**Computational Arithmetic - Geometry for Algebraic Curves**

**Prof Nitin Saxena**

**Dept of Computer Science and Engineering**

**IIT Kanpur**

**Week - 12**

**Lecture – 25**

**Proof of RH for curves: Galois covers**

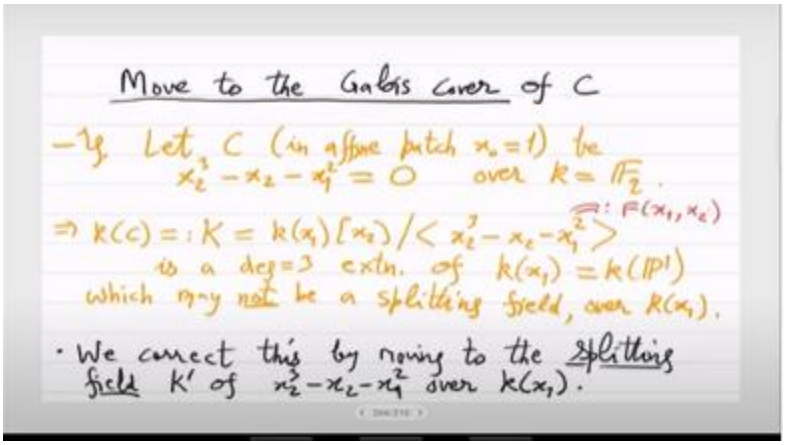
Any questions? So, we have a formula for the number of points in the finite field of size $q^n$ on the given curve. So, the formula is difference from the projective line which in that case will be q raise to n + 1 size. many points, difference with that is given exactly by this $\sum \alpha_e^n$, where $\alpha_e$ are the 2g roots of the complex roots of the L function. So, if once we show that each of these have absolute have norm square root q, we will get the error term to be very small, its square root of the main term. So, we do some reductions before proving the Riemann hypothesis. So, one is of obviously, this base change that Riemann hypothesis is true for a curve defined over finite field Fq, if and only if it is true for any higher field.

So, changing the field will not change the truth or falsehood of the hypothesis, Riemann hypothesis. Second reduction which is based on the first reduction is about the counting. So, as long as we know that the difference with the projective line of size $Q^D$, as long as we know that it is bounded by some let us say multiple of $q^{d/2}$ where multiple should not b should not depend on a and b should not depend on q or d. So, what can it depend on it can only depend on the representation of the curve.

So, curve was given to you via some polynomial or system of polynomial. So, in that a and b can depend, but they should not depend as we change q and d. So if such a estimate is available then again it will imply that Riemann hypothesis is true, if and only if, it is an interesting proof via convergence of infinite series. And here the last reduction, most important reduction is to Galois cover. So this is inspired mainly by splitting fields which appear in Kalwa theory.

So, the key example is if you take this elliptic curve $x_2^3 - x_2 - x_1^2$. So, think of $x_1$ as fixed to some constant. So, then it this is a cubic, but when you quotient by the cubic you only get one root usually you do not get all three roots. So, you want to go to a field

where all three roots are present that is called the splitting field and it is unique the minimum minimal splitting field is actually unique over k x 1 and that again will be transcendence degree 1 field. So, we can think of it as a curve.




and that curve is where we will try to prove Riemann hypothesis. Yes, so there are kind of four fields, one is the field of constants k, k other is k x 1, that is the transcendental field then over that we have algebraic extensions. So, K is the function field of the curve and K ‘ will be its Galois cover. Both these top extensions they are Galois extensions which means that if you write down any polynomial with coefficients coming from k x 1, if it has a root in k ‘ it has all the roots, I mean you if you write an irreducible polynomial. So, any irreducible polynomial which has one root in k ‘ has all roots in k ‘.

So, that is called normality. is not very important here, but it kind of tells you why we are there. At the level of, so the geometry is over the projective line which is basically k x 1, we have a covering by a given curve and we have constructed a new cover C ‘ there. So, such that what happens I just finished the revision do you have any question. So, we are at Galois cover.

So, what is happening is we have the projective line which we covered by the given curve which means basically that any point P 0 here. So, if you look at its let us say second you just project it to one of the coordinates and that will be a obviously it will be a point in on the projective line. So, usually we take it to be x 1. So, p 0 is first coordinate when you project p 0 to the first coordinate then you get a point on the projective line and the second coordinate x 2 that has at least one value is present, the other values may or may not be present. So, in the case of elliptic curve there are three possible values of x 2, maybe only one is present.

So, to get the other values we go to the cover C ‘, where you will see all the missing x 2

coordinates. So this is the new thing that we have done. Yes. Yes. Wait, FQ raised, you are changing the finite field.

No, no, no, no, it is not, it is actually, this discussion is nothing to do with the finite field. So, k could have been complex also. This is a field independent base field independent discussion. Because it is happening because the thing is happening over x 1 which is a transcendental field. So, it is more a property of the transcendental field and where what algebraic extension of that are you going to.

This k ‘ will be some k x 1 of some α. Yeah, where α is a functional thing it is not a constant. No, it is impossible because x 1 is a parameter. So, whatever α is it is a parameter it is based on the parameter x 1. So, if you fixed x 1 then α will become a constant, but by itself it can just be x 2.

So, this is more complicated and it is different from The traditional Galois theory which you study in one or two courses actually, they do not discuss this case, although the theory applies because you can take kx1 as your base field and then over that everything is algebraic and finite. So, it is, but it has an additional interpretation that Galois theory is not aware of. The additional interpretation is that here actually we are covering curves. So the curve basically any point in P1 was covered by few points P0s. and a point P 0 is being covered by few points in C ‘ where it cannot be covered any further.

So, P 0 whatever possibility of points is P 0, P 1, P 2 these we have now available. Yeah, you go to fq bar. Not possible yeah, because the same reason which I said that it is because of x1, it is not because of I mean you can take k to be complex, the problem will not go away. So, it is not an issue with FQ or FQ bar or complex. And the function field part you can think of like this.

So, k x 1 was the function field for the projective line. So, this is embedded in it is a sub field of k x 1 x 2 mod the ideal that defines your curve given curve and this will be a sub field of a bigger field. So for example, this over x2 we have also added y2, both x2 and y2 are algebraically dependent on x1 because everywhere transcendence degree remains 1. So x2, y2 they cannot be independent, they both are actually dependent on x1, I mean the 3 elements x1, x2, y2 the transcendence degree is exactly 1. and the ideal will have now new relations refining y2.

So, the arrows are expected I mean you know that the arrows will be opposite. So, the curve covers the projective line, but the function field is a sub field. The function field of the curve is actually a super field that of the line. So, this is by containment. and the ones above I mean the ones on the curve side are projection.

So, let me just give a concrete example here. So, you started with this elliptic curve. So, this gives you x 2, but you need other two points also. so for that what you can do is introduce this y2. So, x2 is a point corresponding to x the second coordinate corresponding to x1 and y2 is also a second coordinate corresponding to x1.

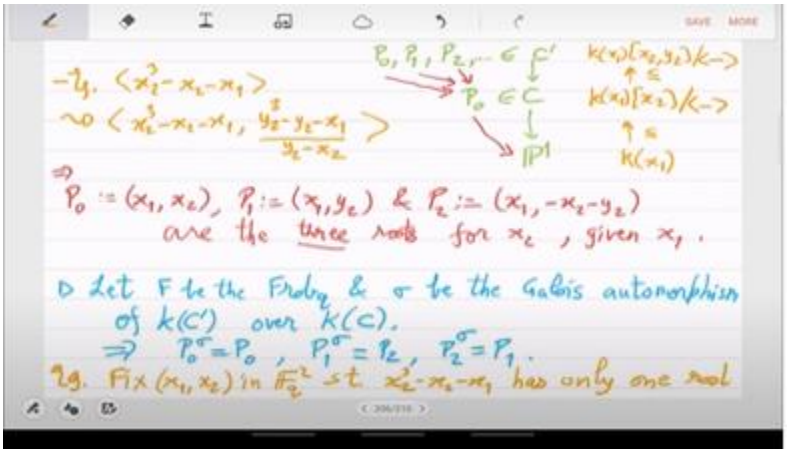
You also want to embed the condition here that x that y2 is different from x2. So, for that I can just divide this by y2 - x2. So for example, this means that for x1, x2 was obtained and then a second, so point P1 via y2 was obtained and point P2 will then be implied because, sorry this is not sqaure, it is cube. So the cubic divided by linear will give you quadratic. so quadratic once you have one root you also have the second root, so you get the three roots, so those are the points, so P0 is the point x1 x2, P2 is the point sorry P1 is the point x1 y2, and P 3 is the point P 2 is the point x 1.

So, this would be you want y 2 ‘ from here I guess you look at the first equation. So, the first equation coefficient of x 2 $^{2}$ is 0 right. So, which means that once you have x 2 y 2 you sum it up and take the negation those are the three points. So, this ideal keeping x1 kind of fixed, you get all values of x2 in the curve C ‘.

How did this curve point . This is just look at the first equation of the elliptic curve So if you have two values of x2 the third has to be negative of the sum because their sum is 0. So these are the three roots for x2 given x1. this is how you can think about this explicitly and yeah so I write this because it's a bit important to now see the connection between these three with respect to the automorphism, the Galois automorphism. So let F be the Frobenius with respect to base field which is Q size Q and σ be the Galois automorphism. of k c ‘ the biggest function field of the curve over k x 1.

Okay so what σ well what Frobenius does is clear Frobenius simply will just raise x1 x2 to qth powers because that again is a root of on the curve and what the Galois automorphism will do is it will fix x1 because x1 sits in the base field here base function field and it will then has it has to move x2 right so how will it move it. So P1 well first of all it will not move x1 x2 point because that point is in the okay I should have said yeah not the line I should say the previous curve. so in this case it will not move x1, x2, so it will move p1 to where, so p0 it will not but then the only place where it can move p12 because p1 has to be moved to I mean x1 will remain fixed so y2 has to be moved but then y2 has to move to a conjugate root the only option is p2 so that is the important thing to remember. So the Galois automorphism is just swapping P1 and P2 fixing P0 and what is the action of Frobenius, what is happening with P0. Yeah actually it is hard to see anything here, because x1, x2 I am using variables here, so this will be tricky.

I cannot make a statement here, I can only give an example, so if suppose x1, x2 you fix in the base field, then the Frobenius action will be clear, right, so Frobenius on P0 will not move it, so P0 will not be moved by the Frobenius because we have picked X1, X2 to be point in the base field, P1 and P2 generally will not be in the base field, Why is that? Well, because when you fix x1, the cubic may have one root in fq, but the other two may be in fq $^{2}$. So, in that case then Frobenius will also swap these two points. So I can just make a kind of a generic statement, but not a general statement because it will depend on how you have fixed x1, x2, but usually what will happen is Frobenius will just fix this point which is in the base field and the other two points it will just swap. So this example is showing you that the Galois automorphism which is acting on the function kind of behaves very, I mean in a related way with the Frobenius and this is what we will use now, because Frobenius is defined also on. a functional x1 x2 because we can we will just define it to be mapping x1 to x1 $^{q}$ which will be for the function x1 you do not have to fix x1 to a yeah but we are looking at a point x1 x2 is something fixed Well yeah, so that is, that has to be explained.




such that x2 $^{3}$ - x2 - x1 has only one root in FQ $^{2}$. the other two roots then they will lie in FQ $^{2}$ or we can be even more specific. So, x1 will be is already in FQ the other one will lie in FQ $^{2}$ the x2 coordinate right. I mean we can fix x2 $^{3}$ - x2 - x1 is an absolutely reducible polynomial. So, we can just randomly fix x1 from f $^{3}$ and hope that x2 $^{3}$ - x2 - that has one root not all the roots.

So, in that case I want to study the Frobenius. So in that case what I had written is true that Frobenius will be fixing P0 and it will be flipping P1 to P2, this is the action of Frobenius, is that clear now? Yeah, I mean I think you cannot see it for by through the function field. Function field you can only see Galois automorphism. What I am saying here for this you just focus on the equation x2 $^{3}$ - x2 - x1. So, there we are in the case where when we fix x1 it splits into a linear factor and a quadratic irreducible.

Now for the quadratic reducible the roots are conjugates under Frobenius that is all, that is all what we are saying, so they are conjugates in FQ $^2$ via F. conjugates over Fq $^2$ via the Frobenius. Yeah, so since we will be intimately using these two actions, it will be good to remember this picture, how the Galois automorphism acts and how the Frobenius acts on base points but also on functional points. So there are multiple actions going on in different domains. Yeah one more thing is needed to be pointed out that is can P1 and P2 be equal.

So, So you fixed x1 and then this x2 $^3$ - x2 - x1, it has a repeating root for x2. So when that happens, I mean by basic algebra you can actually show that there are very few x1s for which it is possible. in particular you can show that x1 is a root of the resultant with respect to x2 of f x1 x2 and its derivative. So it is something to do with f and f '. So when you fix x1 what happens is that this f actually becomes a square full polynomial.

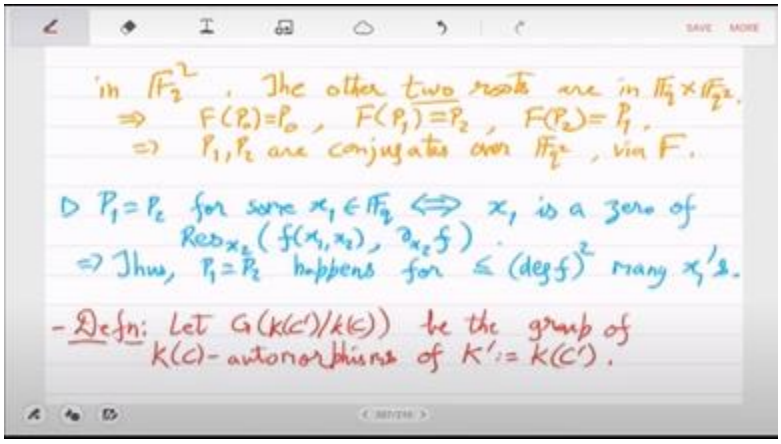
So it is linear times square say. So when you differentiate it this repeating root actually divides both f and f ' and the resultant will take care of this. So, when you eliminate x2 you basically get a univariate in x1 whose roots or whose zeros are exactly characterizing this situation it is if and only if. So, these are the bad x1's but they are very few. because we I mean the geometric intuition is that you are in a one dimensional variety which is basically your curve, so how many singular points are there, so those singular points are always finite because you intersect the curve with its derivative dimension becomes 0, so these are very few. Thus P1 = P2 happens for < = degree of f $^2$ many x1s, the resultant has degree around square it is actually smaller than square, but the point is that it is a finite number.

So again generically speaking or usually when you fix x1 the points you get they are always different the conjugates are different. So this will also be useful to remember. Yeah, but that will be another reduction that will prove Riemann hypothesis on a big field. In fact, that is why we gave this reduction because we will actually do that. How big the field should be that we will soon see.

So, let us define the Galois group, a notation for the Galois group. be the group of key automorphisms. So this is just formalizing that picture. The top field is Kc ' and the middle field for the curve, function field for the curve is Kc. So look at the automorphisms which fix your given function field and move the Galois cover.

So you can see, I mean this is again the standard group automorphism. it is a group and its size is actually equal to the degree of this extension. So, that we can state as a

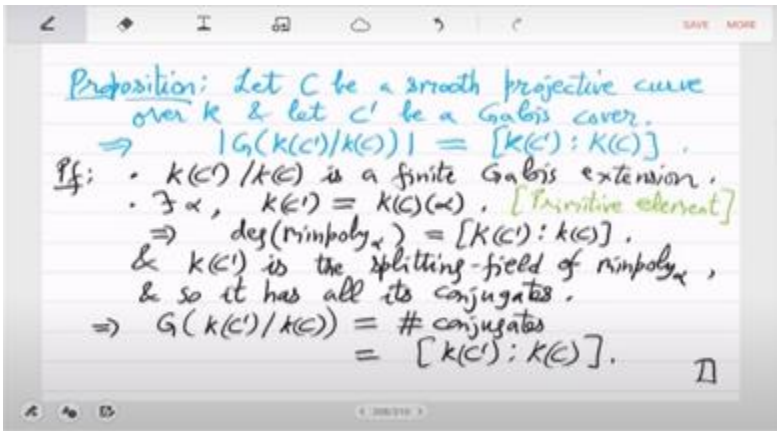
proposition. and let C ‘ be a Galois cover, then the size of the Galois group is equal to simply this.




as expected. Yes, if you have already seen Kalwa theory it is a trivial statement. If you have not seen then the idea is that you just, so Kc ‘ / Kc is a Galois extension So you can by primitive element theorem you can write this I think that is what you were saying before. So there exist an α such that Kc ‘ is just Kc with this α attached by primitive element theorem. and which means that the min poly, the min poly of this element α its degree is exactly equal to the degree of the field extension. This you can do always, this does not require Galois extension, this is just a property of finite algebraic extensions or finite extensions.

The place where Galois theory comes is for the min poly of α there are these many conjugates and they are all present in Kc ‘. mean min poly gets actually it is splitting in Kc ‘. In fact something even stronger Kc ‘ is the splitting field. and so has all its conjugates so to classify the automorphisms you just have to map α to a conjugate and the number of conjugates is equal to the degree so you get all the automorphisms which is equal to the degree. So it is a simple proof, it is a standard proof, this is how you start Kalwa theory anyways.

So all these conjugates are present and they are exactly given by the degree of the splitting field over the base field that you are always fixing by these automorphisms. So, with that yes, so we have the action of these automorphisms on the curve points. So this is an automorphism of the function field, do you see that its action can also be done on the points of the curve? can be seen to act on points P in C ‘, why is that?




Well it is simple, so this whatever Right. Yeah. So, just like you had this x1 , x2, σ will be mapping x1 and x2 to some functions.

And the idea is a simple, you use that function also on points. So I give you two coordinates, use the same function as defined by σ. So it says both the things, σ can be seen to act on points p ‘ and c ‘ via its action on the functions. because σ x1 and σ x2 are, this can be seen as functions. in Kc ‘, so use them to define σ p ‘, that's all, the usual thing.

Yeah, now what Diptushith was saying that σ x1 since it's a rational function it may have poles. So what will you do with the when this point P ‘ is a pole of those functions then you cannot evaluate σ x1 no that would be a problem. so what do you do there yeah so that will also get automatically resolved but let me not think about that here σ x1 is No, no, σ is some arbitrary automorphism of the function field. Yeah, okay, you are saying, okay, in the case when, yeah, when.

No, no, both x1 and x2 may be moving. There is a polynomial in the primitive element, right? Yeah but we are not talking about any explicit representation. So C may be given by, so I think you are getting confused with the representation for the projective line. There we use kx1. That is true, yeah.

So in that representation actually x1 is fixed. But then σ x2 has the same problem. Σ x2 is a maybe, I mean it has to move. if σ is non-trivial automorphism then it has σ x2 will be non-trivial, so it is a rational function. How will you evaluate it? The problem will be when you fix x2 in the base field constants.

No, say you fix it from FQ bar, an actual point. Usually σ X2 has some poles, so let us just look at the image of σ on that pole. Yeah, functionally yes. but on the on actual

points. So, let me not get into this anyways the poles will be few. they will be finitely many, so it's only a problem for finitely many points, for all the other infinitely many points you have action of say σ on them, so that should be good enough I think.

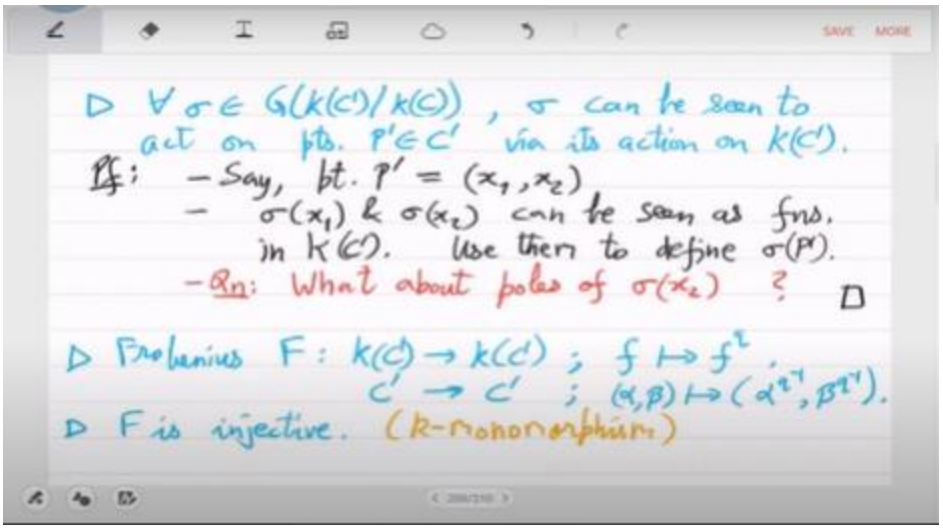
Second is Frobenius, what is Frobenius for functions and points? So Frobenius f at the level of functions will map f to $f^q$ it is simple it is always defined I mean it is defined for all the functions it just exponentiate and on points it will map α β 2 to what. So, for technical reasons it will map by q ‘ $q^{-1}$. So, on polynomials it is what you expect and on points it is. it is like exponentiating by Q, but except you are doing it $Q^{-1}$ which is another kind of Frobenius. So, for example, if α was sitting in $F_{Q^2}$ then $\alpha^{Q^{-1}}$ is actually the same as $\alpha^Q$ and if α was sitting in $F_{Q^3}$.

then $Q^{-1}$ is basically $Q^2$. So, this is just repeated application of F all the way except the last one. I mean the curve is given to you, I mean in our theory it is given to you just by a transcendence degree one function field. No, no, so coordinate ring, yeah, coordinate ring will always by definition have x1, x2.

But the problem is what is σ x2? Yes. Yes. So are you saying that there is no pole? True, I think you have proved that, so there are no poles. There are no poles except obviously in the projective case you have the point at infinity that is always there, that is there for all polynomials point at infinity, but other than that there is, so point at infinity has to be mapped to itself, σ infinity is infinity, but other points are well defined. Yeah, so that is the answer for this question. Okay, good. So, just define σ infinity to be infinity, because that is not an actual point.

Everything else you will have definitions. Although explicitly I do not see why when you go to Galois field extension you will only get polynomials. I guess in this example yeah you are getting of course. So, for example how will you map yeah in this example you can see that. So, y 2 is being mapped to - x2 - y2 and ultimately you can reduce everything to the primitive element theta or what α we said. Yes, so I think that should be fine, but still I am not formalizing that part here.

Okay so yeah we have defined σ everywhere and Frobenius everywhere now yeah one easy property here is that Frobenius is injective. since it is just exponentiating it cannot send non-zero to zero, that is a special property of Frobenius, so it is a key monomorphism. It fixes fq, this is what I am saying, it fixes fq and anything else it cannot send to 0.




Yeah and it is fixing k, yeah maybe an example will be enlightening. So, the Frobenius suppose you have this ideal x 1 - α. right so Frobenius will map it to, so ideals in this case I have taken a principle ideal because you will see the concept already. So Frobenius will map this polynomial to just at the level of ideal is this correct, may be not ideal let me just talk about the polynomial, yes by definition it maps this polynomial to its qth power which comes out to be x1 q - α. this is not good.

I wanted to give an explanation why for the point α β it's like this. Sorry. No, but I wanted to say something about the 0, now the 0 here seems to be unchanged, it remains α. Yeah, but the thing is if α is in FQ then it is. $\alpha^{1/q} = \alpha$. Yeah, so I do not get an explanation for why I did that for the point, but if you look at the order of α, the 0 α so this under the Frobenius it blows up by Q, okay.

the valuation under the Frobenius gets multiplied by Q, so at least this much we can observe. Let us see, yeah I think that this at the level of point it should be this, but what we have to recheck this when we go to the proof of Riemann hypothesis. Of course, the k points on C are exactly the points which are fixed by the Frobenius. this is clear this is why we work with Frobenius because the points that we want to count they are basically the fixed points of this morphism. So, with that setting now what I want to do is I want to relate the count of points on C‘ with C.

because I want a true reduction. So, it should not happen that c had some number of points and in c ‘ there is a totally unrelated number of points right then we cannot do Riemann hypothesis by going to c ‘. So for that what we have to see is basically how a point P in C gets covered by points in C ‘. We have to focus on that cover picture, so

which is algebraically you have to do this So for a Galois automorphism fixing the function field of the curve C define N1 C ‘ σ to be those points in C ‘ such that. $\sigma^{-1}$ fp = p. So, what this is saying is that when you apply Frobenius on this point it is you get a conjugate of the same point.

So, fp = σ p right. So, why are we doing this? as we saw in those explicit examples also, the points which cover your base point, when you apply Frobenius on them, you may not get itself, you may get a conjugate, right. So, this is basically counting that, what are the points for which Frobenius gives a and here conjugate is by σ and n1c, n1c is realized as just n1c1 or identity. So, the number of k points on the curve which we are interested in it is just take σ to be identity or 1 that is the notation. So, now we can give the connection.

So, σ if you So, let me think of this as averaging ok. So, what we will show is that n 1 c is the average over all σs plus order 1. Order 1 means it is not an absolute constant, it is a constant dependent on δ. Let me write this properly then. Okay so N1c is basically the average over these points in C ‘ under σ you count each of these take the average that will come out to the number you want which is N1c with some error. So, the error is essentially a constant, it just depends on the degree of definition of the curve C.

Yeah, so it is the thing that we are interested in, given the given curve was C and you want to find its FQ points, count its FQ points. So, this is the relationship, when you go above you have to basically do averaging with respect to the automorphism group. and it has a really simple proof based on the setting that we have it is quite easy. What you have to do is you just have to observe that a point on LHS in the RHS it will have g many points that cover it. So, basically in the LHS it is counted once in the RHS it is counted g times and then you average you get 1.

So, the counting matches on both sides except for the points for which what may happen is in the cover in C ‘ the conjugates are equal they may not be distinct. so that is a problem right, if a point P is covered by its conjugates in C ‘ where the conjugates are repeated. No, so yeah, so that needs some care right, because in the example also once you fix x1 there was the resultant argument. exactly it's not that so we want to count actual points so it's not true that for an actual point in the cover you have distinct conjugates because there are some bad actual points why are they bad why do they exist so they exist because of because of this you look at $x2^3$ - x2 - x1. So, you can set x1 to something I think in this elliptic curve case you cannot, but in general you can set x1 to something so that the polynomial is square full.

that can happen. I mean a silly example it will not work, but just to show where the algebra will fail suppose you have $x2^3$ - 1 - x1. So, there if you set x1 to - 1 then you get

x2 $^{3}$ which is sqaure full. So, there might be exceptional x1, so these are the exceptional actual points, where the covering picture is not generic, it is somehow a bad case. But for that we will use the resultant argument, we have stated here in blue that the x1 for two conjugates in the cover are equal they are very few. So, they are actually for us they are constantly many because degree of f we are considering as something constant.

So, just from that it will follow. So, that is the error term everything else is nice. So, let φ be the Galois cover. So for a point P in C let the distinct points in C ' / P be $\varphi^{-1}$ P. So, pre image of p are these points which are kind of covering your point base point. So, let us call them q 1 to q r.

So, what is φ, but c ' regardless of what is φ is this morphism or not. I mean you can understand it by the opposite arrow at the level of algebra. It is a morphism. It is a morphism, why is it a morphism, so what is the morphism? It is actually the function field Kc, it is embedded in Kc ', so that embedding is the morphism. So, you have to see the opposite. Yeah, which is why I gave the- It is this arrow the top one going from k c to k c ' that is φ at the level of algebra it is an embedding for the function fields it is an embedding for the curve c ' to c it is exactly the thing which is happening in the picture that for p 0 what are the conjugates they will be mapped they all of them will be mapped to p 0.

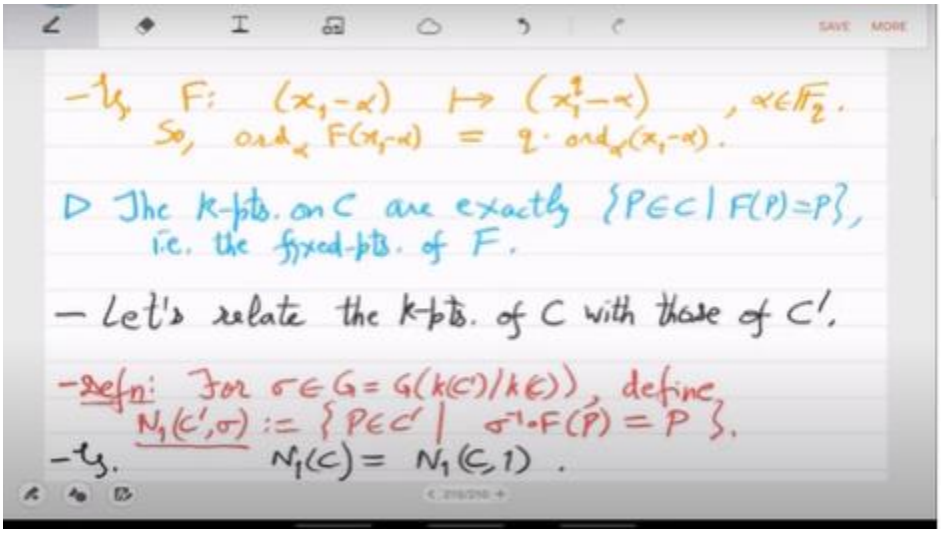
So, there is no I mean at the level of points it is not a very good looking map. So, you should actually think of the embedding. It was projection when you went from C to P 1, but from C ' to C it is not clear what it is, it is not it is not really a projection because P 1 is the point x 1 , y 2. you are mapping that to x1, x2. So, why are you mapping y2 to x2? That is not actually happening, you are not mapping the function phi2 to x2, you are only mapping the point p1 to p0.

which is why I drew that picture. So, it is very explicit what we are doing and we can now talk about the pre-image of the base point P. So, Q1 to QR are those. What can you see about R? So, well we can make first we can observe that So what can you say about f of qi? What is the Frobenius action on qi? These are actual points.

So Frobenius will just permute them. So this is again in a pre-image of p. That is one thing. The other thing is… R the number of pre images yeah it cannot be more than the Galois group, but R can be anything smaller also right there is no reason why it will be exactly equal to Galois group. in some exceptionally bad p's it can be just 1 because what is happening is all the conjugates above it are equal to p 0 = p those things are not ruled out. so y is r < g that is what we should ask it happens only when p has repeated conjugates that is P ramifies. So, ramification is the hurdle here, but we have seen before

that such points are < = δ $^2$ which we are thinking of as constant.

So, there are only constantly many ramified points everything else r = g that is all. So, for unramified point P and unramified key point sorry. on the curve C what can I say yeah. So, this φ $^{-1}$ P which is the number of Q in which is the Q's such that this number is R, is g.




So all these things are equal, okay for an un-femmified k point on the curve C, the points which are above P in the cover that's R, in fact let's just put that, that's = those points, in fact this I think I can say C ‘.

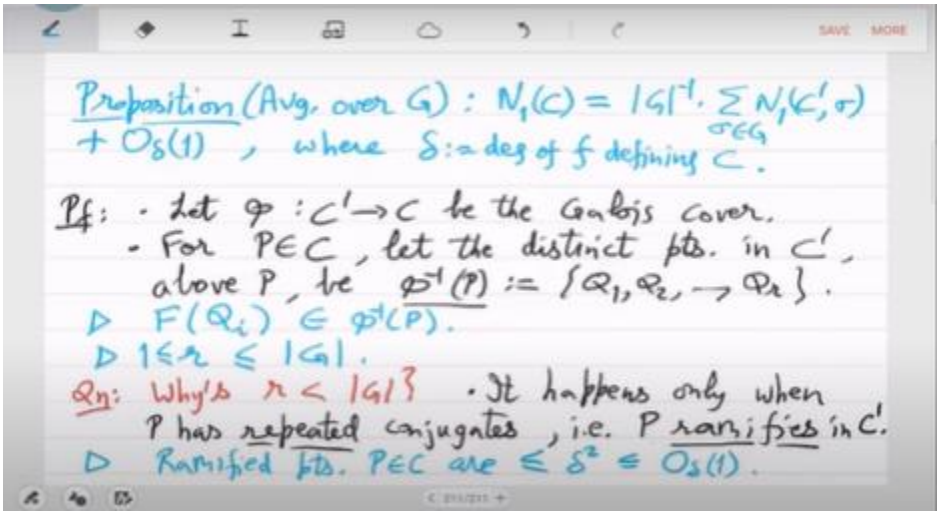
that is the point. It is actually equal to all those points in the cover which are fixed by σ $^{-1}$ f for some σ, right and this is this will be equal to g. So, which is just saying that in the proposition statement. that point q will be counted in one of these summands n1 c ‘ , σ not one yeah so it will be yeah there will be these many counts in fact there will be g many counts for the point P there will be q1 q2 dot dot qg. So, overall in the average it will be counted exactly once. I think you have one more observation has to be made which is if there is a point Q that satisfies F Q = σ Q, then what can you say about its, what can you say about φ Q, then it means that.

φ of fq φ of σ q and then you can swap this which will be equal to φ q because φ q is in the base field now. so σ will fix it, so which is basically saying that, but do I need that this is trivial I think what I need is something like this, this is correct right.

So, any point Q which is being counted in some N1 C ‘ σ. that has to be in the preimage of P. No wait. The definition of earlier is given should be σ $^{-1}$ of SQ is P right. Yes, sorry

wait what. R is equal to next bridge. Yeah, no that is correct that is for that is in the cover right, so there you have to talk about $\sigma^{-1}$ f.

No I think this is the set condition is enough, this says everything. Just this one small observation is needed that if Q ‘ in C ‘ satisfies then φ of q ‘ will be in the curve C. This is the only thing I need I guess. I mean you have to look both ways, so take a base point P in C, how many covering points are there that is given by the first equation, but you also have to see that points which are which I am counting in C ‘ which are fixed points of $\sigma^{-1}$ F for some σ. Then its image under φ is a k point in the curve.




that is true because you just apply φ on that identity and σ will go away. So, you will get that f of φ q ‘ = φ q ‘ which will say that φ q ‘ is a point k point in the curve that is all. So, now we have seen both ways. So, now σ n 1 c ‘ σ small σ covers everything correctly. In the next page, no in the next page it is talking we are making a statement about the cover of unramified points. yeah which is untrammified oh in the in the set no no no I yeah so that should be we sure we can edit that it's in yeah it's in C ‘ intersection preimage that is what was meant it is the q's which are in C ‘ covering the point P that's fine.

But if you look at some random q ‘ in C ‘ which is being counted in N1 C ‘ then it does correspond to some key point on the base curve that's also true. Yes with these two I think we are now set, so thus Q any Q in C ‘, any Q in C, any P in C contributing to think this should be said about q ‘ and c ‘. So, any q ‘ and c ‘ contributing to this sum either has φ q ‘ ramified or has φ q ‘ unramified.

these are the only two cases and both these images they are in the curve C, K point in C. So, which means that. What is the statement check on the level of Q ‘ along with C ‘? Oh,

let us just remove also, let us write this properly. if q ‘ and c ‘ satisfies this, then this happens. It is a k point here. It is saying that any fixed point of $\sigma^{-1}$ f when you quote unquote project down it is a k point that is all.

Note that it is obviously true if q ‘ was a fixed point of f. because if it's a fixed point of f then it's then clearly it has to be a k point, it's a k point of c ‘ and you project down it will remain a k point of c, but it's not just Frobenius we are also putting $\sigma^{-1}$. So, there is some content here it is saying that even with $\sigma^{-1}$ Frobenius actually does its job and it gives you a k point. That can be shown just by applying φ both sides when $\sigma^{-1}$ goes away. it might be easier to apply φ on fq ‘ and σ q ‘.

So, φ on fq ‘ will you can swap φ and f and φ on σ q ‘ you can swap σ and φ. So with the top 2 properties you have now that phiq ‘ is you are getting points in C and and yeah both are in C I mean either it is this point k point in C is ramified or it is unramified and the ramified cases are very few. So the unramified cases will give you g times the number of points, while the ramified cases will be very few, they will just be constant. In fact technically I can multiply this with g, I should multiply this with g, but then the Galois group size is also just degree, so ultimately this finishes the proof.