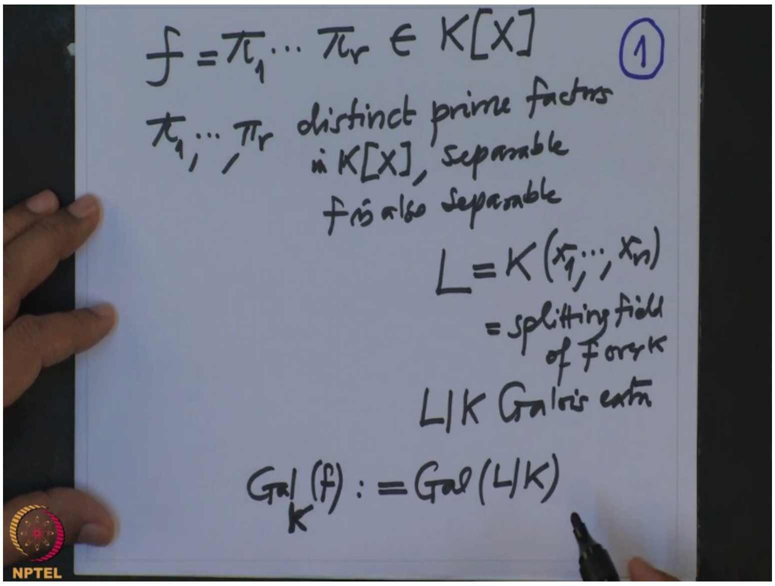
Galois Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture 61

Discriminants

So in the last lecture we have seen for each polynomial we have attached a Galois group and we are studying zeros of this given polynomial in terms of the action of the Galois group on the zeros of that polynomial. So let me go on this furthermore and give little bit of more information more intimate statements.

(Refer Slide Time: 0:57)



$f = \pi_1 \cdots \pi_r \in K[X]$ 1

$\pi_1, \cdots, \pi_r$ distinct prime factors in $K[X]$, separable

f is also separable

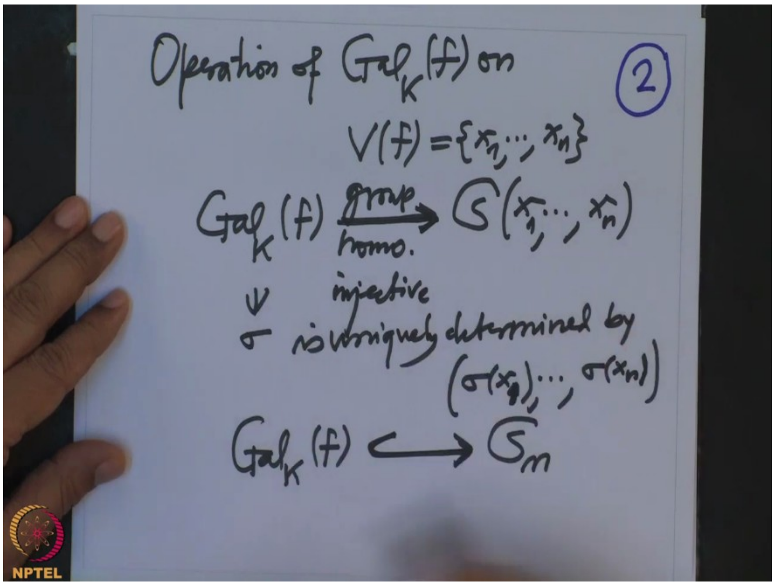
$L = K(x_1, \cdots, x_n)$ = splitting field of f over K

$L|K$ Galois extn

$Gal_K(f) := Gal(L|K)$

So I will assume now f is a monic polynomial which is product of finite remaining prime polynomials distinct so and each… This is a polynomial in $K[X]$, K is a base field and $\pi_1,\ldots,\pi_r$ are distinct prime factors in $K[X]$ and they are all separable. So that means they do not have repeated zero so therefore f is also separable , then we have attached a field to this that is L which is a splitting the field of f, so given all the roots we call them $x_1,\ldots,x_n$, this is a splitting field of f over K and then therefore we have this extension L over K which is a Galois extension because it is normal and separable and therefore there is a Galois group $Gal(L|K)$ and this is how we have defined it to be Galois group of polynomial f over K.

(Refer Slide Time: 2:48)



Operation of $Gal_K(f)$ on

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

2

$$Gal_K(f) \xrightarrow[\text{homo.}]{\text{group}} \mathfrak{S}(x_1, \dots, x_n)$$

injective

$\Downarrow$

σ is uniquely determined by $(\sigma(x_1), \dots, \sigma(x_n))$

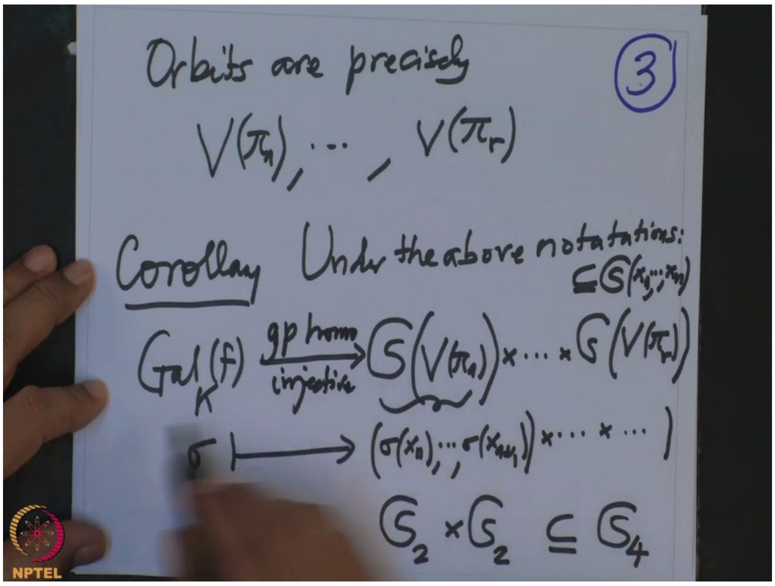
$$Gal_K(f) \hookrightarrow \mathfrak{S}_n$$

NPTEL

And we are studying operation of this Galois group on the roots right and the last time we will see, so operation of $Gal_K(f)$ on $V(f)$ which is $x_1, \dots, x_n$ and therefore the action of morphism is a group morphism from $Gal_K(f)$ to the symmetric group on this $x_1, \dots, x_n$ and this map this is a group morphism and this is Injective. Injective simply because each element σ here is uniquely determined by the tuple $\sigma(x_1), \dots, \sigma(x_n)$. If you know the values of σ on $x_1, \dots, x_n$ then σ is determined that simply means this map is injective therefore one realizes this Galois group of f as a subgroup of S_n.

But this homomorphism this one depends on the numbering we have chosen $x_1, \dots, x_n$. If somebody else chooses the different numbering then this group will be corresponding conjugate subgroups because different numbering will give you permutation and that will be conjugation by that permutation the image will be differ by that conjugation.

(Refer Slide Time: 4:35)



Orbits are precisely

3

$V(\pi_1), \cdots, V(\pi_r)$

Corollary Under the above notatations: $\subseteq \mathfrak{S}(x_{11},\ldots,x_{r\nu_r})$

$$\mathrm{Gal}_K(f) \xrightarrow[\text{injective}]{\text{gp hom}} \underbrace{\mathfrak{S}(V(\pi_1))} \times \cdots \times \mathfrak{S}(V(\pi_r))$$

$$\sigma \longmapsto (\sigma(x_{11}),\ldots,\sigma(x_{1\nu_1})) \times \cdots \times \cdots)$$

$$\mathfrak{S}_2 \times \mathfrak{S}_2 \subseteq \mathfrak{S}_4$$

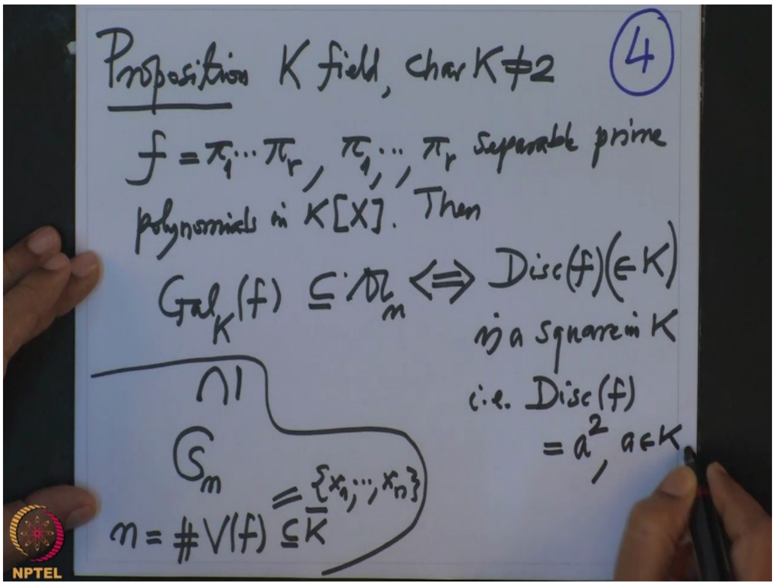
So and last time also last lecture we had proved that the orbits are precisely $V(\pi_1),\ldots,V(\pi_r)$, these are the orbits. So the roots of π_1 will be permuted among itself, π_2 will be permuted among itself and so on, so they will not mingle with each other because that is how the algebraic structure of f is preserved under the operation. So I want to write down the corollary one more corollary under the above notation more more final statement that is Galois group of f over K to now, the earlier it was in the group S_n , but now I am taking permutations on the roots of π_1 cross cross permutations of the roots on π_r and then σ goes to this.

So σ will permute these guys so σ is giving you permutations here, so that is so I did not number it so it is clear that this σ gives a permutation by σ of if you call the roots of π_1 to be x_{11} , $\sigma x_1 \mu_1$, so there are ν_1 roots for π_1 this is this tuple this permutation and so on. So you get here r elements, so note that this group is not isomorphic to this group is contained in $S(x_1,\ldots,x_i)$, this also has the same letters but this group is say for example, you take S_4 and you can take this so S_4 may not be right example so what I am saying is if you take $S_2 \times S_2$ so this one has cardinality so this is also these 2 letters these 2 letters, this is also contained here but not equal.

This one permutes only the 2 fixed letters, this one permutes 2 fixed letters so this is abelian for example this is not abelian and so on. So therefore this is better finer information than that and here also the comment again the same that this is a group homomorphism and it is

Injective. Injective for the same reason because σ is uniquely determine the values on all these guys therefore it is Injective group morphism. So for example, if you know it is $S_2 \times S_2$ then it is abelian, before I do I need one more observation that, let me write that observation.

(Refer Slide Time: 8:09)



Proposition K field, char $K \neq 2$ (4)

$f = \pi_1 \cdots \pi_r$, $\pi_1, \ldots, \pi_r$ separable prime polynomials in $K[X]$. Then

$\mathrm{Gal}_K(f) \subseteq A_n \Longleftrightarrow \mathrm{Disc}(f) (\in K)$ is a square in K

i.e. $\mathrm{Disc}(f) = a^2$, $a \in K$

$\cap|$

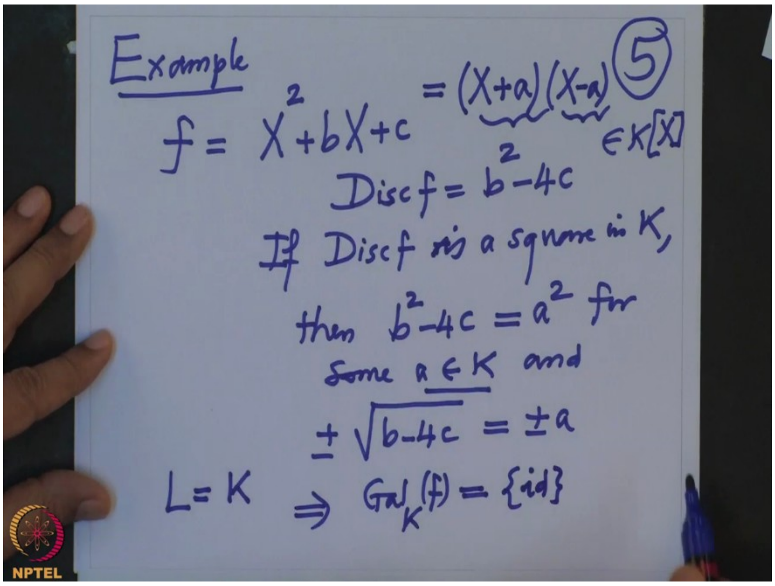
S_n

$n = \# V(f) \subseteq \overline{K}$ $= \{x_1, \ldots, x_n\}$

So this is a proposition and now I will assume K is a field and I will assume characteristic K is not 2, and f is a polynomial which is monic and it splits into these prime factors and each $\pi_1, \ldots, \pi_r$ separable prime polynomials in $K[X]$. This then I want to know, so we have seen above that this Galois group, we know this is a subgroup of S_n subgroup of the symmetric group n, where n is the number of roots, n is cardinality of the roots of f in the algebraic closure and that we write this set as $x_1, \ldots, x_n$, they are distinct roots as many as the degree of f, degree of f is n okay. Okay so now I want to know when is this group contained in the alternative group, so I want to know this.

So this is always so then this Galois group is a subgroup of alternating group A n if and only if the discriminant D i s c, now I write this notation discriminant of f, we have seen the discriminant is a constant like in a quadratic case it was $b^2 - 4c$ so this is in K that was we have approved this but this is contained in n if and only if discriminant is a square in K, just not in K but square in K means what, so that means this discriminant of f is some a square for some a in K, this is what the statement is. So so let me first give a small example to why it is useful so for example this is a very small example, this should be done in the school you do it in the school.

(Refer Slide Time: 11:07)



Example ⑤

$f = X^2+bX+c = (X+a)(X-a) \in K[X]$

Disc $f = b^2-4c$

If Disc f is a square in K,

then $b^2-4c = a^2$ for

Some $a \in K$ and

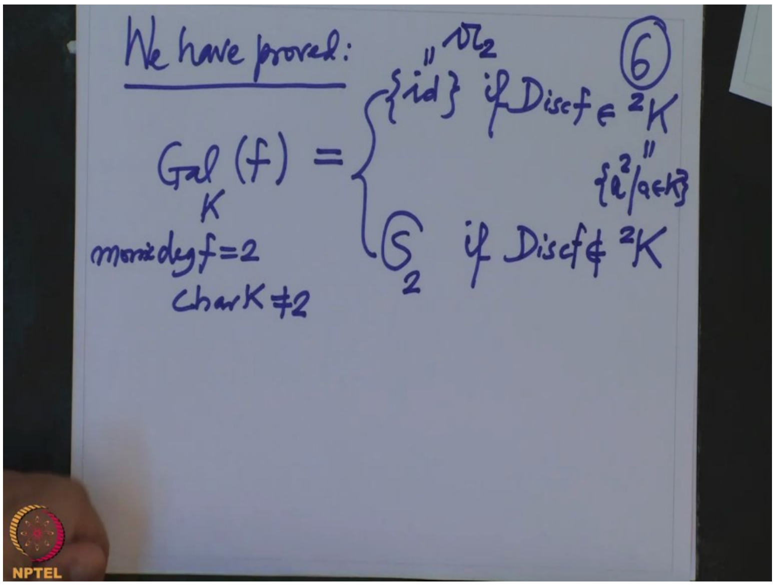
$\pm\sqrt{b-4c} = \pm a$

$L = K \Rightarrow Gal_K(f) = \{id\}$

So example, we take a degree 2 polynomial f, f is X^2+bX+c this is the polynomial and in this case we know what is the discriminant of f, discriminant of f is b^2-4c okay. And suppose this is a square, so if the discriminant of C, discriminant of f if this is a square, if this is a square in K what do that mean? Then that means b^2-4c this is some a square for some a in K that means I know the roots then and therefore the square root of when I write b^2-4c + – , this is same thing as + – a.

So that means this polynomial actually splits in two linear factors X + a and X – a combined where are the factors? They are in $K[X]$ because this is a in K therefore the factors are linear so that means the original polynomial we started with, it actually splits in K only therefore what is the splitting field, this is nothing but K only because the polynomial already splits in K then what is the Galois group, Gal f over K this is nothing but it is a group and what is the extension? The trivial extension so the Galois group is trivial only identity, so this is very easy. Converse is also correct, conversely also same steps so therefore quadratic polynomial can have, so what are the possibilities for Galois group lets write it down.

(Refer Slide Time: 13:32)



We have proved:

6

$$\underset{K}{\operatorname{Gal}}(f) = \begin{cases} \overset{\mathfrak{A}_2}{\overset{\shortparallel}{\{id\}}} & \text{if } \operatorname{Disc} f \in \underset{\overset{\shortparallel}{\{a^2/a\in K\}}}{{}^2K} \\ \mathfrak{S}_2 & \text{if } \operatorname{Disc} f \notin {}^2K \end{cases}$$

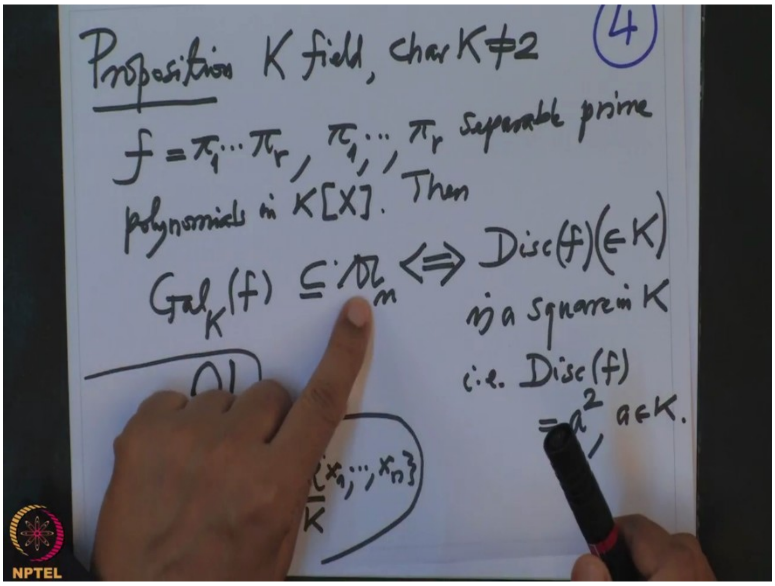
monic $\deg f = 2$

$\operatorname{Char} K \neq 2$

So we have proved Galois group over K of a quadratic polynomial, degree f is 2 monic, monic you can always assume and more importantly characteristic of K is not 2 then there are 2 possibilities and we will write down exactly when is which, this is identity trivial if discriminant of f is a square so that means it belongs to K 2. Remember K 2 is all square, this is a all those a square such that a is in K all squares that is then it is identity otherwise it will have what will be the splitting field? If it is not a square then it is contained in A_n that our proposition I stated but that means in that case it will be S_2 .

I have only 2 possibilities, if discriminant is not in K not a square so it is not in A_2 therefore it has to be S_2 but if it is not A_2 is a trivial this thing, this is a trivial this is the group A_2 so it is, so one can do such things such analysis for degree 3, degree 4, etc, but then all that you need to compute the discriminants so then it becomes a computational that becomes precisely theory of equations alright, so let me prove the theorem I stated first so discriminant so I want to prove this.

(Refer Slide Time: 15:19)



Proposition K field, char $K \neq 2$ (4)

$f = \pi_1 \cdots \pi_r$, $\pi_1, \ldots, \pi_r$ separable prime polynomials in $K[X]$. Then

$Gal_K(f) \subseteq A_n \iff Disc(f) (\in K)$ is a square in K

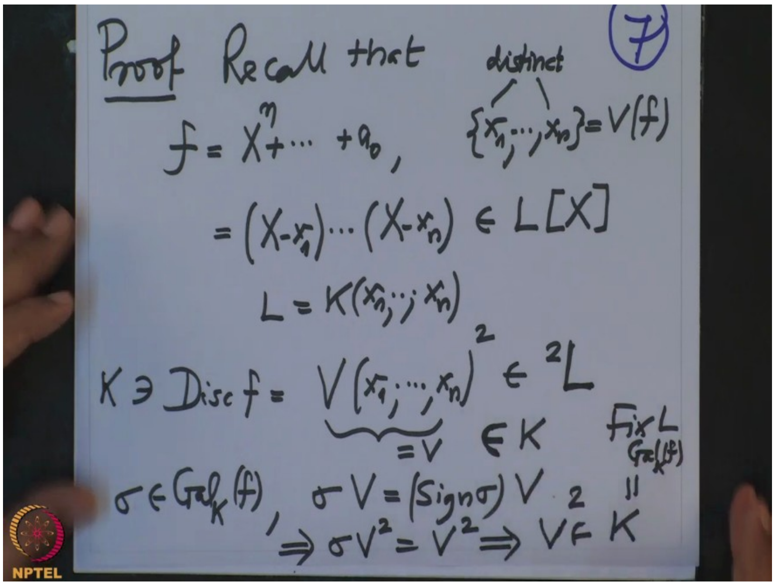
i.e. $Disc(f) = a^2$, $a \in K$.

$\{x_1, \ldots, x_n\}$

$\overline{K}$

Galois group is contained in A n, we know it is always contained in S n in our setup, this is contained in A if and only if discriminant is a square in K, in K is very important alright so proof of the theorem.

(Refer Slide Time: 15:38)



Proof Recall that (7)

$f = X^n + \cdots + a_0$, $\overset{\text{distinct}}{\{x_1, \ldots, x_n\}} = V(f)$

$= (X - x_1) \cdots (X - x_n) \in L[X]$

$L = K(x_1, \ldots, x_n)$

$K \ni Disc\, f = \underbrace{V(x_1, \ldots, x_n)}_{=V}{}^2 \in {}^2L$

$\in K$ $\quad$ $Fix\, L^{Gal_K(f)} = K$

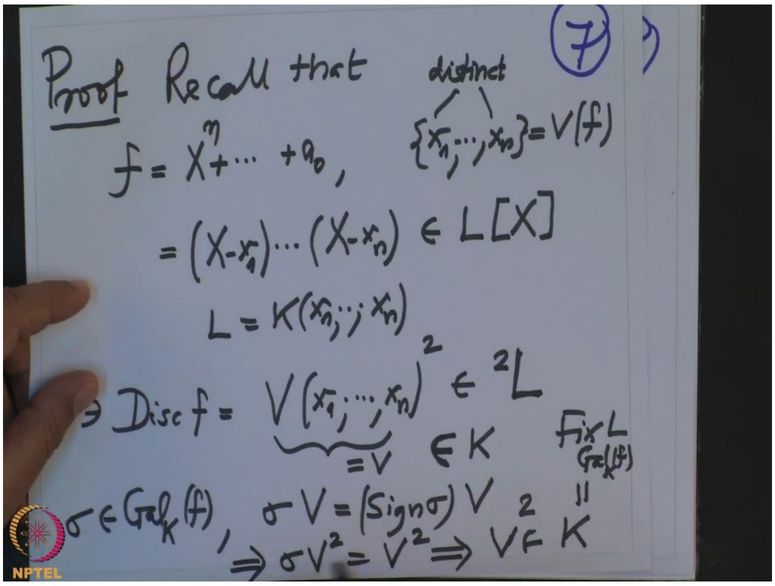
$\sigma \in Gal_K(f)$, $\sigma V = (Sign\, \sigma) V$, $\Rightarrow \sigma V^2 = V^2 \Rightarrow V^2 \in K$

Proof; so let me recall little bit about discriminant, so recall that so a polynomial f beside degree n and it is monic, so X^n+ lower degree terms + a_0 and then what is the discriminant? So then you find a bigger field L so you will go to the splitting field L of f and then you write f as $(X - x_1)...(X - x_n)$ and this is in $L[X]$, this L is a spitting field $K[x_1, \ldots, x_n]$ and this $x_1, \ldots, x_n$ are the zeros of f, they are all zeros and they are all distinct. Then what is the discriminant? If you remember, discriminant of f is nothing but you take the Vandermonde of $x_1, \dots, x_n$ and square of that.

Now remember that this square this Vandermonde is not in K, apriori this is in L so this is in ${}^2L$, this is a square in ${}^2L$, this is always this is what discriminant is. We have also proved that this actually belongs to K then you have proved and how did we prove that? We proved that this by using the following, if I have σ an element in the Galois group then $\sigma(V)$ let me just simply write this as V, this is nothing but sign of $\sigma(V)$.

So this Vandermonde when I apply permutation what comes out is the signature of the permutation, so when will this Vandermonde be invariant? So V^2 is the first of all note that because of this $\sigma(V^2)=V^2$, so that means V^2 is indeed in the fix field then fix field is K because it is a Galois extension, this is a fixed field of under the Galois group which is K because the field extension is Galois. So V square is definitely fixed so V^2 is an element in K that proves this discriminant is indeed an element in K but by definition it was square in L but now the problem is when it is square below alright.

(Refer Slide Time: 18:54)



Proof Recall that distinct (7)

$f = X^n + \cdots + a_0$, $\{x_1, \dots, x_n\} = V(f)$

$= (X - x_1) \cdots (X - x_n) \in L[X]$

$L = K(x_1, \dots, x_n)$

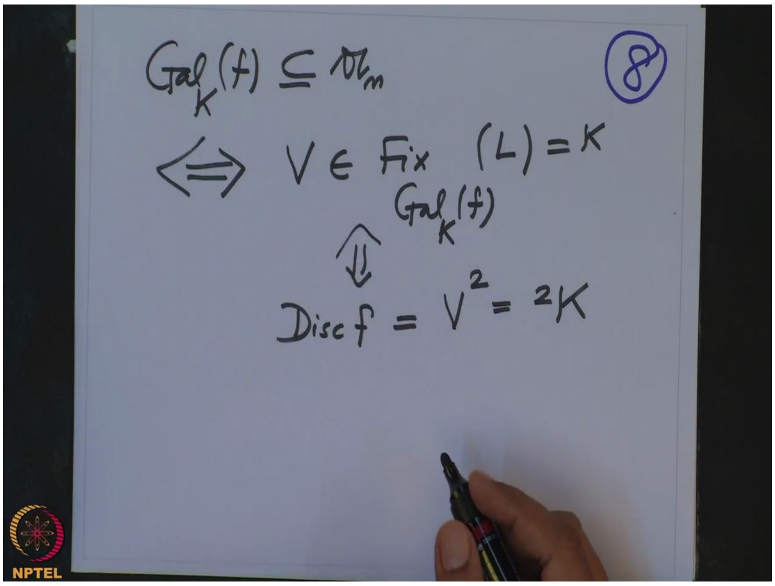
$\Rightarrow \text{Disc} f = \underbrace{V(x_1, \dots, x_n)}_{=V}^2 \in {}^2L$

$\in K$ $\quad \text{Fix}_{\text{Gal}_K(f)} L$ || K

$\sigma \in \text{Gal}_K(f)$, $\sigma V = (\text{Sign}\,\sigma) V$, $\Rightarrow \sigma V^2 = V^2 \Rightarrow V^2 \in K$

So this shows that and when did we use characteristic? So here we have used the fact that the characteristic is not 2 otherwise you know sign of σ is either 1 or – 1 and – V will become V so there will be a trouble, so characteristic is not 2 and V is nonzero. V is nonzero we have used because these roots are distinct so that is where we have used distinct and characteristic is not 2.

(Refer Slide Time: 19:26)



$\mathrm{Gal}_K(f) \subseteq \mathfrak{A}_n$ 8

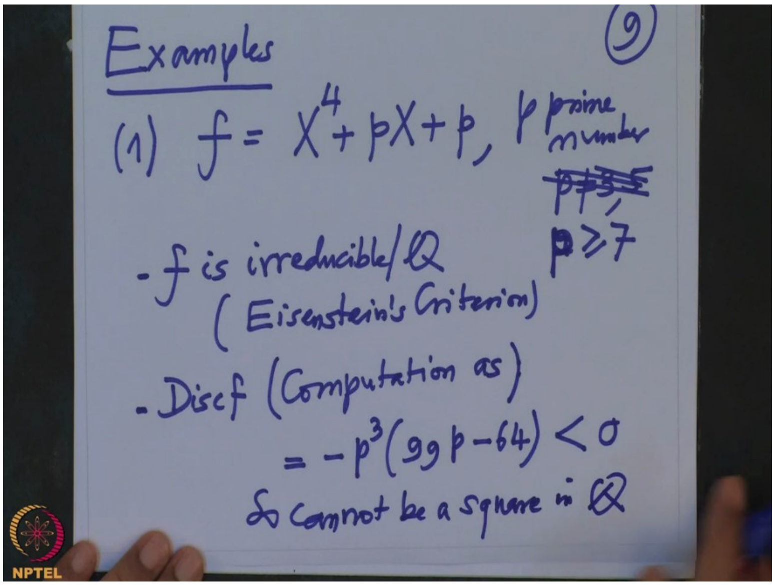
$\Longleftrightarrow V \in \mathrm{Fix}_{\mathrm{Gal}_K(f)}(L) = K$

$\Updownarrow$

$\mathrm{Disc}\, f = V^2 = {}^2K$

So therefore we show that the Galois group of f over K, this is contained in A_n if and only if V is fixed under every element of Galois group, but that means so that implies this discriminant of f which is V^2 , so it is V^2 and V is in this is K, V is in L therefore this is in K^2 . Conversely if it is in K^2 , V and discriminant whichever square it is that and V will differ by only + – and therefore if and only if this is if and only if. So we have proved the statement and if you want to check about the weather G Galois group is contained in the alternating group, we have to compute the discriminant and we have to check it is square or not square and that we have seen in the quadratic case.

(Refer Slide Time: 20:55)



Examples 9

(1) $f = X^4 + pX + p$, p prime number ~~$p \neq 3, 5$~~ $p \geq 7$

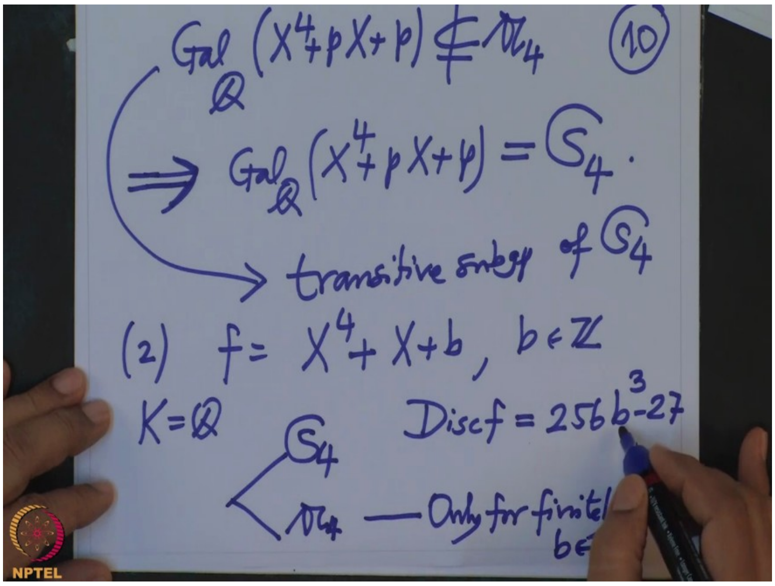
- f is irreducible/$\mathbb{Q}$ (Eisenstein's Criterion)
- $\mathrm{Disc} f$ (Computation as) $= -p^3(99p - 64) < 0$

So cannot be a square in $\mathbb{Q}$

Now let us do little bit more so for example, some couple of examples so that you will know what is needed to be calculated. So first of all some examples at least, so one I look at the polynomial f which is $X^4 + p\,X + p$ and is a prime number, p prime let us assume that p is bigger equal to 7 okay. And now observe, first thing you observe that f is irreducible over $\mathbb{Q}$ and this is Eisenstein's criteria, use that because I will apply it to this is prime, monic both these coefficients are divisible by p and the constant term is not divisible by p^2 therefore this is irreducible over $\mathbb{Q}$ alright.

Second thing you know to compute is to compute the discriminant, now how do we compute the discriminant? This is 4 so discriminant is some determinant know it is a Vandermonde, of course we cannot hope to calculate discriminant by using the Vandermonde because if you want to use Vandermonde and square it then you have to know what are the roots so you have to have different techniques to compute the discriminants. So computation can be done as follows; so that I want to explain how do we want to do computation that I will explain soon or maybe in the next half and I will write down the answer here the discriminant one computes is $-p^3 + 99\,p - 64$ so the discriminant is therefore negative so it cannot be square and our base field is Q.

(Refer Slide Time: 23:30)



$\text{Gal}_{\mathbb{Q}}(X^4+pX+p) \not\subseteq \mathfrak{A}_4$ (10)

$\Rightarrow \text{Gal}_{\mathbb{Q}}(X^4+pX+p) = \mathfrak{S}_4$.

transitive subgp of $\mathfrak{S}_4$

(2) $f = X^4 + X + b$, $b \in \mathbb{Z}$

$K = \mathbb{Q}$ $\quad$ $\text{Disc} f = 256b^3 - 27$

$\mathfrak{S}_4$

$\mathfrak{A}_4$ — Only for finitel

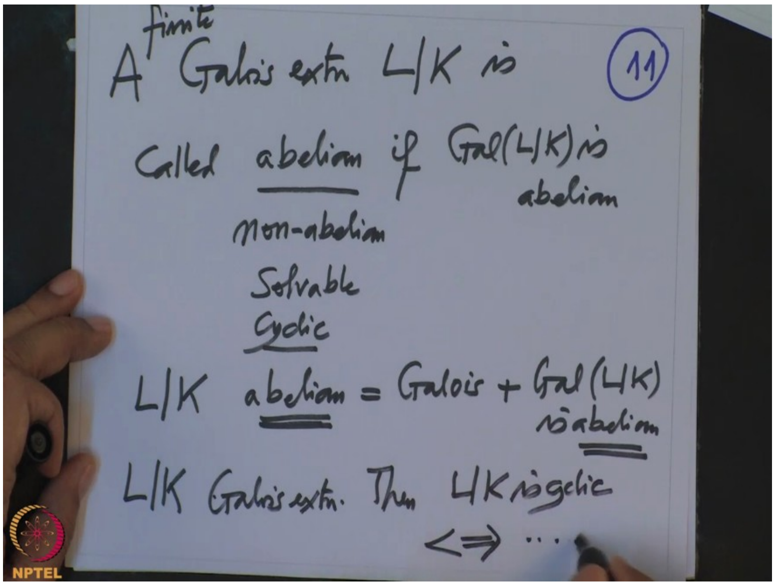
$b \in$

Therefore what do we infer? We infer the Galois group over $\mathbb{Q}$ of this polynomial $X^4 + p\,X + p$, this is not containing A_4 because if it is contained in A_4 the discriminant will be a square but it is a negative therefore it is not containing the square. And from here you conclude the Galois group over $\mathbb{Q}$ $X^4 + p\,X + p$, this has to be S_4 , so we have computed from here to here to do the calculation. Calculation means what? This is not contained in A_4 so it has odd permutation and so on, and so standard finite group theory you can conclude it is a transitive group because we know the polynomial is zero decimal so this group is a transitive subgroup of S_4 and therefore you conclude from that the group has to be S_4 only, so this one.

So 2nd example, you take the polynomial X^4+X+b and b is an integer and I want to calculate the Galois group over $\mathbb{Q}$. So again you write to compute the discriminant of f, this is $256b^3-27$, which is what? Which is now it will depend on b, if b is negative it is definitely, so if b is negative, it is definitely negative with b positive and big then big means it is compared to this. So therefore what answer you will get? You will get answer either S_4 or A_4 , and this A_4 will occur only for finitely many b. So this b only for finitely many b it will be A_4 , otherwise it is S_4 because if b is negative first of all, this is negative and therefore it cannot be square therefore it is here, therefore it is here and so on.

So in all these examples the most important thing now is a computation of a discriminant that is what is very important. And in the next lecture I will indicate how do you compute the discriminant and it is not so difficult, but one has to use the linear more effectively that is one thing.

(Refer Slide Time: 26:41)



A finite Galois extn $L|K$ is (11)

Called abelian if $Gal(L|K)$ is abelian

non-abelian

Solvable

Cyclic

$L|K$ abelian = Galois + $Gal(L|K)$ is abelian

$L|K$ Galois extn. Then $L|K$ is cyclic $\Leftrightarrow$ ...

Another thing is I want to mention here is, I will make a definition here, so a Galois extension L over K finite Galois extension L over K is called abelian if the Galois group is abelian so and I keep calling Galois abelian extension. If I write L over K abelian that means it is a Galois extension + the Galois group is abelian so this adjective your here which we are attaching that is too coming from the group. So for example, if I say Galois group is non-abelian, so non-abelian extension I say that means it is a Galois extension and the Galois group is non-abelian.

If I say solvable extension that means the Galois group is solvable and so on. If I says I cyclic then the Galois group is cyclic and one can write down the characterization so I wanted to write a theorem also so L over K Galois extension, then L over K is cyclic if and only if, this I will do it in the next next lecture and also we will know how to compute the discriminant thank you, we will continue after the break.