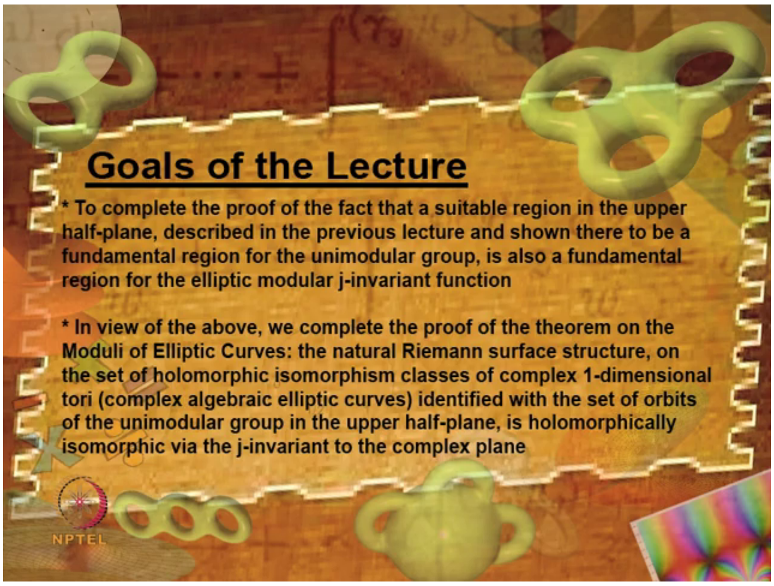
An Introduction to Riemann Surfaces and Algebraic Curves: Complex 1 -dimensional Tori and Elliptic Curves

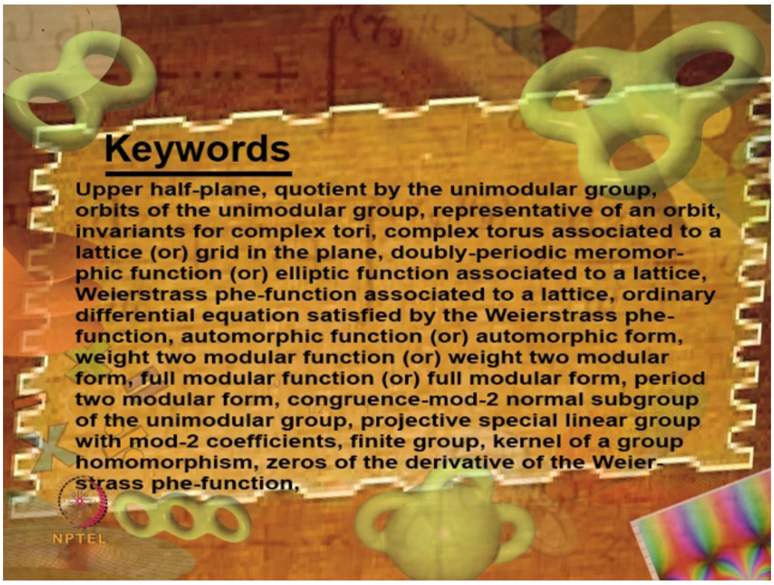
Dr. Thiruvalloor Eesanaipaadi Venkata Balaji
Department of Mathematics
Indian Institute of Technology, Madras

Lecture - 42
Moduli of Elliptic Curves

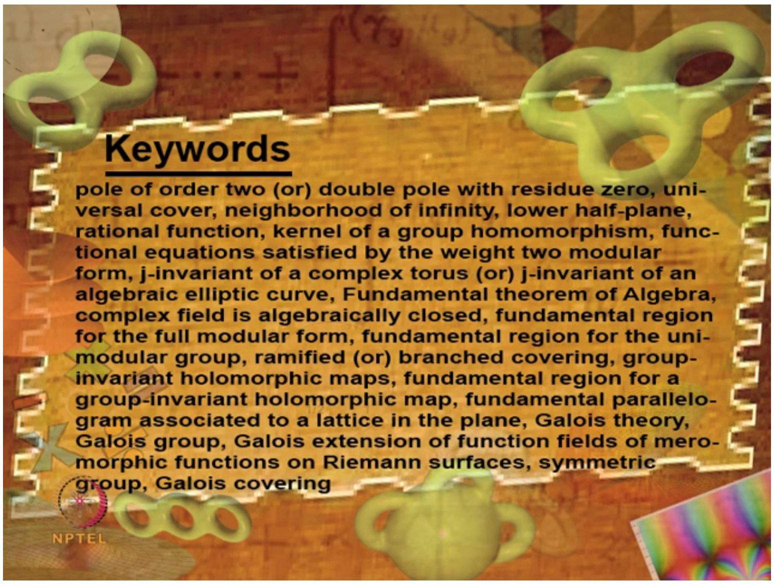
(Refer Slide Time: 00:10)



(Refer Slide Time: 00:15)

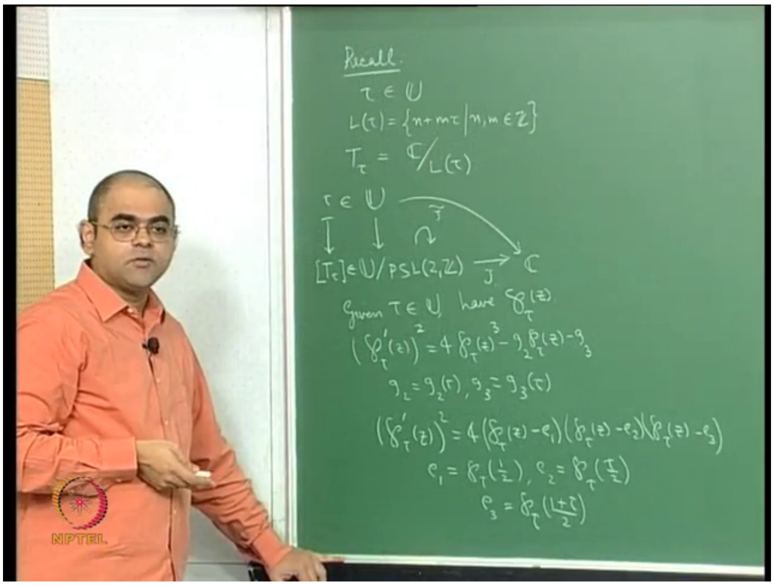


(Refer Slide Time: 00:21)



Recall certain things before I continue. So, you see we at this point we are trying to show that the modular function J tilde is 1 to 1 on the on the region; the fundamental region script D. So, in fact, fact that the statement that script D is a fundamental region for J tilde involves the verification that J tilde restricted to script D is injective; which is what we have to prove. So, let me again, let me recall very quickly certain things to just set up the notation, just recalling notation. So, you see if you recall we start with tau in the upper half plane.

(Refer Slide Time: 01:13)



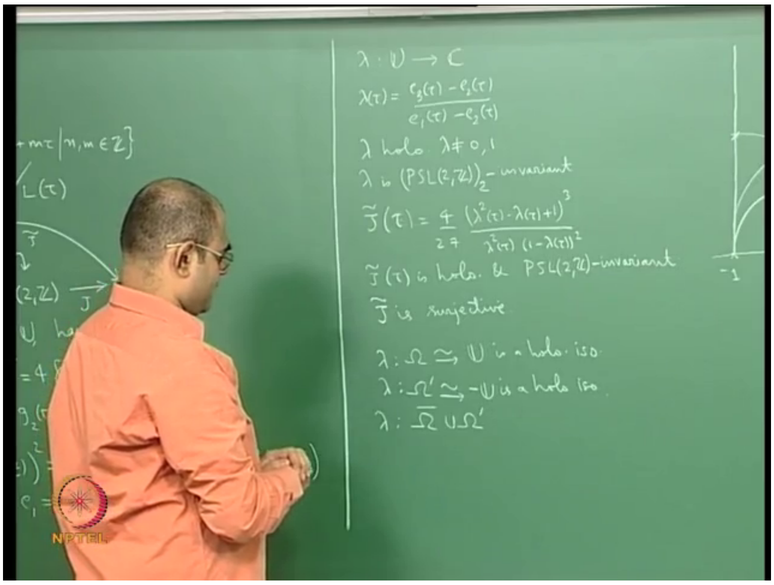
And then you end up with. So, you have the lattice defined by tau which is the set of all n plus m tau, where n and m are integers, and then you have the torus defined by tau which is the complex plane modulo this lattice. And so, you get a map from U to U mod P S l 2 z. Tau going to isomorphism class of the torus defined by tau. And so, if you recall 2 elements tau 1 and tau 2 in the upper half plane will define holomorphically isomorphic tor I if and only if tau 1 and tau 2 differ by an element of P S l to z the unimodular group. These are Mobius transformations which when written in matrix form have integer entries and determinant one. And of course, this is a sub group of P S l 2 r which is the full group of automorphisms of the upper half plane.

And we were trying to show that U mod P S l 2 z is by holomorphic to c. So, what we did was we defined the function J tilde holomorphic map J tilde, and we proved that J tilde goes down to a map j, that is this diagram commutes. So, this J tilde was invariant under the full modular group. And let me quickly recall how we got hold of this J tilde we will need it. So, given tau we have the Weierstrass phi function, have the phi function phi tau phi tau of z. It is a doubly periodic function, and an elliptic function of the simplest kind with 0 of order with a pole of order 2 at every point of this lattice, and it is defined by series expansion.

And then we found that this phi function satisfies the differential equation, the differential equation was phi tau prime of z the whole cube is 4 into phi tau z I think it is a squared, and this is a cubed minus g 2 phi tau z minus g 3; where g 2 and g 3 are functions of tau. And what we did was so this is the natural differential equation. That the Weierstrass phi function satisfies. And we also factorized we factorize the right side, because it is a cubic you have 3 linear factors. And we factorize it as follows phi prime phi prime tau sub z whole squared is 4 times phi tau of e z minus e 1 into phi tau of z minus e 2 into phi tau of z minus e 3, where of course, e 1 e 2 e 3 are also dependent on z. I mean also are dependent on tau, and they are the 0s of the derivative of the Weierstrass phi function.

And in fact, we found that there are essentially 3 0's within a period parallelogram. And these are given by so, we set even to be phi tau of half e 2 is equal to phi tau of tau by 2, and e 3 is equal to phi tau of 1 plus tau by 2. So, within the fundamental parallelogram which is which has vertices 0 1 tau and 1 plus tau, these were the 3 0's of phi prime. And we said e 1 e 2 e 3 to be in this way. And function this gives rise to a function lambda.

(Refer Slide Time: 06:37)



So, we have this helps us to define a function lambda on the upper half plane with values in the complex numbers. It is a holomorphic function and the function lambda is defined by lambda of tau is equal to so, it was I think e 3 of tau minus e 2 of tau by e 1 of tau minus e 2 of tau. So, well I mean that is right. And well so, the point is that as tau varies the as tau varies e 1 e 2 e 3 also vary. And that is how we get lambda as a function on the upper half plane here tau is varying. And lambda is holomorphic, lambda is not equal to 0 1 or 1. And we and of course, and lambda is invariant under the congruence mod 2 subgroup P S l 2 z sub 2 P S l 2 z sub 2 is the is the normal subgroup of P S l 2 z consisting of matrices with entries which give the identity when you read the entries each of the entries mod 2.

So, this is the congruent mod 2 subgroup, and lambda is invariant under the congruent mod subgroup. But actually, what we are looking at is we want a function defined on this. Namely, you want a function defined which is that therefore, this should correspond to a function J tilde, which should be invariant under the full modular group. But this is only a partially modular function. It is only this is this is a modular function which is defined which is modular only for the for this particular subgroup congruent mod 2 subgroups. But you want a function which is in which is invariant under the whole uni modular group.

So, we defined J tilde of lambda to be 4 by 27 into lambda squared. So, J tilde of tau to be 4 by 27 into lambda squared tau minus lambda tau plus 1 the whole cube by lambda squared of tau into 1 minus lambda of tau the whole square. We defined this function J tilde, and what we proved was this that J tilde of tau is see since lambda is not equal to 0 or 1, the term denominator never vanishes, and since lambda is a holomorphic function J tilde of tau is also holomorphic, and this function is the function that we want namely the one that is invariant under the full unimodular group. So, it is P S l 2 z invariant.

And what we have already shown is of course, you can recall, that this set the set of orbits of P S l 2 z in of the group P S l 2 z in U can be identified with set of holomorphic isomorphism classes of complex tor I. And this is not just a set this is a Riemann surface, we proved that. We have proved that earlier namely, we proved that the this group P S l 2 z the action of this group on the upper half plane is actually properly discontinuous action. And then therefore, when you divide by a when you take a quotient by a group with the properly discontinuous action, then the quotient can also be given a Riemann surface structure.

So, this becomes a Riemann surface, structure and if you remember the way we proved that P S l 2 z acts properly discontinuously on U was by proving that P S l 2 z is actually discrete. Of course, it is discrete, because it has entries in the integers. But the more important thing is that that it is that it leaves the upper half plane invariant. So, it is Fuchsian group. And then we have we know that for a Fuchsian group, I mean for a Kleinian group I mean for a Fuchsian group discreteness is equivalent to the group acting properly discontinuously on the half plane or the disk which the group leaves invariant, because by definition a Fuchsian group is a group which leaves a half plane or a disk invariant. And P S l 2 z it is certainly a group of Mobius transformations that leaves the upper half plane invariant. So, it is a Fuchsian group and it is discrete.

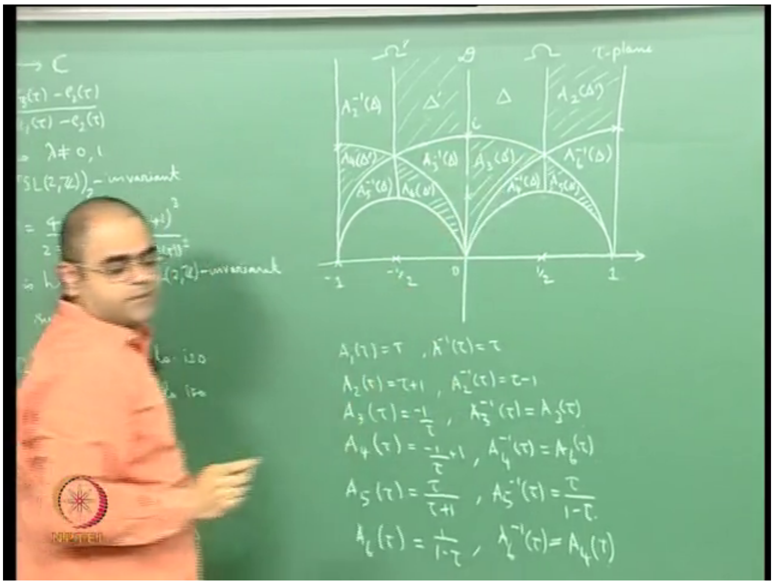
So, it the discreteness is enough to conclude that P S l 2 z is acts properly discontinuously on you. And then since it acts properly discontinuously on you the quotient becomes a Riemann surface such that this mapping canonical quotient map becomes holomorphic. So, this is a Riemann surface. And our aim is to show that this Riemann surface is isomorphic to see. Namely, we are trying to say that for every holomorphic isomorphism class of a torus there is a uni complex number. And that complex number is called the j invariant of the torus.

So, one single invariant is enough to classify all the holomorphic isomorphism classes; that is to classify complex tor I up to holomorphic isomorphism a single invariant is enough a single complex invariant is enough, that is a statement. So, we want to show that this is holomorphically isomorphic to see. So, we are looking for a function j which is a bijective holomorphic map. But a function like this will come from above, because if you give me j then I can take the composition call that as J (Refer Time: 13:07) J tilde, and J tilde will; obviously, be P S l 2 z invariant conversely if I have a J tilde which is P S l 2 z invariant it will go down to a function j. Therefore, we have to find this J tilde and here it is.

Now, we will have to prove a couple of things namely. So, we have to prove that J tilde is. So, we have to prove that this j is both surjective and injective, the surjectivity has already been proved. Essentially because of the use of the fundamental theorem of algebra J tilde be have we have shown. So, let me write that down J tilde is surjective that has already been proved in an earlier lecture. Now, I will have to draw some diagrams to tell you about the injectivity does not come out straight for in a straightforward way. So, the point of the key to finding the injectivity is to is to look at the fundamental region for J tilde which is and in fact, what we are actually trying to show is that the fundamental region of J tilde the same as the fundamental region of P S l 2 z.

So, I will have to draw a diagram so, let me draw it. So, we have basically if you remember. So, let me let me draw it somewhere because, I keep I need to use it again. So, let us so, let me draw it here. So, you see this is the tau plane.

(Refer Slide Time: 14:41)



This is the real axis, this is imaginary axis. And well basically we take; I think I will need semicircle of radius 1. So, let me draw it here. So, that I have enough space. So, this is half. So, here is this well. So, this is half, this is one. So, this is i. So, you see I draw the semicircle centered at half radius half. So, I get this, then I take I do the same thing at minus half, and I end up with this semicircle. And then I also draw circles of radius 1 centered at 0 1 and minus 1. So, I will end up with.

So, I will have one like this, and then I will have then I have one more centered at minus 1. So, you know I will have to draw these vertical lines. So, I will draw one vertical line here. Can I have another vertical line here? And I have circle centered at minus 1 radius 1. So, I will I will get something like this. And I will have a circle centered at one radius 1 that will go like this. And then I take I draw this vertical line passing through this point half. So, but I draw it only up to this. And similarly, I draw another vertical line like this. And you see this, this, this whole region was called as omega. And this region is called as omega prime.

So, let me because I am going to write several things, on this diagram let me explain omega is the interior of the region bounded by this line and this semicircle. So, this all of this is omega. And omega prime is just it is reflection about the imaginary axis. Namely, omega prime is the open set bounded on the left by this line on the right by this line. And below by this by the semicircle all right. And then we also gave and what was what was special about this omega and omega prime was that we proved that this function lambda actually maps omega holomorphically on to the upper half plane. And it maps omega prime holomorphically on to the lower half plane.

So, let me write that down lambda from omega 2 U is a holomorphic isomorphism, and lambda from omega prime to minus U by minus U I mean the lower half plane. That is also a holomorphic isomorphism. And in fact, we also proved that lambda is can be extended continuously to the boundary of omega, and it is monotonic. And what you get is lambda from actually I think if you take omega bar union omega prime, what I will end up and of course, when I when I take omega bar; that means, I am taking the closure. So, I will get the points 0 and 1. And I think. So, so this will correspond to so, you know lambda as you go higher up the lambda values will go to 0. And at 0 lambda takes the value 1. And at one lambda takes the value at value infinity.

So, I will end up so, this should give me. Anyway, let me not worry about that immediately. So, I want you to know I remember this, then we have, then we had this then we had this other important and then we also had that see lambda was only invariant under the congruence mode to subgroup, and we wanted to know how lambda behaved under a general the P S l 2 z element. And that therefore, that lead us to write out certain function functional equations on lambda. And if you remember these functional equations were based on a set of say 6 Mobius transformations which gave a complete set of matrices in P S l 2 z mod 2 z.

So, if you if you remember so, let me write down certain things you know, so, let me write down certain the following Mobius transformations. So, that I mean it is so, you see we have so, let me write this down here, A 1 of tau is tau this, this identity and A 1 inverses of tau is just again tau. Then A 2 of tau is the Mobius transformation tau plus 1 A 2 inverse of tau is of course, going to be tau minus 1. And well A 3 of tau was minus 1 by tau and A 3 inverse as same as A 3. And A 4 of tau was minus 1 by tau plus 1 and A 4 inverse of tau was A 6 of tau.

Where I will define what A 6 is A 5 of tau was tau by tau plus 1, a s A 5 inverse of tau was is tau by 1 minus tau. And A 6 of tau is 1 by 1 minus tau A 6 inverses of tau, is just A 4 of tau because A 4 inverses A 6, A 6 inverses A 4. And the point was if you should take, if you take, 6 of these, then mod if you read the mod 2, you get all the 6 elements of P S l

2 with entries in z mod 2 z. So, that is entries 0 or 1. And then see we studied the certain mapping properties. You see in fact, we called this region as delta. And then we call this region as this open set as delta prime.

So, what is delta is the open set which is bounded by this ray, and this portion of the of the unit circle, and then this ray. And then delta prime was it is reflection under the imaginary axis. Namely, the open set that is bounded by this ray, this segment of the unit circle, and this part of this ray on the imaginary axis. And what we actually proved was I if you remember we proved we checked out that these fellows map these 2 regions on to the total 12 regions that are there in this if you forget the region since enclosed by the semicircles. And I am well it is easy for you it is an easy exercise for you to check that this is what you get.

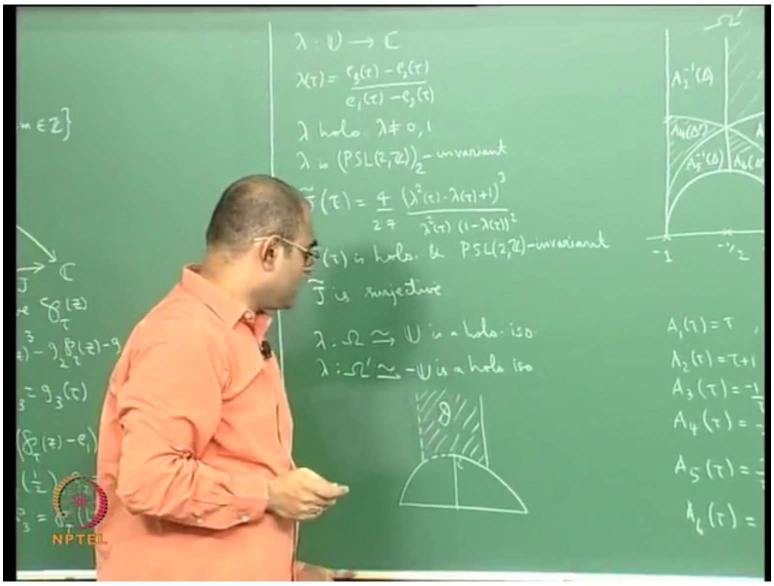
So, you see this is delta this is A 2 of delta. This is sorry; this is A 2 of delta prime. And this is this is A 2 inverse of delta, and this is this is A 3 delta, and this is A 3 inverse of delta. Then this is A 4 this is A 4 of delta prime, and this is A 6 inverse of delta prime. A 6 inverse of delta and this is A 5 of delta. This will be delta prime, and this is A 4 inverse of delta. And this is A 6 of delta prime. And this is A 5 inverse of delta. So, you see basically what is happening is you see, if you take A 1, A 2, A 3, A 4, A 5, A 6, and apply it to delta prime, you get A 1 of delta prime is delta prime A 2 of delta prime is here.

Then you have A 3 of this must be A 3 of delta prime this should be prime; this A 3 of delta prime, then you get A 4 of delta prime, then you get A 5 of delta prime A 6 of delta prime. So, in fact, so, you know if you shade it like this. Essentially, you get these things namely you get this. Basically you see this A 1 through A 6 map delta prime onto these 6 shaded regions, this A 1, this image of A 2, this the image of A 3, this image of A 4, this image of A 5, this is the image of A 6 and what is happening to delta the inverses A 1 inverse through A 6 inverse. That maps delta onto the unshaded regions.

So, this is A 1 inverse of delta which is the same as A 1 of delta which is identity this is A 2 inverse of delta, this is A 3 inverse of delta this is A 4 inverse this is A 5 inverse and this is A 6 inverse, so all these. So, this is how all the all this all these 6 transformations and their inverses map this region, and they are all because they are all they are all Mobius transformation the mappings are conformal and the boundaries are mapped to the boundaries and so on. So, we will we will need this actually. So, that is the reason I am taking some time to recall this. Now you see this region was called a script D. So, script D somewhere here.

I mean basically it encloses the interior of this region bounded by this vertical line segment this vertical line segment and this arc of the unit circle. And then in the boundary you take only this part and this part. That was your script D.

(Refer Slide Time: 28:09)



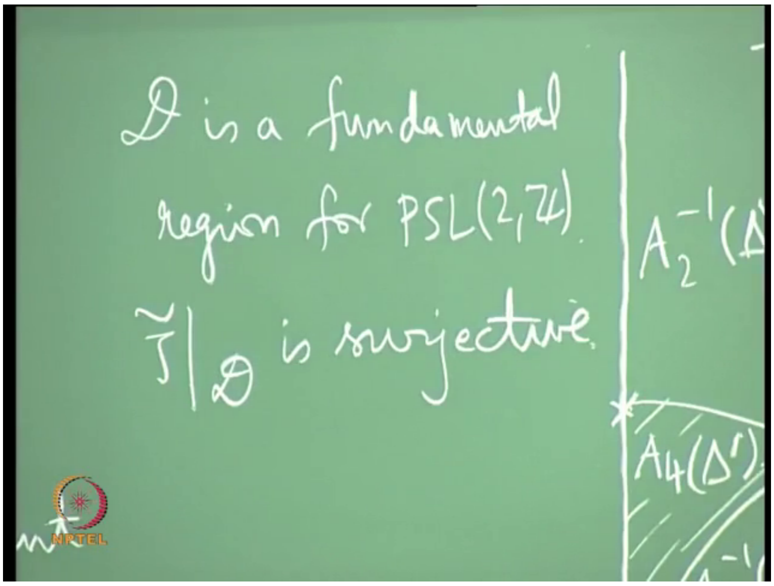
And so, if I if I draw that separately script D is script D is basically is basically this. Well so, you know so, my script D is actually this. So, I put dotted lines here. So, that I am I am removing the boundary, and I remove this. And this is script D script D is essentially this region of course, you see this, this point is this point is i. That if this point is i and this and this point is this point is a complex cube root of unity. And this is it is mirror image and so on.

So, the fact is that what we have already shown is that this script D is a fundamental region for the action of P S l 2 z. What does it mean? It is if you recall that it means that for every orbit every orbit of P S l 2 z in the upper half plane meets this meets this fundamental set at exactly 1 point mind you mind you it is not an open set because I have included part of the boundary. And the reason why I am not including this part of the boundary is because, the values taken by lambda here are the same as the values taken by j here are the same as the values taken by j there because this is translation by 1, and j is invariant. Under P S l 2 z and translation by 1 is a P S l 2 z elements.

So, this this set is actually a fundamental set for P S l 2 z that we have proved. We in fact, the way we proved it was we showed that first of all we proved that any P S l 2 z orbit has to intersect, this that is the first step, we proved and then we proved that if there are if there are 2 points here, which are such that one point which belong to the same orbit under P S l 2 z. And then they are one in the same that is what we proved. So, we proved this is a fundamental region for P S l 2 z; so then the other thing that we proved. So, the other thing we were trying to prove was that for J tilde also this is a fundamental region.

What does that mean? It means that you have to show that J tilde restricted to this is both injective as well as surjective of course; subjectivity is already done. Basically, J tilde is surjective from the J tilde is surjective from the upper half from the upper half plane. So, but then give me any point in the upper half plane that is a representative in it is orbit here. And J tilde will take the same value here. It will take the same value throughout the orbit at every point of an orbit, because it is invariant under P S l 2 z. Therefore, the fact that J tilde is J tilde from U to c is surjective will tell you the J tilde from script D to c is also surjective.

(Refer Slide Time: 31:32)



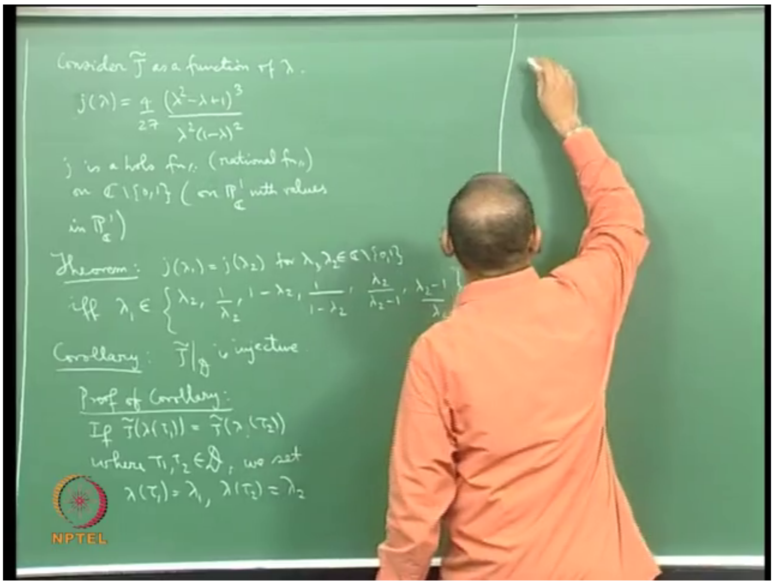
So, let me. So, let me write that also somewhere here. Script D is a fundamental region or set for P S l 2 z and J tilde restricted to script D is surjective. So, the see the therefore, the only thing that is left out to be proved is J tilde restricted to the script D is injective, which is what we have to prove. Once you prove that then it will follow that this j is a bijective holomorphic map, and you know this is a Riemann surface that is a Riemann surface the bijective holomorphic map is holomorphic isomorphism. And that will have proved to you that the set of on the set of isomorphism classes of a complex tor i that is a natural Riemann surface structure which is none other than the usual Riemann surface structure on the complex plane. So, I will have to prove that J tilde restricted to do to script D is injective.

So, how do I do that? So, for that so, that also involves a little bit of clever computation of course, it is not that it looks clever, but it is it is not a trick it is backed by it is backed by some phenomena which are up which are occurring in the realm of Galois Theory. So, there is a Galois there is a certain there is a certain Galois Theory which is going on it. You can look at it as a Galois Theory of Riemann surfaces or you can also look at it as a Galois Theory of fields, but then I do not want to go far of field, but I am going to write down now certain things which may seem magical, but essentially, they are they are not tricks they have come because of delving into some Galois Theory.

So, let me explain. So, here is the so, here is the so, what we are going to do is we are going to consider you see the point is that the analytic properties of J tilde the mapping properties of J tilde are completely controlled by those of lambda. Because J tilde is P S l 2 z invariant and how lambda behaves we know very well because you see if you know how lambda behaves with respect to these then you know how lambda behaves with respect to any element of P S l 2 z. So, you see we already know in some sense the mapping properties of J tilde.

But the important thing is that there is something algebraic going on. The important thing is that you should look at J tilde not as a function of tau, but look at J tilde as a function of lambda.

(Refer Slide Time: 34:37)



So, what we will do is consider J tilde as a function of lambda. So, basically you define j. So, I define small j of lambda by the same formula 4 by 27 into lambda squared minus lambda plus 1 the whole cube by lambda squared into 1 minus lambda the whole squared. Then you see this j is actually a map from the complex plane minus 0 comma 1 to the complex plane minus 0 comma 1. So, j is the j is a j is a holomorphic function on c minus 0 1. J it is a holomorphic function.

In fact, it is a rational function; so quotient of polynomials. So, it is a holomorphic function. So, rational function on complex plane minus 0 1 I have to exclude the values 0. And one because the denominator vanishes, but then if I think of it as a rational function, then I can think of it also as a function from p 1 to p 1 namely at 0 and A 1 I can define the value of the function to be infinity. And at infinity also I can define the value to be infinity because the numerator is higher degree polynomial is a higher degree polynomial than the denominator polynomial.

So, you see so, it is a holomorphic function on this and it is an it is a rational function on p 1 with values in p 1. So, if you want p 1 c is just the Riemann sphere it is the natural Riemann surface structure on the extended complex plane the complex plane along with the point at infinity which you get a Riemann surface structure via homeomorphic to the real to sphere where this stereographic projection. So, that is p 1 c. And so, either you think of j as a function on c minus 0 1 or you think of it as a holomorphic function of c minus 0 1 and or think of it as a rational function from p 1 to p 1.

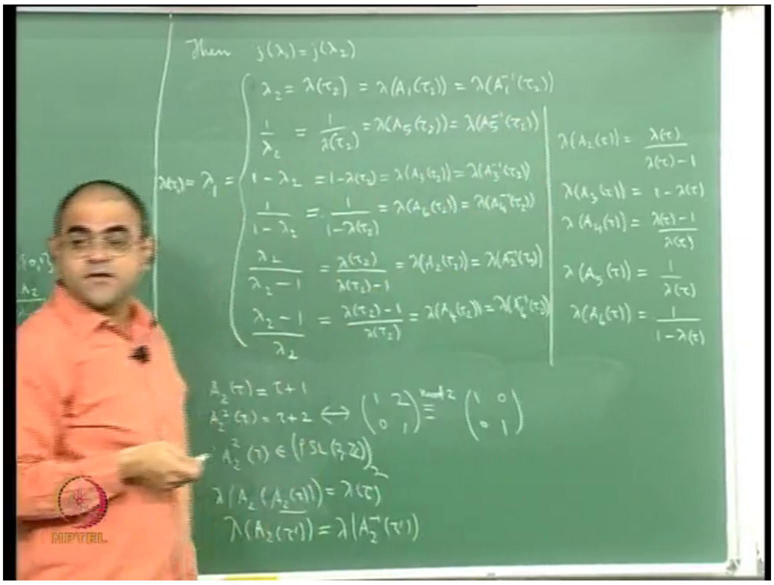
Now, the key to the injectivity of J tilde is the following statement theorem; j of lambda 1 is equal to j of lambda 2 for lambda 1 comma lambda 2 e c minus 0 1, if and only if lambda 1 is belongs to the following set lambda 2 1 by lambda 2. So, let me write out few set of things. They have 1 minus lambda 2 1 by 1 minus lambda 2 lambda 2 by lambda 2 minus 1 lambda 2 minus 1 by lambda 2. So, this is a theorem. So, the Galois Theory is that on say what is actually happening is that from c there is an action of I will try to give this in the exercises, or if I have time I will expand upon it in the end of the lecture. There is an action of the symmetry group on 3 elements. Thought of a symmetric group on acting on 0 1 and infinity.

I mean 0 1 and lambda where lambda is in lambda is a complex number not equal to 0 1. Which for that action this is the orbit of for a given lambda the orbit is given by lambda 1 by lambda 1 minus lambda 1 by 1 minus lambda by lambda minus 1 and lambda minus 1 by lambda, and what happens is; this map from c 0 c minus 0 1 to c minus 0 1 is actually a covering it is a Galois covering and the of course, it is a ramified cover it is a ramified holomorphic covering. And if you look at it as a covering of the meromorphic functions on p 1 over the meramorphic functions on p 1, then it is actually a Galois extension and the Galois group is actually the symmetric group on 3 elements.

So, this is a Galois Theory that is involved, which gives rise to this, I mean it gives the which gives us the with the statement of this theorem. So, but before I so, you know if I so, my claim is if I prove this theorem then we are done. So, let me first get that as a corollary, let me first prove the corollary to the above theorem. It is J tilde restricted to d is injective. So, the corollary to this theorem is J tilde restricted to script D is injective. So, how is that true? So, the proof of corollary, see what you will have is see if J tilde of lambda of tau 1 is equal to J tilde of lambda of tau 2, where tau 1 tau 2 are in script D.

We said lambda of tau 1 as lambda 1 lambda of tau 2 as lambda 2. We said we call lambda tau 1 as lambda 1 and lambda tau 2 as lambda 2, then what you will get is well.

(Refer Slide Time: 40:47)



Then you see what you will get is j small j of lambda 1 is equal to small j of lambda 2, because you know after all small j is just capital j thought of as function on lambda. So, you get j of lambda 1 equal to lambda j of lambda 2. So, what you will get is that you will get either. So, you will get lambda 1 belongs to all these things I mean lambda 2. So, so lambda 1 is equal to well lambda 2 or it is 1 by lambda 2 or so, these are the various possibilities.

So, let me let me write it like this lambda 1. Let me write out all those possibilities lambda 2 by lambda 2 minus 1 lambda 2 minus 1 by lambda 2. So, these are the 6 possibilities for lambda for lambda 1 that is because of this theorem. And now we have to reinterpret this using these mapping properties see actually if you check see. So, let me write this down. So, you see this lambda 2 is just A 1. So, it is see you see it is lambda 2 is actually lambda of tau 2 lambda 2 is just is lambda of tau 2 and by the way the thing on the left side is lambda of tau 1 which is lambda 1, and here I have lambda of tau 2, and what is lambda? Lambda of tau 2 well if you want you can write this as A 1 it is, lambda of A 1 of tau 2.

And is also lambda of A 1 inverse of tau 2 because a and A 1 and A 1 inverse are one and the same lambda of A 2 of tau is was lambda tau by lambda tau minus 1. So, I am writing down these functional equations that we proved several lectures ago lambda of A 2 of tau is lambda tau by lambda tau minus 1 lambda A 3 of tau is 1 minus lambda of tau lambda of A 4 of tau. Is it was lambda tau minus 1 by lambda tau lambda of A 5 of tau is going to be is 1 by lambda tau. And lambda of A 6 of tau lambda of A 6 of tau gave me 1 by 1 minus lambda of tau. I mean these are the essentially the things we have to use diligently.

So now you can more or less I think several of them can be written down directly. So, you see this is see this is this is 1 by. So, the I think several of them can be written down directly from the table this is 1 minus lambda of tau 2, but 1 minus lambda of tau 2 is lambda of A 3 of is lambda of A 3 of tau 2. And A 3 is the same as A 3 inverse. So, this is also lambda of A 3 inverse of tau 2. A 3 is it is own in A 3 is A 3. A 3 is it is own inverse. So, I can write that and see 1 by 1 minus lambda 2 is of this form. So, it is lambda of A 6 of tau 2. So, it is 1 by 1 minus lambda of tau 2 this is lambda of A 6 of tau 2.

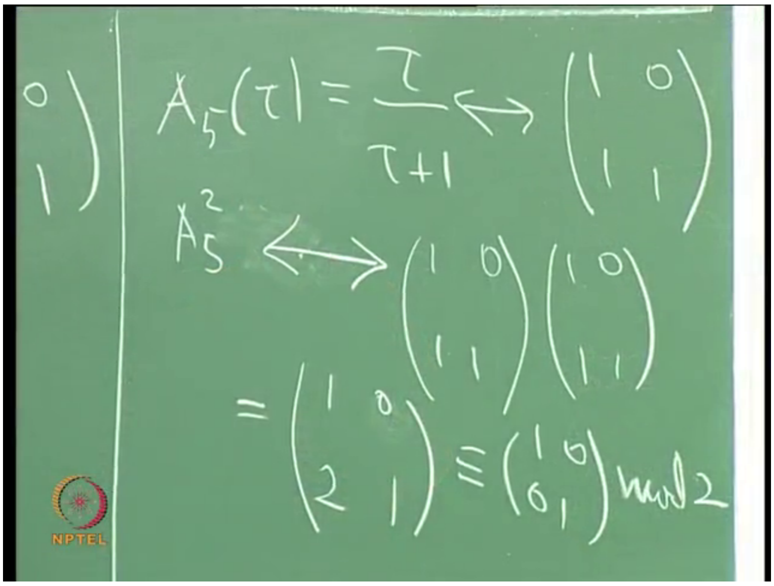
And this is of course, lambda of A 4 inverse of tau 2. Because A 6 is A 4 inverse and A 4 is A 6 inverse. Then lambda by lambda minus 1 lambda 2 by lambda 2 minus 1 corresponds to this one. So, this is so, this is lambda of tau 2 by lambda of tau 2 minus 1 and this is lambda of you see, lambda by lambda minus 1 is lambda A 2 of tau A 2 of tau 2. And now I want to say this is also equal to lambda A 2 inverse of tau 2 because A 2 squared is congruent to 1 mod 2 is congruent to the identity mod 2 see. So, if this is this will also be lambda of A 2 inverse of tau 2. So, I owe you an explanation here, because you see if you take see A 2 of tau is actually what A 2 of tau plus 1.

If you calculate A 2 squared of tau, you will get tau plus 2. And this will this will correspond to the matrix 1 2 0 1. And this matrix is congruent mod 2 to the identity matrix. Because after all if you read mod 2 2 is 0. So that means, A 2 and A 2 inverse they are the same mod 2. Therefore, but you know lambda is supposed to be invariant under congruence, I mean elements congruent identity mod 2 therefore, lambda of A 2 is equal to lambda A 2 inverse. That is the reason. So, you see A 2 squared belongs to the congruence mod 2 sub root, because you see the A 2 squared.

So, if you want I will write down A 2 squared of tau belongs to P S l 2 z congruence mod 2 subgroup. Because it is congruent to identity mod 2; and therefore, lambda of so, therefore, lambda of A 2 squared of tau that is A 2 of A 2 of tau is equal to lambda of tau. Now what you do is; you that is A 2 of A 2 of tau is equal tio lambda of tau, now what you? So, is you replace you replace A 2 of tau by some tau prime then you will get lambda of A 2 of tau prime is equal to lambda of tau which is A 2 inverse of tau prime. So, that is how you get lambda of A 2 is lambda A 2 is. So, this needed some explanation.

But essentially, we are using these. And then the last one is also lambda 2 minus 1 by lambda 2 corresponds to this one, no this one. So, it is lambda of A 4 of tau 2. So, this is just lambda tau 2 minus 1 by lambda of tau 2 that is lambda of A 4 of tau 2. And you see lambda of A 4 of tau 2 is also equal to lambda of A 6 inverse. And the only thing there is left is this you can recognize that this is this that corresponds to this one. So, it is lambda of A 5 of this is 1 by lambda of tau 2, this is lambda of A 5 of tau 2 and interestingly this is also lambda of A 5 inverse of tau 2 the reason being that A 5 is squared is also congruent to identity mod 2.

(Refer Slide Time: 49:27)



See A 5 if I write it down here, see A 5 of tau is the is the transformation tau by tau plus 1, tau by 2 plus 1 and that corresponds to the matrix 1 0 1 1. And if you take A 5 squared you will get I will I so, this. So, A 5 squared will correspond to just multiply this take this pair of this matrix multiplied with itself and then read it mod 2. So, you will end up with you will end up with identity. So, in fact, it will correspond to so, let me write it down 1 0 1 1 times 0 1 1. If I multiply it I will get. So, this is congruent to 1 0 0 1 mod 2. So, the moral of the story is; A 5 squared is also in the congruent mod congruence mod 2 subgroup. Therefore lambda of A 5 is the same as lambda of A 5 inverse.

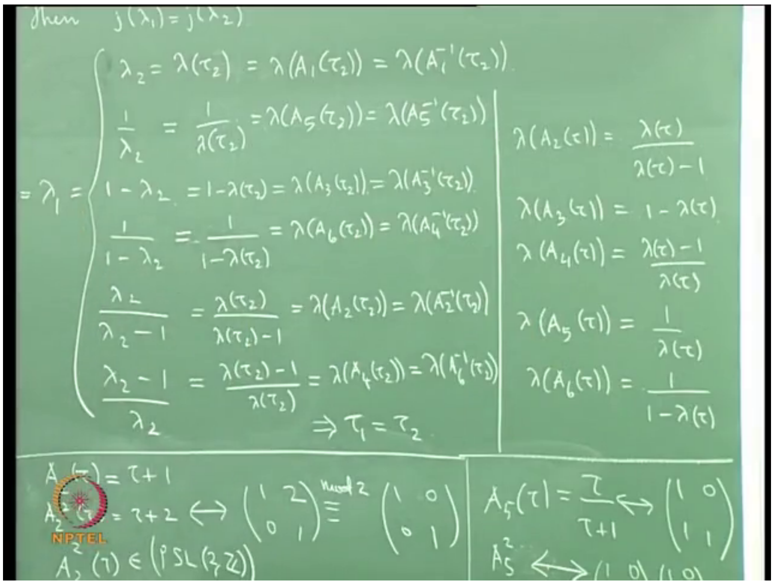
Now, you see look; now I claim you have got the proof of the corollary because you see lambda on the on omega and on you should take omega and omega prime and you take part of the boundary lambda is actually bi holomorphic. So, you see I have see I have my tau 1 and tau 2 are somewhere here in D. So, they may both be here, or they are here in any case you take tau 1 and tau 2 here then all the images of tau 1 under these 6 transformations or the images of. So, let us assume that tau 1 is let us say tau 1 is in this unshaded part.

Then there are 2 possibilities for tau 2 tau 2. May be either in the shaded part or it may also mean unshaded part if tau 2 is in the shaded part then it is going to be in one of the then if you move tau 2 by any of the if you move tau to by any of the any of these it is going to go into the other shaded parts. And similarly, if tau 2 were in the unshaded part, then it will be moved by the inverse by all these inverses into the other unshaded parts. So, the moral of the story is that no matter with what tau 1 and tau 2 you start with this quantity these either the images of tau 2 under A 1 through A 6 or the images of tau 2 under A 1 inverse through A 6 inverses going to completely line omega union omega prime.

And then and of course, you may have to input part of the boundary of course, you have you have you have removed 0 and 1, but lambda restricted to this is actually injective lambda restricted to that is actually inject and that injectivity will force that it you see it will tell you that tau 1 has to be you know, here A 1 of tau 2 or it should be the image of tau 2 under either on either one of these ai s or it has to be the image of tau 2 under one of these a I inverses. But then tau 1 and tau 2 that mean, but on the other hand tau 1 and tau 2 are in d and all these a is and a I inverses are of course, P S l 2 z elements. And the script D is a fundamental reason for P S l 2 z namely you cannot have 2 distinct elements in a P S l 2 z orbit inside d, and that will force tau 1 equal to tau 2.

And that will give you the; that will give you the fact that J tilde of lambda of tau 1 is equal to J tilde of lambda of tau 2 with tau 1 and tau 2 in script D implies tau 1 equal to tau 2 that will give you the injectivity.

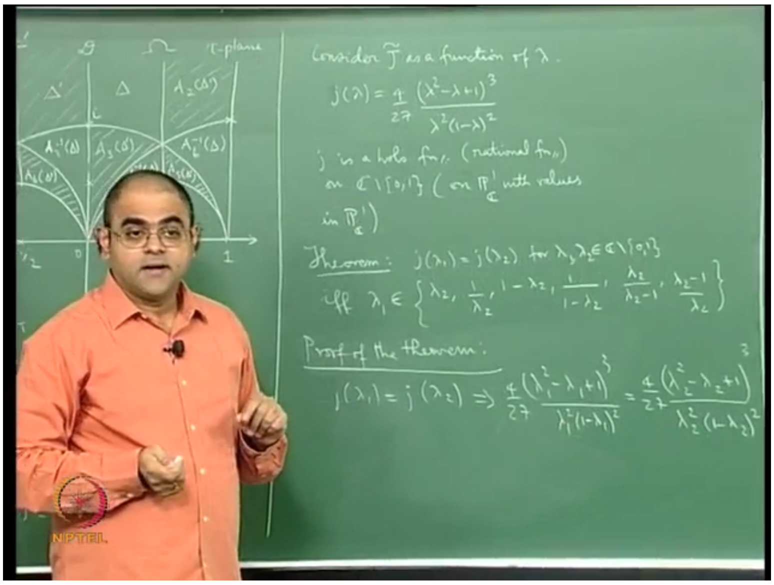
(Refer Slide Time: 53:37)



So, let me draw a line here. And then I will just write here that J tilde that implies tau 1. That is the end of the proof. So, essentially you see the there are 2 ingredients one is understanding the mapping properties of lambda under these 6 transformations in their inverses and the other thing is this theorem. So, therefore, the only thing I will, I am I am left to do is to prove this theorem. So, how do I do that that is done by a purely pure calculation?

So, let me explain that next and then we will be completely done with the statement of the theorem, that the Riemann surface structure on the set of holomorphic isomorphism classes of complex tor I is isomorphism by holomorphic to the complex plane. So, let me try to prove this theorem.

(Refer Slide Time: 54:31)

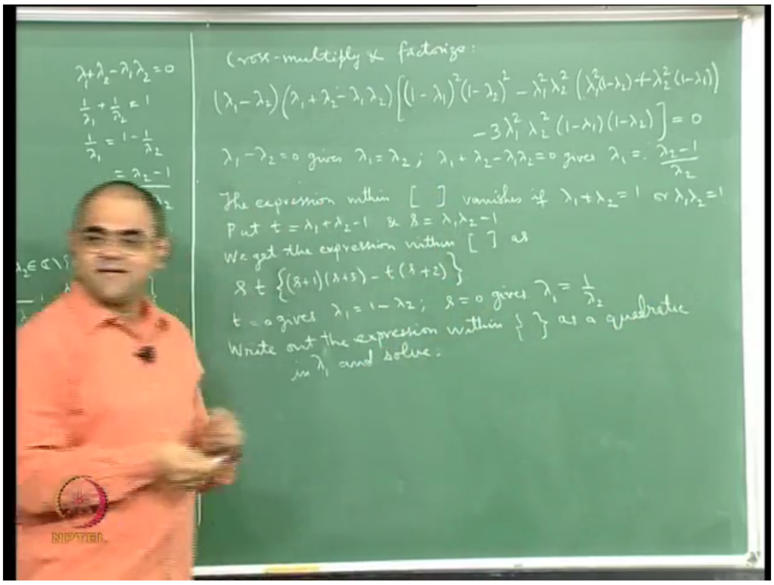


So, proof of the theorem. So, it is so let me explain it involves it involves some computation which you can I tell you what is going on and you can write it down for yourself, and check that indeed what I am saying is true. So, what you do is first I mean it is purely a brutal force computation. But then it is driven by the 4 set that by the first set of Galois Theory.

So, what I do is I start with suppose so, you know you so, I have j of lambda 1 is equal to small j of lambda 2. So, what I get is I will get well I get 4 by 27 lambda 1 squared minus lambda 1 plus 1 the whole cube by lambda 1 squared 1 minus lambda 1 the whole squared is equal to 4 by 27 same expression with lambda 2. This is what I get. Now what you do is that you cancel off the 4 by 27, and simply cross multiply to get a formidable looking degree 10 equation in lambda it is a it is a polynomial of degree 10 in lambda it looks quite formidable. So, you factor you just cross multiply, you cross multiply this.

And then the first thing you can see is if you play around a little with it, then you will see that it can be factorized.

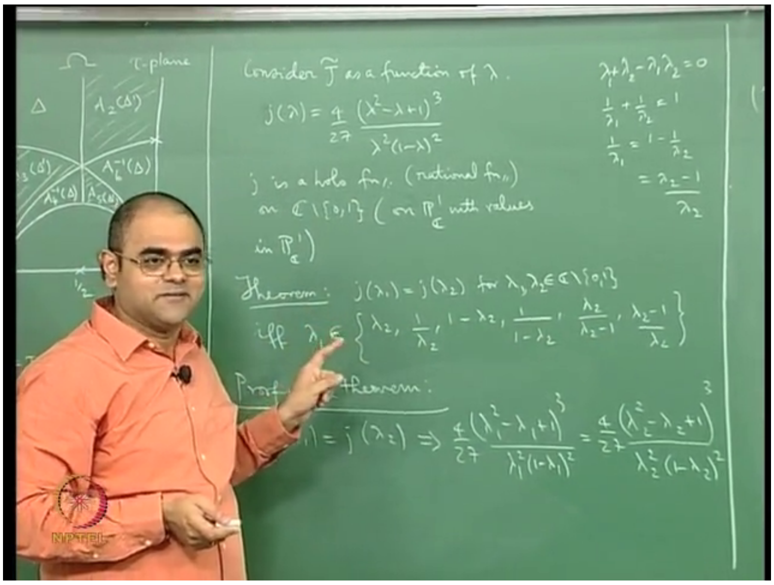
(Refer Slide Time: 56:33)



So, you see and so, you see the cross multiply and factorize, what you will get is you will get lambda 1 minus lambda 2 into, I think the other factors lambda 1 plus lambda 2 minus lambda 1 lambda 2 into you will get a third expression; which looks a formidable, but let me write it out. So, it is 1 minus 1 minus lambda 1 squared into 1 minus lambda 2 squared minus lambda 1 squared lambda 2 squared into lambda 1 squared into 1 minus lambda 2 plus lambda 2 squared into 1 minus lambda 1 minus 3 lambda 1 squared lambda 2 squared into 1 minus lambda 1 into 1 minus lambda 2 is equal to 0. This is the factorization you will get.

So, I will tell you what is the motivation. See you want to say that lambda 1 belongs to this. So, for example, you want one of the possibility is lambda 1 equal to lambda 2. So, you should expect lambda 1 minus lambda 2 to be effective, and obviously, if I in this equation if I plug instead of lambda 2 if I put lambda 1 the equation is satisfied. Therefore, you know you should expect lambda 1 minus lambda 2 to be a factor. And it is and the other possibility see this this possibility is the possibility that if you write it down, if you write this down, see what you will get is lambda 1 plus lambda 2 minus lambda 1 lambda 2 is equal to 0.

(Refer Slide Time: 58:29)



See this is if you divide throughout by lambda 1 lambda 2 you will get 1 by lambda 1 plus 1 by lambda 2 is equal to 1, and you will get 1 by lambda 1 is equal to 1 minus 1 by lambda 2, which is lambda 2 minus 1 by lambda 2. So, you see this being 0 corresponds to this possibility this one; lambda 1 taking the value lambda 2 minus 1 by lambda 2. So, there are only finitely many of these, and you have to cleverly guess which one of them you will get out as a factor.

And this comes out quite easy. So, you see therefore, these 2 correspond to these 2 possibilities this one here and this one here. And then lambda 1 minus lambda 2 equal to 0 gives lambda 1 equal to lambda 2, and lambda 1 plus lambda 2 minus lambda 1 lambda 2 equal to 0 gives lambda 1 is equal to as I wrote down; lambda 2 minus 1 by lambda 2. So, you have got 2 of these guys. Now so, what is left out is the formidable expression inside; which is can see it it looks degree 7. And so, what do you do with that. So, what you do with that is well you notice again, you notice the following thing you will notice that if you if you put.

So, you know the expression these square brackets if you put lambda 1 lambda 2 equal to 1. Or if you put lambda 1 plus lambda 2 equal to 1 it will be it will be it will vanish. The expression within vanishes if lambda 1 plus lambda 2 is equal to 1 or lambda 1 lambda 2 is 1. And you can see this corresponds to the case lambda 1 plus lambda 2 equal to 1 corresponds to the case lambda 1 equal to 1 minus lambda 2, and that lambda 1 lambda 2 is equal to 1 corresponds to the case lambda 1 is equal to 1 by lambda 2. So, you get these 2. And so, the trick is what you do is put s put t equals to lambda 1 plus lambda 2 minus 1. And s is equal to lambda 1 lambda 2 minus 1. Then you should express then you should expect t and s to be factors.

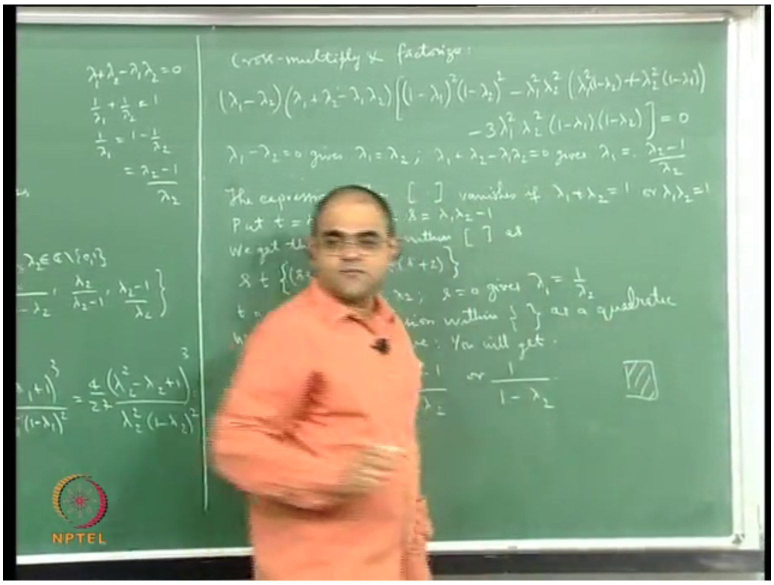
And transform the whole equation inside the brackets into an expression in terms of s and t. So, what you will get is essentially you will get the following thing after some after some simplification, you will end up with s t we get the expression within the brackets as it turns out to be s times t s into t into; what you have here is, s into t into s was s plus 1 into s plus 3 you get this. So, either this is 0, or this is 0, or this expression is 0, but this expression is 0 will either be in s is 0 or t is 0 which gives you these 2 possibilities namely lambda 1 is equal to 1 minus lambda 2 or lambda 1 is equal 1 by lambda 2. So, the only thing that you will have to worry about is the expression within this square bracket.

So, let me put flower brackets so that I can write it like this. So, s equal to 0 gives. So, let me write that s is t equal to 0 gives lambda 1 is equal to 1 minus lambda 2, and s is equal to 0 gives lambda 1 is equal to 1 by lambda 2. So, I will have to only worry about the expression inside the square brackets. So, write out the expression within the square brackets as a quadratic in lambda 1, and solve write out that expression inside the flower brackets as a quadratic in lambda 1 and simply solve using the good old you know, high school formula for a quadratic equation.

And what you and low behold what you end up is either, you will get either lambda 1 is equal to lambda 2 minus 1 by lambda 2 which is this which is this one again, or you will get 1 by 1 minus 1. So, that is it so, the point is that because, you already know that this is what you should get you can guess the factors by substituting properly. So, the moral of the story is that having known this in advance helped, but this is not something that has come out of nowhere it is not just a bunch of tricks. But it is actually a statement of the fact that this mapping lambda going to j from p 1 to p 1 is a Galois cover with Galois group the symmetric group on 3 elements. So, probably in the exercises or in a later lecture I will expand on it.

So, all I want to say is that this comes from Galois Theory, but having known this factorizing it is not a big deal. So, that finishes the proof of this theorem.

(Refer Slide Time: 65:37)



And therefore, we are now we have we can be the sigh of relief we have finally, been able to prove this statement that the on the set of holomorphic isomorphism classes of complex tor i, there is an natural Riemann surface structure and that Riemann surface structure is actually the bi holomorphic to the natural Riemann surface structure on the complex plane.

So, I will stop here what I wish to do here onwards is try to explain how these complex tor I are elliptic curves. So, I will have to give the algebraic aspect you can always you can already see that in the fact that J tilde restricted to d is injective already brought up this lot of algebra. And I told you this is got (Refer Time: 66:28) with Galois Theory, and if you also look at this equation, you see that this is a cubic equation in 2 variables. So, it is of the form y squared is equal to 4 x cube minus g 2 x minus g 3, it is a cubic equation in 2 variables.

And this is the so, it is so, it is algebraic and it defines what is called and it is 0's define what is called an elliptic curve. And what I am what I am trying what I will try to show in the later lectures is that every holomorphic complex torus is actually an elliptic curve. And so, that is how this is a very special case of the more general statement that you take a Riemann surface, and you put one topological condition that it is compact as a topological space. Then low behold it becomes an algebraic curve.

It becomes a curve which is given by a neat algebraic equation. And this is the first case in the case of genus 1 namely, the case of a complex torus; where you are able to directly verify it because you have this differential equation. But in more in, but for genus greater than 2, things are things are more difficult than require more theory.

So, I will stop here.