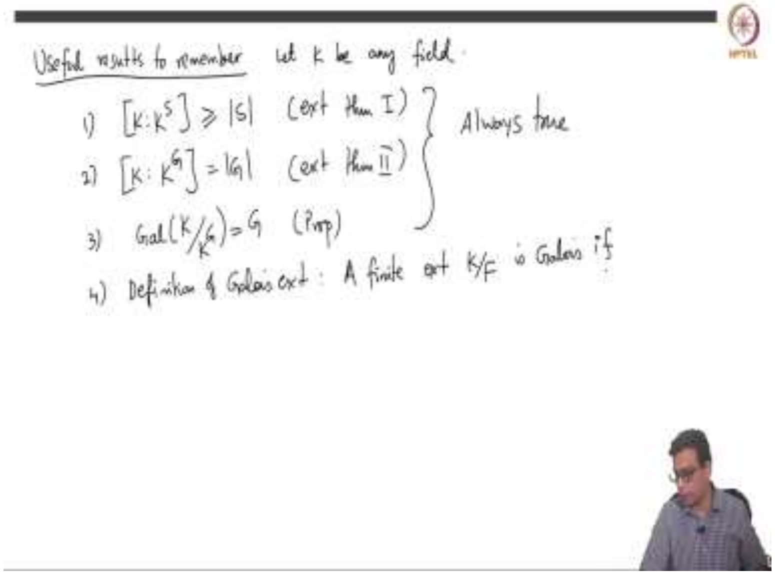
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture 15
Normal Extensions

(Refer Slide Time: 00:16)



Useful results to remember   Let K be any field.

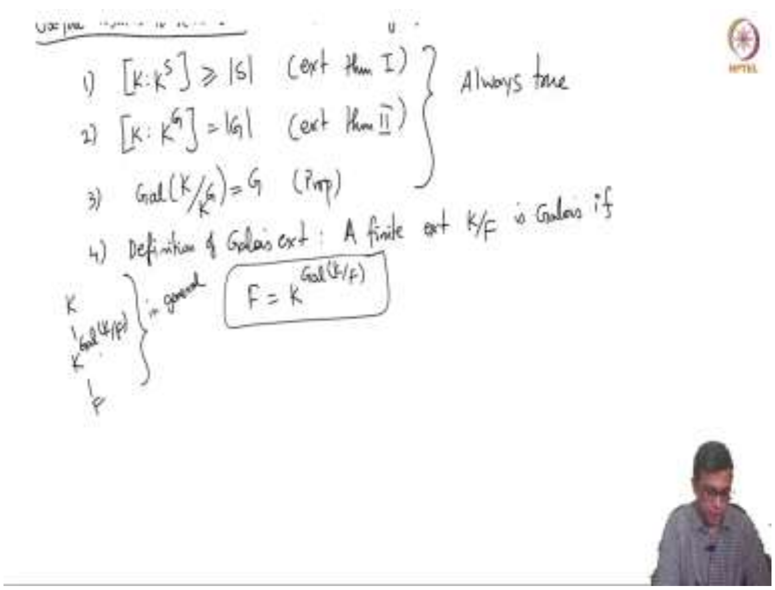
1) $[K:K^S] \geq |S|$ (ext thm I)

2) $[K:K^G] = |G|$ (ext thm II)

3) $Gal(K/K^G) = G$ (Prop)

} Always true

4) Definition of Galois ext: A finite ext K/F is Galois if



1) $[K:K^S] \geq |S|$ (ext thm I)

2) $[K:K^G] = |G|$ (ext thm II)

3) $Gal(K/K^G) = G$ (Prop)

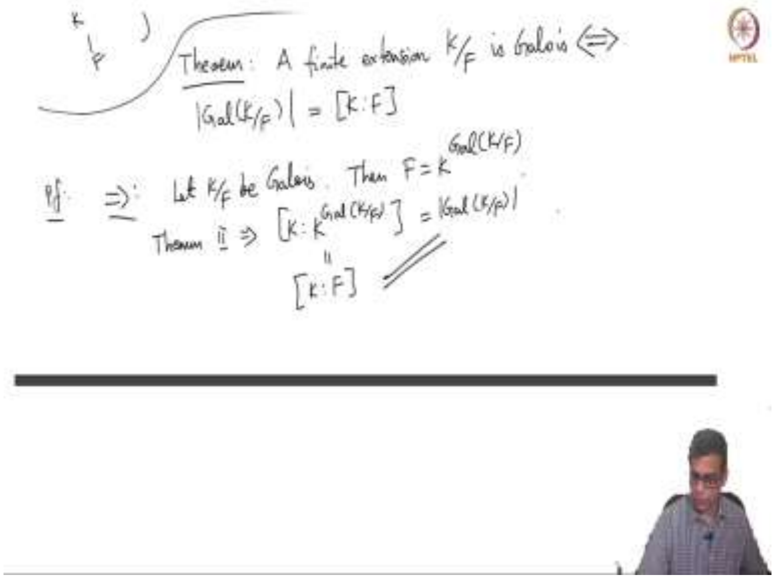
} Always true

4) Definition of Galois ext: A finite ext K/F is Galois if

$$\boxed{F = K^{Gal(K/F)}}$$

$$\begin{tikzcd} K \arrow[d, dash] \\ K^{Gal(K/F)} \arrow[d, dash] \\ F \end{tikzcd}$$

} in general



K | F

Theorem: A finite extension K/F is Galois $\iff$ $|Gal(K/F)| = [K:F]$

Pf. $\Rightarrow$: Let K/F be Galois. Then $F = K^{Gal(K/F)}$

Theorem II $\Rightarrow$ $[K : K^{Gal(K/F)}] = |Gal(K/F)|$

$\quad\quad\quad\quad\quad\quad \| $

$\quad\quad\quad\quad\quad [K:F]$

Welcome back, in the last few videos, we discussed some important theorems about fixed fields and defined Galois extensions and I also gave you a few examples. So, let me start today's video by recalling some of the facts that theorems and definitions I gave. And these are useful, useful forms of useful results, let me call it results to remember So, these are not written in words, but written in, just you know the notation of fixed fields that we learned.

So, there are three facts that we learned corresponding to two theorems and a proposition. So, let K be any field. And the first fact, so I am not going to write the full details and I only want to highlight as compactly as possible. So, this is extension theorem one. If you take any collection of homomorphisms from K to some field, the index or the degree of K or the fixed field is at least cardinality of S.

On the other hand, if you take a group of automorphisms you got a precise inequality, this is the extension theorem two. Remember as I said I am not writing the full hypothesis here; G is a group of automorphisms of K in this example. And using these we proved also a proposition which says that the Galois group of, you take a field K, you take a group of automorphisms G and the Galois group of a, finite group of automorphisms Galois group over of K over KG is exactly G these are always true.

So, this I called a proposition that I proved last time, so these are always true. So, there is no other assumption on this. And the fourth is the definition of Galois extension. And I want to rewrite this as follows, a finite extension, whenever I write a finite extent, I mean a finite explanation of fields always in this course, is Galois if the way to remember this is f is the fixed field of the Galois group of the extension.

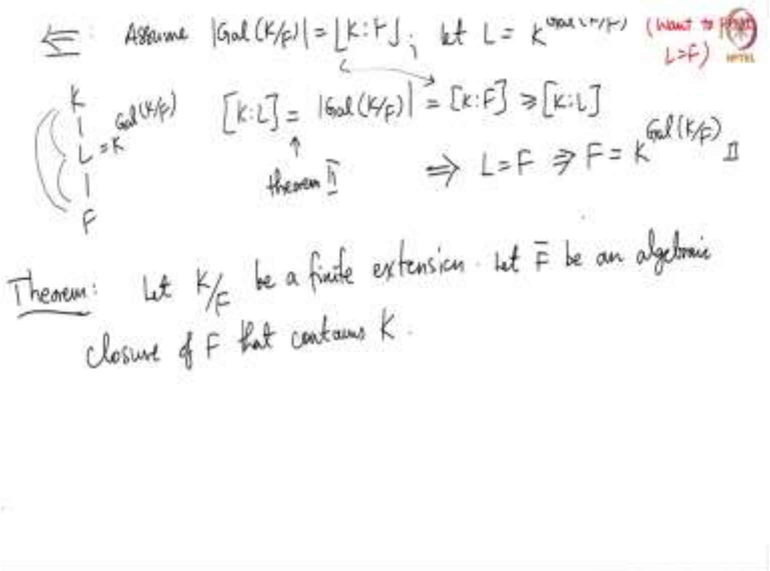
So, this is a useful, this is the condition which makes this Galois. So, in general we have the fixed field sandwiched between K and F. The extension is Galois if the bottom part is exactly equal. So, these are the useful things to remember from the last two three classes. So today, I am going to give you a few other ways to check if something is a Galois extension. And also, I am going to introduce an important class of extensions called normal extensions, which are like Galois, but not quite, they are just slightly weaker than Galois extensions.

So, let me start with this theorem, which is a simple theorem given what we have already proved. So the statement is as follows, a finite extension, K over F is Galois if and only if the cardinality or the order of the Galois group is equal to the degree of the field extension. So, if you look back at the examples that we did, in all Galois extensions, this happened to be the case and in non Galois extensions, that is, that fails. And anyway, we will also see this again later when we do some problems.

So, it is a very simple proof as I told you. So in this direction, suppose so let K over F be Galois. So, I am going to assume that this is a Galois extension. Then, what we have is, it is right in front of you, by definition, F is the fixed field of the Galois group of K over F. So, by theorem two of extension fields of fixed fields, which I have written here, K colon K G is, so in particular K colon Galois K colon K power Galois.

So, this is equal to K colon F by the Gal 1S because F is the fixed field so this is equal. By theorem two, this implies this is equal to the cardinality of the group in question. So, this is theorem two. So whatever group comes here is the group that comes here, so that is all right, so these are equal, so that is done.

(Refer Slide Time: 05:21)



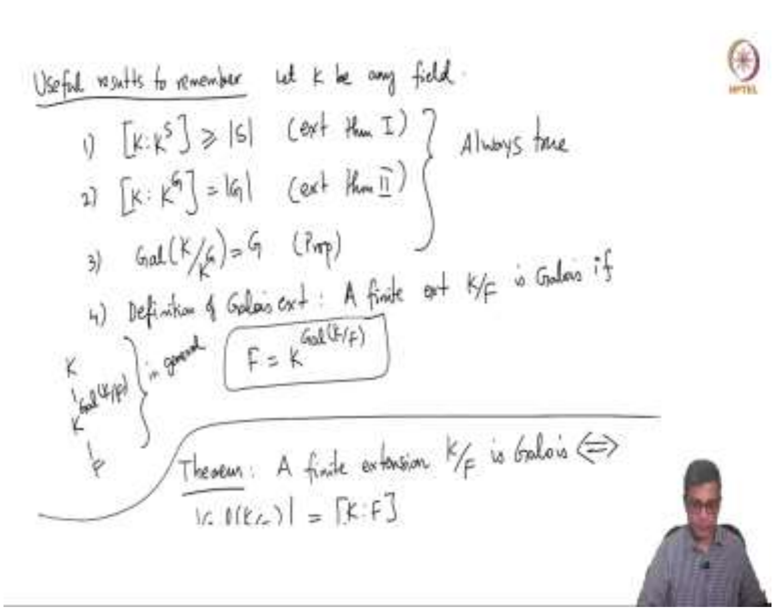
$\Leftarrow$: Assume $|\mathrm{Gal}(K/F)| = [K:F]$; let $L = K^{\mathrm{Gal}(K/F)}$ (Want to prove $L=F$)

$$\begin{tikzcd}[row sep=small] K \arrow[d, dash] \\ L = K^{\mathrm{Gal}(K/F)} \arrow[d, dash] \\ F \end{tikzcd}$$

$$\underset{\substack{\uparrow \\ \text{theorem II}}}{[K:L] =} |\mathrm{Gal}(K/F)| = [K:F] \geq [K:L]$$

$$\Rightarrow L = F \Rightarrow F = K^{\mathrm{Gal}(K/F)} \quad \text{II}$$

<u>Theorem</u>: Let K/F be a finite extension. Let $\bar{F}$ be an algebraic closure of F that contains K.



<u>Useful results to remember</u> Let K be any field.

1) $[K:K^S] \geq |S|$ (ext thm I)
2) $[K:K^G] = |G|$ (ext thm II)
3) $\mathrm{Gal}(K/K^G) = G$ (Prop)

} Always true

4) Definition of Galois ext: A finite ext K/F is Galois if $\boxed{F = K^{\mathrm{Gal}(K/F)}}$

$$\begin{tikzcd}[row sep=small] K \arrow[d, dash] \\ K^{\mathrm{Gal}(K/F)} \arrow[d, dash] \\ F \end{tikzcd}$$

in general

<u>Theorem</u>: A finite extension K/F is Galois $\Leftrightarrow$ $|\mathrm{Gal}(K/F)| = [K:F]$

$$\begin{tikzcd} K^{sep} \arrow[d, dash] \\ F \end{tikzcd}$$

Theorem: A finite extension K/F is Galois $\iff$ $|\mathrm{Gal}(K/F)| = [K:F]$

Pf: $\Rightarrow$: Let K/F be Galois. Then $F = K^{\mathrm{Gal}(K/F)}$.

Theorem II $\Rightarrow$ $[K:K^{\mathrm{Gal}(K/F)}] = |\mathrm{Gal}(K/F)|$ ✓

$$\overset{\shortparallel}{[K:F]} \;//$$

$\Leftarrow$: Assume $|\mathrm{Gal}(K/F)| = [K:F]$; let $L = K^{\mathrm{Gal}(K/F)}$ (want to prove $L=F$)

K [illegible] $[\;:\;]$ [illegible] $|\mathrm{Gal}(K/F)| = [K:F] \geq [K:L]$

$$\begin{tikzcd} K \arrow[d, dash] \\ L = K^{\mathrm{Gal}(K/F)} \arrow[d, dash] \\ F \end{tikzcd}$$

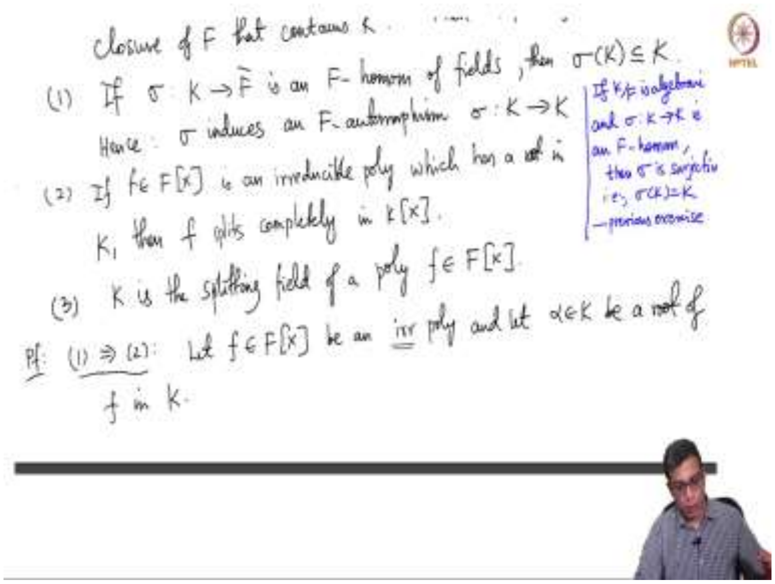
$[K:L] \underset{\substack{\uparrow \\ \text{theorem II}}}{=} |\mathrm{Gal}(K/F)| = [K:F] \geq [K:L]$

$\Rightarrow L = F \Rightarrow F = K^{\mathrm{Gal}(K/F)}$ $\square$

Theorem: Let K/F be a finite extension. Let $\bar{F}$ be an algebraic closure of F that contains K. Then the following are equivalent.

(1) If $\sigma: K \to \bar{F}$ is an F-homom of fields, then $\sigma(K) \subseteq K$.

Hence: σ induces an F-automorphism $\sigma: K \to K$



closure of F that contains K.

(1) If $\sigma: K \to \bar{F}$ is an F-homom of fields, then $\sigma(K) \subseteq K$.

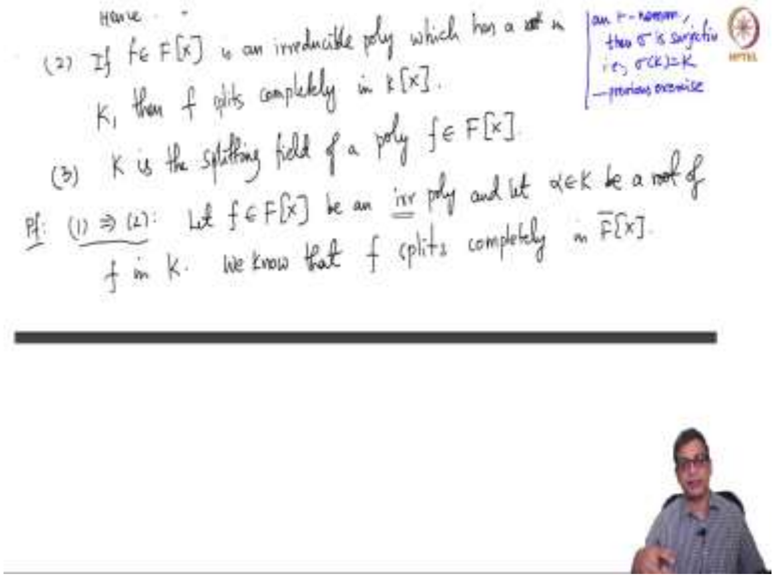
Hence: σ induces an F-automorphism $\sigma: K \to K$

(2) If $f \in F[x]$ is an irreducible poly which has a root in K, then f splits completely in $K[x]$.

(3) K is the splitting field of a poly $f \in F[x]$.

Pf: $\underline{(1) \Rightarrow (2)}$: Let $f \in F[x]$ be an $\underline{\underline{\text{irr}}}$ poly and let $\alpha \in K$ be a root of f in K.

If K/F is algebraic and $\sigma: K \to K$ is an F-homom, then σ is surjective i.e., $\sigma(K) = K$ — previous exercise



Hence

(2) If $f \in F[x]$ is an irreducible poly which has a root in K, then f splits completely in $K[x]$.

(3) K is the splitting field of a poly $f \in F[x]$.

Pf: $\underline{(1) \Rightarrow (2)}$: Let $f \in F[x]$ be an $\underline{\underline{\text{irr}}}$ poly and let $\alpha \in K$ be a root of f in K. We know that f splits completely in $\bar{F}[x]$.

an F-homom, then σ is surjective i.e., $\sigma(K) = K$ — previous exercise

For the other direction. So, if you have a Galois extension, then the order of the Galois group is equal to the degree of the field extension. On the other hand, assume the, that the order of the Galois group is equal to the degree of the field extension. And let us, let L be the fixed field of the Galois extension, Galois group. Our goal is to prove that, L equals F want to prove but a priori it is a subfield of, it is an intermediate field. So, a field that sandwiched between kind of is called an intermediate field of this extension. So, K L is a fixed field of the Galois group.

And now let us just check some things. So, we know K colon L is equal to Galois, the order of the Galois group. This is precisely the statement that you have in theorem two. So, theorem two says that, degree or a fixed field is the cardinality of the group, but this is equal to K colon F by the hypothesis, so this is the hypothesis. But this is at least as much as K colon L, because L is an intermediate field. So, this times this is equal to this whole thing. So, K colon F is at least as much as K colon L. So, we have K colon F on the left hand side, K colon L on the right hand side.

So, this implies that K equals, this L equals F, that is only possibility. Because K colon F is K colon L dot L colon F, but K colon F is equal to K colon L. So, L colon F is one. So, L is equal to F, that means F is the fixed field because L is a fixed field, but F is equal to L, so L is a fixed field. There is a nice test to check Galois whether to take an extension is Galois, because this is a numerical test. In the definition, you have to look at the fixed field. And there could be some more work that you need to do there.

But this is just a numerical check for Galois extensions. All you need to do, know is the Galois group. Otherwise, you cannot check this. So if you know the Galois group and the degree of the extension, you know immediately whether the extensions Galois or not, we are going to make use of this later. So, let me now prove another theorem, which is not really about Galois extensions, but it is about field extensions.

And we will connect to these two Galois extensions later. So let K be K over F be a finite extension, always everything that we are dealing with is a field, K and F are fields and K over F is a finite extension of fields. So, I am going to fix an algebraic closure have of F that contains K. So, in fact, I can just take an algebraic closure of K. So we, from what we recalled about algebraic closures, you know that if you have an algebraic extension K over F, algebraic closure of K and F are isomorphic.

So, I can just took, take any algebraic closure that contains K. So, then the following are equivalent. So, this is a fairly simple three step proof, nevertheless, it is an extremely important result in our course, as we, as we proceed further, you will say, you will see that this, this is going to be very critical to us. If sigma from so the first statement is, I am going to write three statements. The theorem asserts that they are all equivalent. So, each implies the other. So, if sigma from K to F bar is an F homomorphism of fields.

Remember, K contains F, F bar contains F. So, if K to F bar is an F homomorphism if it is a field homomorphism that fixes every element in F. So, suppose it is an F homomorphism of fields, then sigma K is contained in K. So, that is the first assertion. So, hence, this in particular means that sigma from K to sigma induces an F automorphism from K to K. Remember, that you have always an injective map from K to F bar. It is in fact inclusion.

And you then have by this condition image of K is contained in K, that means sigma is a function from K to K. It is always injective of course, but it is also surjective by an exercise we did in the past . So, if K over F is algebraic and sigma from K to K is an F homomorphism then sigma is surjective, that is sigma K equals K. So, this is an exercise that we did earlier.

In one of the problems sessions, I proved this because the roots of K are finite, roots of a polynomial are finite, so those roots have to go to themselves. So, you restrict to a, inject your map on a finite set to itself and that has to be surjective. So, every element of K is in the image. So, once you have sigma K is contained in K it induces in F automorphism, this is not quite required for the statement and the proof, but it is an important observation. So, I wanted to record it in the statement of the theorem itself.

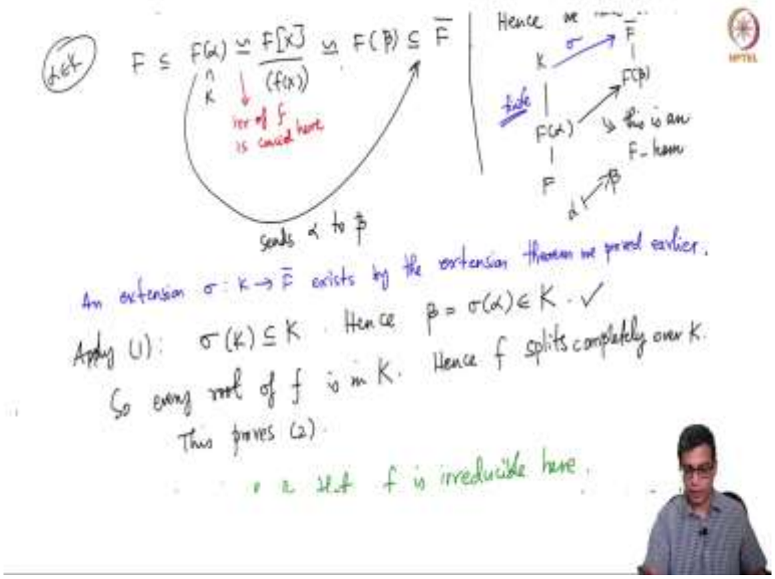
Second statement is if, F is an irreducible polynomial or the base field, is an irreducible polynomial which has a root in K then it has all the roots in K. So, then F splits completely, remember our notation or meaning of the word phrase splits completely that means that it splits as a product of linear polynomials in K X. That means, all the roots of F in some large algebraic closure or F bar in this case actually lie in K that is the content of the third, second statement.

And the final statement is, K is a splitting field or the splitting field of a polynomial F in FX. So, the extension K over F, in fact is the splitting field of something. So, this is something we are familiar with, this third statement actually is equal to one and two also. So, the proof is not difficult at all, it is straightforward with all the theory that we have already developed. So, let us just go through each implication. 1 implies 2, what is the statement, so this is in fact the crucial implication, the others are more easy.

So, this is also is easy, but it requires more work than others. So, let us prof 1 implies 2. So, let f in F X be an irreducible polynomial and let alpha in K be a root of f in K. Note that by hypothesis in 2, F is an irreducible polynomial which is important, it has a root in K. So that, then it splits completely, it can happen that, I am not saying that every polynomial splits completely that of course, will not happen only if it has at least one root it will split completely. So, let us take that one root that we are guaranteed.

We know that, f splits completely in F bar X of course, because f bar is algebraically closed. So, every polynomial splits completely.

(Refer Slide Time: 13:58)



$\alpha \in K$

$F \le \underset{\underset{K}{\cap}}{F(\alpha)} \cong \frac{F[x]}{(f(x))} \cong F(\beta) \le \overline{F}$

irr of f is crucial here

sends α to β

Hence we [illegible]

$$\begin{tikzcd} K \arrow[r, "\sigma"] \arrow[d, dash] & \overline{F} \arrow[d, dash] \\ F(\alpha) \arrow[r] \arrow[d, dash] & F(\beta) \\ F & \end{tikzcd}$$

lift

this is an F-hom

$\alpha \mapsto \beta$

An extension $\sigma : K \to \overline{F}$ exists by the extension theorem we proved earlier.

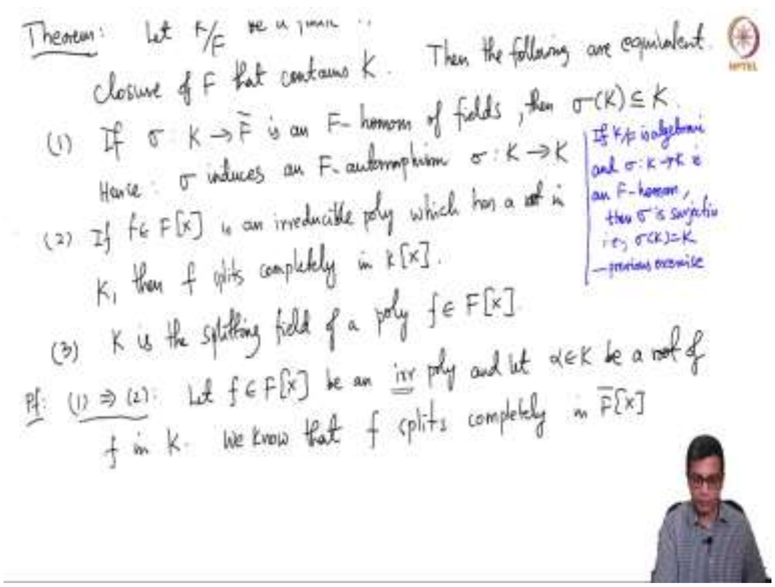
Apply (1): $\sigma(K) \subseteq K$. Hence $\beta = \sigma(\alpha) \in K$. ✓

Hence f splits completely over K.

So every root of f is in K.

This proves (2).

[illegible] f is irreducible here.



Theorem: Let K/F be a finite [illegible] closure of F that contains K. Then the following are equivalent.

(1) If $\sigma : K \to \overline{F}$ is an F-homom of fields, then $\sigma(K) \subseteq K$.

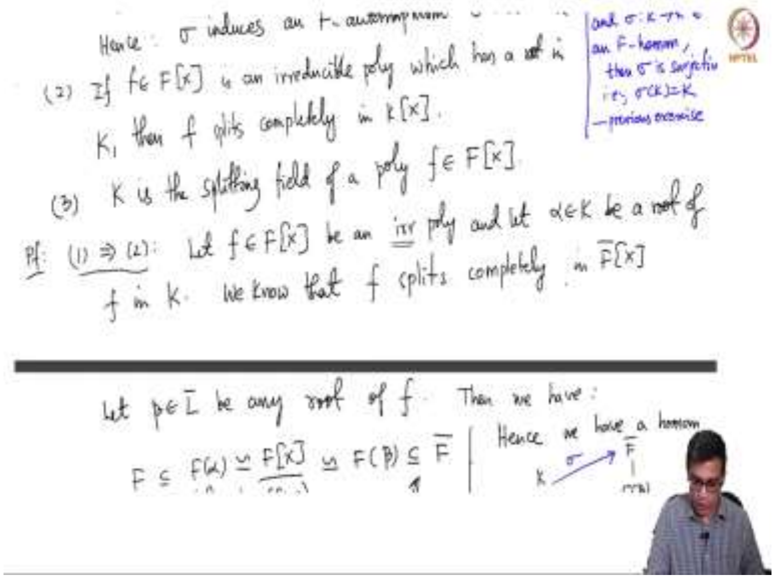
Hence: σ induces an F-automorphism $\sigma : K \to K$

If K/F is algebraic and $\sigma : K \to K$ is an F-homom, then σ is surjective i.e., $\sigma(K) = K$ — previous exercise

(2) If $f \in F[x]$ is an irreducible poly which has a root in K, then f splits completely in $K[x]$.

(3) K is the splitting field of a poly $f \in F[x]$

Pf: (1) ⇒ (2): Let $f \in F[x]$ be an irr poly and let $\alpha \in K$ be a root of f in K. We know that f splits completely in $\overline{F}[x]$



Hence: σ induces an F-automorphism ...

(2) If $f \in F[x]$ is an irreducible poly which has a root in K, then f splits completely in $K[x]$.

(3) K is the splitting field of a poly $f \in F[x]$.

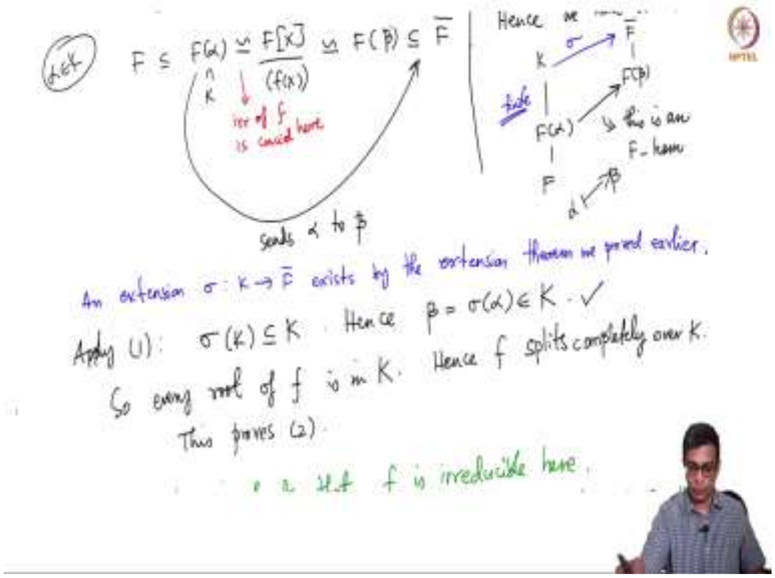
and $\sigma : K \to K$ is an F-homom, then σ is surjective i.e, $\sigma(K) = K$ — previous exercise

Pf: $(1) \Rightarrow (2)$: Let $f \in F[x]$ be an irr poly and let $\alpha \in K$ be a root of f in K. We know that f splits completely in $\overline{F}[x]$.

Let $\beta \in \overline{L}$ be any root of f. Then we have:

$F \subseteq F(\alpha) \simeq \frac{F[x]}{(f(x))} \simeq F(\beta) \subseteq \overline{F}$

Hence we have a homom $K \xrightarrow{\sigma} \overline{F}$



$\alpha \in K$

$$\begin{tikzcd}
F \arrow[r, phantom, "\subseteq"] & F(\alpha) \arrow[r, phantom, "\simeq"] \arrow[d, phantom, "\cap"] \arrow[rrr, bend right, "\text{sends } \alpha \text{ to } \beta"'] & \frac{F[x]}{(f(x))} \arrow[r, phantom, "\simeq"] & F(\beta) \arrow[r, phantom, "\subseteq"] & \overline{F} \\
& K & & &
\end{tikzcd}$$

irr of f is crucial here

Hence we have

$$\begin{tikzcd}
K \arrow[r, "\sigma"] \arrow[d, dash] & \overline{F} \arrow[d, dash] \\
F(\alpha) \arrow[r] \arrow[d, dash] & F(\beta) \\
F &
\end{tikzcd}$$

todo

this is an F-hom

$\alpha \mapsto \beta$

An extension $\sigma : K \to \overline{F}$ exists by the extension theorem we proved earlier.

Apply (1): $\sigma(K) \subseteq K$. Hence $\beta = \sigma(\alpha) \in K$. ✓

So every root of f is in K. Hence f splits completely over K.

This proves (2).

[illegible] f is irreducible here.

So, let be beta any root. So, let bet be any root of F in L bar then we have a sequence of isomorphisms this way. So, we first have F contained in F alpha which is of course in K but F alpha is isomorphic to F X mod small f x. See this is the point where we use irreducibility of f is crucial here because only then this is a field. So, this is isomorphic to that, but this is also same as f beta because beta also has the same irreducible polynomial, but this is in F bar.

So, the upshot is, we get f, so I will try to write here. So hence, we have homomorphism, so I am going to write it like this. So this is of course, an F homomorphism because that is, at every stage in this sequence F is fixed point wise, every element of F goes to itself under all these maps. So this is the picture that we have. And of course, the point is this function, which is what I am denoting here, in fact, this function sends alpha to beta.

So, because X, I can arrange it in such a way that alpha goes to X bar, X bar here goes to beta, so alpha goes to beta. So, under this map alpha goes to beta. Now, by the case here, by extension theorem that we proved, there is an extension in this, let us call that sigma. So, sigma exists an extension like an extension exist by the extension theorems we proved. If you go back and look at those extension theorems, this is exactly the picture that we had.

Any map like this can be extended because this is a finite extension, so algebraic extension was what we use. So, this is certainly possible because it is a finite extension. Now, apply one, the condition one, sigma is a function from K to F bar, it is an F homomorphism. So, sigma K is equal to k. Hence, beta which is sigma alpha is in K. So, remember alpha is in K, so alpha is in K. Its image is beta, but sigma K is contained in K, so sigma of anything in K is in K. So beta is in k.

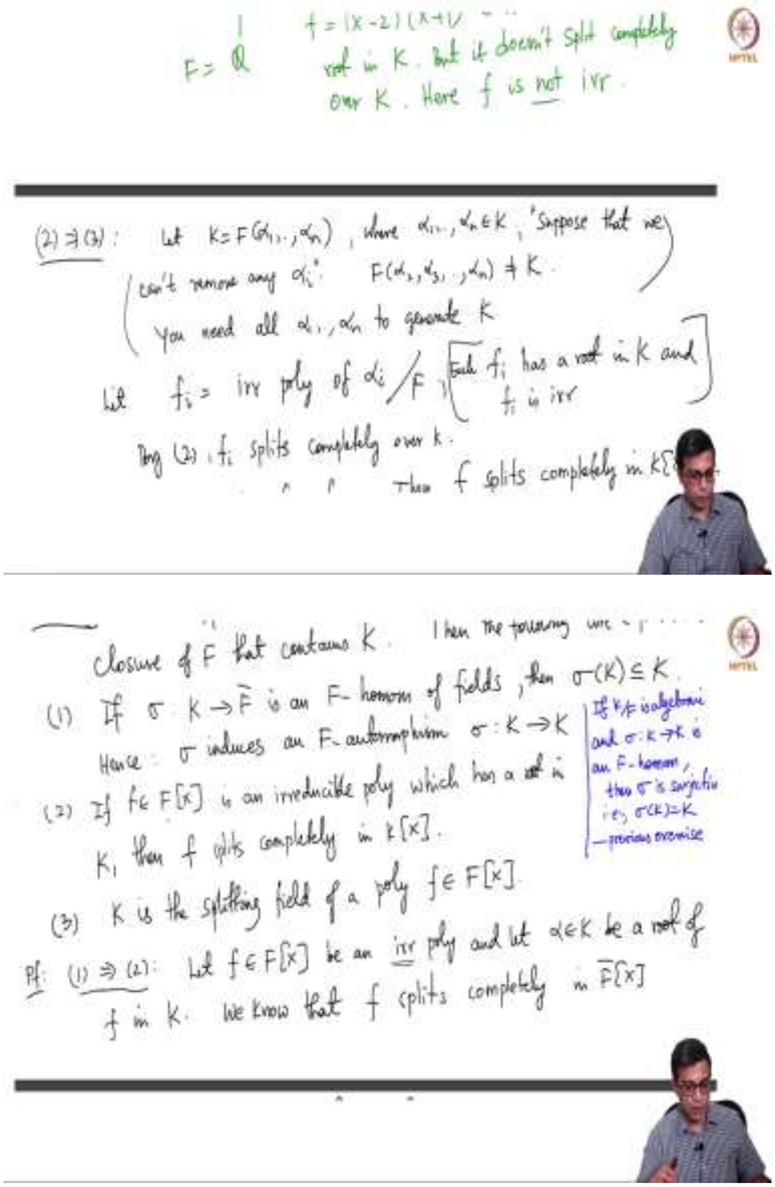
So, every root of f is in K. Hence, f splits completely over K or in Kx. So, this proves two. So, if you have this property that any homomorphisms from, homomorphism from K to F bar has a property that its image is in K, then if you have a polynomial below, irreducible polynomial below, which has a root in capital K, then it must have all the roots in capital K, meaning it splits completely in capital K. So, let me just give you a note here, it is important that f is irreducible here.

So, as you can see in this example, let us take Q adjoint root over Q. So, it is an easy exercise to show that it has these, this has the three, we have not proved equivalence, but we will prove it the three equivalence condition, equivalent conditions of the theorem, the best way to see that is it is a splitting field, it has the third condition, it is a splitting field of x square minus 2, but it does not I mean, it also has the hence the other true properties as we will show at the end of this proof. So, take f to be let us say x square minus 2 times x square plus 1.

So I can take this x square, this has a root in K, k is this, F is this because it has a root but it does not split completely over K. Because of course x square plus 1 does not have roots in K, because roots of x plus 1 are non real, but K is a real field. So that is obviously not going to split completely. So here, f is not irreducible. So there could be factors which contribute roots, but there you cannot say anything about other factors.

So, you can go back and see the proof will fail because if you go modulo F, you would not get a field or at least, you know, you cannot say that it is isomorphic to the field generated by the other roots of this. So it is important, so I have taken a digression to prove that F being irreducible is an important condition here.

(Refer Slide Time: 20:35)



$F = \mathbb{Q}$ $\quad f = (x-2)(x+1) \cdots$ root in K. But it doesn't split completely over K. Here f is not irr.

(2) ⇒ (3): Let $K = F(\alpha_1, .., \alpha_n)$, where $\alpha_1, .., \alpha_n \in K$, Suppose that we can't remove any α_i: $F(\alpha_2, \alpha_3, .., \alpha_n) \neq K$. You need all $\alpha_1, .., \alpha_n$ to generate K

Let f_i = irr poly of α_i / F, [Each f_i has a root in K and f_i is irr]

By (2), f_i splits completely over k.

Then f splits completely in K[

closure of F that contains K. Then the following are

(1) If $\sigma : K \to \bar{F}$ is an F-homom of fields, then $\sigma(K) \subseteq K$.

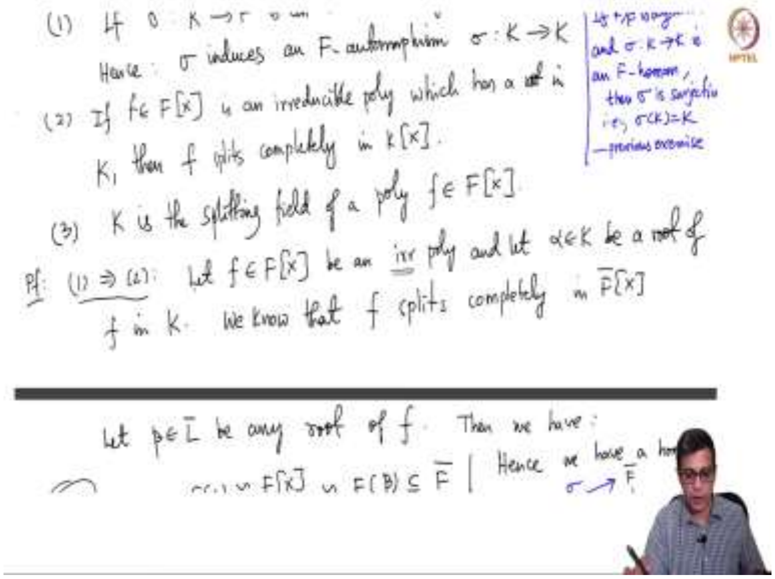
Hence: σ induces an F-automorphism $\sigma : K \to K$

(2) If $f \in F[x]$ is an irreducible poly which has a root in K, then f splits completely in K[x].

(3) K is the splitting field of a poly $f \in F[x]$.

If K/F is algebraic and $\sigma : K \to K$ is an F-homom, then σ is surjective i.e, $\sigma(K) = K$ — previous exercise

Pf: (1) ⇒ (2): Let $f \in F[x]$ be an irr poly and let $\alpha \in K$ be a root of f in K. We know that f splits completely in $\bar{F}[x]$



(1) If $\sigma : K \to \bar{F}$ is an ...

Hence: σ induces an F-automorphism $\sigma : K \to K$

(2) If $f \in F[x]$ is an irreducible poly which has a root in K, then f splits completely in $K[x]$.

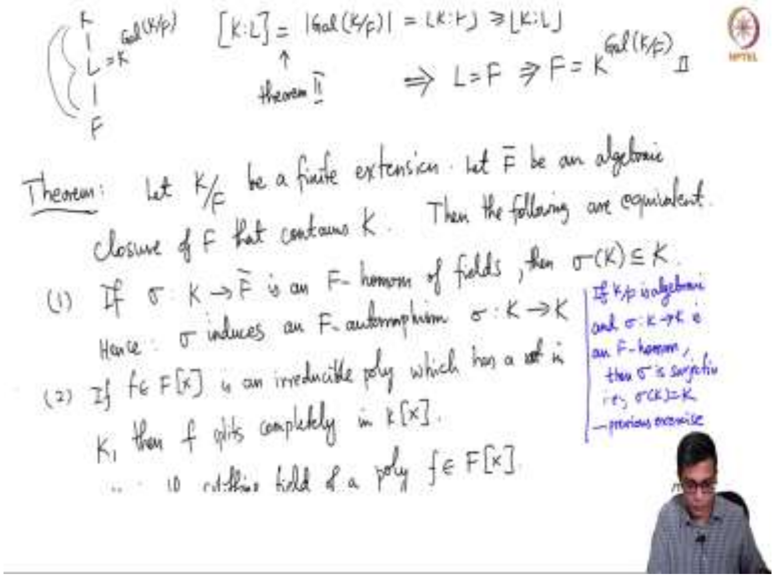
(3) K is the splitting field of a poly $f \in F[x]$.

Pf: (1) ⇒ (2): Let $f \in F[x]$ be an irr poly and let $\alpha \in K$ be a root of f in K. We know that f splits completely in $\bar{F}[x]$

If K/F is algebraic and $\sigma : K \to K$ is an F-homom, then σ is surjective i.e., $\sigma(K) = K$ — previous exercise

Let $\beta \in \bar{L}$ be any root of f. Then we have:

... $F[x]$ ... $F(\beta) \subseteq \bar{F}$ | Hence we have a hom $\sigma \to \bar{F}$



K — $L = K^{Gal(K/F)}$ — F

$[K:L] \underset{\substack{\uparrow \\ \text{theorem II}}}{=} |Gal(K/F)| = [K:F] \geq [K:L]$

$\Rightarrow L = F \Rightarrow F = K^{Gal(K/F)}$ ∎

Theorem: Let K/F be a finite extension. Let $\bar{F}$ be an algebraic closure of F that contains K. Then the following are equivalent.

(1) If $\sigma : K \to \bar{F}$ is an F-homom of fields, then $\sigma(K) \subseteq K$.

Hence: σ induces an F-automorphism $\sigma : K \to K$

(2) If $f \in F[x]$ is an irreducible poly which has a root in K, then f splits completely in $K[x]$.

(3) K is the splitting field of a poly $f \in F[x]$

If K/F is algebraic and $\sigma : K \to K$ is an F-homom, then σ is surjective i.e., $\sigma(K) = K$ — previous exercise

Now, let us complete the proof, let us go to the 2 implies 3 statement and these are now going to be easy for us. So, let us take so what is two, two says that if an irreducible polynomial will has one root in capital K, it has all the roots in capital K, and we are now going to show that it is the splitting field of a polynomial.

So, let, because it is a finite extension, we can write it like this. Let K be this, where alpha 1 through alpha n are in K and suppose that, so we are going to assume that suppose that we cannot remove any alpha i. So, by which I mean, I mean, this is slightly sloppily mentioned written, but what I mean is that if you remove any of the Li, alpha is, it is not equal to K. So, so that means F of, for example, alpha 2, alpha 3, alpha n is not equal to K. So, you need all, all the alpha is to generate K.

You will see I mean, this is just a simple requirement, but you do not, if some alpha is not needed, you just drop it. So, this is nothing serious. Now, let fi be the irreducible polynomial of alpha I over F. So, alpha i is in K, they are of course algebraic because K or F is a finite extension. So, let us take the irreducible polynomial fi is irreducible and it has a root in K.

Obviously, because it has a root namely alpha I, so by and each fi is irreducible. So, this is the situation. So, now apply two, the statement two says that, if an irreducible polynomial has one root it splits completely. So, by two, fi splits completely over capital F, over capital K rather. So, now, let us take the product of these as our f. So, then f splits completely in K X because, the roots of F are the roots of fi's, union of the roots of fi's each fi is splits completely, so f itself does.

And note that K over K is the field generated by f, because you, you have to take all of K to generate the roots of f by this little hypothesis that I made, even if you drop one of the alpha i's you cannot get all of K. So f, so in other words, K is the smallest field, smallest subfield of K containing all the roots, all the roots of f because if it does not contain even one root then you will get a slightly smaller field. So, because alpha is all needed. So, this shows that K is the splitting field.

So this, this last point is trivial, I mean you if you need if you do not need some roots, you can always drop it. The point is there is a single polynomial whose roots generate K. So now that implies 3. So finally, 3 implies 1. If you prove this, you are done, you have proved one implies two, here, you just proved two implies three, now we are going to prove three implies one. So, this is easy. So, let K, so let K by hypothesis in three, the splitting field of a polynomial f in F X over capital F.

So let us take the splitting field of a polynomial F in capital F X over the field capital F. So, suppose that roots are f are alpha 1 through alpha n. So, K is equal to F alpha 1 through alpha n. Now, let us take the hypothesis of one. So, let sigma from K to F bar be an F homomorphism by, by our earlier results or note remarks sigma of alpha i must be alpha j, I mean for every, so this is you understand what I mean here.

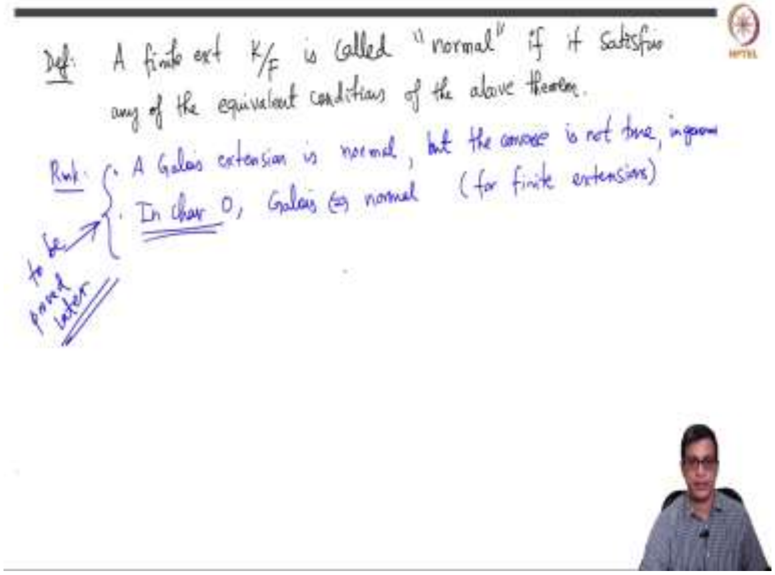
So, for every i if you apply sigma alpha i must equal sigma, I mean it must be alpha j. So, what I really mean is, I am not saying F is irreducible, so let me be a bit careful here. So, by earlier results for every alpha sigma of alpha i is in the set. So, because alpha is irreducible polynomial will be a factor of f, because f satisfies alpha i, alpha i is a root of f. So, irreducible polynomial of alpha i is a factor of f.

So, its roots are also roots of f, but roots of f for this, so alpha i must go to one of these, but the way you might group this you cannot say that every alpha i must go to every alpha j that is incorrect, because small f may not be reducible, but you are guaranteed that root of, the image of alpha i must map to one of these alpha 1 to alpha n.

But this is now we are done because, in other words, sigma alpha i is in K for all i. So, sigma alpha is in K for all i, this implies sigma of K is in K. So that is all because F is generated, K is generated by alpha i through alpha 1 through alpha n or F. Sigma F, of course, is F because everything in capital F is itself under sigma. So, all you need to worry about is alpha i is, where they go, but by this observation image of alpha i must be again in K.

That means any polynomial, every element of K is a polynomial in alpha i's with coefficients in capital F. So, you apply sigma to it and apply the field homomorphism property, you will again land in capital K. So, this completes the proof of the proposition. The first statement is exactly that, if you have any f homomorphism from K to a F bar, then image of K is contained in K, which is what we have just proved.

(Refer Slide Time: 28:04)

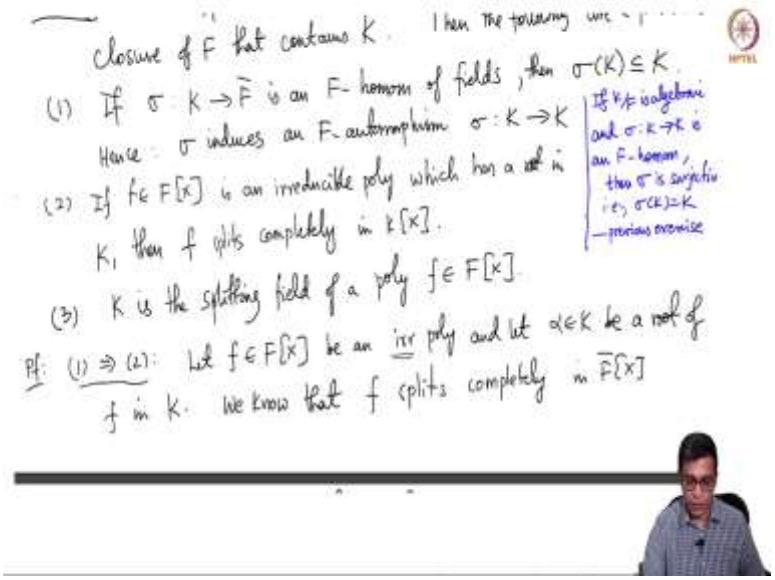


Def: A finite ext K/F is called "normal" if it satisfies any of the equivalent conditions of the above theorem.

Rmk: · A Galois extension is normal, but the converse is not true, in general

· In char 0, Galois $\Leftrightarrow$ normal (for finite extensions)

to be proved later



closure of F that contains K. Then the following are ...

(1) If $\sigma: K \to \bar{F}$ is an F-homom of fields, then $\sigma(K) \subseteq K$. Hence σ induces an F-automorphism $\sigma: K \to K$

If K/F is algebraic and $\sigma: K \to K$ is an F-homom, then σ is surjective i.e., $\sigma(K) = K$ — previous exercise

(2) If $f \in F[x]$ is an irreducible poly which has a root in K, then f splits completely in $K[x]$.

(3) K is the splitting field of a poly $f \in F[x]$.

Pf: $(1) \Rightarrow (2)$: Let $f \in F[x]$ be an irr poly and let $\alpha \in K$ be a root of f in K. We know that f splits completely in $\bar{F}[x]$

So, let me end this video with an important definition. A field extension K over F is called normal if it has, so a finite extension, it is a field extension as I said that goes without saying a finite extension K over F is called normal, if it satisfies any of the equivalent conditions of the above theorem.

So, the most familiar and probably convenient way of checking that is the third one, so splitting field extensions are now called normal, so normal is a nice word for that. And it is, it corresponds to the notion of normal subgroups of a group as we will see later in the course. But a normal extension will also have these other two properties. See, if you just stare at this for a minute, it is important you, you can understand because if you are taking a splitting field of a single polynomial, it has this nice property that every polynomial that has a root splits completely.

So two, condition two seems on the face of it stronger than being splitting field of a single polynomial, but it is in fact equivalent to being the splitting field of a single Polynomial. Let me just add a final remark and then we will end this video. Remark is that, what is the connection of all these two Galois extensions, we will show later that Galois extension is normal. This is true, we will prove this, this is an important observation, but the converse is not true.

Meaning there are non, converse is not true in general let me say, there are normal extensions but which are not Galois. However, in characteristic zero Galois is equivalent to normal, for finite extensions of course. So all this will be done later. So, if you are working for example, with extensions of Q, you can safely remove the word, replace the words Galois and, interchange the word Galois normal. So, this is a new observation for us.

Of course, this will be proved later. But once we prove that Galois extensions are much more easy to understand in characteristic zero because they are simply splitting fields of polynomials. But in general, of course, it has been characteristic prime. It is not true that normal implies Galois it is only always true that Galois implies normal. So, let me stop this video here in the next video, we will do some problems to understand everything that we have done in the last few videos on Galois extensions. Thank you.