Computational Arithmetic - Geometry for Algebraic Curves

Prof Nitin Saxena

Dept of Computer Science and Engineering

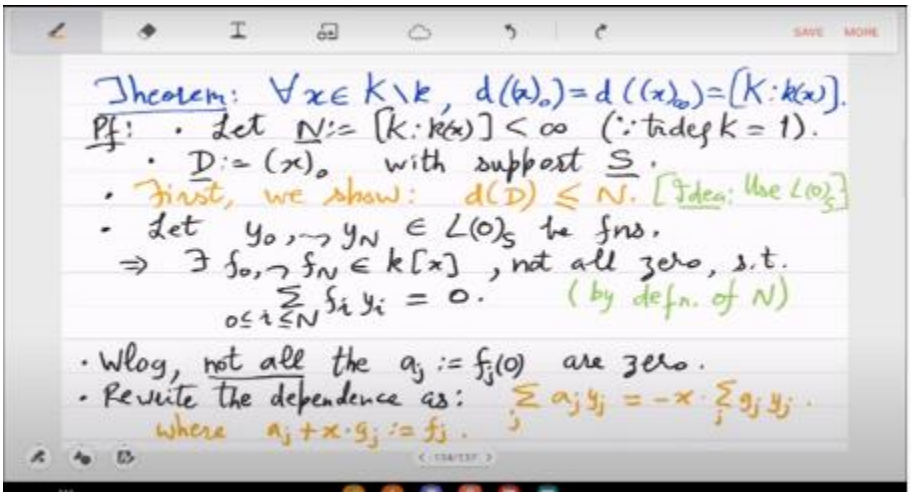
IIT Kanpur

Week - 09

Lecture – 17

Genus of a Curve

Any questions have you studied genius in some math course oh you don't do topology or complex analysis oh I thought every math student will know that Because topology also has this pretty early. Topology was not really a compulsory course. See. So, let us recall the last class, we mainly proved this theorem. which gives exact characterization of the degree of principle divisor of any function, any proper function in the function field, what is the zero part and what is the pole part and it happens to be related to exactly the degree of a field extension. this finite, this algebraic extension.

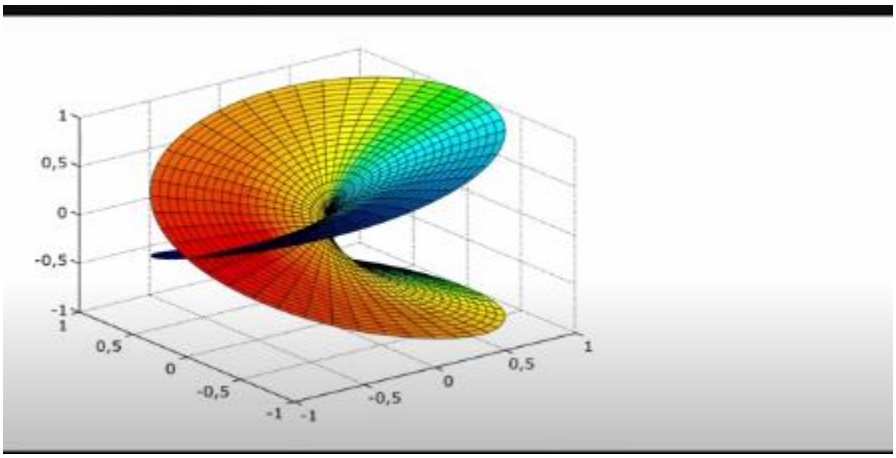


Any questions? And from this we learnt that principal divisors, so in basically for functions the zeros and the poles are equal in number, at least equal in degree, right, which is like a basic fact you would conjecture but it is not very easy to prove for curves, because over curves your function is more complicated, it defined only on the points of the curve. So, your zeros and poles actually come from curves and we are showing in this domain that even here the poles and the zeros are equal in degree. So, that defines the class group div C and div 0 we can mod out by div A which is the principal divisors. So, we get the class group of divisor and the class group of degree 0 divisors and we have an

exact sequence of these abelian groups CL0, CL and Z.

So, now we will do something which is considered quite advanced. We will talk about Riemann's proof of genus and we have not even defined what genus is. So, this theorem will actually be the first definition of genus that you will see. So, since you do not know what a genus is, let us first take a detour on genus. Genus is something that was invented to basically classify curves over the complex field.

So, what happens in complex field, so in complex analysis a curve C is drawn as a Riemann surface so this in itself is an achievement because if you imagine what is happening you have this y^2 equal to say you have a curve $y^2 = fx$ and if y and x both take complex values it is not clear how will you draw this like you can only draw real points you can't really draw complex points so the complex axis generally you learn in school is it comes with the real part and the imaginary part. So, you have the real here and you have the imaginary axis as the y axis. So, x has two axis and y also has two axis. So, there happen to be four axis. So, it is already a very high dimensional question in terms of real pictures.



So, Riemann actually gave a different picture for this, which is this. okay so he said that instead of four dimensions we can actually imagine this in three dimensions so what is done is that the x and y axis here are the real and the imaginary parts of your argument so you can think of that so this in particular is the map of $y = x$ or $y^2 = x$ in our notation this is $y^2 = x$ or in other words $y = \sqrt{x}$. So, you are given a complex and you take square root you get another complex you get two options. So, x is in the bottom plane real imaginary parts and then in the vertical axis is the real part of the answer which is $\sqrt{x}$. So, the real part of $\sqrt{x}$ is what you are plotting in the vertical direction.

There is obviously you are missing something here which is the imaginary part of √ (x). So, that part of y you are missing. So, that is compensated by the coloring. So, the colors actually are the imaginary parts. So, this is what is called the Riemann surface representation of a complex curve.

So, you can see that this is not so easy to imagine if even after all this coloration, but at least Riemann defined this you can now draw this you can imagine in 3D space what and the first thing you want to study is like is this thing continuous and next thing you study is whether this thing has holes. So, are there places on this Riemann surface which the equation will not touch. So, it will be a whole right. So, the number of holes is called genus. No, no color is a spectrum, it is a real number right, colors from 0 to 1.

So, you can see that the red is not a single red. It starts from orange and it again ends in orange and then it converts to yellow and green and there are all these shades. Color is also an axis, yes, but it is being colored inside the surface. So, there are two things which are happening. First is a curve has become a surface because you want to visualize it in the real 3D space or real 4D space.

So, curve will become non-curve. So, in this case it has become a surface is locally it will be a two dimensional object. So, you will have two tangents which are independent. So, I mean basically a plane in 3D if you draw a plane. So, here it is locally everywhere it is a plane which is why you see these rectangles and the rectangle has a color.

So, this color tells you what is the imaginary part of √ z √ x and the height of the rectangle from the base plane tells you the real part of √ x. Yeah, so whenever somebody says rematch surface representation of a curve, it is this. This is pretty nice looking because $y^2 = x$, if you remember, is bitrational to the line. So, $y^2 = x$ is actually the kind of the simplest curve you can think of because it is just a line in a way algebraically. So, this is why the surface you are seeing here will have no holes; I mean, it will be continuous everywhere and differentiable in all aspects.

This is a genus 0 Riemann surface, and the complex curve is referred to as having genus 0. Yeah, so that's the picture, and then things will get crazy, which we will now do algebraically. So, complex curves—yeah, I mean, sure, you want to understand, even before homeomorphism, the difference between, as I said, \(y^2 = x\) and \(y^2 = x + x^3\), right? Are these two things different? Now you know from your algebraic development that these two things are very different: \(y^2 = x\) is just a projective line, while \(y^2 = x^3 + x\) is not. So, let us write that down. So, you want to understand the difference between these two, and you can also set y = x.

So, what is the difference between \(y = x \), \(y^2 = x \), and \(y^2 = x + x^3 \)? So, the first two things are simply the projective line, at least up to birational equivalence. The third thing is completely new. You can demonstrate that I mean you have already seen that these two are not bi-rational. So, geometrically, can you identify a difference? Believe it or not, the difference is that in the last one, there is a hole, while in the first two, there are no holes. You can see this when you draw this Riemann surface over the complex plane, which I will not do.

No, the first two things are what I just drew, correct? The sentence "Yes." is already grammatically correct. Yeah, but I don't want to say that because you don't see a sphere here. The sentence is already grammatically correct. So, yeah, I mean you are thinking in terms of homeomorphism, which we have not yet defined.

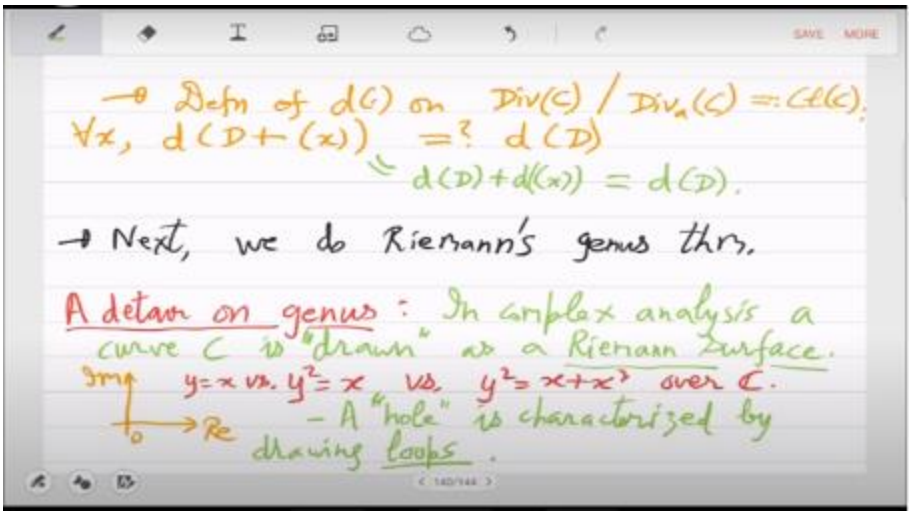
The sentence is indeed grammatically correct as it stands. No corrections are needed. The sentence is already correct as it stands: "It is just a short detour." I do not want to divert into a course on complex analysis. The sentence is already grammatically correct.

If you prefer a slight rephrasing, you could say: "I do not want to take a course in complex analysis." So, yes, that is the rough goal of Riemann and those who came before him. The sentence is already grammatically correct. Yes, there will always be a hole, and that hole essentially signifies that. So, it is currently unclear what it signifies.

In the picture, you will see that in the 3D space, there is discoloration in a part where there are no colors because that part does not exist on the surface. But can it be measured, and can it be calculated? So we will formalize that, in fact. (The original sentence is already grammatically correct.) No, no, hold on; we have not defined the genus yet. So, we have just defined that picture, and the difference between the graphs of \(y^2 = x \) and \(y^2 = x + x^3 \) is that there will be a location where there are no colors; that location will not exist on the Riemann surface.

The sentence is grammatically correct as it is. No changes are needed. So, that part will naturally be called a hole. How is a hole characterized? So, by drawing loops, we can achieve the desired outcome. The sentence is grammatically correct as is.

No changes are needed. So, you have this continuous, I mean, almost everywhere continuous Riemann surface. So, you start drawing loops around these rectangles. If everything inside the loop is present, then it is not a hole. (The sentence is already grammatically correct.) If there is a loop that you can draw inside of which the space is empty, then that is a hole.



The number of such empty loops will be referred to as the number of holes, which is called the genus. To formalize it effectively, you must demonstrate that you essentially need to use this equivalence of loops. So, two loops are considered equal or equivalent if there is a suitable transformation from one to the other. So this nice transformation is what Deeptajit was referring to as a homeomorphism. I mean, it should essentially be an invertible transformation that takes you from one loop to the second loop and back.

The sentence "Sorry." is already grammatically correct. If you would like to expand it, you could say, "I'm sorry." Homotopy. (This word is correct as it stands. If you meant to provide a fuller sentence or context, please share that for correction.

) Yes, homotopy; in the category of loops, it is an isomorphism. So, for example, this is loop 1, this is loop 2, and this is loop 3. By transformation, it is meant that you can somehow map every point on loop 1 to loop 2 and every point on loop 2 to loop 3. So, in this sense, you can go back; you can transport yourself from loop 1 to loop 3 in any way you want.

So, all these loops are the same loop. (The sentence is already grammatically correct.) Moreover, if you can, if there is a loop that collapses to a point, then it is a no-loop, and this will only be possible if everything inside the loop is present on the surface. If everything is present on the Riemann surface, then you can continue shrinking the loop all the way to the origin. To the center-right. So, it will become an infinite simile, an infinitely small loop.

So, we say that there is no loop that represents the zero genus case. Yes, of course. (The sentence is already grammatically correct.) So, these things came first, and whatever we

saw in the last two months came last. But we do not want to keep doing this translation because it is confusing, at least for me, and is also very painful.

You have to define things here; you need to clarify what we have defined in the course, and then you have to show that they are equivalent. It is not very easy. So, that is what is meant by a nice transformation. (The original sentence is already grammatically correct.

) So, for example, loop 4 is simply a point. Here, Loop 1, Loop 2, and Loop 3 are the same. So, we count this as 0 loops and this as 1 loop. I mean, I shouldn't say it's just one loop; maybe this also converts into four, and four shrinks to a point. So, whenever a loop can be transformed into an infinitesimal loop as much as desired, we say that essentially there is no loop, and we call that genus 0; otherwise, the genus is the number of actual loops. The genus of a curve is defined geometrically as the number of distinct classes of loops.

So, this is the case of genus zero. So, if everything inside is present, then you can shrink it to a 0-loop, which has genus 0. If this occurs everywhere on the Riemann surface, and if there are holes—like this one is a hole and this one is a hole—then it means that the genus is greater than 0. So, in particular, the genus will always be a non-negative integer, and it will align perfectly with our geometric intuition of what a hole is on a surface. Why shouldn't we expect the genus to be equal to the number of poles? Yeah, but which pole? The sentence is already grammatically correct: "There is no global function." Except for the equation of the surface, such as \(y^2 = x \), I mean, you cannot really say that \(y^2 = x \) has a pole because that is kind of the defining object.

So, it has no poles; it only has zeros. So, you need to look at some other functions. So, that was the starting point of Riemann's theorem: Is there a magical function whose poles or zeros can tell you about the whole? So, what you are asking is also what Riemann asked, and he was able to solve it completely. Actually, that is what we will see. Maybe you deserve one more picture, which is quite a famous image of a torus. The sentence "Where?" is grammatically correct as it stands.

If you would like a more complete expression, you might say, "Where is it?" or "Where are we going?" depending on the context. Yeah, maybe - one. (The sentence is already grammatically correct.) Yes, it depends on whether you are counting the zero loop or not.

I do not want to count it. (The sentence is already grammatically correct.) Yes, perhaps. (The sentence is already correct.) Sure, here’s a corrected version of the sentence: "Yes, let's say - one.

" The sentence "Fine." is already grammatically correct, but if you're looking for a more complete expression, you could say "That is fine." or "It's fine." So, there is one 0 loop, one 1 loop, and many 1 loops. The count is the number of distinct loop classes - 1, and this is also the number of holes. So, this is another example; this is your first example of genus 1.

So, you should think of the blue part as a donut. So, it is basically a cylinder to which you have joined the endpoints. So, it is basically a ring—a three-dimensional ring. So, essentially, you have only two kinds of loops: one is a loop that you can wrap around the ring, and the other is a loop in which the ring is essentially a circle, right? So, the orange one is the larger circle of the ring, and the red one is the thinner circle of the ring. Any third loop can be collapsed into one of these.

(The original sentence is already grammatically correct.) Now the red one can be collapsed to a point, making it a 0-loop because everything inside it is present. The orange one is very different because, ultimately, it gets trapped and stopped by the hole. So, I think there should be distinct loop pluses of 2. So, this is a genus-1 object.

This means that the number of holes is one. So, this is how it is defined: when you are doing actual geometry or algebraic topology, this is the way you will understand it. First, you can observe the hole in the Riemann surface, and then, to generalize it, you can study it via loops. Is that clear? So, that is a brief detour. (The original sentence is already grammatically correct.) Now, the central question is, "Why?" The sentence is indeed correct as it is.

No changes are needed. Yeah, so orange is the only one that is whole. But on that surface, you will find two loop classes, right? Yes. So, the genus will be 2 - 1. (The original sentence is already grammatically correct.) But in the case of two holes, how many loop classes will you get? You should get it.

You get one by going around one hole. You should get it. One goes around one hole, another goes around both holes, and the constant one. So, you may be right. Okay, that is problematic. So, you are saying one around this, one around this, and another one around this, while the others are silly? So, you have distinct loop classes.

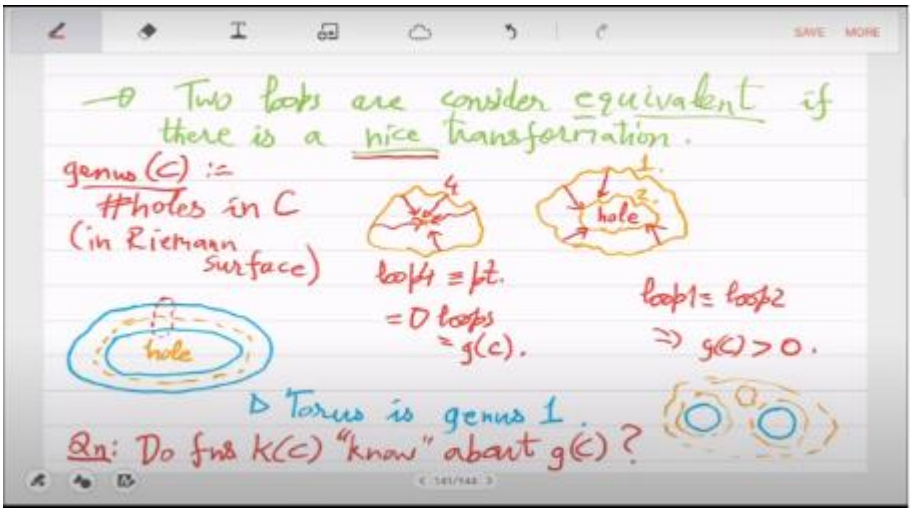
(The original sentence is already correct.) So, what is the answer? Then it is 2 raised to the power of n, yeah. Okay, so let me avoid going into that kind of formula. No, these are not equivalent; these are two different holes.

How will you—oh no, that will not be. I don't think so, no. Yeah, I think you are, and we

might be confused by the 1, 2, 3 example, maybe. Yes, that example may not be very good. So, the genus should ultimately just count the number of holes, as we all agree. Events are seen in the Riemann surface representation, which is the only way to imagine a complex curve. The number of holes should correspond to the genus, and we are achieving that.

So either there is no hole, which means that there is only one loop class, or there is one hole in the case of a torus, which is genus 1, or in this example. So, yeah, you can think about this; this is a whole area in itself that will not be touched on in this course. But what we want to question now, which is Riemann's basic question, is: do functions Kc, the function field of the curve, know about the genus? Once you have defined the geometric genus, the question is whether, algebraically, the largest objects you have are these rational functions defined on the curve. The sentence is already grammatically correct.

That is Riemann's question, and it has an incredible answer. So, the LD sheaf that we have defined, Riemann showed, actually knows about the genus. So, the difference between the L dimension and the DD - LD gives you the genus. So, Riemann demonstrated this in an important year. That this \(l_d - d_d - 1 \) is equal to the negative of the genus. Okay, so this connects the geometric definition of genus with the algebraic object, which is the dimension of L.



That is true for the minimum of this. If you minimize the difference between L and d, you get the genus. Now we are not in the complex case; we are in the case of finite fields. In finite fields, there is no known representation, so we cannot draw anything. We cannot define genus; there is no geometric definition of it.

So what we will do is just cheat and take this as the definition of genus. But it does not. (The sentence is already correct.) So, Riemann showed that it gets stuck in genus. It cannot go below - g - 1. Yeah, that was the brilliant insight of Riemann, and it is completely unexpected.

I don't know if there is any good intuition for that. The sentence is already grammatically correct. However, if you're looking for alternative phrasing, you could say, "Why was this done?" But for him, it was a theorem. So, he wanted to say that you can think of this as a way to compute the genus. He wanted to compute the genus without drawing anything, so it has to be an algebraic concept. The algebraic expression is ld - dd, which is something you can actually compute.

So it's kind of an optimization algorithm that will give you the genus. We will actually take this as the definition of genus because we do not have any other alternative for it. So, the left-hand side becomes the definition, but for that, we must show that in our world the minimum also exists; perhaps the minimum does not exist. For complex curves, he has shown that it exists and, in fact, it is equal to minus the genus; however, in our case, it may not be true. It is almost equal for low genus these two things are almost equal. So, for example, when the genus is 0, you would expect that, let's say, random divisors LD and DD will be very similar, and as the genus increases, there are more holes.

Thus, these LD sheaves actually start behaving in a wild way. Yeah, for random D's, I mean this is not true for every D, but for a large enough degree, exactly. So, for a random D, you would expect this to be an equality. Well, by the end of our proof, we will compute it. So, we will compute it over finite fields as well. Since we do not have any way to define genus over finite fields, we intend to use this theorem, which we have not yet proved, as a definition.

So, the theorem will now be this. So there exists a number g, which we will call g, for the curve above. So, the curve for us is always a function field of transcendence degree one, right? So, that is what is given to you over a base field \(k \); it can be anything. So, there will be a number such that for all proper rational functions, \(x \) is the minimum over all \(m \). Okay, this will actually be an even more specialized and stronger statement than what I said before.

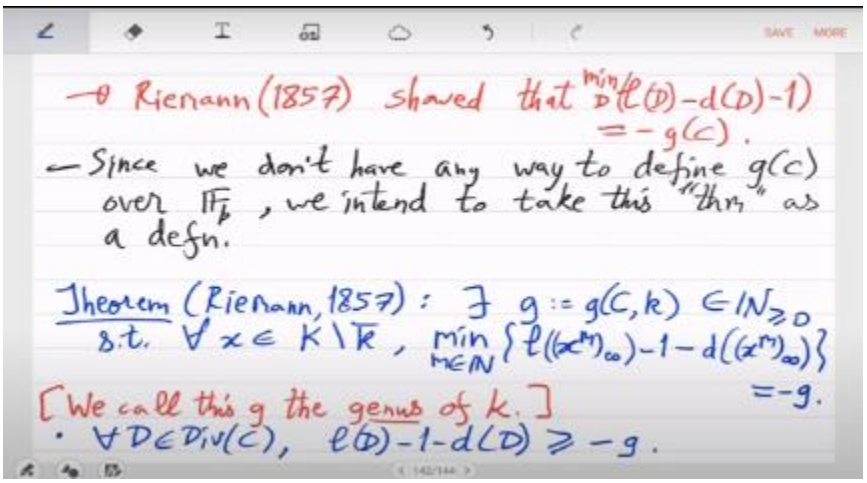
If you just take a rational function and look at its powers and poles. Okay, so the L dimension of that - 1, minus the degree of that, = - g. It is lower bounded. That is what we will show, and this is why this number exists; we call it the genus, the genus of k. The other part is that for any divisor \(ld - 1 - dd \) >= \(-g\).

So, basically, the second part is that this minimum is independent of the divisor. It seems like your sentence is incomplete. Could you provide more context or the full sentence for correction? So, you actually can. So, here we are only going to minimize over the integers m. Actually, I think I do not need negative integers; I believe natural numbers should be enough.

This theorem states that no small \(k \) is our base field. No, Riemann, you know that in those days, they did not have finite fields. They would only think about the field of complex analysis, which is why I showed you that picture of Riemann. Well, that is because the proof exists. No, look at the first red part; Riemann showed this for complex curves on his surfaces.

Because he already had a definition of genus, which is based on holes. Now we do not have a definition of genus, but we will go through his proof, and the minimum that we obtain will be called genus. Yeah, the minimum is a number, and that number for us is genus. Because we do not have any other option for the definition of genus. So, actually, we are in a completely hypothetical world; we cannot see holes, and we cannot even define them. So, whatever algebra gives us, we will just call that genus, and we will hope that everything works just as well, which it will.

So, it will be more accurate to say that it is an abstraction of Riemann's proof. Any questions? Actually, what we have seen now is that the proof is quite easy. We have already done the development, so just recall the degree proof that we discussed in the last class; we will refer to it. So, let's begin with some proper function on the curve and consider the finite field case, as it will provide a stronger proof than Riemann's. As in the previous class, "begin" is the degree of the field extension.



And let \(s \) be big enough, which we also discussed in the last class. Remember, we had this for big K; we have a basis, and then for the basis YJ. We had valuations, and we wanted S to be significant enough according to those valuations. So, it is the same S as in the last class, and it is the same from the last class. We know from that proof that for all \(t \), what we obtained is \(n \times t \) <= \(L x^{s + t} \), where \(L \) is the dimension. We had shown that the L dimension of the pole part of \(x^{s+t} \) is lower bounded by \(N \), which is a constant for us in this setting.

As you exponentiate \(x \) more and more, the L dimension increases in a linear way. This is what it is saying: we received this in the last proof. This is here. So, Lx + t is at least the size of b, and we actually gave you this many elements as well. So, we are at that part of the proof; let us continue from there. So, writing \(m \) = \(s + t \), we deduce that for all \(m \) at least \(s \), let us check the difference \(l - d \).

This difference is at least \(nt \) from the above, minus what is the degree. The degree we have shown is \(m \) times the degree of \(x \) at ∞, which is \(\text{begin} \), so that is - \(S_n \). So, that is the proof of the genus or the lower bound. So, as m increases, the difference (l - d) remains lower-bounded by s times n, both of which are independent of m. Therefore, irrespective of how high a divisor you take, the (l - d) difference will not become small.

It will always be lower bounded by this absolute constant in our setting of s times n. Therefore, this implies that the integer μ, the minimum of M, exists. So, we can define this as 1 - g, where we will call g the genus. So, that is the first part of the theorem. Do you have any questions? All we have done is show that the L dimension grows almost linearly; it grows very quickly compared to the degree.

So, the difference between L and the degree cannot fall below a certain point. There is an absolute threshold that it cannot cross, and that threshold is called the "genus." Does it depend on X? Yes, that is the second part. (The sentence is already grammatically correct.) Yes, it does right now.

So, let us do the second part now that the genus depends on nothing except your curve. So, that will also complete the geometric intuition. But before that, perhaps I can mention one thing, as it will be useful for the computation. So, note that \(n \) is the degree of the extension. So, intuitively, if you have a function like f(x, y) = 0 for the curve, and if that describes the curve of degree d, then this would be <= the degree of the curve and s.

So, you have to recall what was correct; this was the valuation of essentially the conjugates of y. So, that will also be upper-bounded by the degree. So, this means that the

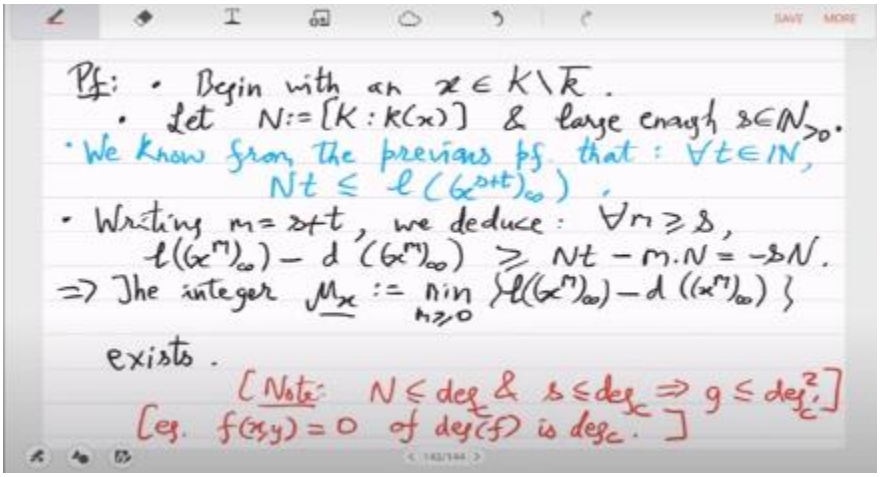
genus is upper-bounded by the square of the degree. So, the genus is not too large. I mean, this number—this proof also indicates that the genus is only quadratic in relation to the degree of the curve.

So, it is not that this can be exponentially large. The sentence is indeed already grammatically correct. No changes are needed. It depends solely on the degree in a polynomial manner.

So, you could potentially write an algorithm for this. The degree of D in relation to x is. D (x). Well, I meant the degree of the curve. So, I haven't defined it properly, but an example is if your curve is \(f(x, y) = 0 \). Then, the degree of this polynomial. So, I mean, a curve can be presented to you in a very complicated way.

However, the curves you will imagine first are these planar curves embedded in a plane. They are provided by a single equation. So, regardless of the degree, you can see that big N is bounded by that, and S is also bounded by it. So, the genus is bounded by a quadratic of degree. So, it is a small number; it is not a very large number. So, now let us address the second part of the theorem, which states that you can also minimize over all possible divisors and obtain the same genus.

You do not need to work only with x ∞; it can be any divisor. So, let us prove that. Let us write down its zeros and pole parts. We separate the divisors into zeros and poles: d 0 and d ∞, they are both positive. So particularly means that d0 is greater than atleast D. Therefore, what we will do is we will connect them.



Yeah, but you can express any divisor as a difference of positive numbers. The definition of d_0 is 2d. You can express any divisor in positive and negative parts. The positive part

is d zero, and the negative part is d ∞. So, it is not \(x_0 \); it is now a general \(d_0 \). I care only about their positivity. So, what I want to do is study \(ld - \text{degree of } d \), and I want to show that this is again lower bounded by genus.

For that, yes, you are correct; we somehow have to connect this with \(x_\infty \) because our first part is from \(x_\infty \). We will do this in two steps: first, we will connect \(d \) with \(d_0 \). Since D0 is at least D, what you can deduce is that L (D) - D (D) is at least L (D0) - D (D0).

That is from the LD sheaf that we studied. If you increase the divisor, the difference can only get smaller. From this, I can deduce something. Well, let us consider that the other connection is from here to ∞. So, as x approaches ∞, since d0 is positive, I can also connect this; I mean, I have this inequality trivially, and I can now examine the L sheaf of the left-hand side (LHS) and the right-hand side (RHS). The sentence is already grammatically correct as is: "So, what does that give me?" This gives me L of - d0 + or - d of that.

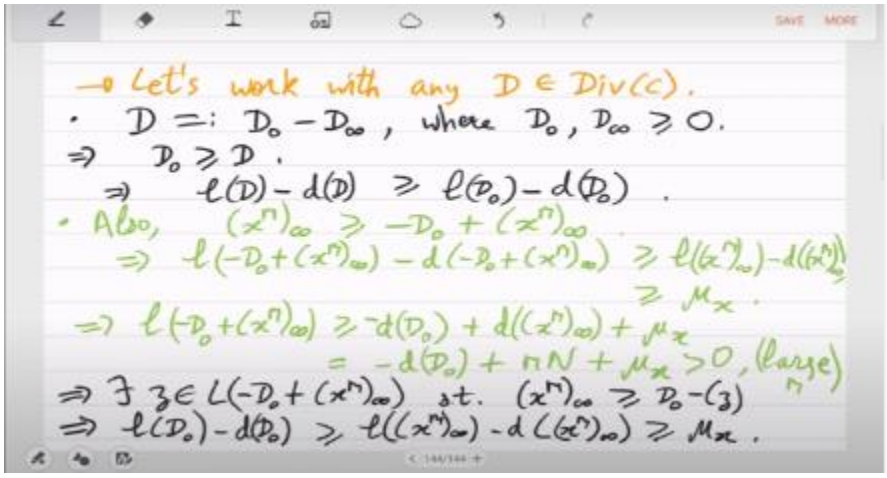
It is at least - d (x m) ∞, right? We have shown in the first part that it is lower-bounded by 1 - g. So, these are the two connections, and now let us combine them. Actually, sorry, maybe I should—no, it's okay; I think g has already been defined, so it's fine.

I think mu, yeah, maybe mu x. Yes, you are right. This integer—yes, maybe μx is a better term here—depends on x. Let's stick with μx. Okay, so that is equal to the degree of \(d\) - \(d_0\) - the degree of \(d_0\) + the degree of \(x_{\infty} m x_{m \infty} + \mu x\), which is what the degree of \(x_{m \infty}\) was. We know exactly that, yes, and \(m\) is growing arbitrarily while \(d_0\) has been fixed for the discussion. So, since m continues to grow, it will eventually become positive at some point.

So, the l dimension of - d 0 + x m ∞ is positive; that is what we have learned from this. Okay, so this means that a function exists; the L dimension is positive, so there is a function in the L-sheaf that meets the definition of an L-sheaf. So, by that, you will essentially conclude that the z divisor of z - d0 + xm ∞ must be non-negative, >= 0. So, we have rearranged it. (The original sentence is already grammatically correct.

) What do we learn from this? (The sentence is already grammatically correct.) So, we again use the L minus degree difference of both sides to deduce that this is at least L - D (X_m ∞), which is at least μ_x. Is that clear? So, all I have done is look again since Xm ∞ is a larger divisor. So, L - D for that will be <= L - D of the RHS. Corrected: Therefore, L - D for that will be less than or equal to L - D on the RHS.

Now, you just have to observe one thing here: L (D0) - Z is the same as L (D0). The sentence is already grammatically correct. So, yes, the dimension of the L sheaf does not change if you add a principal divisor. The sentence is already grammatically correct as it is. Maybe we should write this down.



Yes, so L (D0) is the same vector space isomorphic to L (D0) - Z. What is the isomorphism? Sure! Here's the corrected sentence: "Yeah, so if you have a function \(f \) such that \(f + d_0 \) >= 0, then you have to construct a function \(g \) such that \(g + d_0 - z \) >= 0." (Note: The original sentence is already grammatically correct.) So, for that, you just use f of z; that is the isomorphism.

So, up to the principal divisors, the L sheaf is well-behaved, and the degree is also well behaved. So, that is what I did. So, I have written that L - D is at least L - D (xm ∞), and yes. So, now connect the two, and you will get what we want. So now we have L (D) - d (D), >= μ(x). That was the second part of Riemann's theorem: for any divisor, you define μ(x) via some fixed proper function x.

However, the lower bound is also satisfied by any other divisor. Sir, could you please move back a little? Yes. As we show, a degree of 0 means that we obtain the space at some dimension. So, we know there is a divisor in L - d $_0$ + x ∞, right? There is a z, but how do you know it is a principal divisor? No, there is a function, and the sheaf has functions.

These are the functions of the curve. So, I just wanted a function such that it would... I mean, essentially, \(xm\) ∞ and \(d_0\) should be somewhat interchangeable, and they become interchangeable if the only difference is a principal divisor because, for principal divisors, both \(l\) and degree are well-behaved. So, that is what I have achieved. So now

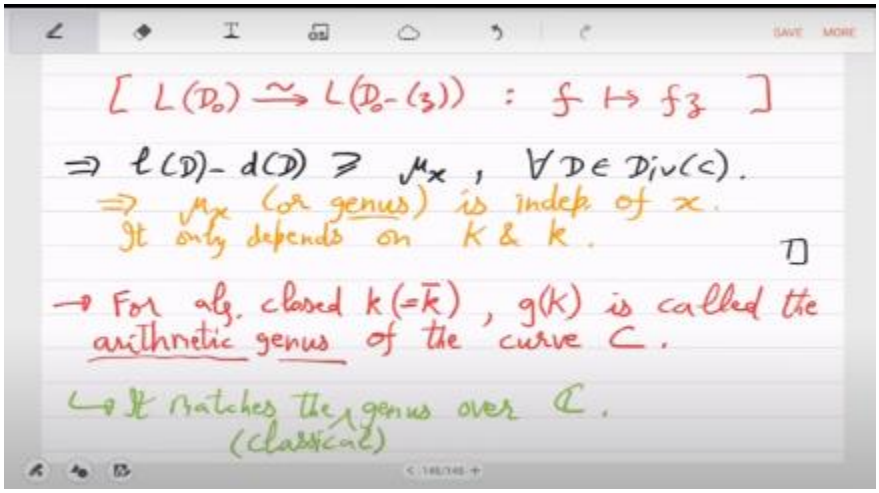
I have an immediate connection with my ex. Since I have a connection of D_0 with μ_x, I also have a connection of D with $\text{big } D$ and μ_x, where $\text{big } D$ is a general arbitrary divisor.

So, actually, in this genus that we have defined, every divisor satisfies this lower bound. The original sentence is grammatically correct. No changes are needed. Yes, this actually means that μ_x is independent of x; it only depends on the curve, which means the function field, a transcendence degree 1 function field, and small k. So, what is the curve that you have drawn, and what is the base field that you are studying? So, as these two things change, the genus may also change; however, it does not matter what the function is. So, this is an amazing proof, or even a statement, of Riemann, because it somewhat controls all the functions defined on the curve.

It is a property, so the genus becomes a canonical characteristic of the curve. The sentence is indeed grammatically correct as it is. No corrections are needed. So, yes, of course, we will take small k to be algebraically closed. For an algebraically closed field k, which means it is equal to $\overline{k}$, the genus of k is called the arithmetic genus. For a function field with a transcendence degree of one, or for the equivalent case of a smooth projective curve C, the arithmetic genus is considered when you are over $\overline{F}_p$.

The sentence is grammatically correct as it is. Yes, and if you are curious, you should know that the third part is obvious. So, the way we have defined it, of course, for the standard notion of genus in geometry for complex curves, it matches this exactly. That is clear by definition and by construction. So, all these other definitions that you have, which existed before, state that in complex curves, they are all equal to this.

So, all the classical definitions that exist are consistent with this. Yes, that is the story of the genus. The sentence is already grammatically correct. Yes, Deepthujit was interested in an algorithm. So, Riemann's proof provides an algorithm for computing the genus. So, what I mean is that I will just provide a sketch.



The simplest case, which is also frequently used in computer science, is the case of $y^2 = f(x)$ over f(p). This is called a hyperelliptic curve. (The sentence is already grammatically correct.) For hyperelliptic cases, this is not a very good example for genus; however, you will see the algorithm, and then you can try to generalize it. So, the basic idea in this case is that you have to compute the LD sheaf, which is the key object in Riemann's proof.

So, you first compute L (x) and M ∞. So, if you have computed the L dimension of \(x \) to the \(M \) ∞, where \(x \) is the same \(x \), then you know that for not very large \(m \) (with \(m \) being some \(d^2 \), where \(d \) is the degree of the polynomial \(f \)), the difference \(l - d \) will become the genus. Therefore, the degree of \(x \) to the \(m \) is easy to compute; you just have to compute the \(L \) sheaf. The sentence is already grammatically correct as it is: "So, what is that?" So, this is equal to functions on this curve.

Sorry, not this f; let us make it a capital F. Let the function small f be such that the principal divisor plus this >= 0. So, you essentially have to compute, and since you know this is a vector space, you need to find a basis for it. So, I will make just two observations. The first is that xm ∞ is very easy to compute. I mean, whatever the curve representation is, you just have to compute the zeros—actually, the poles—of \(x^m \), which will be very simple.

In this case, the only pole is at infinity. Sorry, yes, the point at infinity, indeed. The zero is simply when \(x \) equals 0, and the pole is just a point at infinity. Yes, and when you raise it to \(m \), all you are doing is increasing the multiplicity of this pole. So, it is very easy to compute this divisor; I mean, you explicitly know it. The sentence is already grammatically correct.

However, if you want a slight variation, you could say: "How easy is it to compute \(f \)?" So, if you can write it like this, it is a rational function. (Note: The original sentence is already grammatically correct.) So, you write it as \(ax + by + cx + dy \) for the unknown polynomials. Okay, any rational function where the degree of \(y \) can be reduced to 1 because \(y^2 \) = \(F(x) \) can be simplified. So, whenever you see \(y^2 \), you should replace it with that. Thus, your rational function generally looks like this: you just have to find \(a, b, c, \) and \(d \), and you already know \(x \) as \(m \) approaches ∞.

What are the points that appear there? You just plug those into this representation, and you will obtain a linear system in ABCD. We have a basis. (The sentence is already grammatically correct.) You can understand the basics of solving a linear system in that way; it wouldn't be a very large system because you know that, I mean, you have an upper bound on the L dimension, which is not very large. So, the matrices you are using in your algorithm are not too large.

So, if you can solve the linear system, you can find the basis. (This sentence is already grammatically correct.) You can find the L dimension, which enables you to determine the genus. You can generalize it fairly quickly for any curve. What is the boundary of M? Yeah, M, that will come from the proof.

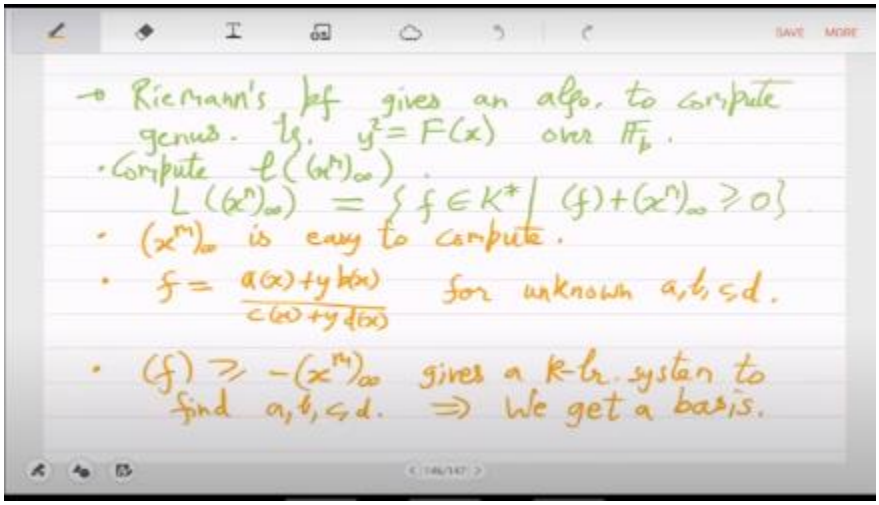
No, it is only that. We will know about genus G and S only, N, S, and G, but we do not know about M. Yeah, so that means you have to guess that it can't be too bad. Basically, s + t comes from here; this is the key equation. In this last equation, we said to let t tend toward ∞; however, in an algorithm, we never actually do that. We will make it big enough so that the next inequality, which is this one, can be reduced.

The sentence is already grammatically correct. Yeah, but you just pick t to be, say, bigger than l times ∞. Because you are only working with integers here, it is important to consider their properties. So, if you make the other part fractional. So, basically, if you are saying that something is <= 2 + 1/2, then it has to be 2 or less.

So, just use it. (Note: The original sentence is already grammatically correct.) So, these things can be worked out. I mean, you have bounds for everything; they are pretty small, and s + t gives you m. So, I do not think there will be any serious issues; it should converge very quickly to the general case. No, I will be surprised; this is foolproof.

So, details are missing, but it is not surprising that you can encompass everything here. The proof is clear; I mean, it is as explicit as it gets. Everything is in terms of degrees,

and all of that pertains to the field extension. So, what will we do next? Let us put on record that the genus is always non-negative. The sentence is already grammatically correct. However, if you want a more formal version, you could say, "Why is that so?" Remember that we do not have a concept of holes.



So, this is not trivial. We have just defined μx to be an integer. It can be negative. (The sentence is already grammatically correct.) It can be - 10 degrees. So, why can't the genus be - 10? How do you demonstrate that? So, we have shown that L d - d d is always at least 1 - g.

Therefore, let d be 0. So, the degree is 0. And I am 1. So, you get that 1 is greater than or equal to 1 - g. Therefore, you conclude that g is a non-negative integer. So, g-ness will not be anything surprising; it will be a positive number except when it is. Therefore, you can still imagine the same kind of holistic interpretation that was present in complex analysis.

It is counting something. (The original sentence is already correct.) Now, the other unsatisfactory part of the proof is that it is an inequality. Mathematicians, especially pure mathematicians, love equalities. So, they would want ld - dd to equal 1 - g, but you can actually show that this is false. You can always find divisors such that the left-hand side is strictly greater than 1 - the genus.

So, what is the hidden equality in this context? That will be our next lecture. (The sentence is already grammatically correct.) The degree of specialty of a divisor D is defined as δ(D), which is L(D) - D(D) + G - 1, and, by Riemann's theorem, >= 0. So, can we interpret this degree of specialty, and can we characterize it completely? So, when it

is not 0, the ideal case would be when it is positive. Why is it positive? So, what is special about the divisor? Why is it far from the genus? So, how is delta D related? So, how does delta d change with respect to d? So, sometimes it is 0; I mean, you know that at least once it is 0, while at other times it is positive.

So, why is it positive? (The sentence is already grammatically correct.) So, this was answered in an exact way by Gustav Rock a few years after Riemann; he was Riemann's student. So, next we will prove what is called the Riemann-Roch theorem. So, the Riemann-Roch theorem will be the most beautiful thing you can expect. It will be an equality where delta D is replaced by some canonical object of the curve, and it will indicate how the degree of specialty is changing with the divisor.

The canonical object that it will define is called a canonical divisor. But it will require more abstraction, so we will start it tomorrow. Rock actually died very early, but this is the theorem for which he is extremely famous. And Riemann died a few months before Rock. So, Riemann died a few months after Rock, who was only 26 years old.