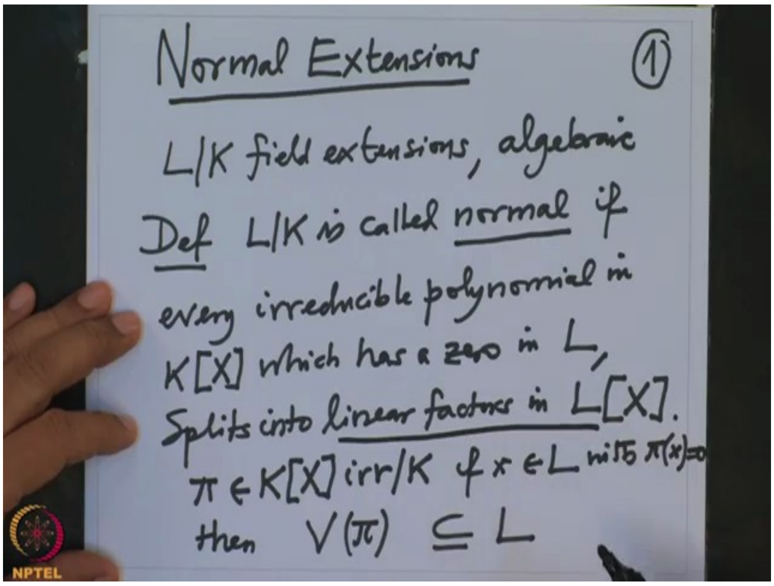
Galois' Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science, Bangalore
Lecture 50
Normal Extensions

(Refer Slide Time: 00:31)

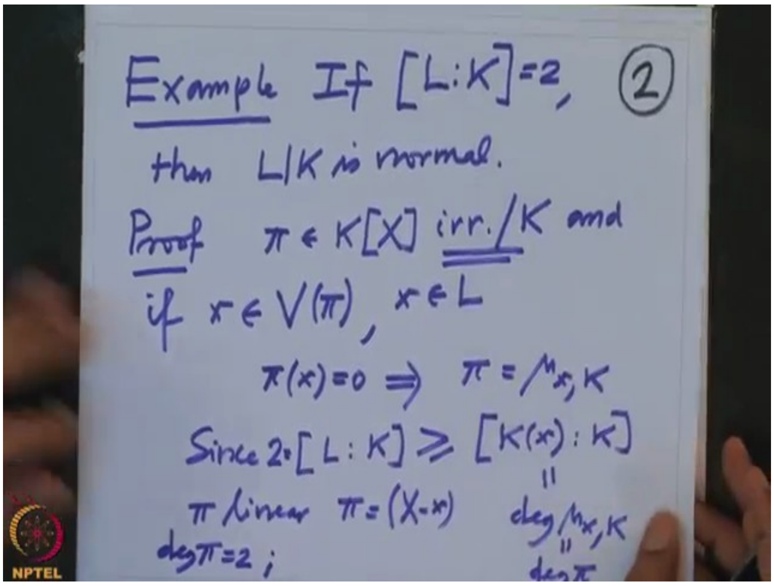


Now we come to the study of normal field extensions, so normal extensions we want to study and very name here normal we will show that this will correspond to the normal sub groups that is why, actually the normal extensions came first and normal sub groups came later, so this should be studied earlier, anyway but the group theory developed much later than the field extensions for example that was because of Galois essentially who realize that studying field extensions and studying their Galois groups together is a very useful thing and this has led to many solutions of difficult problems.

Alright so we have a field extension so L over K field extension, now I am not assuming that it is finite extension but I am assuming that it is algebraic, normal field extension and assume that it is algebraic, may not be finite, for example the algebraic closure so I have not come to the algebraic closure here but after this I will come to algebraic closure so algebraic extension may not be finite okay.

So I will say that definition, L over K is called normal if every irreducible polynomial in $K[X]$ which has a zero in L splits into linear factors in $L[X]$, so let me write this in symbols, so what do I say, if I have an irreducible polynomial $\pi \in K[X]$ irreducible and I say irreducible over K if there is small $x \in L$ with $\pi(x)$ is 0 that means π has a 0 $x \in L$, so if then all zeros of π they are contained in L, this is the set of all zeroes in the closure in the bigger field all of them should lie in L, that means this π splits actually into linear factors in $L[X]$, then the field extension is called normal.

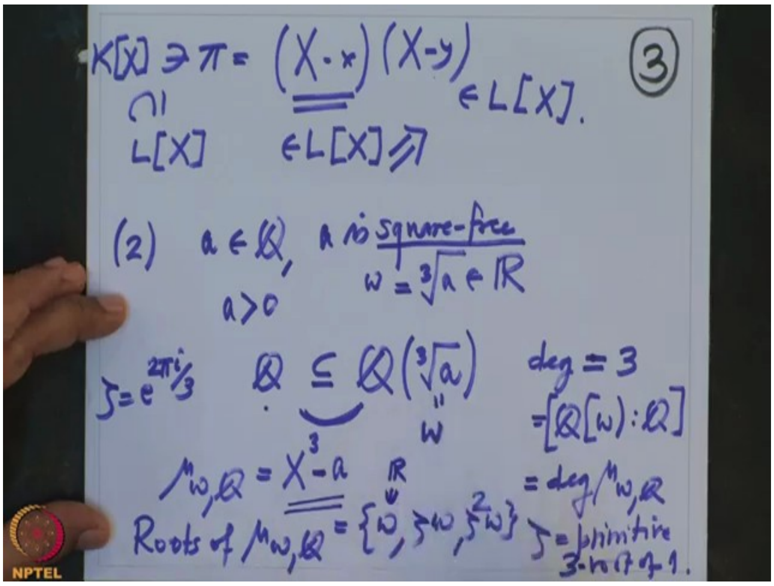
(Refer Slide Time: 04:49)



For example, so let me give you example immediately so for example if the degree L over K is 2 then it is always normal, then L over K is normal, proof, so what do we have to prove? We have to prove that every irreducible polynomial which has a zero in L that splits into linear factors in L, so let pi be irreducible and suppose irreducible over K and if x is a 0 of π and x belongs to L then because x is a 0 of π, $\pi(x)$ is 0 and π is irreducible, this π must be the minimal polynomial of x over K and therefore the degree of because this degree is true.

So since L over K is bigger equal to $K[x]$ over K, this is the degree of μ_x which is degree of π, so π has to have degree bounded by 2, so either π is linear in that case we have nothing to prove or π is quadratic, so π linear then π must be equal to capital $X - x$ which is already done although the degree of π is 2 then I know if I know one 0 then I know the other 0 by quadratic equation formula, so then I know the zeroes of π are precisely.

(Refer Slide Time: 07:06)



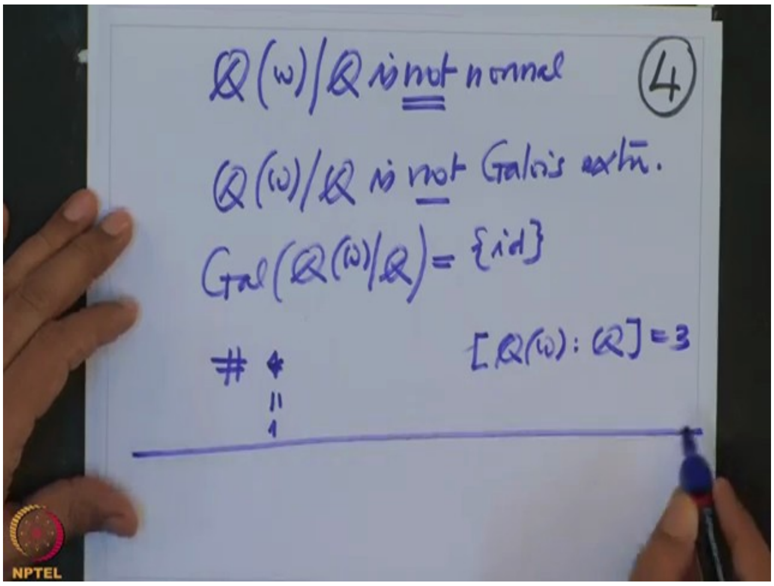
So π will be then $\pi(X-x)(X-y)$ and this factor is in L and this is in $K[X]$ which is contained in $L[X]$ therefore the other factor also has to be $L[X]$ so that implies both these thing implies this factor also in $L[X]$, so therefore π factors into linear factors in $L[X]$ so that means the degree to extensions are always normal and this statement corresponds in a group theory every sub group of index 2 is normal okay so this is one example at least.

Now I should tell you also example of a field extension which is not normal so 2, now let us take, remember we have given a field so take any positive rational number $\mathbb{Q}$, $a \in \mathbb{Q}$ which is square free, a is square free and we are considering this will a positive and we are considering $\mathbb{Q}$ cube root of a, real cube root of a, so this I denote is this is in a in real number, so this is ω , now this field extension and we are considering this field extension, this one.

Now this field extension, the degree of this field extension is 3 so this is $\mathbb{Q}(\omega)$ over $\mathbb{Q}$ this degree is 3 in fact this is simple so this is should be the degree of the minimal polynomial of omega over $\mathbb{Q}$ but the minimal polynomial of ω over $\mathbb{Q}$ is nothing but $X^3 - a$ and we need this unity stability therefore we have put this condition square free and this is three, so this field extension is degree 3 and I want to claim it is not normal, that means what?

I should give you a polynomial which is irreducible over $\mathbb{Q}$ it has a root in this but not other roots are there but well this is the irreducible polynomial in $\mathbb{Q}[X]$, it has one root here but the other roots are the complex roots, other roots are the roots of $\mu_{\omega,\mathbb{Q}}$ are precisely that ω and then $\zeta\omega$ and $\zeta^2\omega$ where ζ is a primitive cube root of one, these are the roots and this is ζ is complex in fact ζ is $e^{\frac{2\pi i}{3}}$, so this is complex non-real root therefore this is real and this is non-real, this is also non-real so it has only one root and the remaining roots are not there, therefore it is not normal.

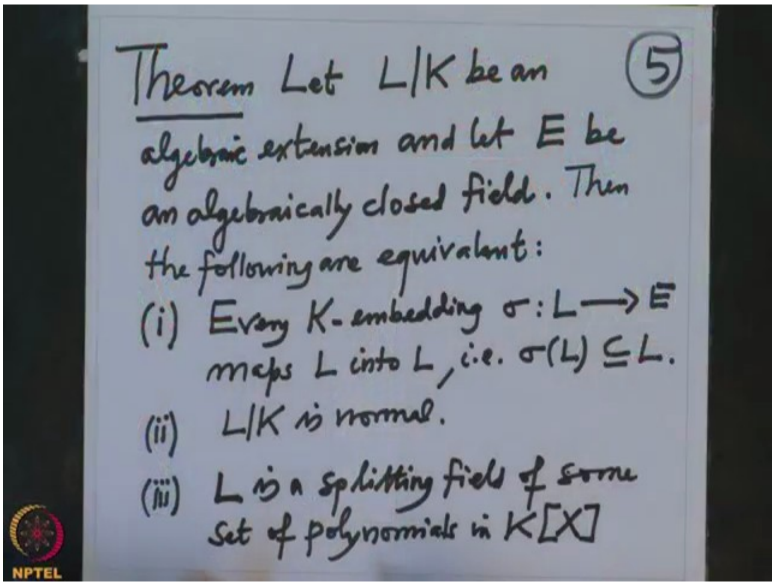
(Refer Slide Time: 11:13)



So what we checked is $\mathbb{Q}(\omega)|\mathbb{Q}$ is not normal and if you remember we have seen also this is not a Galois extension, $\mathbb{Q}(\omega)|\mathbb{Q}$ is not Galois extension, in fact in this case we know the Galois group of $\mathbb{Q}(\omega)|\mathbb{Q}$ this is trivial only identity and the degree is 3 so the cardinality of this group which is trivial group, cardinality of this group is 1 and degree of the extension is 3, so therefore it is not Galois, so this is not normal therefore.

So now we can have many more examples like that and we need to characterize this, so this definition is not suitable for deciding whether field given finite field extension is Galois or not so we are always looking for equivalent definitions so that means we are looking for theorems which say that the statements are equivalent, so that is what I am going to state now theorem, this is characterization of normal extensions.

(Refer Slide Time: 12:40)

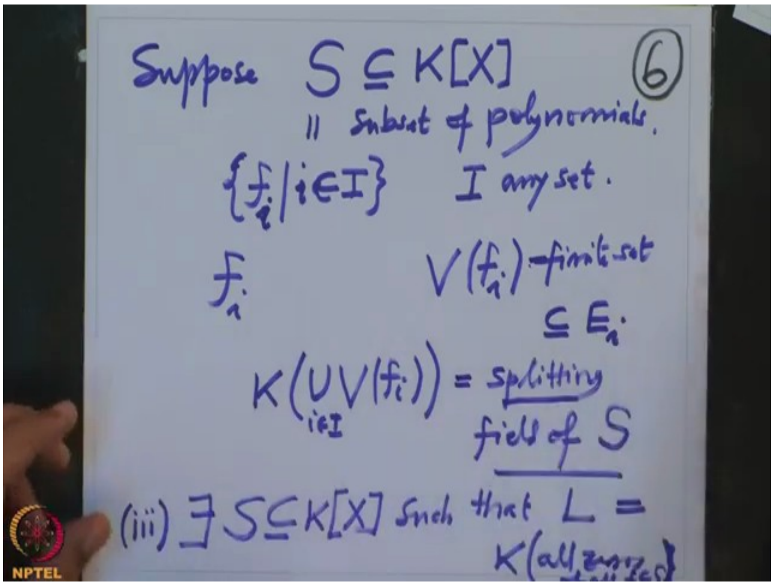


So theorem, let L over K be an algebraic extension and let E be an algebraically closed field, remember we have defined what is an algebraically closed field, algebraically closed field means only irreducible polynomials are linear or equivalently there is no proper algebraic extension of that field, these are equivalent and soon we will prove that the field of complex numbers is algebraically closed.

And also we will prove that how do we extend a given field to an algebraically closed field that will be called algebraic closer of a field, so this things soon we will prove that but right now I need only the algebraically closed field that means the only polynomials which are irreducible in that polynomial ring over that field are linear ones okay then the following are equivalent.

So 1, every K-embedding σ from L to E maps L into L so that is σ of L is contained in L. 2, L over K is normal, 3, capital L is a splitting field of some set of polynomials in $K[X]$, so the last statement here that means I have a subset of polynomials in $K[X]$ so that if I take all zeroes of, so let me recall this precisely that will help in the proof also, so what is the last statement, that means the following.

(Refer Slide Time: 16:36)

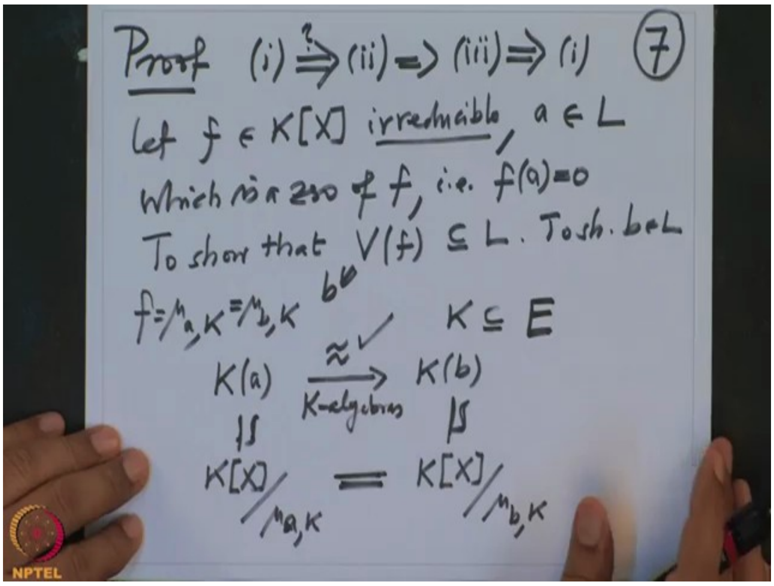


So suppose I have a subset S of the polynomial ring these are polynomials, this S maybe finite, may not be finite, this is subset of polynomials so to each polynomial so I will write this as f_s as s varies in s, this is my index in set so indexing set is, so let us call it i in I they are many polynomials, I may not be finite set, I is any set, then to each polynomial in f_i, I have the zeroes, $V(f_i)$, this is a zero set of f_i in a bigger field so this is finite set so this set is a finite set, this is a finite set.

So I take all of them and adjoin to L, adjoin to K, see this zero set may not be in K so it maybe the larger field, this is in a larger field E_i, so I take all of them and then adjoin it to K, so K adjoin all $V(f_i)$'s union $i \in I$, this is precisely what one mean by the splitting field of the set S, this is the smallest field where all the zeroes of all the polynomials lie in that field, this is what one mean by this L so the assertion 3 says there exist a subset S of the polynomials such that L equal to K adjoin all zeroes of all $f \in S$, that is called a splitting field of this one.

So that is the statement 3, this is because I am not assuming that L over k is finite if I would have assumed that L over K is finite then S finite or even one polynomial will be enough but I am not assuming that L over K is a finite extension therefore one has to consider arbitrary subset of polynomial so now let us prove that this statement are equivalent.

(Refer Slide Time: 19:55)



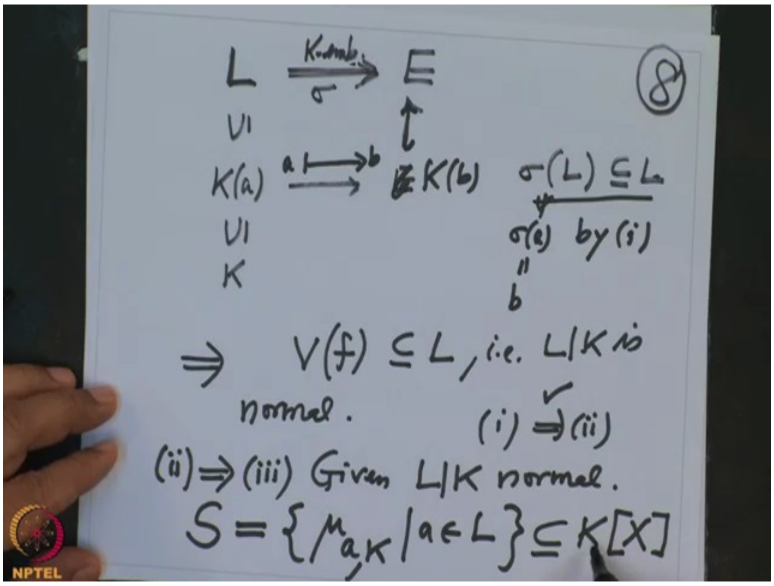
So proof we are going to prove one implies 2, implies 3, implies 1, this is what we will complete there, proof of the equivalence okay alright so what do you have to prove I have to show you the statement so we are proving one every K-embedding maps L inside L this is what given to us and this L over K is normal, we have to prove it is normal, normal means if an irreducible polynomial has one 0 in L then it splits into linear factors over L, this is what normal means alright.

So I am proving this, so let f is a polynomial in $K[X]$ irreducible and suppose a in capital L which is a zero of f so that is f of a is 0, then I want to prove that f splits into linear factors in $L[X]$ that means it is normal that is what I want to check, so alright now take, I want to say that if all the zero lie in, so to show that $V(f)$ is contained in L so these are all zeroes, so take any b, I want to show b is in, so to show b belongs to L alright.

So now look at b, so E is algebraically closed field, E is algebraically closed field and which contains K and this is b is a 0, so $f(x)$ is here so this is algebraically closed therefore remember the last one, so that is, so this b is a 0 of okay so note that if I look at the simple extension $K[a]$ and $K[b]$, they are isomorphic as K-algebras because they are roots of the same irreducible polynomial first of all because this is irreducible, this f has to be mu a K which is also equal to $\mu_{b,K}$ and this is isomorphic to $\frac{K[X]}{\mu_{a,K}}$, this is isomorphic to $\frac{K[X]}{\mu_{b,K}}$ but this mu b and mu a they are equal so these are equal.

So therefore these are isomorphic, these are actually equal, these are isomorphic, therefore these are isomorphic, so they are as K-algebra they are isomorphic therefore we have an extension so this shows that we have an extension L.

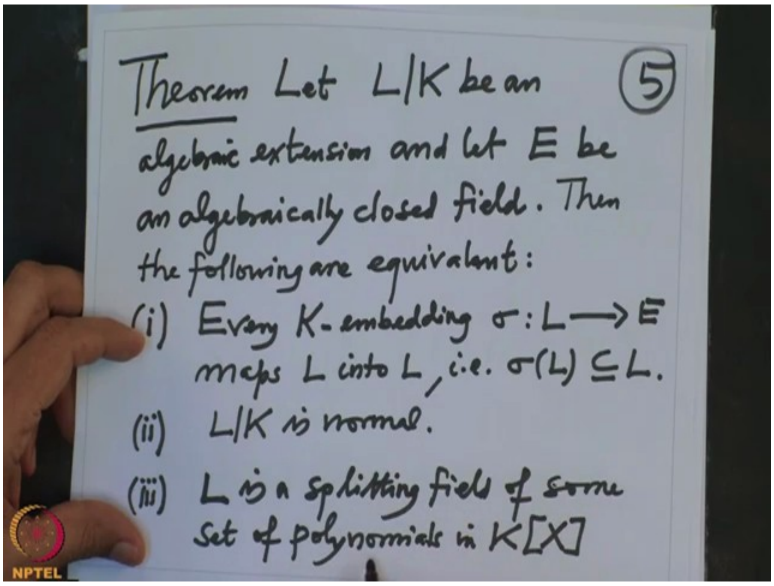
(Refer Slide Time: 24:05)



So L is here l to E, I say there is an embedding here because this I am extending to see K is here, this is contained, this is contained and I have so E is algebraically closed so E is here, so I use the last theorem to extend these two here, this is an extension of this so this is K-embedding but then this should map by one assumption is this σ, let us call this as σ, σ maps L inside L but this σ, this is an extension of this so we have an embedding, this embedding I have extended from here, this is a goes to b, this is $K[b]$ and this is contained here and therefore I have extended here.

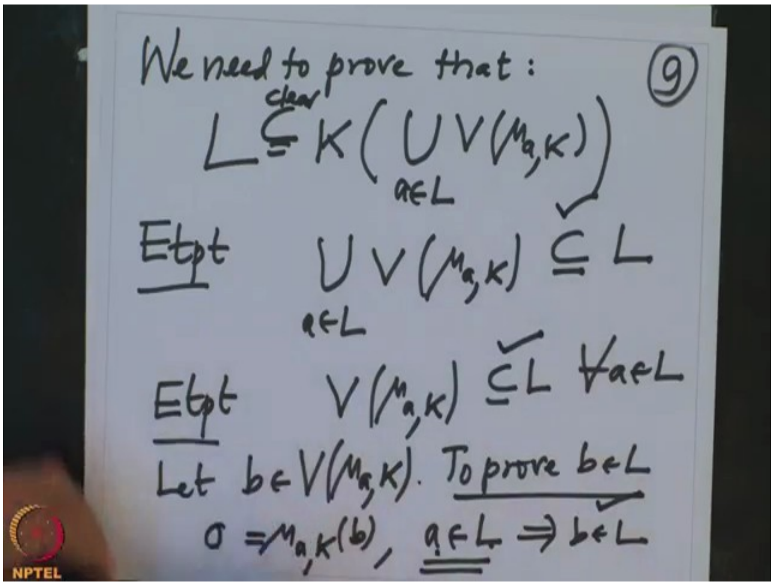
So this K-embedding should map because of the given condition 1, so this by 1, so I particular b which is $\sigma(a)$, $\sigma(a)$ belongs to a but $\sigma(a)=b$ so I have proved that every root b contained in L, therefore this proves that $V(f)$ is contained in L so that is L over K is normal, that proves 1 implies 2, so 1 implies 2 we have proved okay now 2 implies 3, we have given that, given L over K is normal and what we want to prove?

(Refer Slide Time: 26:21)



I want to prove that, I will show you this, I want to prove that L is the splitting field of some set of polynomials in $K[X]$ so I have tell which set I can take so look at the set S, this is look at all minimal polynomials of elements $a \in L$, this is a subset of $K[X]$, so take any element in L and look at minimal polynomial and collect all these polynomials and look at that set and obviously this set I want to show that this L is a splitting set that means what I should check that, so I should check that, so we need to prove the following.

(Refer Slide Time: 27:10)

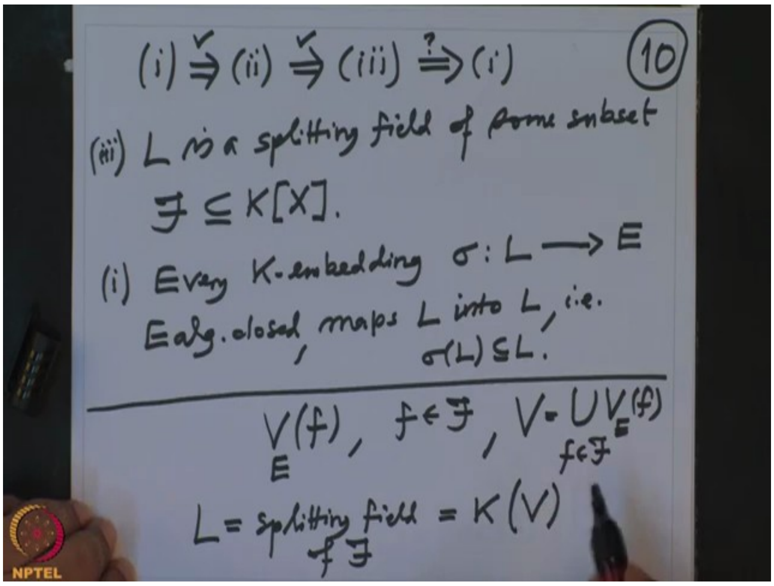


So we need to prove that L is precisely equal to K adjoin with all those unions of the zero sets of the polynomials that we are considering as a varying in L, this is what we want to prove, obviously all elements of L are here so this is clearly contained, this is clear conversely I want to prove that any element here is an element in L, so because K is contained here it is enough to prove that the union a in L, $V(\mu_{a,K})$, this is contained in there.

That means and to check that, enough to prove that each element in this union is contained there, $V(\mu_{a,K})$ is contained in L for every $a \in L$, so that means every other zero of the minimal polynomial of a over K is contained in L, so let b be a zero of minimal polynomial of a then to prove b belong to, so to prove b belong to L, but this b is a zero of minimal polynomial, this zero and one zero a which already lie in L.

So by definition, by condition of 2, 2 says normal, normal means if an irreducible polynomial has one zero in L then every other zero is also in L, so one zero a is in L therefore the other zero b is also in L, this is clear therefore we have proved that this inclusion is clear and once you have proved the inclusion is there, the union is there and once union is there, K the smallest field which contains all these guys they are also contained there therefore 2 implies 3 is proved.

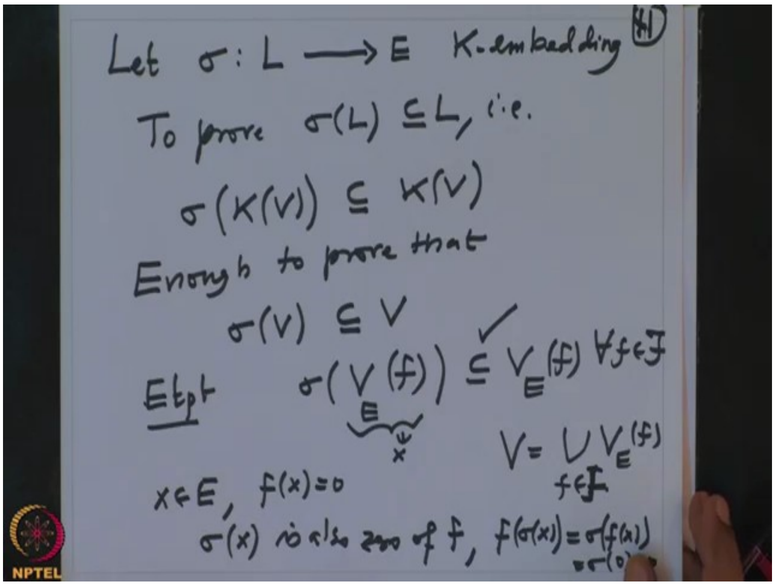
(Refer Slide Time: 29:31)



Now only one left, 3 implies 1, so 1 implies 2 implies 3, this already we have proved this implications and now we want to prove 3 implies 1, this we have to prove and what is 3? 3 is L is a splitting field, this is 3, L is a splitting field of sums of set f of polynomials with coefficients in K that is the condition 3 and condition 1 is every K embedding σ from L to an algebraically field, E algebraically closed maps L into L that is σ of L is contained in L, this is what condition 1 is.

So now we want to prove that 3 implies 1 so that means we have given that L is a splitting field of some substrate f of the polynomials with coefficients in K, so let us consider all zeroes of all polynomials in the field E, E is algebraically closed field that was given and where f is varying in the given subset f and now you take V to with their union, $V_E(f)$, f varies in F then what we have given is L is nothing but the splitting field of this set F which is nothing but K adjoin with the set V. So it is the smallest field, it is a field of E which contains all these zeroes of all the polynomials and now we want to prove that we have an embedding σ .

(Refer Slide Time: 32:16)



So let σ be an embedding from L to E, K-embedding any embedding and then we want to prove that, so to prove σ of L is containing, this is what we want to prove but to prove that it is enough to prove that σ of this means so that is $\sigma(K(V))$ is contained in KV but for this it is enough to prove that σ of V is contained in V but for this because V is a union enough to prove again it is enough to prove that σ of $V(f)$, zeroes are in E is contained in $V_E(f)$ for all $f \in F$ because V is a union of all these things is a union of this.

But this is immediate from the observation we are being using in this course quite often namely if x is a zero, if x is in E and $f(x)=0$ that means it is an element here, x is an element here, then what is σ of that? $\sigma(x)$ is also zero of f, this is immediate because f of $\sigma(x)$, σ is an embedding so and f is a polynomial so this is same thing as

$\sigma(f(x))$ but $f(x)$ is zero so σ zero which is zero therefore if x is a zero of f then $\sigma(x)$ is also zero of f that precisely means this inclusion.

So that prove this inclusion and therefore this proves $\sigma(V)$ is contained in V, therefore that proves that if I take any element of L then it is a combination with elements in V and therefore $\sigma(V)$ will contained in L. So that was what we wanted to prove, that is precisely 1, so with this it finishes the proof of this theorem. Okay with this we have finished the proof of the characterization of normal field extensions and we will continue this study further in the next lecture, thank you.