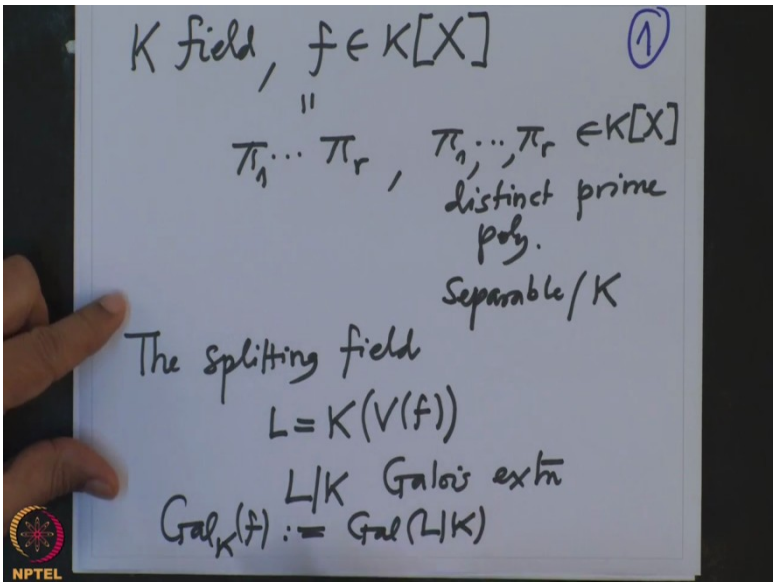
Galois Theory
Professor Dilip Patil
Department of mathematics
Indian Institute of Science Bangalore
Lecture 60
Operation of Galois group of all inaugural on the set of zeros

(Refer Slide Time: 0:35)

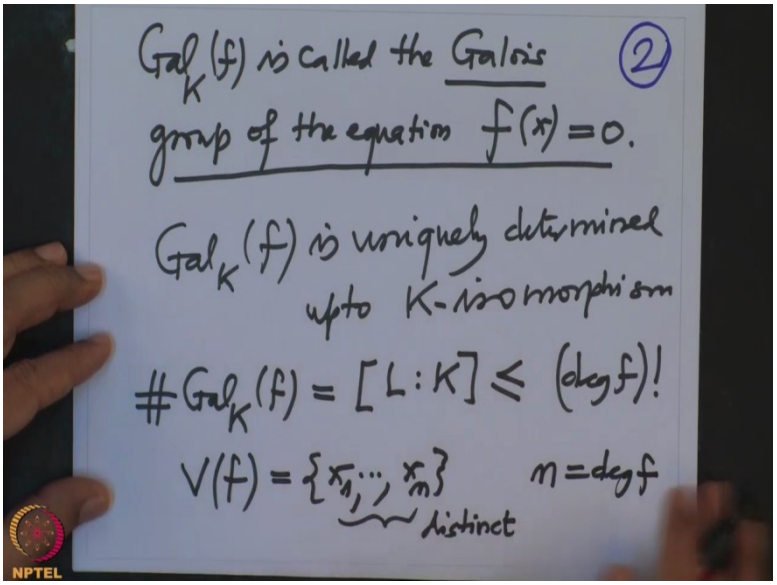


Alright, so let us resume our discussion about Galois group of a polynomial, so recall our notation we have of a field K it may not be characteristic 0 it is a arbitrary characteristic field and we have a polynomial $f \in K[X]$ and we are assuming that f is a product of distinct prime polynomials, so $\pi_1 \ldots \pi_r$ are distinct prime polynomials in $K[X]$ distinct prime polynomials. and also we are assuming all this prime polynomials are separable.

Did not really necessary to assume but we can reduce to that case they are separable over K therefore with this we have the 0 set of this polynomial the splitting field the minimal splitting field or splitting field that is $K(V(f))$ this is L and we are considering L over K this is the Galois extension because f is separable and this L is a splitting field and we want to study then the Galois group, $Gal_K(f)$ this is by definition Galois group of L over K and we know this only depends on F because we have seen that splitting fields are any 2 splitting fields are K isomorphic.

Therefore this L doesn't depend on f it only depends on isomorphism class of L, so this is a Galois group.

(Refer Slide Time: 2:50)

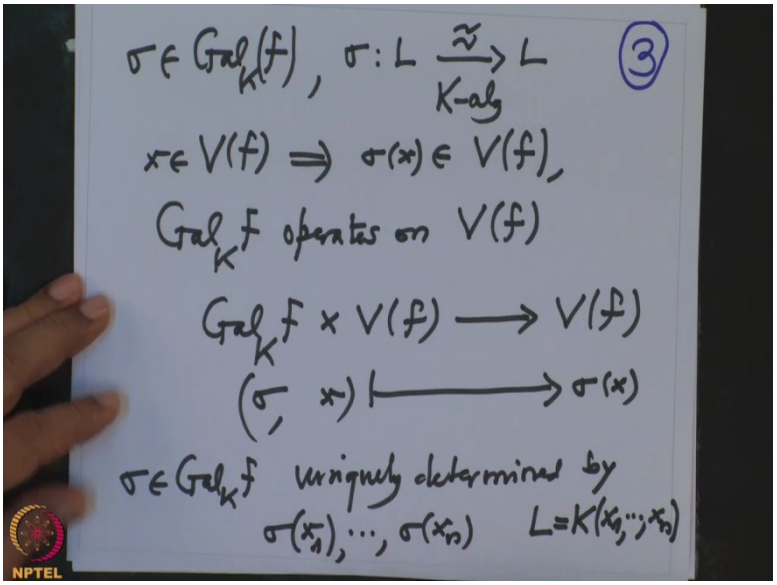


This is called that Galois group of the equation, so $Gal_K(f)$ is called the Galois group of the equation $f(x)$ is 0 that is how in earlier days it was written. And we want to study the roots by using the lower groups and now I will give some indication how you go on in concrete examples. Alright the bursting to notice this group is isomorphic this is uniquely determined up to a K isomorphism.

$Gal_K(f)$ is uniquely determined up to K isomorphism, alright. So first thing to notice because it is a Galois extension the order of this Galois group is same thing as degree of this field extension L over K because L over K is Galois and this degree is less equal to degree f factorial, this is very easy to check because, okay.

There is one thing another thing I want to write is $V(f)$ these are the roots $x_1, \ldots, x_n$ they are the zeros of F and they are all distinct they are distinct and n is the degree of f, this we know.

(Refer Slide Time: 5:04)

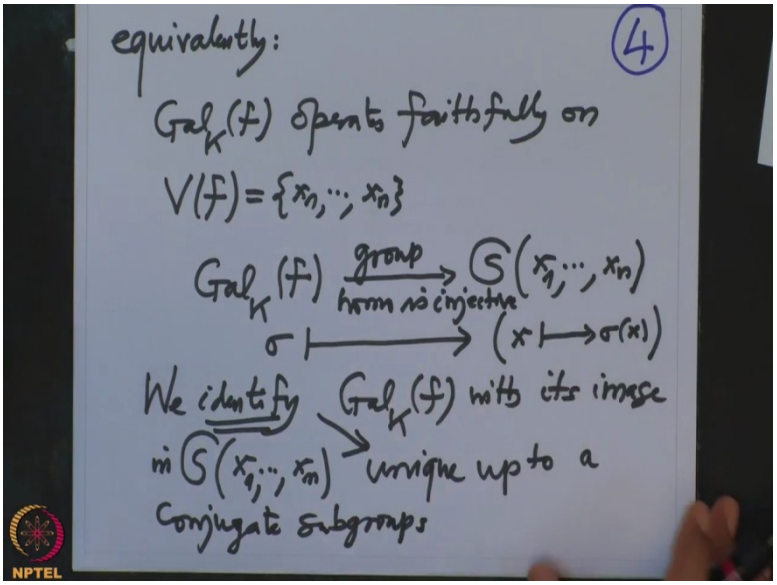


Moreover we know that if I have a σ element in the Galois group then the σ is an Automorphism of L, K Automorphism K algebra Automorphism and if x is a root, if x is in $V(f)$ then we know that $\sigma(x)$ is also in $V(f)$, so this means in other words this means the Galois group f operates the $V(f)$, this operation is nothing but the natural operation of the Galois group on the splitting field and that we are restricting to here.

So this is the map, operation map. This is Galois group cross $V(f)$ this is a very natural map σ and any x is close to $\sigma(x)$ as we have been using this observation again and again, this is one thing. Another thing to note is that any σ in Galois group this is uniquely determined by the tuple, if I know the values of this σ on the roots this σ is uniquely determined by this.

simply because L is generated or K is by these elements $x_1, \ldots, x_n$, $x_1, \ldots, x_n$ are precisely the roots of F, so if I know these values then I know completely σ on L because any element of L is actually a polynomial in $x_1, \ldots, x_n$, so therefore all the values of σ will be determined by these values.

(Refer Slide Time: 7:23)



So therefore this means what? This means, so equivalently this operation is faithful, so that means Galois group operates faithfully on the 0 set $V(f)$ which is $x_1, \ldots, x_n$, what does that mean? So this means when operation will give you a map from the group, now group theoretically thinking, operation one should think the map this from the Galois group to the permutations of this $x_1, \ldots, x_n$.

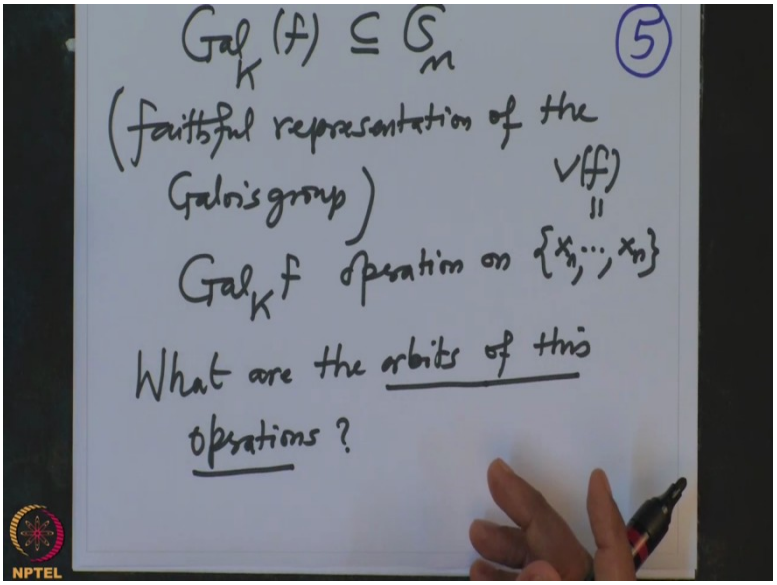
And if a σ goes to these permutations, what permutation? Namely X going to $\sigma(x)$ and this because σ is uniquely determined by these values on this $x_1, \ldots, x_n$ only one σ will go to the given tuple, so that means this group homomorphism is injective because σ is uniquely determined by its values on this.

So this is injective but when we say this, now if I choose a different numbering then this will give you a different, so that means we are identifying, so this we identify $Gal_K(f)$ with its image m S of $x_1, \ldots, x_n$ but when we did this identification we have chosen a fix numbering, we have chosen some numbering, somebody else may some different numbering.

But if one chooses a different numbering then that will be unique up to a conjugation, so therefore when you make this identification if somebody chooses different numbering then you don't get that given Galois group but you will get the conjugate subgroup in $S_1, \ldots, S_n$, so this is uniquely determined, this identification is unique up to a conjugation, conjugate subgroups.

So I hope it is clear, so this if you chose, if somebody choose a different numbering then this given Galois group will be changed to its conjugate subgroup.

(Refer Slide Time: 10:35)

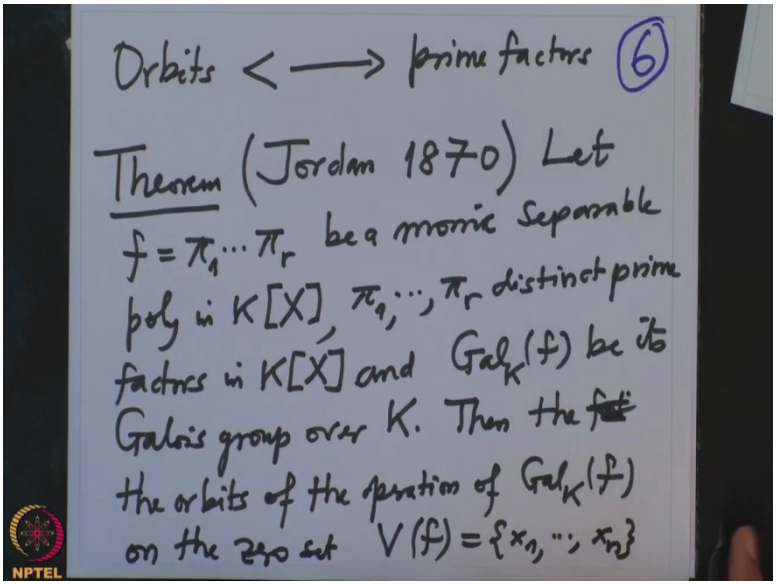


Anyway this is an injective homomorphism that we will use and therefore we are identifying this Galois group of f with the permutation group 1n and now the most important factor gain I want to, this is also called a faithful representation, I want to avoid using big words, so this is called faithful representation of the Galois group, so this is only the language I want to use which is not so important.

But now I want to understand this Galois group operation on the 0 set $x_1, \ldots, x_n$, so for example 11 says understanding and operation means what are the orbits? What are the stabilizers? And so many other things, right? So 1st about the orbits, so what are the orbits? What are the orbits of these operations? And what is the have to do with f?

So remember we only started with a polynomial f and this group, 0 set all this is created after f, so when we say orbits what is that to do with F and can you recognize the orbit in terms of f?

(Refer Slide Time: 12:29)

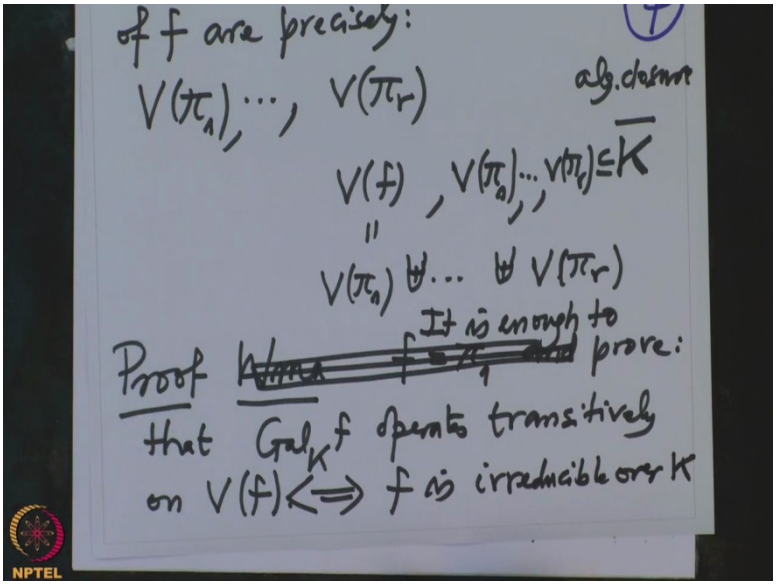


So that is what I will prove is, orbits are precisely they corresponds to the prime factors, so that shows this group theory orbit and this is an algebra, this is a prime factorization, so what do I want to prove? The following theorem, so this is a theorem. This year is due to Jordan and the year is something like 1870. Jordan was the 1st who wrote the on Galois theorem.

And in that book all these statements are proved not only that he also proved so-called Jordan canonical form which now is taught in linear algebra courses and he thought it actually for the finite field because he wanted to understand the general linear group GL and K of a finite that was the reason he proved Jordan canonical form.

Alright, so what does that Jordan theorem say? So let f equal to $\pi_1, \ldots, \pi_r$ be a Monic separable polynomial in $K[X]$ and $\pi_1, \ldots, \pi_r$ are distinct prime factors in $K[X]$. And then we have $Gal_K(f)$ be its Galois group over K then the following are equivalent. Then the orbits the operation of Galois group of f on the zero set $V(f)$ which I will denote $x_1, \ldots, x_n$.

(Refer Slide Time: 15:27)



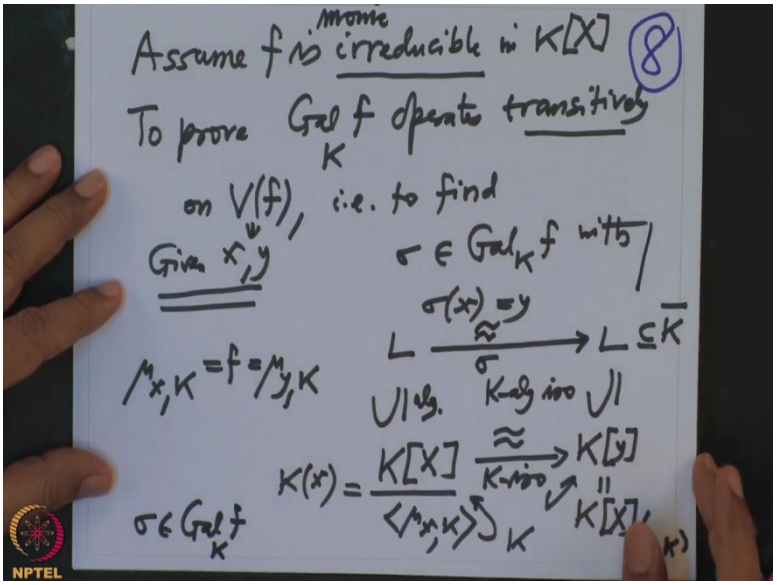
Zero set this of f are precisely $V(\pi_1),\ldots,V(\pi_r)$ when I write V means I fix an algebra closure $\overline{K}$ this is algebra closure of K and when I write zero set that is in $\overline{K}$, so all these elements, all these $V(\pi_1),\ldots,V(\pi_r)$ they are subsets here also $V(f)$ is a subset and we know that $V(f)$ is nothing but the union $V(\pi_1)\cup\ldots\cup V(\pi_r)$ and this is a big joint union because we are assuming the prime factors $\pi_1,\ldots,\pi_r$ at distinct prime factors therefore this is decomposition form we will prove this.

So proof, okay so how many orbits are there? As many as the prime factors. Okay and how are we going to prove this? we may assume f equal to π_1 and then I have to prove what? I have to prove that $Gal_K(f)$ operates transitively on V of f if and only if, so we should prove that, so we may assume, so don't say we may assume.

We will prove that this one operates, so it is enough to prove the following statement that this operation is transitive if and only if f is irreducible over K. So this is what we want to prove.

Alright, so that 2 statements assuming if it is irreducible I want to prove it is transitive and assuming transitivity I want to prove f is irreducible. So proof of this so 1st is which one?

(Refer Slide Time: 18:23)



First is, assume f is irreducible in $K[X]$ and I want to prove, to prove Gal f operates transitively on $V(f)$, this is what I want to prove. So what does transitive operation may? That means given 2 elements x and y in f I want to find that is given x and y to find σ in Galois group with $\sigma(x)$ equal to y. So I have given x and y and I want to find σ which carries x to y.

And we are assuming f is irreducible, so and we are actually assuming its monic also, monic and irreducible prime. So look therefore X is 0 of f, so what will be the minimal polynomial of X over K? That will be f and that is also minimal polynomial of y over K. So x and y are both have the same minimal polynomial and I want to prove that there is an Automorphism of the splitting field which will carry x to y.

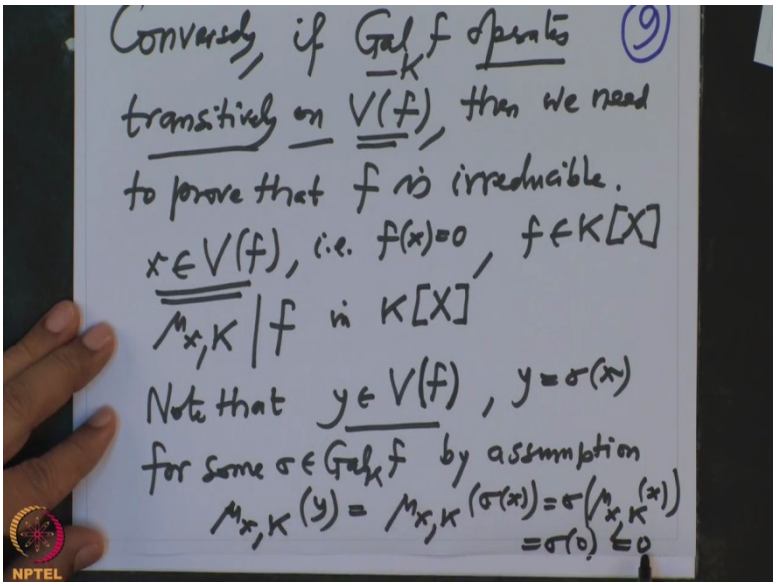
So now here we have this $K[X]$ polynomial ring and this K small y this is nothing but $\frac{K[X]}{\langle \mu_{y,K} \rangle}$ a minimal polynomial y this is a caution and then if I send capital X to y, so this is minimal polynomial of x, K there is a minimal polynomial, so this is a K algebra also isomorphism here, K isomorphism because map small x to y and this map is well-defined therefore I have this.

Whether I write round bracket or square bracket they are same we are being saying this, so I have an Automorphism K isomorphism from $K[X]$ to $K[y]$ this is K is contained here, K is contained here and now I have a splitting field earlier which was containing $\overline{K}$ and this is contained here and there is L here, this is contained here. Now first I say that this

K isomorphic this is algebraic extension therefore by Chinese theorem I can extend this to embedding from L to $\overline{K}$ but now L is a splitting field therefore L is normal therefore I can actually exchange this K isomorphism to K isomorphism σ this is K algebra isomorphism.

Isomorphism is also clear because first of all it is an embedding and 2nd is last remark shows that if I am an algebraic extension and any injective map from L to L that is actually surjective therefore it is actually K algebra isomorphism in other words this σ is actually an element the Galois group of f. And what does this σ do? This σ maps x to y that is what precisely I was looking for, so that proves that the Galois group operates transitively on the zeros of f.

(Refer Slide Time: 22:29)

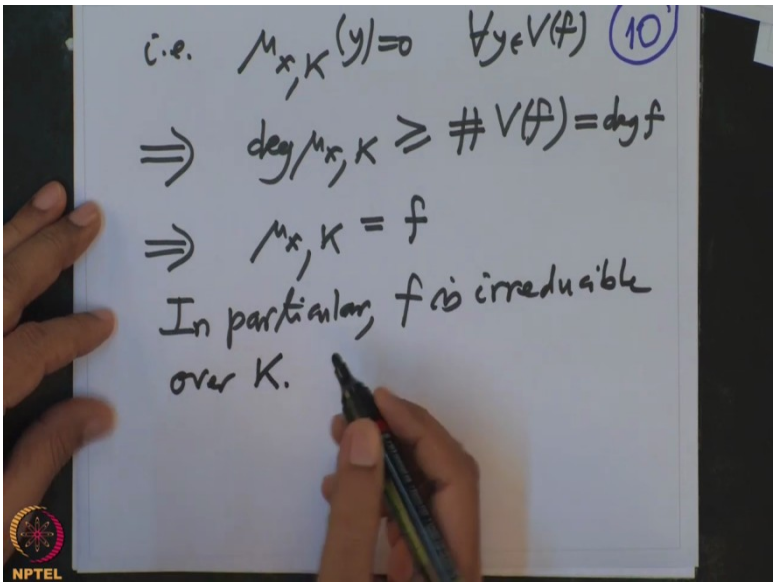


Conversely I have to prove that, so conversely if Galois group operates transitively on the zero set then we need to prove that f is irreducible, all right. So how I'm going to prove that? Alright, so we know that operates transitively, so let us take I want to prove f is irreducible. So first of all know that look at any x in $V(f)$ and look at the minimal polynomial effects.

Since $f(x)$ is 0 this means f of x is 0, so if the polynomial vanishes at f, f is in $K[X]$ and this polynomial vanishes therefore the minimal polynomial have to divide f in $K[X]$ conversely I will prove that f divides μ_x , so note that if I have any other 0 of f then I know this y because this alloys group operates on $V(f)$ transitively, so I have given this x, I fix this x I have any other y then this y has to be of the form $\sigma(x)$ for some σ the Galois group this is why assumption .

Which assumption? Mainly the Galois group operates transitively on this 0 set, so therefore I have this σ and now what is y is therefore $\mu_{x,K(y)}$, this y is same thing as $\mu_{x,K}$ of $\sigma(x)$ but this σ will come out, so this $\sigma(\mu_{x,K}(x))$ which is $\sigma(0)$ which is 0. So therefore y is also 0 of μ .

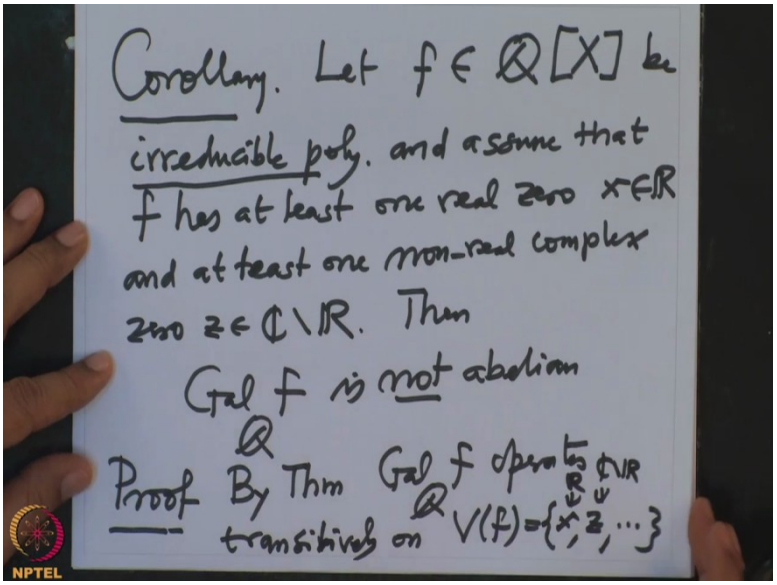
(Refer Slide Time: 25:25)



So that is $\mu_{x,K}(y)$ is also 0 and we approved it for every 0 y of f, so therefore this shows that the degree of mui and they are all distinct, so degree of μ is at least the cardinality of $V(f)$ but this is exactly equal to the degree of f because we are assuming that f has distinct zeros, so therefore that proves that $\mu_{x,K}$ is actually F because other away we have already seen before.

So that means this f is in particular f is irreducible over K, okay.

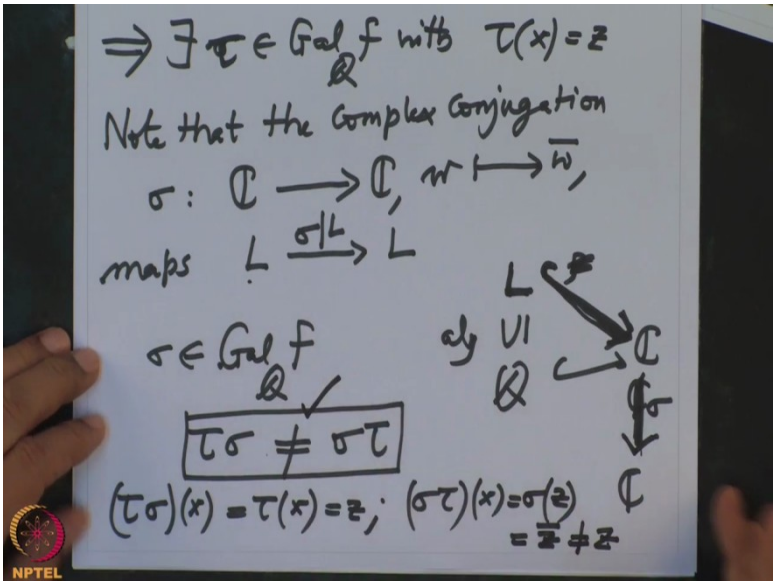
(Refer Slide Time: 26:43)



So let me deduce one, so we approved that the orbits are precisely the zeros of the prime factors, so I want to deduce one corollary from here. So corollary this, let f be a polynomial over $\mathbb{Q}$ rationals be irreducible polynomial and assume that the f has at least one real zero x and at least one nonreal complex zero z this is in $\mathbb{C}$ minus real numbers this x is in real numbers and both are zeros of f then I want to conclude that the Galois group of f over $\mathbb{Q}$ is not Abelian.

Proof I have given that it is irreducible I could have said monic doesn't matter changes divide by the unique the Galois group doesn't change, so the Galois group operates transitively, by theorem Galois group of f operates transitively on the 0 set of f, the 0 set of f contains these 2 guys x and z this is real and this is complex but not real and there may be more.

(Refer Slide Time: 28:57)



So in particular it can, so therefore there exist an element σ in the Galois group let me call it Tao, Tao in the Galois group with τ of I want to take x or y, so $\tau(x)$ equal to z this is one and also look at I want to claim note that the complex conjugation which is I denote by σ then from $\mathbb{C}$ to $\mathbb{C}$ w going to $\overline{w}$ this will map, maps the splitting field L inside L.

So the σ restricted to this splitting field will be a map from L to L this is clear because you know this $\mathbb{Q}$ is here, splitting field is here and we are assuming splitting field, so because this is algebraic extension there is an embedding from L to $\mathbb{C}$, this embedding exchange to the embedding I want to call it, still let's call it rho but this embedding because L is normal it will map L inside L.

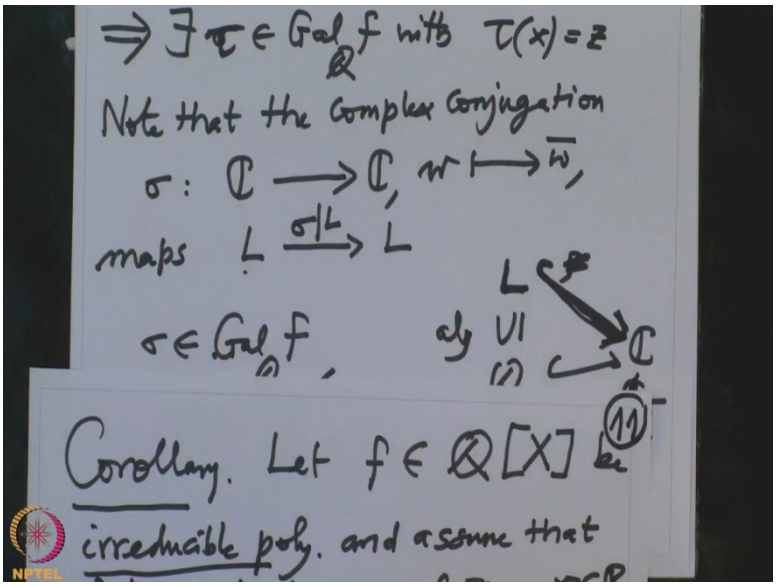
So to do it little bit more carefully you do it like this, this is an algebraic extension and there is $\mathbb{C}$ to $\mathbb{C}$, so this is a complex conjugation. So now look at this, this map, so this L is also containing $\mathbb{C}$ because we are assuming L is algebraic and $\mathbb{C}$ is algebraically closed field definitely there is an embedding here and this followed by σ that will map L inside L.

So that means this complex conjugation is an Automorphism of L, so this σ belongs to Galois group of f over $\mathbb{Q}$. So I have 2 elements in the Galois group and I want to show that they don't commute $\tau\sigma$ is not same as $\sigma\tau$ if I show this that will mean that the Galois group cannot be Abelian because I have 2 non-commuting elements.

So how do I check this? Let us check this by checking I will evaluate this on x both sides evaluate on x, so what is the left side evaluated on x? Now $\sigma(x)$, x is a complex conjugation, this σ is a complex conjugation and x is real therefore this is $\tau(x)$ but $\tau(x)$ is z this is the left-hand side and what is this it? $\sigma(\tau(x))$, so $\sigma(\tau(x))$ is, $\sigma(\tau(x))$ but $\tau(x)$ is z.

And σ is a complex conjugation, so this is $\bar{z}$ and $\bar{z}$ is not z, so this is not z because it's nonreal. So this is not equal, so therefore these are not equal therefore the group is not Abelian and therefore we have proved that the Galois group is non Abelian.

(Refer Slide Time: 32:50)



So you see here the corollary is very interesting because on one side the statement is about the polynomial and about the roots and nonreal about the description of the roots, other side is the operation of the Galois groups, the Galois group is not Abelian. So it's a property of the group which you have attached to the polynomial.

So this kind of information is very important we are extracting information about the roots from the group and conversely this is what the interplay was expected in this theory that we want to study polynomials and we want to extract information about the roots of the polynomial from the knowledge of the Galois group and conversely also.

This interplay is precisely a theory which is known as Galois Theory and today it has gone it has very far-reaching consequences in many fields including algebraic geometry,

commutative algebra, complex function theory, number theory and so on and I will continue with some examples in the next lecture, Thank you.