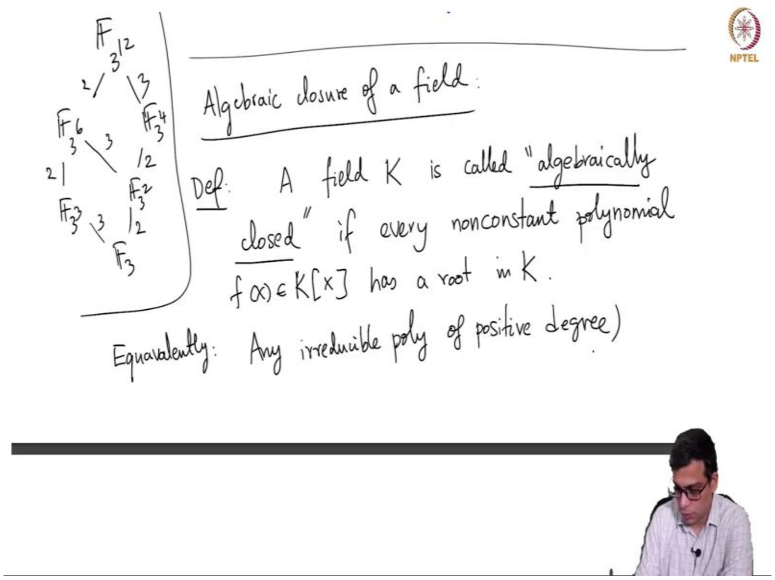
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Review of field theory – Part 3

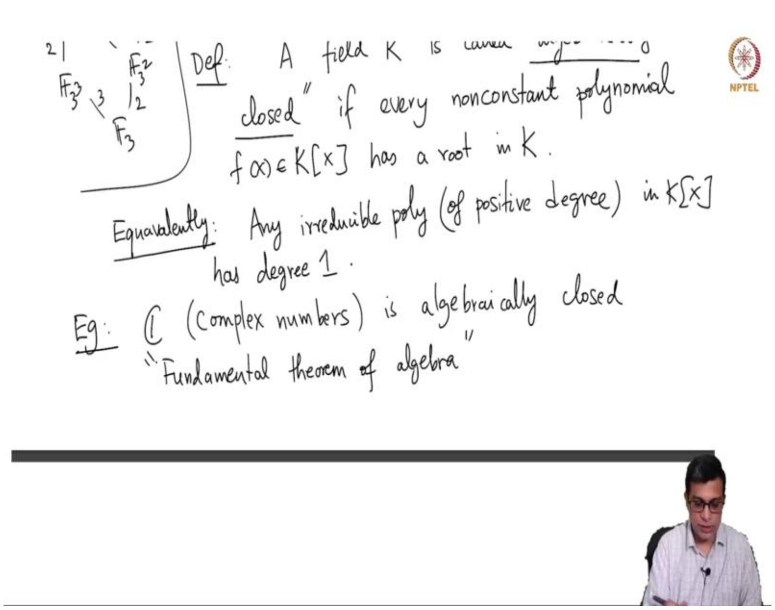
(Refer Slide Time: 00:15)



Algebraic closure of a field:

Def: A field K is called "algebraically closed" if every nonconstant polynomial $f(x) \in K[x]$ has a root in K.

Equivalently: Any irreducible poly of positive degree)



Def: A field K is called "algebraically closed" if every nonconstant polynomial $f(x) \in K[x]$ has a root in K.

Equivalently: Any irreducible poly (of positive degree) in $K[x]$ has degree 1.

Eg: $\mathbb{C}$ (complex numbers) is algebraically closed
"Fundamental theorem of algebra"

Welcome back. So far we have started recalling the basic notions in group theory, ring theory, field theory that we require in order to study Galois Theory. So I want to do one more video where I recall some important results in the field theory. So last video, I talked about finite fields and we talked about splitting fields. So the next topic I want to quickly recall. Now I will again not prove these things in detail and my goal is only to important, recall important facts.

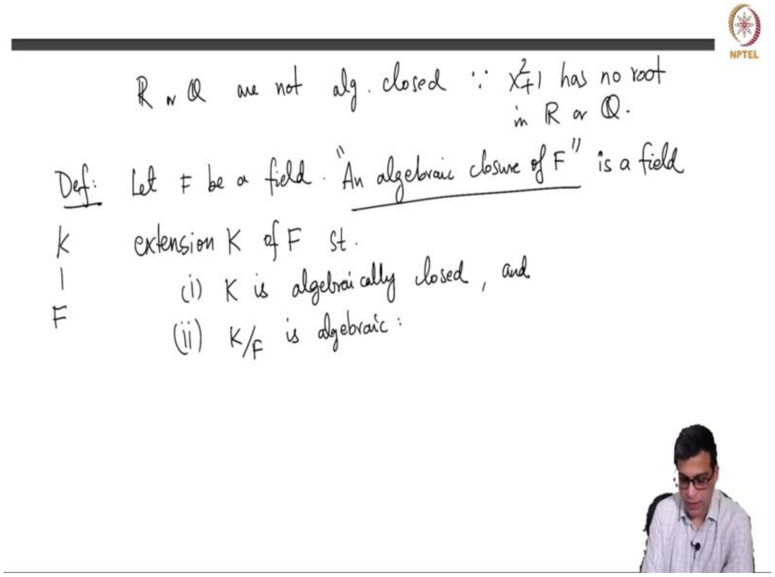
So, the important notion that I want to recall for you is the notion for algebraic closure of a field. So let me first define a field F, let me use K. A field K is called algebraically closed. It is called algebraically closed if every non-constant polynomial small f over K has a root. This is a very simple statement; every polynomial non-constant of course because constants cannot have, non-zero constant cannot have a root.

So, every non-constant polynomial has a root in K, equivalently every any irreducible polynomial of positive degree. I will put that in brackets just to avoid constants again. Every irreducible polynomial in Kx has degree 1. Clearly if a polynomial has roots it is not irreducible. So these are equal. I mean one can check it is a trivial verification that these 2 conditions are equivalent.

So if you have a degree 2 or higher polynomial, if it has a root, it cannot be reducible. And if you have and the only irreducible polynomials that is given means any polynomial of degree 2 or higher will have to factor because its Kx is ufd and you can keep factoring until you get a linear factor which corresponds to a root.

So this is what an algebraically closed field is, the standard example for this is C, the complex numbers is algebraically closed. C stands for the field of complex numbers. It is algebraically closed and this is the statement of fundamental theorem of algebra that has lots of different proofs, which you may have learned in some other course. So this is the fundamental theorem of algebra.

(Refer Slide Time: 03:37)



$\mathbb{R}$ or $\mathbb{Q}$ are not alg. closed $\because$ X^2+1 has no root in $\mathbb{R}$ or $\mathbb{Q}$.

Def: Let F be a field. "An algebraic closure of F" is a field extension K of F st.

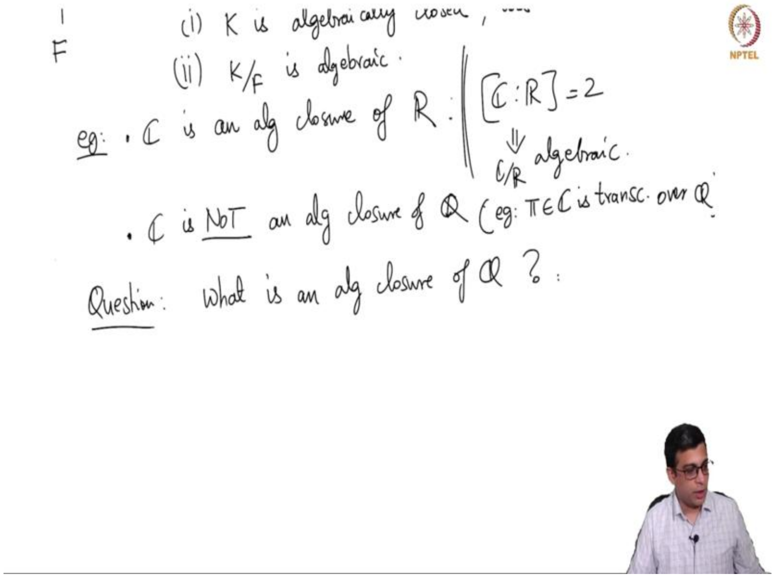
$$\begin{tikzcd} K \arrow[d, dash] \\ F \end{tikzcd}$$

(i) K is algebraically closed, and

(ii) K/F is algebraic.

On the other hand R or Q are not algebraically closed. Let me shorten this by saying. This is because X square plus 1 has no root in R or Q. So these are not algebraically closed. Now let me define the algebraic closure of a field. Let F be a field and algebraic closure of F is a field extension K of F. So K must contain the field F such that it has 2 properties. One, K is algebraically closed. K must be algebraically closed and very important, the extension K over F is algebraic. So the first condition is not enough.

(Refer Slide Time: 04:57)



(i) K is algebraically closed, and

(ii) K/F is algebraic.

eg: • $\mathbb{C}$ is an alg closure of $\mathbb{R}$. $\Big\|$ $[\mathbb{C}:\mathbb{R}]=2 \Downarrow \mathbb{C}/\mathbb{R}$ algebraic.

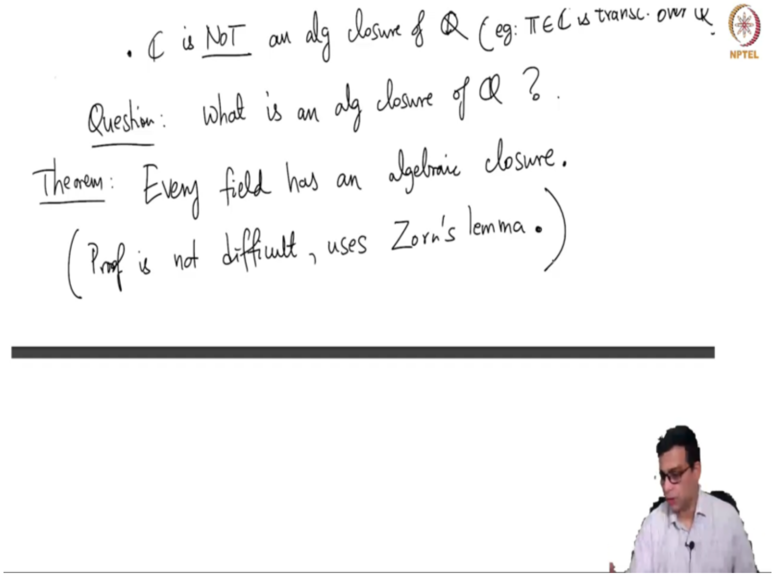
• $\mathbb{C}$ is NOT an alg closure of $\mathbb{Q}$ (eg: $\pi\in\mathbb{C}$ is transc. over $\mathbb{Q}$

Question: What is an alg closure of $\mathbb{Q}$?

So, again the standard example for us is C is an algebraic closure of R, because C is algebraically closed and C colon R is 2. So it is a degree 2 extension. So it is algebraic. I mean this is trivial. C is algebraically closed and C over R is algebraic. On the other hand C is not an algebraic closure of Q.

C is algebraically closed fine, but it is not algebraic over Q. So example is transcendental over. So it is not algebraic. So the extension is not algebraic. So in order to be a algebraic closure you need to have 2 properties. It has to be an algebraically closed field and it has to be an algebraic extension of Q. So the question is, if C is not the algebraic closure, what is an algebraic closure?

(Refer Slide Time: 06:26)



• $\mathbb{C}$ is NOT an alg closure of $\mathbb{Q}$ (eg: $\pi \in \mathbb{C}$ is transc. over $\mathbb{Q}$.

Question: what is an alg closure of $\mathbb{Q}$?.

Theorem: Every field has an algebraic closure.

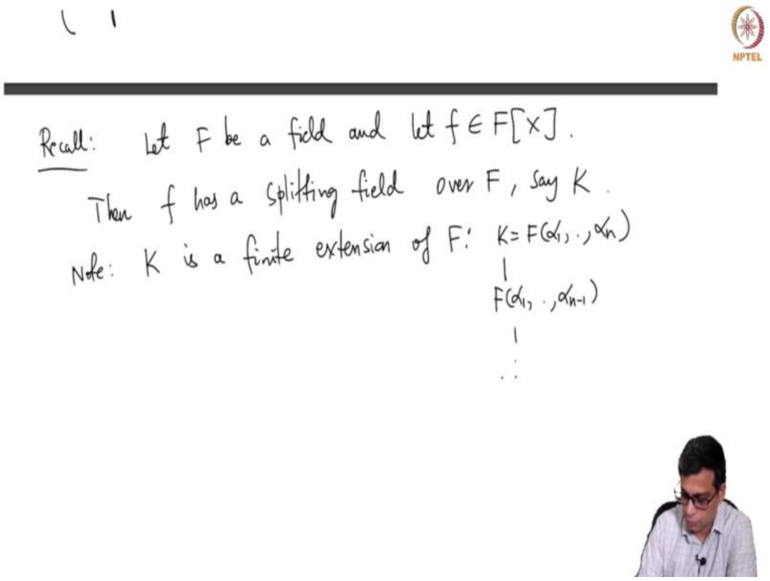
(Proof is not difficult, uses Zorn's lemma.)

Does it exist? And here is where I will state it as a theorem. I do not want to go to the proof of this because it takes me away from what I want to do. It is a nice proof. It uses Zorn’s lemma but it does not reveal anything for us as far as this course is concerned. So later on if I have time I will just make a separate video just covering this theorem which says that every field has an algebraic closure, simple statement and the proof uses Zorn’s lemma so you have to construct a series of fields and show that you can add roots of all polynomials.

Remember we can add roots of 1 polynomial, namely we can construct splitting fields. But to construct algebraic closure you have to do, you have to add root of all polynomials. At the same time make sure that you do not introduce transcendental elements. So this is proof is not difficult, uses Zorn's lemma which you may have heard learned before. It is, for example it is used to show that every commutative ring has a maximal ideal.

So we will not do the proof for today. But it is a standard fact you can find this in any textbook on algebra. So every field is an algebraic closure. The question then is how many algebraic closures can it have? Is it unique? And that is what I want to again state as a theorem without getting into the proof. But before stating that I want to develop I want to express a few theorems about extending field homomorphisms which are going to be useful for us later.

(Refer Slide Time: 08:12)



Recall: Let F be a field and let $f \in F[x]$.

Then f has a splitting field over F, say K.

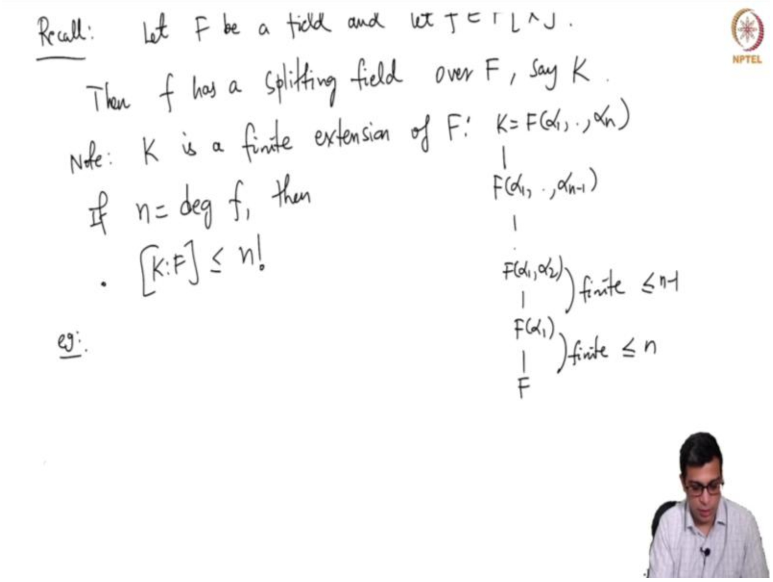
Note: K is a finite extension of F: $K = F(\alpha_1, ., \alpha_n)$

$$\begin{array}{c} K = F(\alpha_1, ., \alpha_n) \\ | \\ F(\alpha_1, ., \alpha_{n-1}) \\ | \\ \vdots \end{array}$$

So, I want to also recall for you what is a splitting field. So let F be a field and let small f be a polynomial over the field F. Then we know that have small f has the splitting field over F. I mentioned this last time you can add roots 1 by 1 and eventually reach a field where you have all the roots and that field is generated by the roots of small f.

So some important facts. I mean the, these are standard facts. So note that in say K, note that K over F, K is a finite extension of F. It is in fact, we can also talk about its degree but first point is it is a finite extension. Because remember, K is generated by the roots. So you have extensions like this.

(Refer Slide Time: 09:41)



Recall: Let F be a field and let $f \in F[x]$.

Then f has a splitting field over F, say K.

Note: K is a finite extension of F: $K = F(\alpha_1, \ldots, \alpha_n)$

If $n = \deg f$, then

- $[K:F] \leq n!$

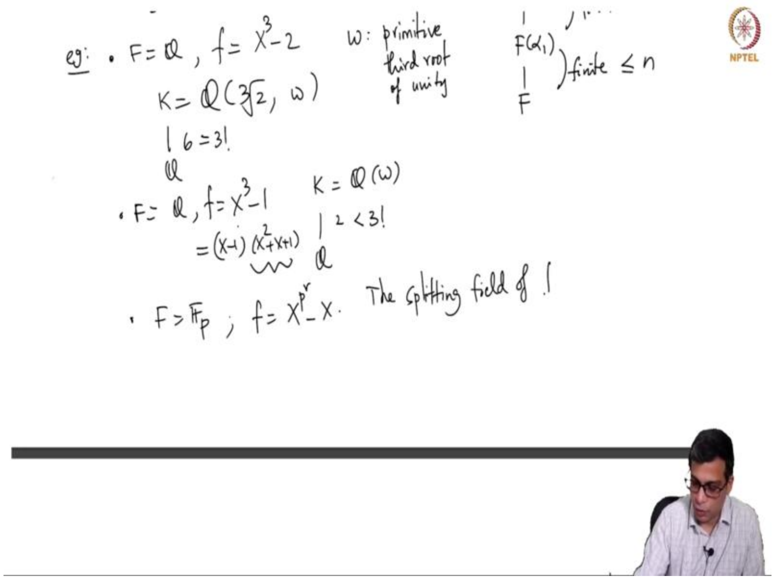
eg:.

$$\begin{tikzcd}
K = F(\alpha_1, \ldots, \alpha_n) \arrow[d, dash] \\
F(\alpha_1, \ldots, \alpha_{n-1}) \arrow[d, dash] \\
\vdots \\
F(\alpha_1, \alpha_2) \arrow[d, dash, "\text{finite } \leq n-1"] \\
F(\alpha_1) \arrow[d, dash, "\text{finite } \leq n"] \\
F
\end{tikzcd}$$

So this is finite because it is generated by a single algebraic element. This is finite and so on, so the whole thing is finite. In fact this tower also tells you that if n equals degree of F then K colon F is less than n factorial because this is at most n cause F small f is a root of is a polynomial that alpha 1 satisfies.

So its irreducible polynomial will have degree less than equal to small f because it defines small f. And this is less than equal to n minus 1 because now you can clear out x minus alpha 1 from F and you look at the degree n minus 1 polynomial that you get and so on. So this is true and you can have equality sometimes and it can also be a strict inequality sometimes. So 3 examples that I mean we have couple of examples that will illustrate this.

(Refer Slide Time: 10:35)



eg: • $F = \mathbb{Q}$, $f = X^3 - 2$ $\quad \omega$: primitive third root of unity

$$\begin{tikzcd} K = \mathbb{Q}(\sqrt[3]{2}, \omega) \arrow[d, dash, "6 = 3!"] \\ \mathbb{Q} \end{tikzcd}$$

$$\begin{tikzcd} F(\alpha_1) \arrow[d, dash] \arrow[u, dash] \\ F \end{tikzcd} \Big) \text{finite} \leq n$$

• $F = \mathbb{Q}$, $f = X^3 - 1$
$= (X-1)\underbrace{(X^2+X+1)}$

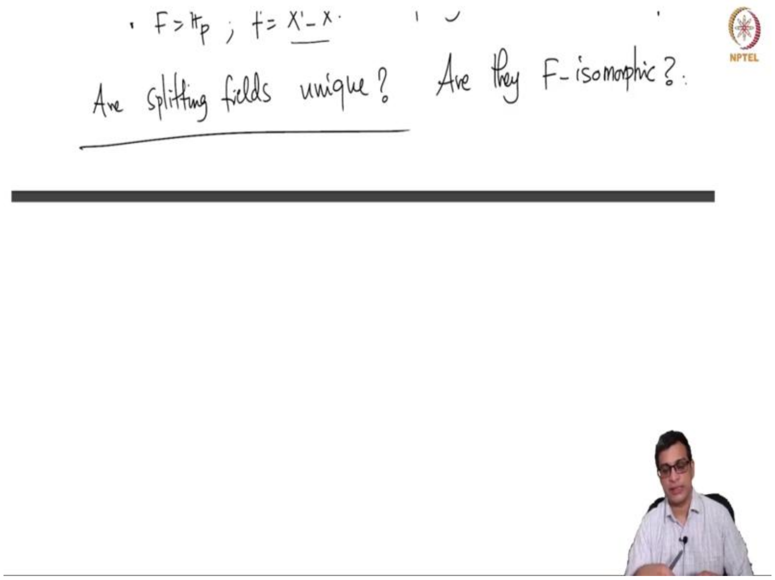
$$\begin{tikzcd} K = \mathbb{Q}(\omega) \arrow[d, dash, "2 < 3!"] \\ \mathbb{Q} \end{tikzcd}$$

• $F = \mathbb{F}_p$; $f = X^{p^r} - X$. The splitting field of f

You take F to be Q and small f to be x cube minus 2, then K is actually Q adjoined cube root of 2 and omega where omega is primitive 3rd root of unity. And this degree over Q is 6, which is 3 factorial. On the other hand if you take F to be Q and small f to be x cube minus 1. Here K is actually just Q adjoined omega and the degree is 2 here and the irreducible polynomial is x square plus x plus 1.

This is of course less, strictly less than 3 factorial and one final example if you take F to be the finite field of P elements and you take small f to be X power p or minus X. The splitting field small f over capital F is nothing but the finite field with P power R elements.

(Refer Slide Time: 11:48)



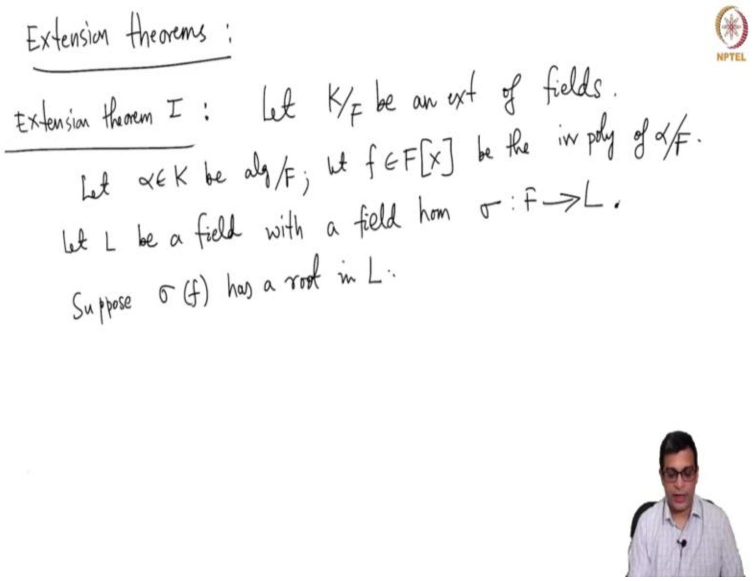
· $F \supset \mathbb{F}_p$; $f = \underline{X' - X}$.

Are splitting fields unique? Are they F-isomorphic?

This is something that we have, we have mentioned as part of our structure theorem of finite fields. The unique field of order P power R contain is consists of roots of this polynomial x power p power r minus x. So now what I want to address first before getting to the uniqueness of algebraic closure is uniqueness of splitting fields. So the splitting fields unique. So when we ask such a question in mathematics it means, are they isomorphic?

So, are they isomorphic? In fact we want them to be isomorphic over the base field. Are the question is, are they F isomorphic? Remember I talked about F homomorphism of fields in the previous video which means that there is an isomorphism which fixes F point wise.

(Refer Slide Time: 12:56)



Extension theorems :

Extension theorem I : Let K/F be an ext of fields.

Let $\alpha \in K$ be alg$/F$; let $f \in F[x]$ be the irr poly of α/F.

Let L be a field with a field hom $\sigma : F \to L$.

Suppose $\sigma(f)$ has a root in L.

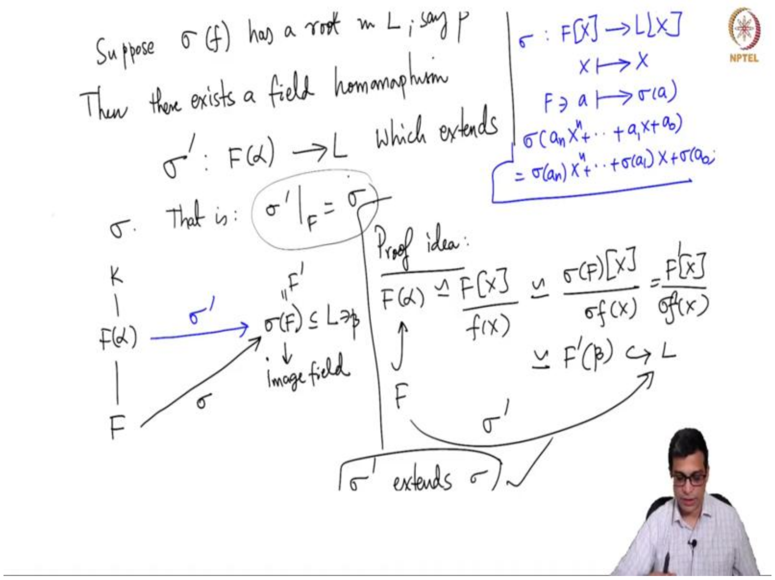
And in this context I want to introduce this very important extension theorems that we will use at a few places in the rest of the course. So I want to state one simple case first which I call 1, extension theorem 1 and then I will generalize this to an arbitrary situation. So this is the following. So I will not write maybe the full statement or let me actually write the full statement and also draw a picture.

So, let F be a field, an arbitrary field. Let K over F be an extension. In fact, I could have just maybe we can write like this. Let K over F be an extension of fields. Let alpha be an element of K which is algebraic over F. So I am really interested in knowing F alpha not in K. So on the other hand let L be a field.

Before that and let small f be a polynomial in capital FX, be the irreducible polynomial of alpha over F. Now let L over K be another field extension. In fact let me write it like this. Let L be a field with a field homomorphism. So F is in fact isomorphic to subfield of L, but I want to state it in this generality. Remember any field homomorphism is by definition injective because the kernel of a ring homomorphism is an ideal.

A field homomorphism sends 1 to 1. So the kernel cannot be all of F. And any field has only 2 ideals, namely F and 0. So the kernel has to be 0. So it is an injective map. So that means F is isomorphic to its image which is a subfield of L. Suppose, sigma of F has a root in L, when I write sigma of F I mean the following. So let me just write it like this. So sigma is a function from F to L.

(Refer Slide Time: 15:36)



Suppose $\sigma(f)$ has a root in L; say β

Then there exists a field homomorphism

$\sigma' : F(\alpha) \to L$ which extends σ. That is: $\sigma'|_F = \sigma$

$\sigma : F[X] \to L[X]$

$X \mapsto X$

$F \ni a \mapsto \sigma(a)$

$\sigma(a_n X^n + \cdots + a_1 X + a_0)$

$= \sigma(a_n) X^n + \cdots + \sigma(a_1) X + \sigma(a_0)$

$$\begin{tikzcd}
K \arrow[d, dash] & \\
F(\alpha) \arrow[r, "\sigma'"] \arrow[d, dash] & \overset{F'}{\overset{\shortparallel}{\sigma(F)}} \subseteq L \ni \beta \\
F \arrow[ur, "\sigma"'] &
\end{tikzcd}$$

Image field

Proof idea:

$$\begin{tikzcd}
F(\alpha) \cong \dfrac{F[X]}{f(X)} \cong \dfrac{\sigma(F)[X]}{\sigma f(X)} = \dfrac{F'[X]}{\sigma f(X)} \cong F'(\beta) \hookrightarrow L \\
F \arrow[u, hook] \arrow[u, phantom]
\end{tikzcd}$$

$F \xrightarrow{\sigma'} L$

σ' extends σ ✓

So sigma naturally entrench to a function from fx to lx. I will use by abuse of notation, same letter sigma to denote that. So here X goes to X that is all and constants go to if A belongs to F, it goes to sigma of A. So then basically what it does is sigma of a polynomial is simply sigma of an x power n, sigma of a1 x plus sigma of a0. So that is what sigma of F is and I am now assuming that sigma of F has a root in L.

So, if that is the case then there exists a field extension sorry there exists a extension, there exists a field homomorphism. Let me write this like this homomorphism, sigma prime from F alpha to L which extends sigma. So what I mean is, that is sigma prime restricted to F is sigma. So all this will become clear if I draw just a picture. So here F here, F alpha here, of course F alpha sits in K but K is irrelevant for in this theorem.

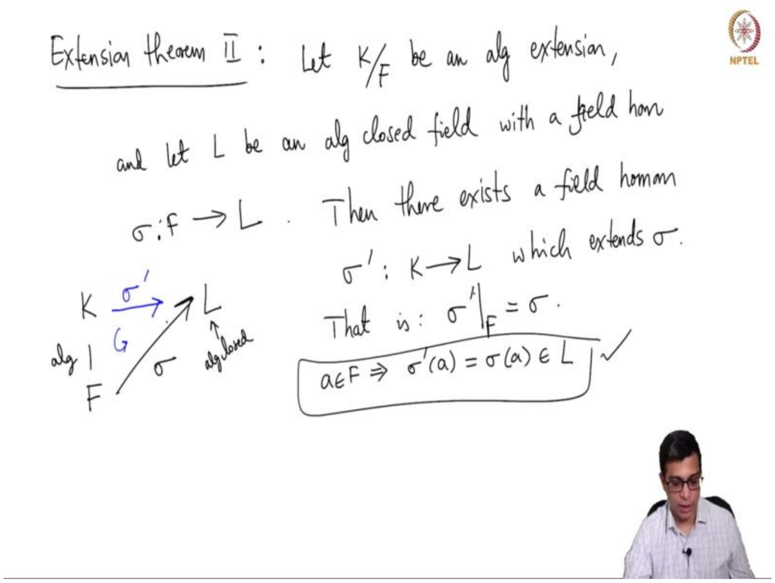
And then I have a function from F to L so and F, sigma of F has a root in L. So I will call that beta. So beta is an element here. So now I am claiming that there exists a function from F alpha to L which I am calling sigma prime which makes this diagram commutative, which means that if you take an element in F apply sigma, you get something in L. But you can also think of it as an element in F alpha and apply sigma prime, you get the same value.

So, that is how, that is what we mean when we say sigma prime extends sigma. So I claim that such a thing exists and the proof idea is very simple. So we know that F alpha, this is standard field theory is isomorphic to fx modulo small fx. This I claim is basically equal to sigma of F, X modulo F prime X or rather sigma of F. So if you wish you can actually, so sigma F is a field, image field and that is contained in L.

So, if you wish you can call that F prime. So what I am really doing is F prime X modulo, modulo F prime sigma F of X. So that is of course contained in L. So this F prime, this is actually nothing but isomorphic to F prime beta. So beta is here. So this is F prime beta which is contained in L. So and this is the map that I construct. So F is contained in F alpha. F alpha is isomorphic F prime, F prime beta which is contained in L.

So, this composition gives me the function sigma prime and the way construction goes it is clear that it extends sigma. So the sigma prime extends sigma, namely that sigma prime restricted to F is sigma. So this is the construction. So if this is not clear, just pause the video, think about it, this are very standard things.

(Refer Slide Time: 20:14)



Extension theorem II: Let K/F be an alg extension,

and let L be an alg closed field with a field hom

$\sigma : F \to L$. Then there exists a field homom

$\sigma' : K \to L$ which extends σ.

$$\begin{tikzcd} K \arrow[r, "\sigma'"] & L \\ F \arrow[u, "alg"] \arrow[ur, "\sigma"'] & \end{tikzcd}$$

G

alg closed

That is: $\sigma'|_F = \sigma$.

$\boxed{a \in F \Rightarrow \sigma'(a) = \sigma(a) \in L}$ ✓

So, this part is clear, using this basic ingredient we have the extension theorem 2 which is much more general but essential idea is this extension theorem 1 ends Zorn’s lemma. So you have to generalize this more in a more general situation. So here you have the following. So let K over F be an algebraic extension now.

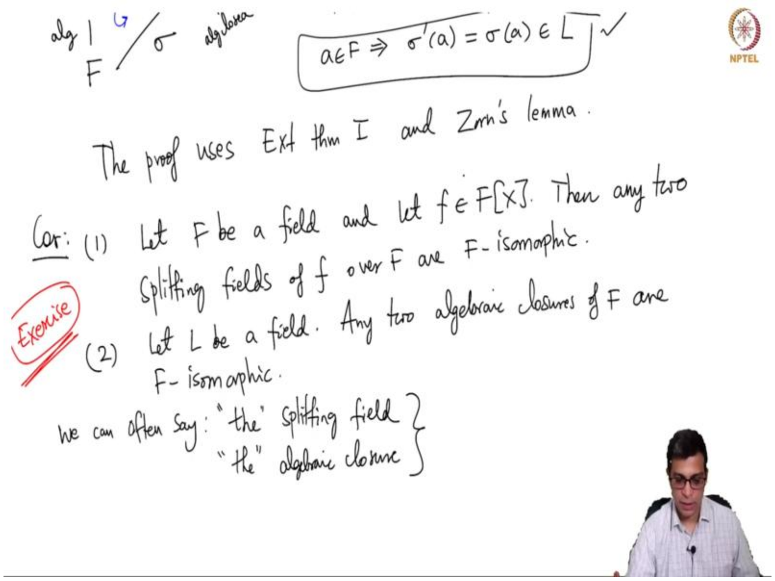
Earlier I took an algebraic extension generated by a single element. Now I am taking an algebraic extension without any assumptions and let L be an algebraically closed field with a homomorphism, with a field homomorphism of course. I do not need to always say this field homomorphism sigma from F to L.

So, the picture is we have F, K, L, sigma is a field homomorphism and this is an algebraic extension. Earlier it is similar to the earlier picture except that I am not doing for F alpha, I am doing for entire K. And now I am assuming L to be algebraically closed, not just a field where this particular polynomial has a root. So L is algebraically closed. Then there exists a field homomorphism, sigma prime from K to L which extends sigma that is as obvious as before.

It is simply saying that the restriction of sigma prime to F is just sigma. So that means there is a map here which I call sigma prime which extends sigma. So this is a commutative diagram which means that if you take an element in capital F to repeat what I said earlier, take an element in capital F. So if A is in capital F then sigma prime of A, think of A as an element of K and apply sigma prime or apply sigma to it, you get the same answer.

So, this is what we mean by extension. This is essentially a combination of such things. But remember this need not be a finite extension. If it is a finite extension K over F, one can just do finitely many steps of such things and argue that one gets the extension sigma prime. But for non-finite algebraic extensions, one has to use Zorn’s lemma.

(Refer Slide Time: 23:09)



$\boxed{a \in F \Rightarrow \sigma'(a) = \sigma(a) \in L}$ ✓

The proof uses Ext thm I and Zorn's lemma.

Cor: (1) Let F be a field and let $f \in F[x]$. Then any two splitting fields of f over F are F-isomorphic.

Exercise

(2) Let L be a field. Any two algebraic closures of F are F-isomorphic.

We can often say: "the" splitting field
"the" algebraic closure

So, the proof uses extension theorem 1 and Zorn's lemma. So this is a standard proof. Again you can do this, read this in any book. You look at subfields of K where you can extend to which you can extend sigma. So of course, that is an non-empty set because F is contained in it. And then you look at all such things, family of all subfields of K to which you can extend sigma and then you show that there is a partial order in which you can given by the inclusion, every totally ordered subset as a maxima element.

So, the family itself has a maximal element. And then you argue that it has to be K, because if it is not, you can extend it further by using the 1st statement because you can always extend it to an algebraic element, a single algebraic element. So this in particular gives me 2 corollaries which I want to state. And in the video there corollary 1 is let F be a field and let F be a polynomial over it then any 2 splitting fields of small f over capital F are F isomorphic.

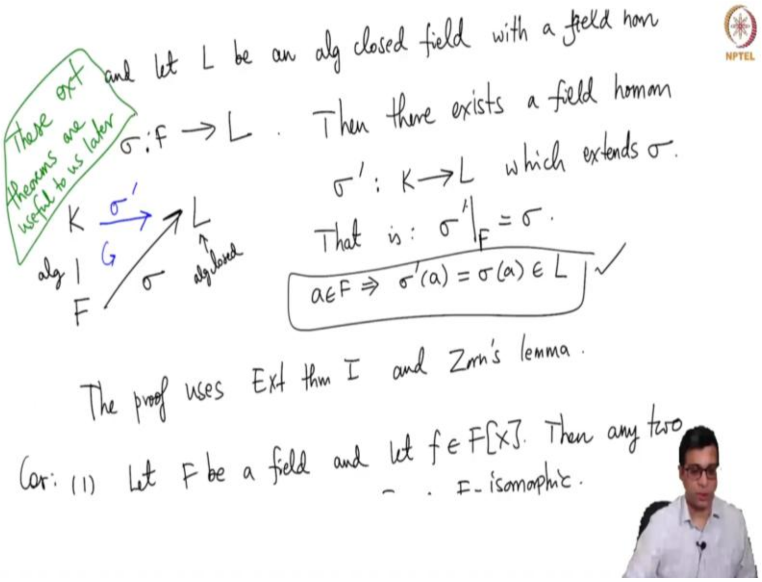
This proof is rather easy because you can take. You can in fact use just the extension theorem 1 because you have a finite extension, splitting fields of finite extensions. So you can, no need to use Zorn's lemma just induction and extension theorem 1 will give you the required statement. So all you do is you take L also to be F. So you can construct this or you can figure out how to do this. It is a good exercise.

So, in fact let me write the 2nd corollary also and then leave both as an exercise. So any 2, so again let L be a field, any 2 algebraic closures of F are F isomorphic. So these are in both statements that we will constantly use and both are good exercises. So in my problems session later on I will try to do this explicitly using the extension theorems.

So, the point is because any 2 splitting fields are F isomorphic, we often say, we can often say the splitting field though we have to keep in mind that it is only up to isomorphism and the algebraic closure. So this is an important conclusion for us. We can talk about this splitting field of a polynomial or the algebraic closure of a field.

So, in particular you know that Q has an algebraic closure and that will sit inside C. So maybe in a exercises we discuss this. But even otherwise even apart from the corollaries, these extension theorems themselves are very important to us. Both extension theorems are very important.

(Refer Slide Time: 26:47)



These ext theorems are useful to us later

and let L be an alg closed field with a field hom $\sigma : F \to L$. Then there exists a field homom $\sigma' : K \to L$ which extends σ.

That is: $\sigma'|_F = \sigma$.

$$\boxed{a \in F \Rightarrow \sigma'(a) = \sigma(a) \in L} \checkmark$$

$$\begin{tikzcd} K \arrow[r, "\sigma'"] & L \\ F \arrow[u, dash, "alg"] \arrow[ur, "\sigma"'] & \end{tikzcd}$$

G
alg closed

The proof uses Ext thm I and Zorn's lemma.

Cor: (1) Let F be a field and let $f \in F[x]$. Then any two

F-isomorphic.

These extension theorems are useful for us. So we will use them later. So make sure that you understand the statements. I am again reminding you that I am not proving this. These are essentially, I proved the 1st one but 2nd one is a standard argument using Zorn’s lemma. So I will not do this. But please understand the statement because that will be useful for us later. So let me stop here and then in the next video will continue with Galois Theory. Thank you.