Computational Arithmetic - Geometry for Algebraic Curves

Prof Nitin Saxena

Dept of Computer Science and Engineering

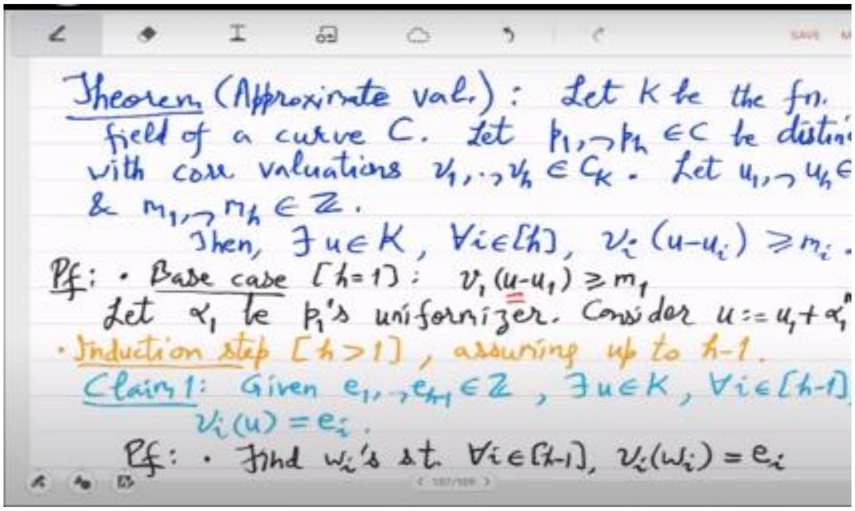
IIT Kanpur

Week - 07

Lecture – 13

Divisor on Curves

So last time we have started proving this theorem about approximate valuation. It basically says that if you are given points p1 to ph and points always mean DVR and valuations. So they define valuations v1 to vh respectively and what you want to find is a u in the function field such that the valuation of u minus some offset function which is already provided to you is at least m i an integer which is already provided. So, the only unknown here is u can you and the key thing is that you have to find out u that works for all these inequalities simultaneously. that is the hard part because in the base case when h = 1, let us make this bigger. So when h = 1 that is the base case, so there you only have one inequality.



<u>Theorem</u> (Approximate val.): Let K be the fn. field of a curve C. Let $p_1, .., p_h \in C$ be distin
with corr valuations $v_1, .., v_h \in C_K$. Let $u_1, .., u_h \in$
& $m_1, .., m_h \in \mathbb{Z}$.
Then, $\exists u \in K, \forall i \in [h], v_i(u - u_i) \geq m_i$.

<u>Pf</u>: • <u>Base case</u> $[h=1]$: $v_1(\underset{=}{u} - u_1) \geq m_1$
Let α_1 be p_1's uniformizer. Consider $u := u_1 + \alpha_1^{m}$

• <u>Induction step</u> $[h>1]$, assuming up to $h-1$.
<u>Claim 1</u>: Given $e_1, .., e_{h-1} \in \mathbb{Z}$, $\exists u \in K, \forall i \in [h-1]$,
$v_i(u) = e_i$.
Pf: • Find w_i's s.t. $\forall i \in [h-1]$, $v_i(w_i) = e_i$

So in that case you can pick your u to be just u1 plus the uniformizer for v1 α1 to the m1, right. So you will have actually exactly valuation equal to m1. That is easy, it will work whether m1 is 0 positive or negative, right. So, you will get at least valuation v1 to be exactly m1.

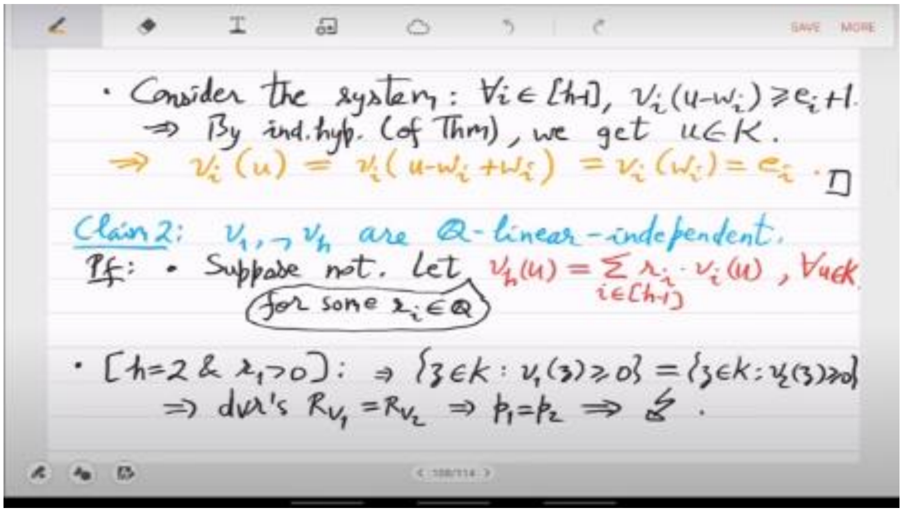
But when you have both v1 and v2, then it is actually trickier because now you have two uniformizers and two numbers m1, m2 and also two offsets u1, u2. So, you do not know how to do a similar trick, it is not very easy. So, these are the offsets. So, when you have multiple offsets then it's a problem and multiple valuations. So, first thing we showed claim 1 is I mean we will basically the proof will be induction on H, how many inequalities you have, how many valuations you have.

assuming that you have shown it till h - 1, you can immediately get claim 1. So, what claim 1 is saying is that assuming the theorem for h - 1 up to h - 1, you will always be able to find the u such that vi u = given ei. So, this is a simpler statement than the theorem statement. The theorem statement has an offset because it is a stronger result. The stronger result will give us the weaker result which is claim 1.

It is defined in a way so that you get claim 1 by induction. The proof of this is very simple. You first find wi such that vi wi = ei. So, this is not a common thing you do it for every ei and then you apply the theorem. So, now you use wi as the offset and find a u such that vi u - wi is at least ei + 1.

So, by the theorem statement for each - 1 you will get that the valuation of u is exactly ei. Is that clear? So, on the given points and the valuations which you can also think of as multiplicity that is why we call it M. So, for given points Pi's and given multiplicities Ei's what claim 1 is saying is that you can find a U such that that points multiplicity is exactly Ei. Okay. That is the key thing you want to prove about functions versus points on the curve.

Yeah, but we haven't shown, now we have to show the induction step, right. So, you want to get to h now from h - 1. So, for that we will need to show that, we will actually do many things, but first thing we did is claim to showing that the valuations are always independent. suppose not so we have this for the sake of contradiction we have this dependence Vh on every u is equal to a linear combination of Vi u for the same Ris suppose there are rational numbers Ris such that Vh is a as a function as a valuation function it is a linear combination given by Ris of Vi. So it is true for every u in the function field.



- Consider the system: $\forall i \in [h-1]$, $v_i(u-w_i) \geq e_i+1$.
  $\Rightarrow$ By ind. hyp. (of Thm), we get $u \in K$.
  $\Rightarrow v_i(u) = v_i(u-w_i+w_i) = v_i(w_i) = e_i$. □

Claim 2: $v_1, \ldots, v_h$ are $\mathbb{Q}$-linear-independent.

Pf: • Suppose not. Let $v_h(u) = \sum_{i \in [h-1]} r_i \cdot v_i(u)$, $\forall u \in K$
for some $r_i \in \mathbb{Q}$

- $[h=2 \ \& \ r_1 > 0]$: $\Rightarrow \{z \in k : v_1(z) \geq 0\} = \{z \in k : v_2(z) \geq 0\}$
  $\Rightarrow$ dvr's $R_{v_1} = R_{v_2} \Rightarrow p_1 = p_2 \Rightarrow \lightning$.

And then we showed that there are contradictions in every case. I will not repeat that proof. Any questions till now? At some point I will post this. But you can also see the proof in the old lecture notes. what we have to do is the inductions we have to complete the induction step.

So, our plan now is that we will construct this u which is a combination of the offsets u i's we will find these x i's such that we will in fact design these x i's in such a way that u which is ∑ x i u i will work it will give you the theorem statement. So U minus the offset valuation is equal to this thing. So we'll basically design Xi so that X1 - 1 and Xi valuations are under control. So let's move in that direction. Oh I need another claim which follows from claim 2.

So, I want to show that there exist functions z 1 to z h in the function field such that the determinant of the matrix v i z j. is non-zero, it is an invertible matrix, okay. So this is an h cross h matrix, it is a square matrix and we are saying that it is an invertible matrix. There exist such value functions whose valuations have this define this invertible matrix. This actually is an easy consequence of claim 2.

It again is a is an evidence of vi's being independent. But how do you find these Z1 to Zh? So, kind of an inductive proof. So, suppose you want to find Z1. So, let us look at an equation. The solution set of ∑ R i V i z 1 = 0.

So, consider this solution set it is a vector space of course. Now, what I want in I do not know what z 1 is what I want is that. a Z1 such that the rank of the solution set is 1 less. I want to claim that such a Z1 exists. This is because vi's are independent.

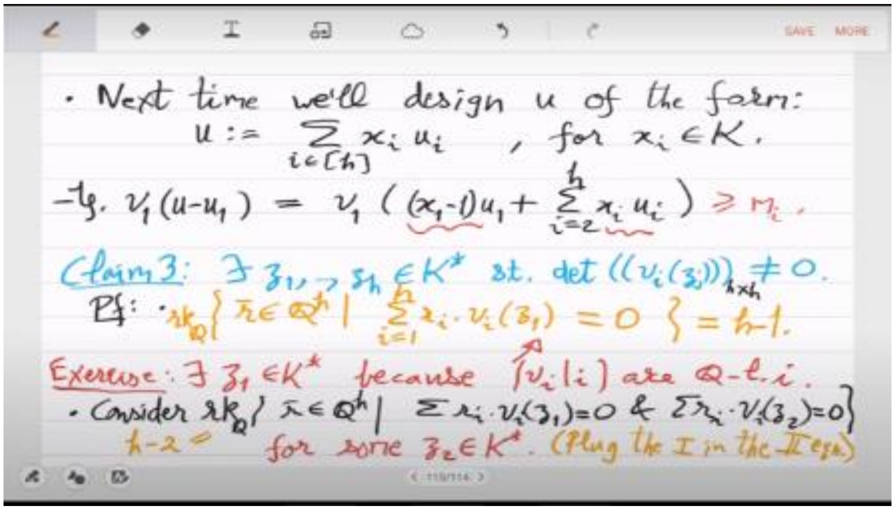
Do you see this? See for all the z1s in the function field, the rank of this is always maximal which is h. What would happen? This should just be linear algebra. I think you should think of vi the function as a vector evaluated on all possible z1s. Think of it as an infinite vector and you have shown that these vectors v1, v2, … vh they are linearly independent. So, it basically means that there has to be a z1 at which this rank is smaller than expected, it is smaller than the maximum which is H.

Do you see this? So, just prove this by linear algebra and claim 2, we have shown claim 2 that was the important thing. Next what we will do is, or this only gives us Z1, we also want now Z2. So, we look at two constraints. So, consider the vector space of the solution set. of this and some other Z2 and the claim is that this = h - = h - 2 for some z2 in k *.

Now the first constraint already reduces the dimension by 1, so you are in R ‘ cannot be more than H - 1 dimensional solution set. The second constraint what you, so Z 2 think of it as unknown, Z 1 is fixed. What you do is that from the first constraint you say you find R, you express R1 or Rh as a combination of R1 to Rh - 1 and plug that in the second equation, right. So, second equation is a linear constraint in R’, but now one less. So, you only have R1 to Rh - 1.

So you rearrange and you basically do what you did in the orange part that there will be a Z2 because of the linear independence of V1 to VH - 1 sorry V1 to VH because of the linear independence of that there will be a Z2 such that the dimension is 1 less than the number of Rs which is H - 1 - 1 is that clear. So, the plug the first in the second. So, when you plug it in then you basically instead of R 1 to R H you are looking at only R 1 to R H - 1 and by the first orange conclusion you will now have H - 2 for the solution set. Yeah. So, we have found Z 1 we have found Z 2 and then we can just continue this and we can find What do you mean plug the first one? Oh, the first one vi z1 are just known numbers, right.

So, suppose you have an equation, this is giving you the equation r1 + r2 + r3 = 0. So, you write r3 as - r1 - r2 and just substitute that in the second equation. So, r3 is eliminated. So, now actually you are only looking at h - 1 ri's. And since this vi, z2 are unknown, valuations which will be, which you know are linearly independent, you will find a z2, so there is a solution set is smaller of r ‘.
So, it is again coming from claim 2. And yes, so when you keep doing this.



- Next time we'll design u of the form: $u := \sum_{i\in[h]} x_i u_i$, for $x_i \in K$.

-ly. $v_1(u-u_1) = v_1\left(\underbrace{(x_1-1)}u_1 + \sum_{i=2}^{h} \underbrace{x_i} u_i\right) \geq m_i$.

Claim 3: $\exists z_1, \to z_h \in K^*$ st. $\det((v_i(z_j)))_{h\times h} \neq 0$.

Pf: $\cdot\, rk_{\mathbb{Q}}\{\bar{x}\in\mathbb{Q}^h \mid \sum_{i=1}^{h} x_i \cdot v_i(z_1) = 0\} = h-1$.

Exercise: $\exists z_1 \in K^*$ because $\{v_i \mid i\}$ are $\mathbb{Q}$-l.i.

- Consider $rk_{\mathbb{Q}}\{\bar{x}\in\mathbb{Q}^h \mid \sum x_i\cdot v_i(z_1)=0 \;\&\; \sum x_i\cdot v_i(z_2)=0\}$ $h-2 =$ for some $z_2 \in K^*$. (Plug the I in the II eqn)

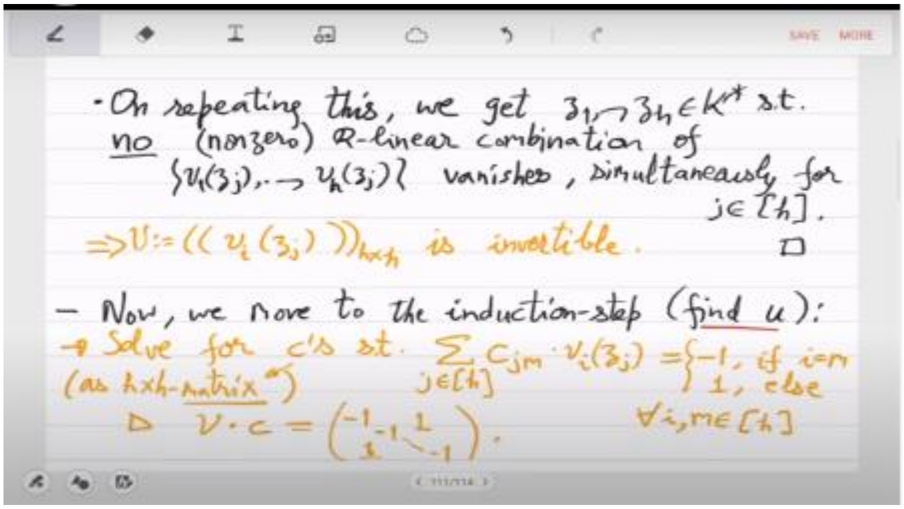
So on repeating this we get z1 to zh in K star such that no non-zero Q linear combination of so, v i z j vanishes simultaneously. Okay so you look at these vectors v1 to vh evaluated at zj for all j so you have these h vectors you have what you have shown is that there is no single vector which is orthogonal to all of them right because the first one had already reduced the dimension to h-1 second one will make it h-2 when by the time you reach h you would have h-h. So the only vector which is simultaneously orthogonal to all these is the 0 vector, nothing else, which is another way of saying that this matrix is invertible.

right which is the same as saying the determinant is non-zero, is that clear. Yeah I do not think I needed to do all this I could have also said in the beginning that just because vi's are linearly independent functions. you should be able to find z1 to zh. For example, if you just picked in a sense randomly from the function field, you will actually satisfy this determinant being non-zero condition. But I guess you get some idea of the proof also.

Key thing is basically looking at these vi's these infinite factors evaluated at all possible z's and you are given that these infinite factors each of them are linearly independent. So, you should be able to basically find a minor h cross h which is also invertible this is what the proof is doing ok. So, how does this claim help in the induction step. so once you have this invertible matrix you solve for that is you want to find u that would be the goal now and for you will find excise explicitly. So, let us solve for the following equations solve for c's such that ∑ c j m times v i z j = - 1 if i is m and 1 otherwise it is basically.

So, think of C as a matrix. it has entries j, m we will be doing this for all m. Think of this as h cross h matrix I think it is basically the matrix which when you multiply with this V i Z j matrix the product is 1 everywhere except in the diagonal you have - 1 is that right yeah I am doing this for all I m. So in the matrix product if you look at the m , or i , mth entry, the i , mth entry is this linear form and this value is - 1 only in the diagonal when i is m otherwise it is 1. So this is a simple C , V matrix equal to all 1 except in the diagonal that is happening So this matrix times the C matrix = - 1 and everywhere else we have 1, right. I hope this subscripts are not messed up.

So, i , mth entry of this product matrix is what the constraints I have written. So, anyways this c is easy to find because v is invertible. So, c = v $^{-1}$ times this matrix. So, it exists because v is an invertible matrix we just showed and so, c's are. yeah in general they will be rational numbers.



- On repeating this, we get $z_1, \ldots, z_h \in K^*$ s.t. no (nonzero) $\mathbb{Q}$-linear combination of $\{v_1(z_j), \ldots, v_h(z_j)\}$ vanishes, simultaneously for $j \in [h]$.

$\Rightarrow V := ((v_i(z_j)))_{h \times h}$ is invertible. □

- Now, we move to the induction-step (find u):

→ Solve for c's s.t. $\sum_{j \in [h]} c_{jm} \cdot v_i(z_j) = \begin{cases} -1, & \text{if } i=m \\ 1, & \text{else} \end{cases}$ $\forall i, m \in [h]$
(as h×h-matrix)

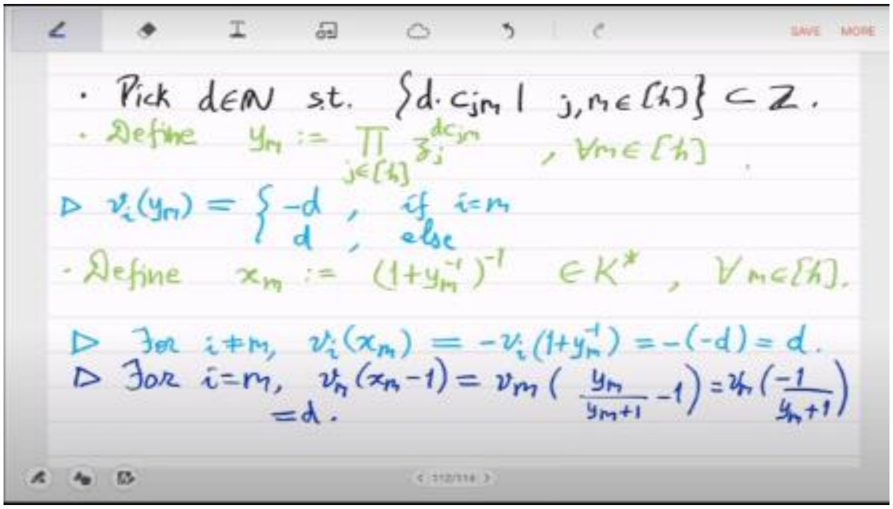
▷ $V \cdot c = \begin{pmatrix} -1 & & 1 \\ & -1 & \\ 1 & & \ddots -1 \end{pmatrix}$.

So, we convert them into integer or integers okay basically look at the denominator that you get in the solution matrix and multiply by the LCM, D is the LCM. So, these will become the matrix C will become an integral matrix now and now we have a sequence of mysterious design. So, first design is define ym to be product of zj dCjm, yeah so you want to take a product of the zj's that we had found raising it to these exponents which are now integers that we just found So, where is this? This is happening in the function field right. So, y m is now a function. So, we have designed these h functions from z j and let us record its valuation.

So, what is the valuation of y m, v i y m? So, by this orange property which we wrote you should be able to deduce that valuation of ym is there was a - 1 right that - 1 will become - d and + 1 will become + d if i = m otherwise fine this is the point of this design so we have found these y1 to yh such that when they look at their valuations v1 to vh they are a sequence of - d and + d is that clear and finally another mysterious design of a rational function which is xm which will be (1 + ym $^{-1}$)$^{-1}$, okay. So these will be my xm's which will define the u that the theorem wanted. So let us check the valuation. So valuation of xm is what? So, when I is different from M what happens? V I is you are taking this will be = - V I 1 + Y M $^{-1}$ and what is the valuation of 1 + Y M $^{-1}$? So valuation of vi1 is 0, vi ym $^{-1}$ is what? This is - d, right. So 0 , - d, so the answer will be - d which is d.

Fine, so VI (xm) is D and the other thing I have to see is Xm-1. So what is that? Sorry, Vm (xm-1). So, Vm (xm – 1) is do you have any handle on that? So, xm - 1 will be this right which is Which what do you know about this? So, valuation of y m + 1. So, valuation of v m y m is - d and v m 1 is of course, 0.

So, this valuation is - d and inverted. So, d this is again d. Okay so we have checked that for this design of rational functions vi value is d for i different from m and vm (xm-1) is also d. Okay so let us now move to the design of u for the theorem. So, u will be ∑ xi ui the offsets and you have to check the valuations now. So, u - ui = m in each and m ≠i.



· Pick $d \in \mathbb{N}$ s.t. $\{d \cdot c_{jm} \mid j, m \in [h]\} \subset \mathbb{Z}$.

· Define $y_m := \prod_{j \in [h]} z_j^{dc_{jm}}$, $\forall m \in [h]$.

$\triangleright$ $v_i(y_m) = \begin{cases} -d , & \text{if } i=m \\ d , & \text{else} \end{cases}$

· Define $x_m := (1+y_m^{-1})^{-1} \in K^*$, $\forall m \in [h]$.

$\triangleright$ For $i \neq m$, $v_i(x_m) = -v_i(1+y_m^{-1}) = -(-d) = d$.

$\triangleright$ For $i = m$, $v_m(x_m - 1) = v_m\left(\frac{y_m}{y_m+1} - 1\right) = v_m\left(\frac{-1}{y_m+1}\right)$
$= d$.

So, yeah let us check v i of u - u i. that is what you want in the theorem statement right you want to evaluate the valuation of ith valuation of u - ui. So, this will be what will you get from here. So, let us check vi of Well vi of xi - 1 we have evaluated already. So, that is d or d + yeah vi ui and this part vi (xm).

Vi (xm- um). Okay. Yeah, but I want the valuation of the sum. Can I control that? Okay yeah so the thing is what you want here is that this should be less than equal to mi right this is what you want to show in the for the theorem statement and here in the valuation of the summands you see that you are getting these two numbers but d for now is free right so you can just pick d to be large enough so that these two values they exceed or they at least are m i. So, let us just remember that in the design. So, fix D large enough such that d + vi uj is greater than equal to the max of mi's for all ij. Is this fine? So if I pick D to be a big enough number then well actually kind of we had already fixed D.

We also had this, we have said that pick a D such that D times C j m is our integers but there are many such possibilities for D. So you keep on increasing D such that all these constraints are satisfied. That is easily done and then now you can deduce that vi of u - ui since both the summands it is at least mi, valuation is at least mi. So, your theorem statement is done.

Is that clear? So, this completes the induction step. gives you the theorem. So, we constructed ultimately u as a combination of the offsets and these xi's how are they constructed. So, they are basically I mean if you want to reverse engineer the proof you should look at this expression u - ui and from this you can see why we designed these mysterious looking rational functions ym xm. Okay and one more thing we should remember from this proof because the whole the subsequent part of the course is really an attempt to understand this corollary okay or investigate this corollary which is that the thing that we showed here in the very beginning claim 1, a claim 1 that given multiplicities and points you can always find a function which has those valuations. Let us just remember that as a corollary of this theorem.

So, S is a subset of S is a finite subset of the smooth projective curve C and you are given multiplicities candidate multiplicities. So, these are of course integers. So, you are allowed to specify p as a 0 or as a pole and you can also give multiplicity 0 of multiplicity 1 or 2 or pole of multiplicity 100. So, - 100 then there always exists a rational function f. So K remember is this function field of the smooth projective curve such that these multiplicities are matched.

So this is a very important result. In fact this is the most important result you have seen till now in these two months. And this important result is what we will now kind of go really deep into in the next two months. So, you have some your favorite finitely many points p's and multiplicities and you want to study these functions. So, we are obviously not saying that there is a unique function like there actually there are infinitely many f because any f you can multiply by constants, constants are infinitely many. So, obviously you have always you have infinitely many functions which will have these 0's and poles with this multiplicity.

But now we will be interested in measuring how many. They are infinitely many but you can actually show that the set of these functions kind of form a vector space over the base field and you are interested in computing the dimension of that vector space. That will be the goal and we will do a lot of stuff in this. basic question following Riemann. So, any questions till now or maybe I should have discussed the this question over the affine line. So, when C is the affine line or the projective line, what do you think are these functions, how many are they? Yeah, so since you know divisors, it's easy to get confused.

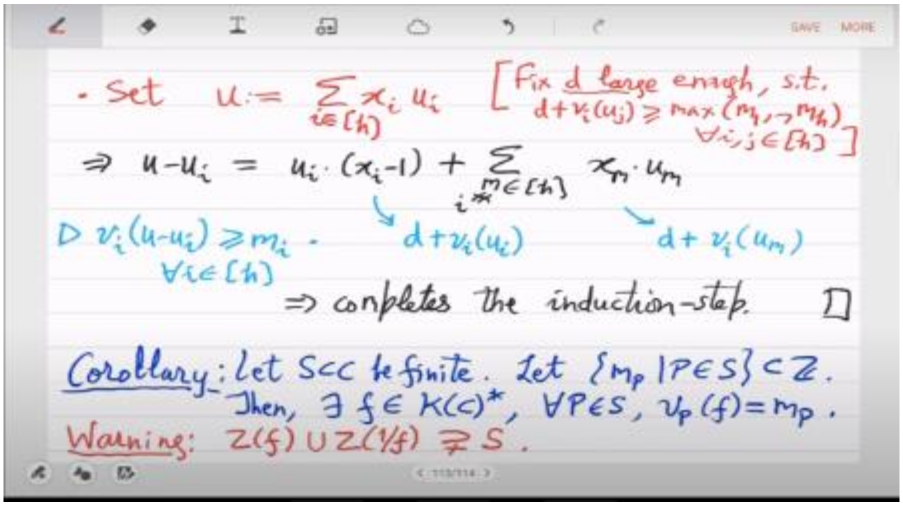
But the others don't, so heavily fine. Not saying that. No, no, we haven't defined divisors. So, in case you already know divisor, you may confuse this with saying that. Maybe I should make a note here. So, here is the warning for the experts. well also for the non-experts actually, I will formulate it in the following way.

This f that you have, it may have other poles and zeros outside s. So, zeros of f and zeros of 1/ f may actually be strictly bigger than s. This corollary is not saying that the zeros and the poles are just S. There are, there will, there potentially could be points which are outside what you were given in the input which is S. Yeah, so that actually gives you a lot of extra leeway because there are still these unknown points which can be zeros or poles.

You don't have to worry about them. Those are kind of don't care zeros and poles. Important ones are only these s and for that there is a match. Yeah, that's one thing and second is you can work out the, set of f's in the case of projective line. Just to get an understanding of how these f's look like.

The proof I have given is actually very tricky. You do not immediately understand what this f is, but if you work it out for the projective line, essentially what happens is if you say that 1 has to be a 0, then you look at the function x - 1. right and if you say that 2 has to be a pole then you look at the function 1 / x - 2. So, those kind of things suffice they give you complete understanding over the projective line. Obviously, over a curve it can be trickier because 1 / x - 2 may I mean in the case of a actual curve you have you will have two coordinates x and y. So, you cannot simply do 1 / x - 2 you have to think about what is the point x , y.

And then for a point which has two coordinates you have to define an f which satisfies these conditions so that that will be trickier. So, I think yeah you can easily work out the case of projective line.



- Set $u := \sum_{i\in[h]} x_i u_i$ [Fix $\underline{d}$ large enough, s.t. $d+v_i(u_j) \geq \max(m_1,\dots,m_h)$ $\forall i,j\in[h]$]

$$\Rightarrow u-u_i = \underbrace{u_i\cdot(x_i-1)}_{d+v_i(u_i)} + \sum_{i\neq m\in[h]} \underbrace{x_m\cdot u_m}_{d+v_i(u_m)}$$

$\triangleright\ v_i(u-u_i) \geq m_i$. $\forall i\in[h]$

$\Rightarrow$ completes the induction-step. □

Corollary: Let $S\subset C$ be finite. Let $\{m_P \mid P\in S\}\subset\mathbb{Z}$. Then, $\exists f\in k(C)^*$, $\forall P\in S$, $v_P(f)=m_P$.

Warning: $Z(f)\cup Z(1/f) \supsetneq S$.

take C to be the projective line and find Fs. That will be a good example to understand this proof and the corollary. So, let me move to the next topic which will be the like the cornerstone of whatever happens in arithmetic geometry, which is the divisor class.

Uh, before that I have to correct some things I said last time. Uh, yeah, last time I ha- I was talking about the degree definition of a point, what is degree, right? Uh, that have- that I have to correct. So maybe you can correct in your notes the base field small k we would now like to think of it as a finite field. It may not be fp ‘, it may just be some fq. So in that case what is a point and a point will always be a DVR for us.

We will not think in terms of point as x, y. We will actually think of it in terms of DVR. So, you have to ask the question what is the DVR or what are the DVRs of this function field k. In the algebraically close case DVRs actually correspond to an actual point. In the finite field case DVRs will actually correspond to irreducible polynomials.

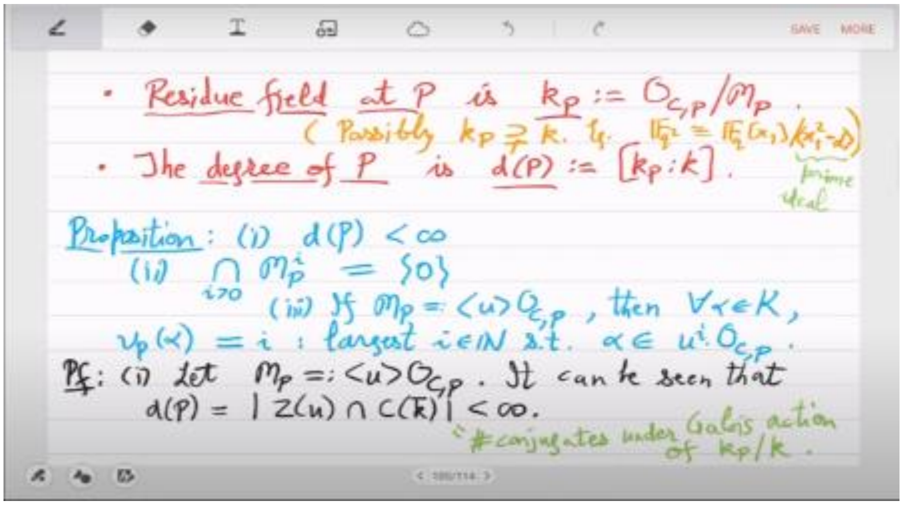
So it will not be an actual root, it will be a root with all its conjugates. So for example, if you don't have √ 2 available, then point cannot be √ 2, then point will be actually √ 2 and - √ 2. So they will be clubbed together, so your polynomial will be x ^{2} - 2. Okay, this we had seen also when we classified the valuations of the affine line. There we saw that the valuations come from irreducible polynomials.

So, it is the same thing. Now, we are just making it more explicit and we will measure this how many conjugates are there. So, but think of a point always as a DVR. It is always a valuation for us a DVR and hence the stock. that's what a point is, it's a cluster of conjugates.

And how many conjugates that is measured by degree of the point P. Okay. So, D of P is just the number of conjugates in that cluster. Is that clear? So, I am just correcting what I said last time. Yeah, so example is like an FQ ^{2} finite field. What may happen is that you have a point P which is √ α coming from x1 = √ α.

It is not present in the base field FQ, it is present in FQ ^{2}. So, the point P that you will be looking at it cannot have √ α so what it will actually have is it will be given via this irreducible polynomial x1 ^{2} - α that prime ideal so when you look at ocp mod mp you will actually go to an extension from fq you will go to fq ^{2} so we will say degrees 2 is that clear this was always 1 in the algebraically close case the degree was always 1 because you actually got a real point. Now you may not you will generally not get that. So, you have to talk about degree because you are representing it like you can also think of computation about this. So, you will actually represent the point via an irreducible.

So, how much do you have to store? So, that storage space is given by degree. okay it's not an actual point but this irreducible the bigger the irreducible is the bigger the degree is bigger your storage is so yeah just remember this part if you have any questions you can ask so for the rest of the course the goal is to study the set of all functions from the approximation that appear in the approximation theorem the use only for curves of course. So, in transcendence degree one function field what are the functions whose zeros are at least that in the set S. Zeros and poles come from the set S with specified multiplicity So, we want to look at the set of all those functions, it should be easy for you to see that the set of those functions is of vector space, because if f1 and f2 their 0s come from S with the specified multiplicity then f1 + f2 also satisfies that condition. So, you can add these functions, so you actually get a vector space.



- Residue field at P is $k_P := \mathcal{O}_{C,P}/\mathfrak{m}_P$.
  (Possibly $k_P \supsetneq k$. Eg. $\mathbb{F}_{q^2} = \mathbb{F}_q(x_1)/\langle x_1^2 - \alpha \rangle$)
  prime ideal
- The degree of P is $d(P) := [k_P : k]$.

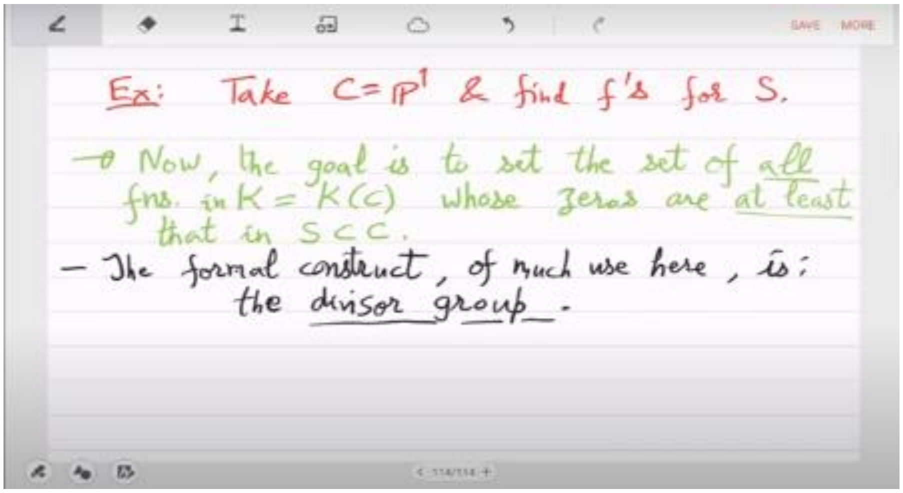
Proposition: (i) $d(P) < \infty$

(ii) $\bigcap_{i \geq 0} \mathfrak{m}_P^i = \{0\}$

(iii) If $\mathfrak{m}_P = \langle u \rangle \mathcal{O}_{C,P}$, then $\forall \alpha \in K$,
$v_P(\alpha) = i$: largest $i \in \mathbb{N}$ s.t. $\alpha \in u^i \cdot \mathcal{O}_{C,P}$.

Pf: (i) Let $\mathfrak{m}_P =: \langle u \rangle \mathcal{O}_{C,P}$. It can be seen that
$d(P) = |Z(u) \cap C(\bar{k})| < \infty$.
$\because$ #conjugates under Galois action of k_P/k .

Vector space is obviously infinite in size. Yeah, it will always will may not always be infinite, but usually it will be infinite. So, we definitely do not want to talk about size, we want to talk about dimension. Why is the dimension finite? I am not sure about that, that we will see. Yeah, so the formal construct for this is the divisor class or divisor group.



Ex: Take $C = \mathbb{P}^1$ & find f's for S.

→ Now, the goal is to set the set of all fns. in $K = K(C)$ whose zeros are at least that in $S \subset C$.

- The formal construct, of much use here, is: the divisor group.

So, this will be divisors of a curve, maybe I start next. So now focus on divisors which is unfortunately seems to be an overused concept, I mean you have divisors of integers, but as we develop the theory you will see that it is exactly mirroring that, just like integers have divisors, function fields also have a concept similar to that, which we will again use the term divisor for it. yeah but it may be too early right now to get into that comparison let us just develop the algebra for now so it is the free abelian group generated by the points which is the DVRs, this is called the group of divisors. of a smooth projective curve which we have seen is every transcendence degree one function field. So, any transcendence degree one function field respectively smooth projective or equivalently smooth projective curves you can look at the DVRs or respectively the points and just take a linear combination of the points in a formal way.

Okay, so for now there is no relationship. So, if the points are p1, p2 you can just look at 2p1 + 3p2 or p1 - p2 and so on. These are all just formal objects living in this free abelian group. The points no, no, no I just gave a whole prelude to that. The points are if you have a problem with algebraic closure just work with DVRs, P is just a DVR.

So, equivalently. No, no, no by P in C, P in C we mean DVR. No, no, I just, so in my notation, the big P is a DVR. You think of, so you can remove the geometry completely, don't work with smooth projective curve, just work with the function, some transcendence degree one field k, go over the DVRs or if it is a curve then go over the stocks. Over the algebraic closure definitely that is what we have proven. But over finite field I have gone fast and I do not want to get into those details what exactly is the correspondence.

But I mentioned I hinted that the correspondence is essentially by irreducible polynomials. So, to think to think of a DVR. let us say when you are in a finite field to think of a DVR you have to think about not just an actual point but the cluster of its conjugates. So it is actually a cloud, it is a cloud of the point with its conjugates that is what a point is, it is a cloud. If you really want to think about the point but it is actually we will just go with DVRs because what we want is the valuation and all that we want to talk about degree of the point.

So in this case you have to remember that degree of P may be may not be equal to 1. What do you mean by free abelian? Oh, free is just take all possible combinations. If you are not, there is no relationship. So, it is not that p1 and p2 are equal or 2p1 = 3p2.

There is no relationship. These are all, just think of p1, p2 as symbols. So, you have, you can take any combination, they are all, So, you go over the points in the curve or the DVRs in the function field and you are allowed to take any combination. The only way two combinations will be equal if they are equal for every coordinate.

That's the only content here that. What is the operation in this group? Addition. Addition. It's an abelian group, it's the addition, yeah. So, p + p is to that. Yeah, exactly, yeah.

So, for example, so p1 + p2 and p2 - p1 + p3. So, this will be 2p2 + p3, fine. Yeah, and of course, what is P1 - P1? Yeah, so there is also a 0 in this group, but this 0 is not any point. It will not correspond to any point. It is a formal object in the group.

Point is just P1 but if you subtract P1 with itself you get basically empty. So it is the empty point. What is the use? There is a valuation and there is a degree and this degree is related to the Frobenius action. So it will count everything correctly when we reach zeta functions which will be next month. So we want to keep a count of how many points are there in a finite field. So for that count you need the degree to be working well with divisors. Otherwise, the same conjugates if you throw, if you separate them, then you have to keep track of them across summations in the divisor group.

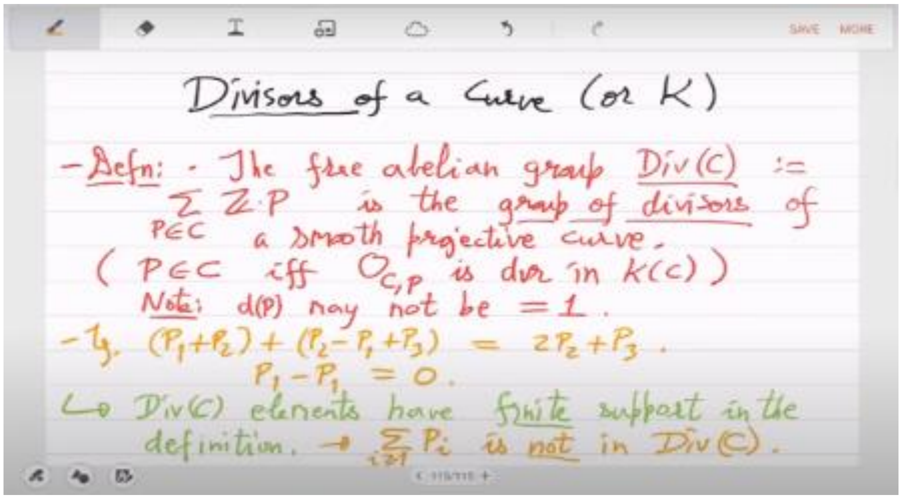
I do not want to do that. Correct, yeah. Yeah, I again hinted that in that example, the $\sqrt{\alpha}$ example. So look at the orange example, so base field is small k is Fq, you took a point which is essentially point like $\sqrt{\alpha}$. $\sqrt{\alpha}$ is not in the base field, it is in the bigger field Fq^{2}. So when you will look at Kp, the residue field of that point, residue field will actually come out to be Fq^{2}. And the point that we are talking about the DVR, the DVR is basically given by the prime ideal $x1^{2} - \alpha$.

Because the prime ideal has a base representation, but the roots do not have a base representation, roots have a representation in the residue field. So we take, basically we keep account of the storage space for us because we will say in computers we will only store $x1^{2} - \alpha$.

We can't store $\sqrt{\alpha}$. It doesn't exist in FQ. So we keep a track of the degree, dp is 2. And all this pain is being taken to keep the counting of points in the finite field correct on the curve because Riemann zeta function is supposed to count it exactly. We do not want to go into approximation. So, we want to keep track of that exactly. So, I mean as you can imagine we cannot keep working with the algebraic closure because ultimately we are interested in finite fields.

So, at some point there has to be a bridge built between finite fields and infinite fields. So, this is the point this is the divisor group that we are defining for any finite field including also algebraic closure. So, the other thing is. Yeah, I think this is the notation here is a bit bad. The notation seems to suggest that you can take infinitely many points.

But when I say $\sum$, I mean the support is finite. have finite support by definition I am not deducing this. So, you should think of $\sum$ as just summing up finitely many points for all the other points it is understood that the coefficient is 0. okay, the non-zero integral coefficients will appear only finitely many times, because I mean we do not have yet a way of summing up infinitely many things, like these are discrete points. So, you cannot do a infinite sum, it is only a finite sum. So, that is already inbuilt in the definition.



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 $\mathcal{O}_{C,P}$ is dvr in $k(C)$)

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).

So, which also means that, this ∑ p i i >= 1 is not allowed, okay. These kind of sums will not be allowed because this is infinite support, okay. Continuing with the definition any element in diff c is a divisor of K. Yeah, so I mean if you want to really set up an association with integers, the integer ring that you studied in school, you should think of Diff C as the integers for your curve and any element in diff c is called a divisor. In fact, diff c you should think of as a set of divisors of the curve and the points pi's you should think of as prime numbers.

So, divisor is nothing but a product of primes. So, what was in school product of primes here it is actually a sum of primes. Okay, so there is this philosophical shift from looking at products of numbers to sum of, sum of primes. That is why this comparison is, could be confusing in the beginning.

Just take logs. Yeah, so you did log in class 10th, so with product of primes and log, now you have divisors. Who defined this structure first? Yeah, I credit for everything Vail, but I am not sure. I think the biggest, I mean the most impactful results I think are due to Vail, because this is remember we are doing this for any curve. General curves were not studied before Vail over finite fields. Yeah, but I think Hassa must have also developed something, which we will generalize to curves.

Yeah, needless to say these things people had done for complex curves, like Riemann proved things only for complex curves. So, we will be giving Riemann's proof for the divisor group after the mid sem. That was for complex, but then we will generalizes it to any field. I we can now immediately define the order map. So, order at a point of a divisor should do what? So, it should send a divisor to the number a p such that d is a p times So, the coefficients we will call them orders of the respective point or prime.

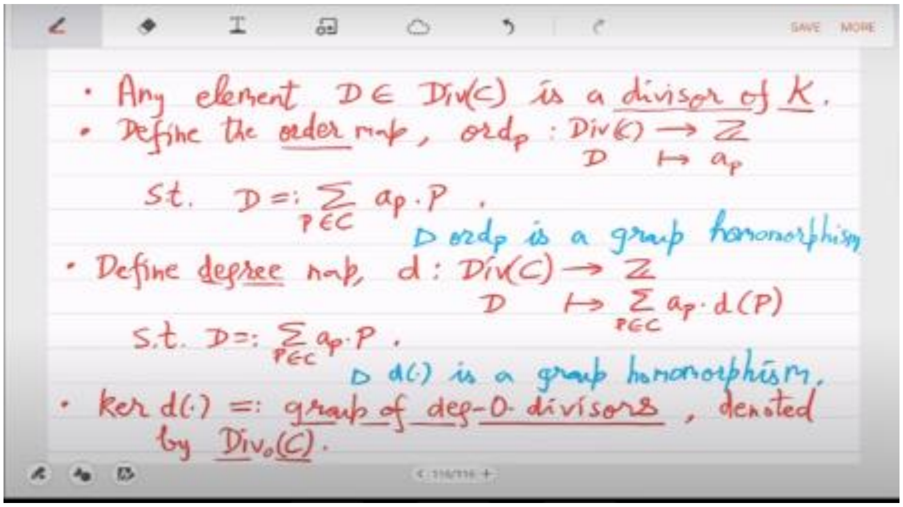
No, no, no, no for a point this order is for a point. So, for p 1 it is 2 and for p 2 it is 3, 5 is what you are calling 5 will be the degree we will define that I mean obviously, order is a group homomorphism. it is a group with respect to addition, group homomorphism with respect to addition, right. div c is with this is an additive group and integers obviously here an additive group.

So, this is just a group homomorphism, sums go to sums. we can also similarly define degree. So, degree is yes slightly more complicated than you would think. So, this will be you would think it is ∑ But what it should be? Exactly. The degree that we have defined for a point before. Okay, so for a divisor ∑ AP times P.

degree is basically ∑ AP but you have to weigh on the degree of the point itself as well. Because the point as I said it is actually not a real point it is a cloud of conjugates. So how big the cloud is you have to put that weight there because you want to keep track of the count of finite field points properly. So, that is the motivation of course, you may not be able to see that immediately, but there is some intuition for this. This is also a group homomorphism.

Is that clear? So, when you add two divisors, if you are looking at the same point in D1 and D2, then the degrees will be equal. So A of P1 and A prime of P1 you can simply add, right? And if the points in D1 and D2 that you are looking at are different, then they will contribute in different places. So this again is a group homomorphism almost trivially with respect to addition. Yeah its kernel is an important object. So, kernel of D is called the group of divisors of degree 0.

I mean obviously they are degree 0 and they form a additive group again. So, those elements are called degree 0 divisors. For example, it could be p1 - p2, if p1 and p2 are of equal degree or if they were actual points then their degree is just 1. So, in that case p1 - p2 is a degree 0 divisor. and this has a special respect that we give, it is called, it is denoted by div 0 C. Okay, most of that all, almost all the time we will be actually working with this div 0.



- Any element $D \in Div(C)$ is a divisor of K.
- Define the order map, $ord_P : Div(C) \to \mathbb{Z}$, $D \mapsto a_P$

  s.t. $D =: \sum_{P \in C} a_P \cdot P$.

  $\triangleright$ ord_P is a group homomorphism
- Define degree map, $d : Div(C) \to \mathbb{Z}$, $D \mapsto \sum_{P \in C} a_P \cdot d(P)$

  s.t. $D =: \sum_{P \in C} a_P \cdot P$.

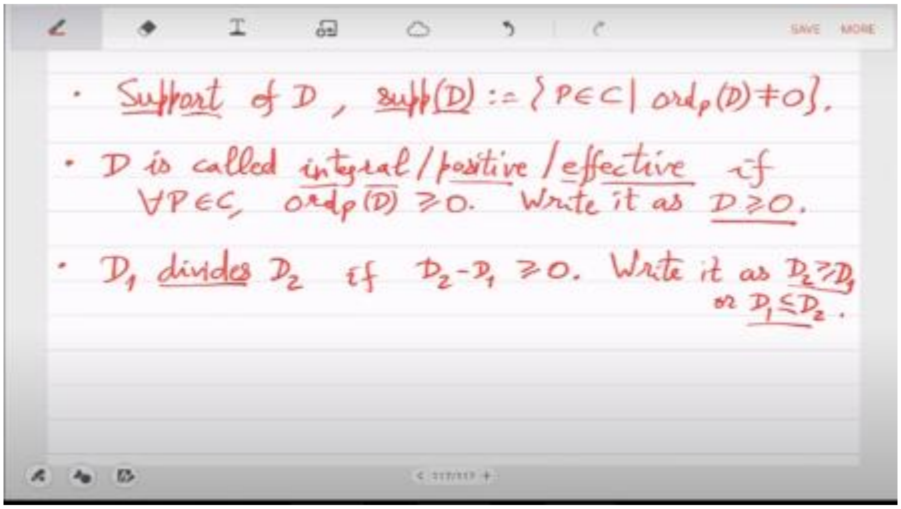
  $\triangleright$ $d(\cdot)$ is a group homomorphism.
- $\ker d(\cdot) =:$ group of deg-0 divisors, denoted by $Div_0(C)$.

Yeah, there are other small things we have to define, let us do that on Friday. Any questions? Actually, let me continue and define two things. There are lot of keywords. So, support of D. this I kind of already mentioned it is the points that actually appear whose order is actually which are actually appearing in the divisor D that is the support set.

So, D will be called integral or positive or effective depending on the literature that you use. If for all the points on the curve the order is what? Non negative. Okay, so the integral divisors I mean again you can think of integers right. So, integers which have prime factors with exponents non negative they are called integers. So, similarly integral divisors positive or effective you can define.

Based on this you can define when does a divisor divides another divisor. So, d 1 divides d 2 just like numbers if d 2 - d 1 >= 0 that So we say that a divisor D is >= 0 if and only if it is integral or positive or effective. And we say that D1 divides D2 if the difference is that which in other words every order that you see in D2 is at least that in D1. Then you can define divisibility like this.

and unsurprisingly this can be written as D2 > D1 or D1 <= D2. There is no, this is well defined. So we can, we are, remember we are defining these inequalities now in our own way. We are comparing these formal sums. It is not automatically defined. Oh and what happens if D1 <= D2 and D2 <= D1? If D1 divides C2 and D2 divides C1 then what happens? Yeah then they are equal right. So, this is not a stupid notation it actually follows what you think it should. Okay I think yeah this maybe we can continue next time.



- Support of D, $\underline{\mathrm{supp}(D)} := \{P \in C \mid \mathrm{ord}_P(D) \neq 0\}$.
- D is called integral/positive/effective if $\forall P \in C$, $\mathrm{ord}_P(D) \geq 0$. Write it as $\underline{D \geq 0}$.
- D_1 divides D_2 if $D_2 - D_1 \geq 0$. Write it as $\underline{D_2 \geq D_1}$ or $\underline{D_1 \leq D_2}$.