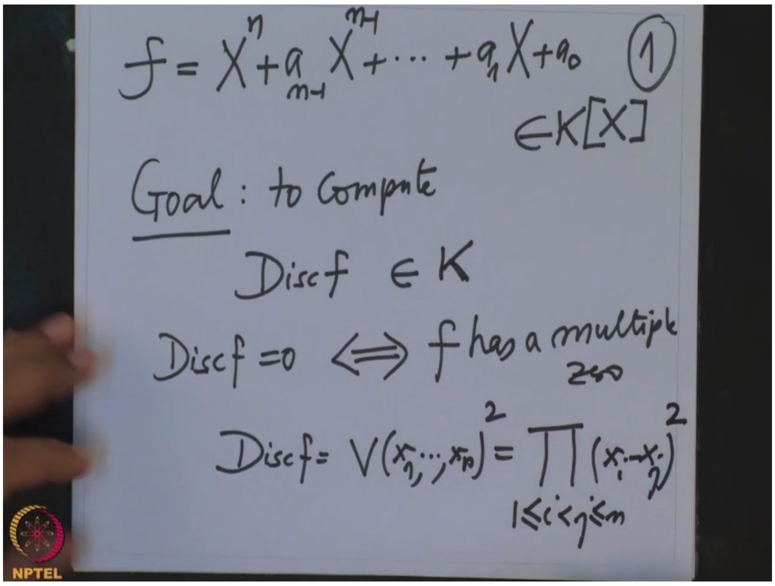
Galois Theory
Professor Dilip Patil
Department of mathematics
IISc Bangalore
Lecture 62
Examples for further study

(Refer Slide Time: 0:53)



$f = X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ ①

$\in K[X]$

Goal : to Compute

$\operatorname{Disc} f \in K$

$\operatorname{Disc} f = 0 \iff f$ has a multiple zero

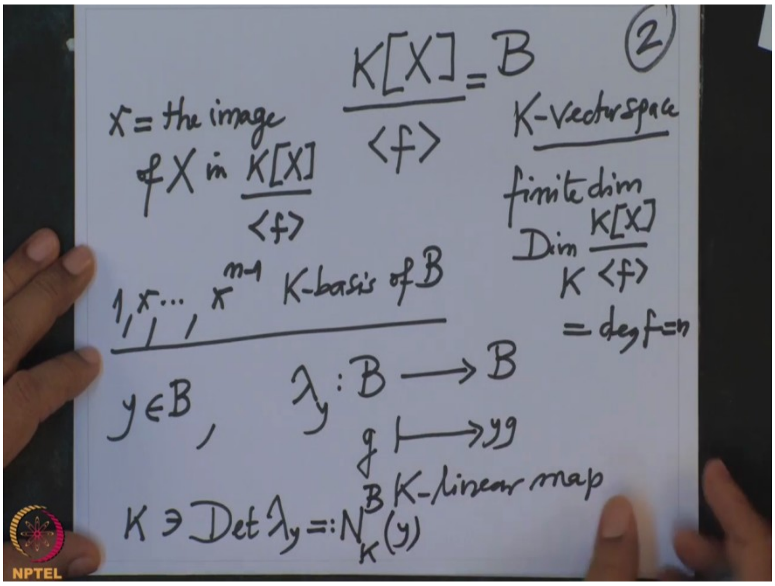
$\operatorname{Disc} f = V(x_1, \ldots, x_n)^2 = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2$

Alright, so in the last lecture we saw one uses a discriminant to computer nature of the Galois group and now I will give without proof how one does compute the discriminant without knowing the roots of the polynomial. So start with the polynomial f monic f is a monic polynomial $X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$ this is a polynomial with coefficients in K and we don't need to assume if irreducible. So arbitrary monic polynomial.

And our goal is to compute discriminant of f and we know definitely this is in K that is because it is the symmetric in, so we have checked that this polynomial is symmetric polynomial and therefore it is a polynomial in elementary symmetric functions and elementary symmetric functions of the roots are precisely this coefficients therefore that we have included that it is in K, okay this is in K.

so we want to compute this constant and if it is zero we know this discriminant is zero if and only if f has a multiple zero. In fact we know the formula for the discriminant that is in terms of the roots that is discriminant of f equal to Vandermonde $(x_1, \ldots, x_n)$ square is Vandermonde is product one less equal to i less than j is equal to n $(x_i - x_j)^2$. So if you want to compute this it is a horrendous job because given a polynomial of very high degree it will be nearly impossible to compute all the zeros.

(Refer Slide Time: 3:11)



$\frac{K[X]}{\langle f\rangle} = B$ 2

x = the image of X in $\frac{K[X]}{\langle f\rangle}$

K-vector space

finite dim

$\text{Dim}_K \frac{K[X]}{\langle f\rangle} = \deg f = n$

$1, x, \ldots, x^{n-1}$ K-basis of B

$y \in B$, $\lambda_y : B \longrightarrow B$

$g \longmapsto yg$

K-linear map

$K \ni \text{Det}\,\lambda_y =: N_K^B(y)$

Okay, so here is the recipient of the polynomial f monic that I already written we have this $K[X]$ and go mod ideal is generated by f that I get a vector space, this is a K vector space and the division algorithm will tell you this K vector space is finite dimensional. In fact the dimension of this vector space, dimension of $\frac{K[X]}{\langle f\rangle}$ this dimension equal to the degree of f.

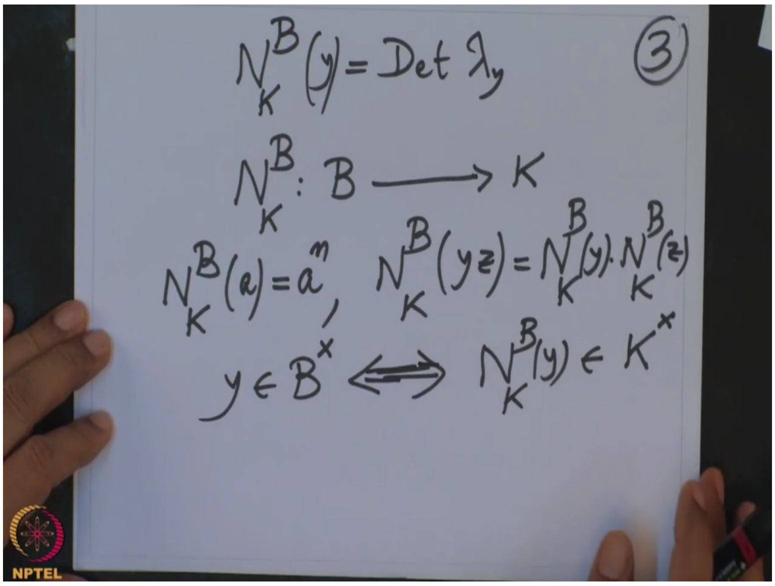
And what is the base is? In fact the base is you can write down take the small x, let small x be the image of capital X in this residue in $\frac{K[X]}{\langle f\rangle}$ and the base is then $1, X, \ldots, X^{n-1}$ this is a basis where this degree is n that is clear this is all you use the divisional with them, if you have given any polynomial, any element here will be a polynomial mod f but that polynomial after dividing by this monic polynomial f I can assume it is degree less n minus 1 and read that mod f means read, right replace capital X by small x.

And then you get a linear combination of these guys and this is unique because division algorithm is unique therefore this is a basis. Okay when this is a basis remember for any y let us call this as B this B is a finite dimensional K vector space and this is the basis. This is the K basis of B this is what I will be using. Now given any element y in B you look at the multiplication from the left by that y lambda y this is B to B.

Any element g going to y def g this is clearly K linear map of the vector spaces and therefore determinant of that make sense. Determinant of y this makes sense and this determinant will therefore be an element in K and this is how many cross how many determinants? This will be n cross n determinant. So this is also Vandermonde this is a norm.

Norm of B over K of the element y.

(Refer Slide Time: 6:16)



3

$$N_K^B(y) = \text{Det}\, \lambda_y$$

$$N_K^B : B \longrightarrow K$$

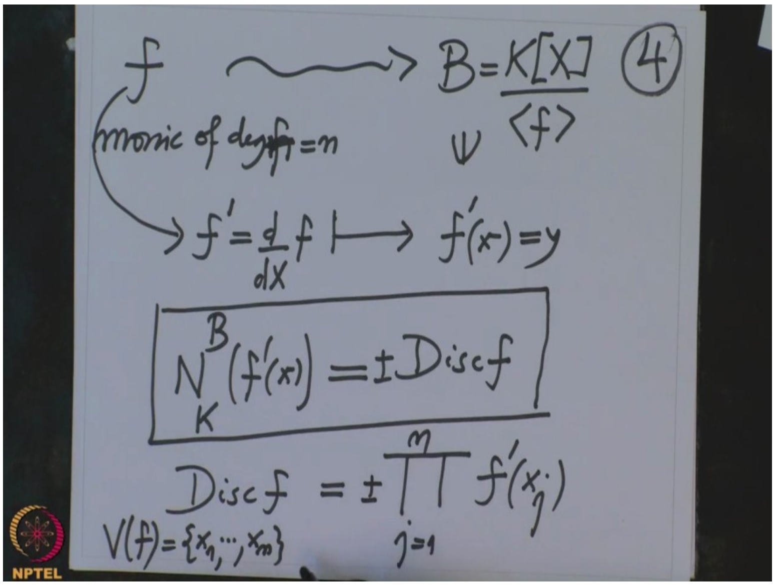
$$N_K^B(a) = a^n, \quad N_K^B(yz) = N_K^B(y) \cdot N_K^B(z)$$

$$y \in B^\times \iff N_K^B(y) \in K^\times$$

So let me write it on the next page. So norm of norm B over K of y this is the determinant of the linear map lambda y. So the norm we have said earlier also norm of B over K this is a map from B to K and it is multiplicative map, this is first of all the property which satisfies the norm of B K if I take any constant any a this is a power n and norm of this y times z is norm of B over K y times norm of B K over z.

This is trivial because determinant is multiplicative, determinant of a times B equal to determinants a times determinant B therefore this is clear. And also it is clear that if y is a unit in B if and only if norm y is a unit but norm y is an element in K, its unit in K means its nonzero constant. And this norm is also used to study some special properties of the B. Namely what are the units and so on? So I will not go too much into this.

(Refer Slide Time: 7:57)



$f \rightsquigarrow B = \frac{K[X]}{\langle f \rangle}$ (4)

monic of $\deg f = n$ $\quad \Psi$

$\to f' = \frac{d}{dX} f \longmapsto f'(x) = y$

$$\boxed{N^{B}_{K}(f'(x)) = \pm \operatorname{Disc} f}$$

$$\operatorname{Disc} f = \pm \prod_{j=1}^{n} f'(x_j)$$

$V(f) = \{x_1, \cdots, x_n\}$

Now I want to write down a formula for the discriminant in terms of this norm, so we have given f monic of degree n then from the f degree n, degree of f equal to n from here you go to the residue class ring B which is $\frac{K[X]}{\langle f \rangle}$ and let us take an element we have given f, so we can differentiate it, differentiating is not a big problem, so this is $\frac{d}{dx}$ of f, formal derivative of f.

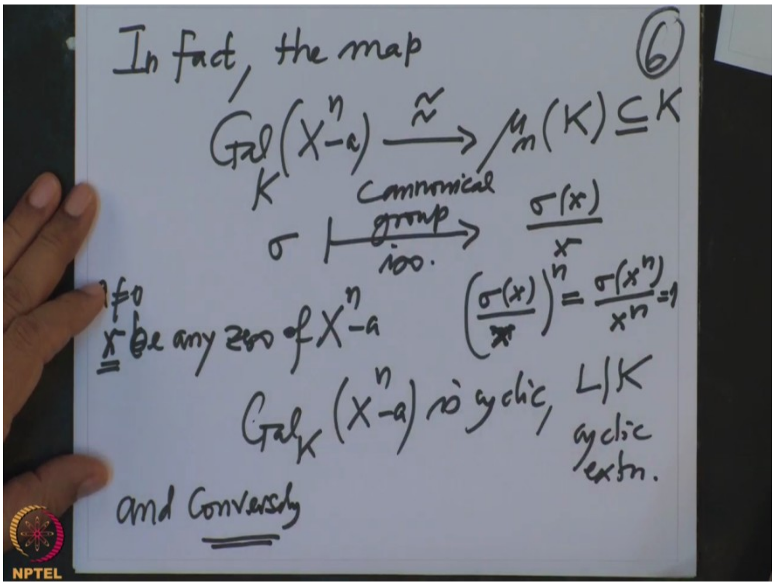
And now read f in this ring that is we take the image of f in the ring B but that is what you take this derivative and plug in instead of capital X small x, so $\frac{K[X]}{\langle f \rangle}$ this is an element in B, so this is my y and compute the norm of $f^{'}(x)$ and this is nothing but the discriminant or maybe I have to see the sign plus minus, so this is the discriminant of f, this is a nice formula this is how we compute.

So for example if we wanted to compute cubic discriminant then this f prime will be degree 2 and finding a norm of degree 2 will not be so difficult because it is a degree 2 polynomial and then only the matrix in all will be 3 by 3 and therefore this is computable and this doesn't require the knowledge of the zero's of f, so this is how one computes effectively.

In fact this way you can use it even you can write down some small software in using some computer algebra packages you give f and then they will give you the discriminant and then testing whether it is square or not etc. also discriminant has another nice formula but that again involves the roots but it is a nice formula discriminant of f is product product is running over j and you take $f^{'}$ and evaluated the roots x_j .

So this is running over the roots of f. So this is $V(f)$ equal to $x_1,\ldots,x_n$ and this doesn't even require the fact that, so you see here is it has repeated root then f prime will be 0 at somebody and therefore this site is 0 and this is again plus minus sign, so that one can determine the sign just from the the determinant side, so I will not spend more time on the discriminant in more that is way to compute and one can lose a computation for small degree polynomial degree 3, degree 4 one can possible because you can compute the determinant of degree 3 on order 3 and order 4.

(Refer Slide Time: 11:19)



In fact, the map

6

$$\mathrm{Gal}_K(X^n-a) \xrightarrow{\approx} \mu_n(K) \subseteq K$$

Cannonical group iso.

$$\sigma \longmapsto \frac{\sigma(x)}{x}$$

$a \neq 0$

$\underline{\underline{x}}$ be any zero of $X^n - a$ $\quad \left(\frac{\sigma(x)}{x}\right)^n = \frac{\sigma(x^n)}{x^n} = 1$

$\mathrm{Gal}_K(X^n-a)$ is cyclic, $L|K$ cyclic extn.

and Conversly

Alright, now I want to say something more about the cyclic extensions. I want to list all cyclic extensions but this I will do it almost with the proof but some of the details I will leave it. For example suppose I have, so we will assume here, we assume that my base field K contains roots of unity. If necessary I will attach replace K by K and adjoin all the roots unity.

For example in characteristic zero you apply this attach all the roots of unity in Cj, see it's a big group and you don't need so much you attach any truth and truth of unity this is a finite cycling group and attach that, so you still get a finite extension, alright. So I will assume that it contains roots of unity we don't need all n-th roots of unity and that n will depend on the degree etc.

So assume that and suppose that is X^n-a , this is a polynomial in $K[X]$ and it is separable and irreducible that means what? What condition one need to put is characteristic should not be divisible by n, P should not divide n this is characteristic of K and the separability will be there and irreducibility is another thing to check when will such a polynomial be irreducible.

But assume that then under this assumption then the Galois group over K of this polynomial is cyclic of order n in fact I will give you an isomorphism.

So in fact the map from Galois group of X^n-2 air cycle group I need a cycle group of order n and who can be better than $\mu_{n,K}$ this is cycle group of order n and we are assuming this is containing K now all n-th roots of unity are lying in K, so this is cyclic of order n and I want to give you a map first, so take any Sigma and map it where and fix any root.

Let x be any zero of X^n-a in the splitting way of course x any fix that and map its σ to $\sigma(x)$ by X. first of all acts cannot be zero because it's root of this and a is nonzero of course because it's irreducible polynomial, so look at these map. First of all this map doesn't depend on X and this map is an isomorphism. So that proves that the Galois group of this polynomial is cyclic.

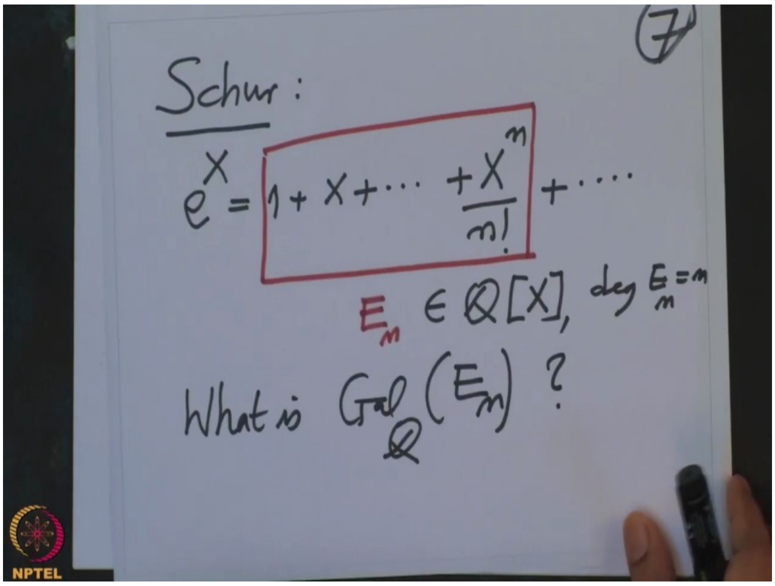
So that means this extension splitting field of, so that means this is cyclic. $Gal_K(X^n-a)$ is cyclic, so that also means also we are saying that L over K is cycling extension, so this map is canonical because it doesn't depend upon the choice of X, so this is a canonical group homomorphism, canonical group isomorphism. It is clear that this is the n-th root of unity because you see you raise it to n when you raise this to n, what will it be?

This is $\sigma(X^n)$ this is X here, no divided by x power and but x^n is a and $\sigma(x^n)$ will be $\sigma(x)$ whole power n this is σ , so this is 1, right? So therefore this map is indeed a map here it is clear that it is a group homomorphism and it is also clear that it doesn't depend on x, so it's canonical. Okay and conversely what does that mean?

And conversely means given any cyclic extension where the base will contain cyclic extension of degree n where the base will contains n-th roots of unity than there exist a polynomial X^n-a such that this L is a splitting field of X^n-a , so that characterizes all cyclic extensions and this was multiplicative similarly one can do it additively but I will not do it now because we're running out of time.

And now I will only state 2 important results due to Schur which are difficult to prove and it will require quite a bit effort but maybe it is a good way for studying further one wants to study more, so this is Schur, alright.

(Refer Slide Time: 18:09)



7

Schur:

$$e^X = \boxed{1 + X + \cdots + \frac{X^n}{n!}} + \cdots$$

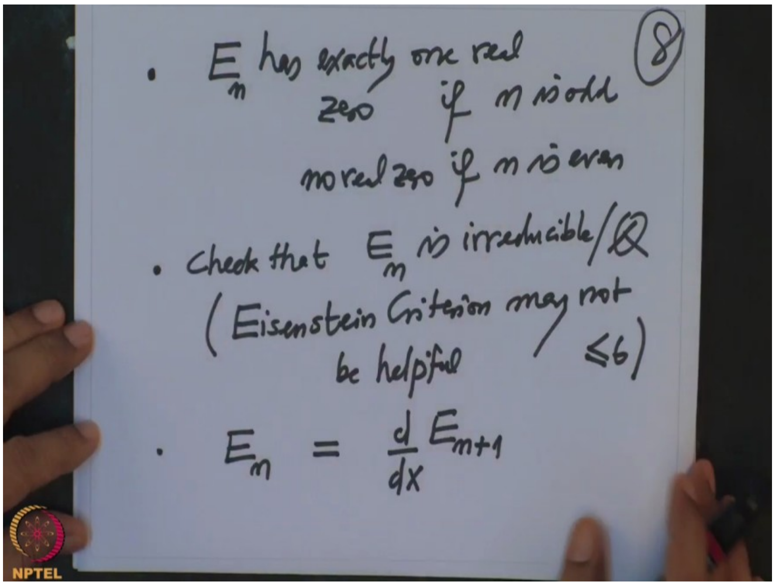
$E_n \in \mathbb{Q}[X]$, $\deg E_n = n$

What is $\mathrm{Gal}_{\mathbb{Q}}(E_n)$?

So you look at the exponential series e power x this is 1 plus x so on so on x power n factorial by n factorial and so on. And I want to make a polynomial, so I issued only consider up to here and that I will call it E_n . E_n this is a polynomial in $\mathbb{Q}[X]$ degree of E_n is m. The problem is to compute the Galois group of this over $\mathbb{Q}$, so what is Gal Okay En?

When I say what is that, means how can you describe this Galois group in terms of the known groups and answer is very nice but not so easy to prove.

(Refer Slide Time: 19:31)



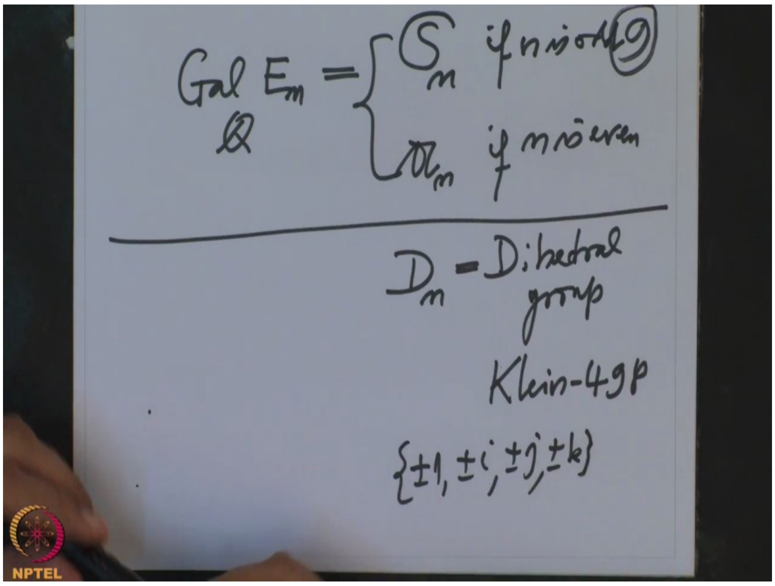
8

- E_n has exactly one real zero if n is odd
  no real zero if n is even
- Check that E_n is irreducible$/\mathbb{Q}$
  (Eisenstein Criterion may not be helpful ≤ 6)
- $E_n = \frac{d}{dx} E_{n+1}$

Alright, so I will tell you the answer, so I will list some of the facts according to the difficulties. So first of all note that E_n has exactly one real zero if n is odd and no real zero if n is even. Secondly check that E_n is irreducible over $\mathbb{Q}$ and remember here Eisenstein will not help Eisenstein criterion may not be helpful. It is helpful only up to I think n equal to 6.

It is helpful because when n grows when you clear the denominator n factorial, n factorial has many square divisors, so it may not help. Now then the 3rd important thing is what is the relation between E_n and E_{n+1}, the relation is if I differentiate E_n, E_{n+1} you will get E_n this is easy of course this I should have stated in the beginning, so these are irreducibility is difficult, alright.

(Refer Slide Time: 21:41)



$$\operatorname{Gal}_{\mathbb{Q}} E_m = \begin{cases} S_m & \text{if n is odd} \\ A_m & \text{if m is even} \end{cases}$$

D_m - Dihedral group

Klein-4 gp

$\{\pm 1, \pm i, \pm j, \pm k\}$

So now the result this is Schur he has computed the Galois group and says Galois group of E_n over $\mathbb{Q}$ is S_n if n is odd and A_n if n is even and this requires quite a bit of a proof, so I'll not indicate the proof here and once you do this then you can do many more examples where the Galois group is S_n or A_n once you have this then also you can try to see when the other groups how do you compute?

How do you write down polynomial is whose Galois group is this? For example D_n , D_n is dihedral group or what is Klein-4 group? Klien-4 is simple because this order 4 degree or 8 what is that? Quaternion group, so the quaternion group plus minus 1, plus minus i, plus minus j, plus minus k this quaternion group is also order 8 group this is non-abelian group.

And what equation will you write down whose Galois group is this? What equation will you write down this is Galois group and so on. So when one wants to study Galois Theory more, later you have to devise a method how do you find a polynomial? Polynomial of the primitive element, minimal polynomial of the primitive element which describes the field extension.

And this minimal polynomial also called Galois resolvent or primitive element is also called Galois resolvent these are the terms used by Jordan and you know people later who tried to study Galois Theory much more intimated way. And also one can do much more this but then the methods will be used from the other subject's especially algebraic geometry, algebra curves or more from complex analysis side.

Or more from algebraic topology that computation of fundamental groups of a topological space is closely related to the computation of the Galois group and so on. So with this I will stop here and I hope you have enjoyed this course very much, I tried to keep the prerequisite as little as possible but because of that probably I cannot go on more because the time constraint, so thank you very much for your attention.