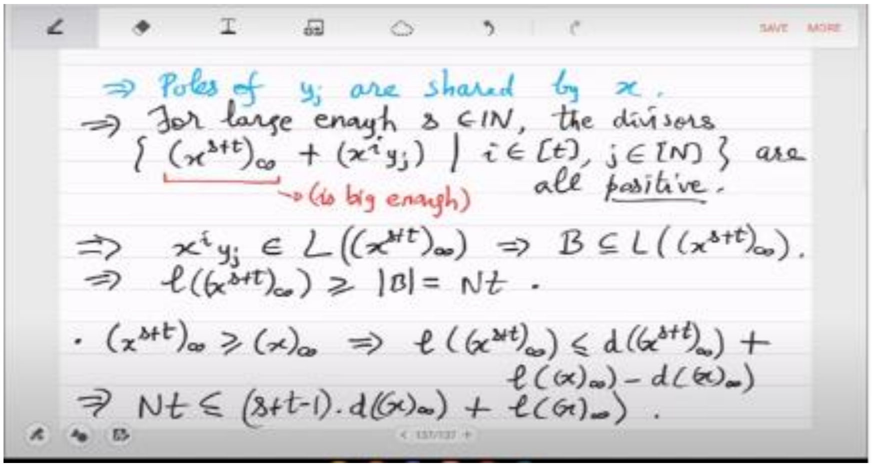
So, you just clear denominators. Yeah, yeah, yeah. No, no see otherwise 1 over ^{2} root 2 will also become integral. Because you will say that no, it is not $2x^2$ - 1, it is x^2 - half. Those are not our standards. So, where am I using this? That previous property actually connects the poles of y, j with the poles of x and this is the important part. this part is present to balance the negative terms.

So whatever negative order the principal divisor x i y j has, it will be made positive. So this is big enough. And since this is big enough it will clear away all the negativity that is there in your life that is the reason. So, all these are positive divisors and yeah.

So, what does that mean in terms of L sheaf. It means that x i y j is in L sheaf right of this. So b is a subset of that. So we have identified a lot of functions in this L sheaf that are independent. So that lower bounds the L sheaf dimension. So this means that the L of this is greater than equal to size of B which is NT right. So we have a lower bound on the L sheaf of this divisor and this is obviously greater than equal to x ∞ , right? The x to the s + t divisor, uh, ∞ divisor is at least the divisor of x ∞ .

So from this you use the L - d relationship, L shift dimension - degree. So that will tell you that, uh, L of this is less than equal to degree of that. So, L - D of this bigger divisor will be less than equal to L - D of the smaller divisor. So, that is which implies that n t is less than equal to so s + t - 1 times degree of + L of x ∞ yeah. final result you have now T something like it's a free parameter for now. So, because L - D of the bigger divisor is less than equal to L - D of the smaller divisor you get that NT is upper bounded by I mean degree of this thing is S + T - 1 times this thing + the smaller L chief.

What do you do next? What you do next is you take T to ∞ because T is free. So you make T extremely large, so large that, everything else will disappear and you will get n less than equal to degree of x ∞ . Is that clear? Right, so we have a lower bound. except that we have a lower bound not on x0, we have a lower bound on x ∞ . So, see in the first part we have shown, oh sorry, big D, what was big D? We had taken big D to be x0 and we had shown that degree of x0 is at most n.



$\Rightarrow$ Poles of y_j are shared by x.

$\Rightarrow$ For large enough $s \in \mathbb{N}$, the divisors $\{ \underbrace{(x^{s+t})_\infty}_{\text{(is big enough)}} + (x^i y_j) \mid i \in [t], j \in [N] \}$ are all positive.

$\Rightarrow \quad x^i y_j \in L((x^{s+t})_\infty) \Rightarrow B \subseteq L((x^{s+t})_\infty)$.

$\Rightarrow \quad \ell((x^{s+t})_\infty) \geq |B| = Nt$.

$\cdot \ (x^{s+t})_\infty \geq (x)_\infty \Rightarrow \ell((x^{s+t})_\infty) \leq d((x^{s+t})_\infty) + \ell((x)_\infty) - d((x)_\infty)$

$\Rightarrow Nt \leq (s+t-1) \cdot d((x)_\infty) + \ell((x)_\infty)$.

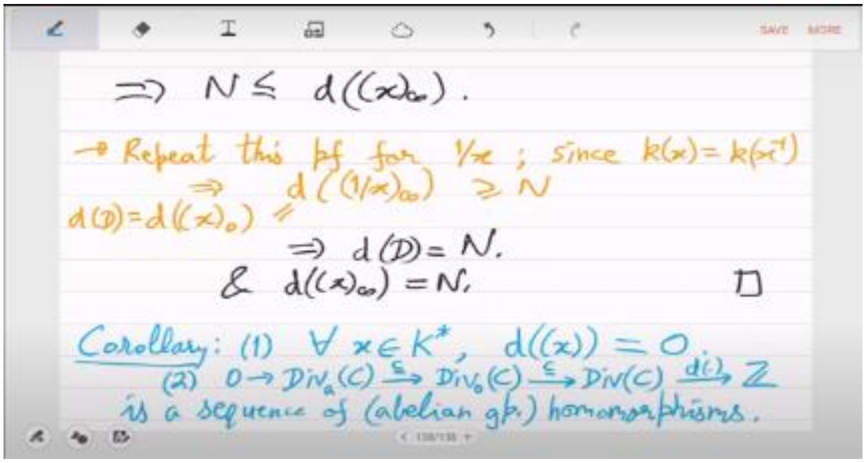
We want to show that degree of x0 is at least n. We have shown now for x ∞ . How do we go from here to x0? From x ∞ to x0? 1 by x, yeah. So, so essentially repeat this proof for 1 over x. Now since kx and kx $^{-1}$ are the same base fields this proof will give you that degree of x0 is lower bounded by n. Is that clear? So the poles of x will be zeros of 1 by x and in fact when you repeat the proof you will actually get 1 by x ∞ .

So the poles of 1 by x which is zeros of x. So you will get maybe I should write that. you will actually get this when you repeat the proof which will be degree of x0 which is your big D that's the line of argument and combined with the first part you have shown that degree of D is n is that clear And of course, you have also shown that degree of x ∞ is n. So, you have shown two things. You have shown that for a rational function the principal divisor has equal zeros and poles and you have also shown that the cumulative degree is exactly the degree of the field extension algebraic. No, the- so the divisors are actually equal, right? X zero and one by X ∞ , it's the same- Sigma P is the- Sigma P is the same, yeah.

And then I'm applying it on degree, but actually the divisors are equal. know that was clear also one hour ago but the problem was how do I show equality I guess for equality you need this proof this longer proof. Oh, we are all- no, no, we are working with the- the function field of the curve.

Yes. So, we are always in the smooth projective model. That we decided a month back. So, then you already know what the function look like, right? What- what is the function like? You have G over H where G and H are the same degree. Mm-hm. You might have different degrees because then it won't be a very different function. Yeah, but how do you show that the- our explicit definition of degree of a polynomial matches this abstract definition of small d? I don't want to get into that because I don't think it's- that part is not easy.

In fact, ultimately, it will need this long proof. You can't avoid it. It's already a simplified proof. Okay. Any questions? yeah so this is a major technical result it will clarify many things in the subsequent work that we will do what you learn now immediately is are these properties so for all functions what do you know about the degree of the principal divisor What is the degree of x? It is 0 because it has two parts, x0 - x ∞ , both are equal, degrees are equal, so it's 0, right? So all rational functions are degree 0. And now I have a containment. So this div AC, actually sits in diff 0 C, which obviously sits in diff C.



$\Rightarrow \ N \leq d((x)_\infty)$.

→ Repeat this pf for $1/x$; since $k(x) = k(x^{-1})$

$\Rightarrow \ d((1/x)_\infty) \geq N$

$d(D) = d((x)_0) \ /\!/$

$\Rightarrow d(D) = N$.

$\& \ d((x)_\infty) = N$, □

Corollary: (1) $\forall \ x \in K^*, \ d((x)) = 0$.

(2) $0 \to Div_a(C) \xrightarrow{\subseteq} Div_0(C) \xrightarrow{\subseteq} Div(C) \xrightarrow{d(\cdot)} \mathbb{Z}$

is a sequence of (abelian gp.) homomorphisms.

So let us see this as a map and degree is a map from this two integers. So this is a sequence of abelian group homomorphisms. Okay. So degree, we have defined this to be a homomorphism from the div C group to integers and div C has a subgroup div 0, div 0 has a subgroup, all the principal divisors. Div A is the principal divisors. Okay. So yeah, so with this tower of subgroups, now we can define actually two quotient groups, div mod div 0 and div mod div A. So the, the class group, maybe not the class group just the, this first group, I mean CL stands for class actually, so this class of C group is div C mod div A is the, group of divisors of divisor classes.

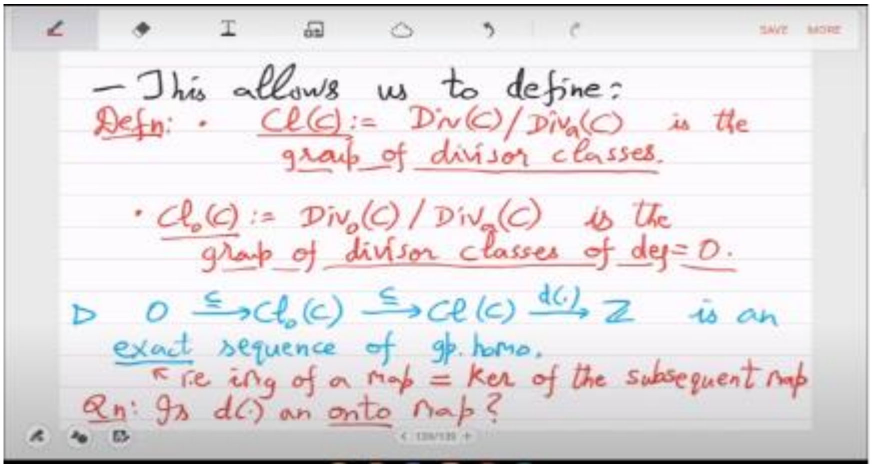
So, let us erase this and CL0C is more interesting We couldn't define this before because we didn't know whether div A is a subgroup of div 0 but now we know. So the degree 0 divisors which you would have expected in the first instance to somehow connected to rational functions of the curve, right. That how close is it actually to functions on the curve that is measured by CL0.

So this group is a cornerstone of all of algebraic geometry. So this is the group of divisor classes of degree 0. So this is what we will usually call the class group and it has many, many properties, too many to actually even mention in this course. But we'll see what can be done. So what is the connection between them? So we can write down a sequence, CL0C is kind of contained in CLC. and this degree also acts on this and this is an exact sequence of again group homomorphisms.

So do you know what is an exact sequence? Okay, exact sequence just means that in these arrows, image is contained in the kernel. Sorry, equal. Yeah. Yeah. That is image of a map. is equal to kernel of the subsequent map. So whenever you have a sequence of homomorphisms you are interested in understanding the image of the previous map.

and kernel of the next map so that both of them are obviously in the same place, they are in the same group. So you want to see what is the connection between them. When these two are equal, you call the sequence exact. Here it is trivial to check. The image of the very first arrow is 0, which is also the kernel of the second arrow. right and similarly the image of the second arrow is in the, is equal to the kernel of the third arrow because I mean when is degree 0, it's 0 only for degree 0 divisors.

So it's, it's a triviality here. Yeah, now the question about, yeah, Madhavan asked this question, is this degree map onto? So, if I extend the z arrow 0, map the whole of z to 0, right. So, the last arrows kernel will be the whole of z, whether the third arrows image is the whole of z, that is the question of onto. So, is degree an onto map? . yeah so it will be true so I leave this as an exercise. I guess this degree so containments are trivial but the degree is if you work it out there is some non-triviality here yeah so the non-triviality is the following see we have defined degree on diff c what is the definition on diff c mod div A that should be worked out.



– This allows us to define:

Defn: • $Cl(C) := Div(C)/Div_a(C)$ is the group of divisor classes.

• $Cl_0(C) := Div_0(C)/Div_a(C)$ is the group of divisor classes of deg = 0.

▷ $0 \xrightarrow{\subseteq} Cl_0(C) \xrightarrow{\subseteq} Cl(C) \xrightarrow{d(\cdot)} \mathbb{Z}$ is an exact sequence of gp. homo.

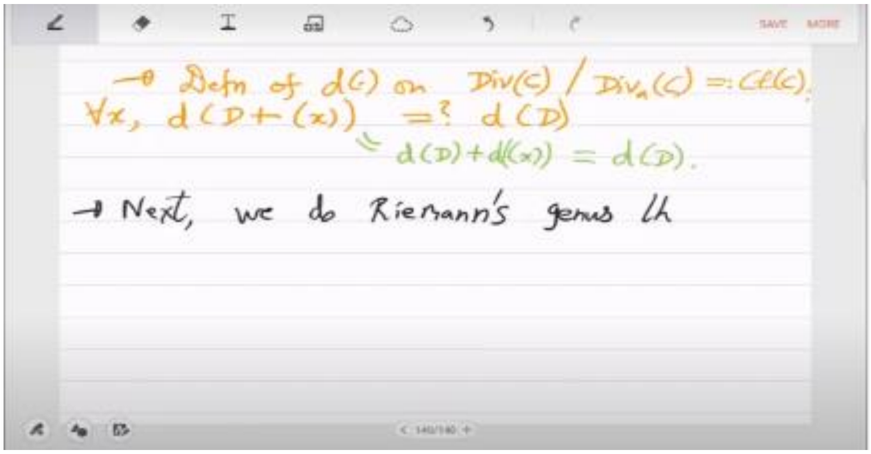
↖ i.e img of a map = ker of the subsequent map

Qn: Is $d(\cdot)$ an onto map?

So, definition of degree on div C modulo div A C. So, the issue is the following you can have now not only a divisor D but you can add any rational function right because D + X and D is the same should be the same I mean D + X and D are the same in this CLC But how do you define degree so that the degree of d + x and d is also the same no matter what x is.

It should be true for all x. So is our older definition of degree does it satisfy this condition that you have to check. Yeah. So, this is the non-triviality. So, you have to check it.

So, this is actually the, so degree is additive and degree of a function is 0. We have shown it. So, that is why. What I wrote you have to actually check. This is the check. So, this checkpoint is passed. So, you can actually add whatever rational function you want to your divisor and degree will not change and this is why our degree the definition was fortunate it also works for the class group. Okay, so I think that should be enough for today. Yeah, so what we will do next is Riemann's theorem.



→ Defn of $d(\cdot)$ on $\mathrm{Div}(C) / \mathrm{Div}_a(C) =: Cl(C)$.
$\forall x$, $d(D + (x)) \overset{?}{=} d(D)$
$= d(D) + d((x)) = d(D)$.

→ Next, we do Riemann's genus th