



**Algebra II**  
**Professor S Viswanath**  
**The Institute of Mathematical Sciences**  
**Lecture 26**  
**Normal Extensions**

(Refer Slide Time: 00:16)

Normal extensions

Def: let  $K/F$  be an algebraic extension. We say that  $K/F$  is a normal extension if  $\exists$  a collection  $\{f_i(x) : i \in I\} \subseteq F[x]$  such that  $K$  is the splitting field of this collection, i.e. (A) each  $f_i$  splits over  $K$ .  
 and (B)  $\nexists F \subseteq E \subsetneq K$ , then  $\exists i \in I$  st  $f_i$  does not split over  $E$ .

We will talk about normal extensions. These play an important role in Galois theory, which is where we are eventually headed. So, let me make the formal definition first and then I will make some remarks about it. So, let  $K$  over  $F$  be an algebraic extension. So,  $F$  is some fixed some based field  $F$  and taken algebraic extension of  $F$ , be an algebraic extension.

We say that  $K$  is a normal extension or the extension  $K$  over  $F$  is normal if there exists a collection of polynomials. So, if there is a set, let us call it a collection  $f_i$  of  $x$ ,  $i$  running over some index set. So, it could be an infinite collection of polynomials there exists a collection of polynomials with coefficients in  $F[x]$ . So, this subset, this collection  $f_i$  of  $x$  is a subset of  $F[x]$ , such that  $K$  is the splitting field of of this collection. So, that is the definition, but let me just say what I mean by the splitting field of a collection. We talked about the splitting field of a single polynomial.

So, the splitting field of a collection means that each  $f_i$  splits over  $K$ . So, recall, there were two properties for a splitting field of a single polynomial. So, similarly, here, I have two properties, let me now call them capital A and capital B, each  $f_i$  splits over this field  $K$ , it splits completely into a product of linear factors and property B says that this does not hold for any proper subfield of  $K$ . If  $E$  is a proper subfield of  $K$  containing  $F$ , then at least one of the  $f_i$ 's does not split over  $E$ . So then there exists at least one  $f_i$ , there exists  $i$  in  $I$ , such that  $f_i$

does not split over this field E. So that is what we mean by being the splitting field of the entire collection.

(Refer Slide Time: 03:21)

Remark: We can replace  $B$  by equivalent condition

$B'$ : The subfield of  $K$  generated by  $F$  and the roots of all the  $f_i, i \in I$  coincides with  $K$ .

Ex.  $F = \mathbb{Q}$   $K = \mathbb{Q}(\sqrt{2}, i)$   $K/F$  normal extension.

Let  $f(x) = x^2 - 2$  and  $g(x) = x^2 + 1$ .

$K$  is the splitting field of  $\{f, g\}$ :  $A$   $f(x) = (x - \sqrt{2})(x + \sqrt{2})$   
 $g(x) = (x - i)(x + i)$

So, you know, just like what we did earlier, so, remark we can replace this condition B remark as before, the splitting field of a single polynomial, we can replace B by the equivalent condition B dashed, by the equivalent condition, let us call it B dash again, capital B dash which says that K is generated. So, the subfield of K generated by F and the roots of all the fi's put together. So, the roots of all the fi, this subfield coincides with K itself. It is not a proper subfield, but in fact the the whole field. So, and I will sort of leave this proving the equivalence of B and B dashed to you, it is along the same lines as what we did earlier for a single polynomial.

So, here are some examples. So, if I take F to be a field Q, and I take K to be the field which is Q adjoin with two elements, one of them is the root 2, the other is i, then, this is a normal extension. So, claim is that K over F is actually a normal extension. And to prove this, I have to exhibit a collection of polynomials for which this is the splitting field. And here, it is sort of I mean, if you look at the the elements, we adjoin root 2 and i, it sort of tells you what the polynomial should be. So, let us take the polynomial fx equals x square minus 2 and so let gx be x square plus 1.

So, the claim is that K over f, K is the splitting field of this collection f, g. So, claim is that K is the splitting field of the collection. Well with this case, just two elements f and g. So, let us just verify the two conditions quickly. A, both of them should split over this field. And that is fairly obvious, because over this field f splits as x minus root 2 into x plus root 2 and both

minus and plus root 2 are in this field.  $gx$  similarly splits as  $x$  minus  $i$  into  $x$  plus  $i$ . And again, it is easier to check  $B$  dash in this case rather than  $B$  itself.

(Refer Slide Time: 06:19)

$$\textcircled{B}': \mathbb{Q}(\sqrt{2}, i) = K$$

$$\mathbb{Q}(\sqrt{2}, -\sqrt{2}, i, -i) = K \quad \checkmark$$

$$\mathbb{Q} = F$$

Prop<sup>n</sup>: Let  $K/F$  be an algebraic ext<sup>n</sup>. The following are equivalent:
 

- (1)  $K/F$  is a normal ext<sup>n</sup>
- (2) Let  $L$  be an algebraic closure of  $K$ . For every  $\varphi: L \rightarrow L$  is an automorphism of  $L$  st  $\varphi|_F = \text{id}$  ( $F$ -automorphism), we have  $\varphi(K) = K$ .

Remark: We can replace  $\textcircled{B}$  by equivalent condition
   
 $\textcircled{B}'$ : The subfield of  $K$  generated by  $F$  and the roots of all the  $f_i, i \in I$  coincides with  $K$ .

Eg.  $F = \mathbb{Q}$      $K = \mathbb{Q}(\sqrt{2}, i)$      $K/F$  normal extension.
   
 Let  $f(x) = x^2 - 2$     and     $g(x) = x^2 + 1$ .
   
 $K$  is the splitting field of  $\{f, g\}$ :
 
$$\textcircled{A} \quad \begin{aligned} f(x) &= (x - \sqrt{2})(x + \sqrt{2}) \\ g(x) &= (x - i)(x + i) \end{aligned}$$

So, what  $B$  dash says, is that if you take this field  $Q$ , so, what is this field  $K$  that we are talking about?  $Q$  of root 2,  $i$  and we have  $Q$  here. So, what it says is, if you consider, so this is your  $K$ , this is your  $F$ , you take the subfield of  $K$  which is generated by  $Q$  together with the roots of all these polynomials. So, what were the roots? They were plus root 2 minus root 2  $i$  and minus  $i$ . If you adjoin the roots to  $Q$ , you take the subfield generated by this then it should give you all of  $K$ .

In this case, that is fairly obvious, because as soon as you adjoin root 2 and  $i$ , you get everything. So, this is in fact  $K$ . So, we have checked condition  $B$  dashed also. So, this is an

example of a normal extension. Now, this is a slightly unsatisfactory state of affairs, because to, to check or verify that something is a normal extension, what you have to do really is to hunt for some polynomials, you have to find a collection of polynomials for which this is the normal, I mean, for which there is a splitting field.

Of course, in practice, that is how we will construct examples, you pick some polynomials and look for sort of the splitting field of that entire collection. But sometimes we want a more intrinsic characterization, meaning, without having to look for those polynomials, maybe in terms of other sort of abstract characterizations, and this is sometimes useful. So, let me just formulate this characterization as a proposition. So, it says let  $K$  over  $F$  be an algebraic extension. Then the following statements are equivalent, statement 1 says this extension is normal  $K$  over  $F$  is a normal extension.

So being normal means of course, that it is a splitting field of a collection of polynomials. But the other additional thing I am talking about is point number 2 here, which says that if  $L$  is an algebraic closure. So, you take an algebraic closure of  $K$ , if  $L$  is an algebraic closure of  $K$ , and find from  $L$  to  $L$  is a field automorphism, is an automorphism of  $L$  such that, when you restrict it to the base field  $F$  you get the identity. So, this by the way, this sort of thing keeps occurring all the time and we usually give it a name. So, we say such a map is an  $F$  automorphism.

So, putting the  $F$  in front, just says that it acts as identity on  $F$  or it fixes  $F$  pointwise. So, given an  $F$  automorphism of the field  $L$ , we have, so, if  $L$  sorry, let me read this again, if  $L$  is an algebraic closure of  $K$  and  $\phi$  from maybe I should to rephrase it a little bit. So, let me say let  $L$  be an algebraic closure of  $K$ , then for every automorphism for every  $F$  automorphism of  $L$ , we have the following fact that  $\phi$  of  $K$  equals  $K$ . So probably you should just do this on a next page.

(Refer Slide Time: 10:28)

we have  $\varphi(K) = K$ .

(3)  $\forall \alpha \in K$ , the min poly  $m_\alpha(x) \in F[x]$  of  $\alpha$  over  $F$  splits completely over  $K$ .

Proof: (3)  $\Rightarrow$  (1): Consider  $\{m_\alpha(x) : \alpha \in K\} \subseteq F[x]$ .

Clearly, (3)  $\Rightarrow K$  is the splitting field of this collection.

(1)  $\Rightarrow$  (2) Let  $\{f_i(x) : i \in I\} \subseteq F[x]$  be such that  $K$  is its splitting field.

(3)  $\Rightarrow$  (1):

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2}, i) = K & & \mathbb{Q}(\sqrt{2}, -\sqrt{2}, i, -i) = K \quad \checkmark \\ | & & \\ \mathbb{Q} = F & & \end{array}$$

Prop<sup>n</sup>: Let  $K/F$  be an algebraic ext<sup>n</sup>. The following are equivalent:

(1)  $K/F$  is a normal ext<sup>n</sup>

(2) Let  $L$  be an algebraic closure of  $K$ . For every  $\varphi: L \rightarrow L$  is an automorphism of  $L$  st  $\varphi|_F = \text{id}$  ( $F$ -automorphism), we have  $\varphi(K) = K$ .

So, let me say for every  $F$  automorphism, we have  $\varphi(K) = K$ . So, every  $F$  automorphism of  $L$  always preserves  $K$ , that is the statement we want to make. And fact 3 says that for every  $\alpha$  in  $K$ , take any element of  $K$ . So, this is, this statement does not involve the algebraic closure, for every  $\alpha$  in  $K$ , the minimal polynomial  $m_\alpha(x)$ , this is a minimal polynomial of the element  $\alpha$  over the field  $F$ . The min poly  $m_\alpha(x)$  splits completely over  $K$ .

So, this is saying that if you can show that your extension is normal, that is if you can exhibit one set of polynomials for which it is a splitting field, then, in fact, no matter which  $\alpha$  you take from your field, its minimal polynomial will also split completely. In some sense, it

is a splitting field of every element if you can just take the entire collection. So, I mean, we are going to do that in just a moment. So, let me prove this. So, these are three equivalent characterizations. The second characterization is in terms of homomorphisms.

So, let us prove, we will prove it in the following way, we will show that 1 implies 2 implies 3 implies 1. That will show equivalence of all the statements. So, let me start by showing that 3 implies 1. So, suppose I know this, that for every  $\alpha$  in  $K$ , the min poly of  $\alpha$  over  $K$  splits completely over  $K$ . And now I need to show property 1, which is that  $K$  is a normal extension of  $F$ , which means I must exhibit a collection of polynomials for which  $K$  is the splitting field.

So now here, the collection of polynomials is obvious. So, consider the collection of polynomials, just take the minimal polynomials  $m_\alpha(x)$  for every  $\alpha$  in  $K$ . And this is a very large collection, if you will, of polynomials with coefficients in  $F$ . Clearly,  $K$  is the splitting field of this collection. Meaning when I say clearly, of course, I mean, assuming 3. So maybe I should say, clearly, if I assume 3, then it implies that  $K$  is the splitting field of this collection. Why? I need to check two properties, that every polynomial in my collection splits, that is what 3 says.

And the fact that it is a splitting field says that, if I take  $F$  and take the roots of all these polynomials, the field subfield they generate should be the whole field. But remember,  $\alpha$  is the root of  $m_\alpha(x)$ . So, what I am doing really is to  $F$ , I have to adjoin every single  $\alpha$  in my, in  $K$ . So of course, when I adjoin every  $\alpha$  in  $K$ , of course, I am going to get  $K$ . So, this is sort of the trivial direction such that, if you have this entire collection of minimal polynomials, splitting over  $K$ , then definitely it is a normal extension, because you can take that whole collection as your collection trivial.

Now, let us show 1 implies 2. So, this means that I am going to assume 1 that it is a normal extension, meaning there exists a collection for which it is a splitting field. And I will prove 2, which is that any homomorphism of the algebraic closure will have to preserve this subfield  $K$ . So, let us start with the definition, let  $f_i(x)$  ranging over some index set, subset of  $F[x]$  be such that  $K$  is its splitting field. And what are we supposed to do? We are supposed to take an algebraic closure.

(Refer Slide Time: 15:10)

Let  $L$  be an algebraic closure of  $F$ .  $\varphi: L \rightarrow L$  be  
an  $F$ -automorphism of  $L$ . Need to show:  $\varphi(K) = K$ .  
 $K =$  the subfield of  $L$  generated by  $F$  & the roots of  
all the  $f_i, i \in I$

If  $\alpha \in L$  is a root of  $f_i$ , then  $\varphi(\alpha)$  is a root of  $f_i$   
in  $L$ .

$$\Rightarrow \varphi(K) \subseteq F(\{\text{roots of } f_i, i \in I\}) = K$$

Repeat w/  $\varphi^{-1}$  in place of  $\varphi$ ;  $\varphi^{-1}(K) \subseteq K$   
 $\Rightarrow \varphi(K) = K$ .

$$\textcircled{B}: \mathbb{Q}(\sqrt{2}, i) = K$$

|

$$\mathbb{Q}(\sqrt{2}, -\sqrt{2}, i, -i) = K \quad \checkmark$$

$$\mathbb{Q} = F$$

Prop<sup>n</sup>: Let  $K/F$  be an algebraic ext<sup>n</sup>. The following are  
equivalent:

(1)  $K/F$  is a normal ext<sup>n</sup>

(2) Let  $L$  be an algebraic closure of  $K$ . For every

$\varphi: L \rightarrow L$  is an automorphism of  $L$  st  
 $\varphi|_F = \text{id}$  ( $F$ -automorphism), we have  $\varphi(K) = K$ .

we have  $\varphi(K) = K$ .

(3)  $\forall \alpha \in K$ , the min poly  $m_\alpha(x) \in F[x]$  of  $\alpha$  over  $F$  splits completely over  $K$ .

Proof:  $(3) \Rightarrow (1)$ : Consider  $\{m_\alpha(x) : \alpha \in K\} \subseteq F[x]$ .

Clearly, (3)  $\Rightarrow$   $K$  is the splitting field of this collection.

$(1) \Rightarrow (2)$  Let  $\{f_i(x) : i \in I\} \subseteq F[x]$  be such that  $K$  is its splitting field.



So, let us prove 2 now, to prove that we will start with an algebraic closure. So, let  $L$  be an algebraic closure of  $K$ . And let us take a automorphism of  $L$  which is identity on  $F$  be an  $F$  automorphism. Now we just need to show that  $\phi(K) = K$ . Now, need to show  $\phi(K) \subseteq K$ . So, this, this sort of argument already appeared, in fact, we need to show  $\phi(K) \supseteq K$ . So, this sort of argument already appeared when we were proving uniqueness of the splitting field. In fact, it is exact same argument. So, let us just quickly repeat it.

So, what is the argument  $K$  recall is nothing but the subfield of, well of itself if you wish, or the subfield of  $L$ , which is obtained as follows, you take  $F$ , and it is generated by  $F$  and the zeros of all these polynomials. So maybe I will just write it in words  $K$  equals the subfield of itself or  $L$ , that hardly matters. So,  $K$  is nothing but the subfield of  $L$  generated by  $F$  and the roots of all the  $f_i$ 's put together, but we observed the following statement that in the proof of the uniqueness of splitting fields, that if  $\alpha$  in  $L$  is a root of  $f_i$ , then  $\phi(\alpha)$  is also a root of  $f_i$ .

Well, in this case, again in  $L$ . Why is that? Because, I mean, in the earlier proof, it was  $L$  and  $L$  dash when we were trying to show uniqueness of splitting fields, here it is an automorphism both sides we have  $L$ . So, if  $\alpha$  is a root of  $f_i$ , then when you apply  $\phi$  to it, it continues to be a root of  $f_i$ , in again in  $L$ . And why was this? Because the map  $\phi$  was identity on the base field, it was identity on the coefficients. So, you concluded that  $\phi(\alpha)$  is again a root. So, what does that mean?

It says that, since  $K$  is just the subfield of  $L$  generate by  $F$  and all the roots of the  $f_i$ 's, then you apply  $\phi$  to  $K$ , which means, you have to apply  $\phi$  to all the roots of all the  $f_i$ 's and see what you get. But the roots of  $f_i$ 's under  $\phi$ , map again to the roots of  $f_i$ 's. So,  $\phi$  is sort of




preserves the set of all the roots of all the  $f_i$ 's, that collection is preserved by  $\phi$ . So, when you apply  $\phi$  to  $K$ , what are you going to get? Well, you, the image certainly lies inside the subfield. So,  $\phi$  maps  $F$  to  $F$  also, its identity on  $F$ .

So,  $F$  goes to  $F$  and the roots of  $f_i$  map back to the roots of  $f_i$ . So, it is just the subfield generated by  $F$  and, well, again, the roots of  $f_i$ . But that is exactly  $K$  once more. So, if you see if you look back, it is the same proof really for the uniqueness as well. So,  $\phi(K)$  is a subset of  $K$ . And now we repeat the argument with  $\phi^{-1}$  in place of  $\phi$ , repeat with  $\phi^{-1}$  in place of  $\phi$ . And well, when you do that, what do you conclude?

You conclude that  $\phi^{-1}(K)$  is a subset of  $K$  and therefore,  $\phi(K)$  is equal to  $K$ . And that is exactly what we needed to prove in part two of this proposition that  $\phi$ , whenever you take an automorphism an  $F$  automorphism of  $L$ , then  $K$  is preserved by that automorphism. So that is, that is two parts of what we need to show, 3 implies 1, 1 implies 2 and let us finish this off by showing that 2 implies 3.

(Refer Slide Time: 19:54)

$(2) \Rightarrow (3)$



let  $\alpha \in K$  & let  $m_\alpha(x)$  be its min poly over  $F$ .

$\uparrow$   
 $F[X]$


⊙ Suppose  $m_\alpha(x)$  does not split completely over  $K$ . — (\*)

$L$	$L$	$\alpha_2$	Since $L$ is algebraically closed, $m_\alpha(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in L$
$ $	$ $	$ $	
$K$	$K$	$ $	
$ $	$ $	$ $	
$F$	$F$	$m_\alpha(x)$	

Assume  $\alpha_1 = \alpha$

By (\*),  $\exists$  some  $\alpha_i \notin K$

say:  $\alpha_2 \notin K$ .




$\text{Ex: } \mathbb{Q}(\sqrt{2}, i) = K$   
 $\mathbb{Q}(\sqrt{2}, -\sqrt{2}, i, -i) = K$  ✓  
 $\mathbb{Q} = F$

Prop<sup>n</sup>: Let  $K/F$  be an algebraic ext<sup>n</sup>. The following are equivalent:

- (1)  $K/F$  is a normal ext<sup>n</sup>
- (2) Let  $L$  be an algebraic closure of  $K$ . For every  $\alpha \in L$ , if  $m_\alpha(x)$  is the minimal polynomial of  $\alpha$  over  $F$ , then  $m_\alpha(x)$  splits completely in  $L$ .

$\varphi: L \rightarrow L$  is an automorphism of  $L$  st  $\varphi|_F = \text{id}$  ( $F$ -automorphism), we have  $\varphi(\alpha) = \alpha'$



So, what does this mean? We have to assume part two, which means that, this stability under automorphisms under  $F$  automorphisms. And we need to show 3, which is that every element  $\alpha$ , so take an element  $\alpha$  in  $K$ , and look at its minimal polynomial, be it is minimal polynomial over the base field  $F$ . So, in other words, this is an irreducible polynomial, irreducible monic polynomial satisfied by  $\alpha$  coefficients in  $F$ .

Now, we need to show that  $m_\alpha$  splits completely over  $K$ . So, let us assume the contrary suppose  $m_\alpha$  of  $x$  does not split. Now, what does that really mean? Well, it says, so remember,  $L$  is the algebraic closure, I have  $K$ , I have  $F$ . Now I have this polynomial  $m_\alpha$ . And there is an element  $\alpha$  in  $K$ ,  $\alpha$  is the element I started off with, the polynomial  $m_\alpha$  of  $x$ . Well, that is got coefficients in  $F$ , so maybe I will write it down to as  $m_\alpha$  of  $x$  is a polynomial with coefficients in  $F$ ,  $m_\alpha$  has certainly one root in  $K$ , because  $\alpha$  is certainly a root of  $m_\alpha$ .

But what we are assuming here is that  $m_\alpha$  does not split over  $K$ . In other words, when I write out the factorization of  $m_\alpha$  of  $x$  into a product of irreducible over  $K$ , all factors are not linear, I do not get  $n$  roots in  $K$ . So not all roots of  $m_\alpha$ , lie in  $K$ . So, some roots, you will only see in higher extension fields. So, in particular, I will certainly find all  $n$  roots in  $L$  for sure. So, let us let us go to  $L$  so that  $m_\alpha$  splits completely there.

So, since  $L$  is algebraically closed, here is what I know,  $m_\alpha$  of  $x$  will certainly be, I can write it as  $(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$ . So, I am just going to assume, I mean,  $m_\alpha$  is of course monic here, because it is a minimal polynomial for some  $\alpha_1, \alpha_2, \dots, \alpha_n$  coming from the algebraic closure.

Now let us, let us assume that the first root  $\alpha_1$  is  $\alpha$  here. That is the  $\alpha$  I began with. So, let us let us call  $\alpha_1$  as that  $\alpha$ . Now, the assumption we have made  $m_\alpha$  does not split completely over  $K$  means that at least one of these  $\alpha_i$ 's is not in  $K$ . So, by assumption, so maybe I should call this something star by star there exists some  $\alpha_i$  which is not in  $K$ .

So, let me just call it  $\alpha_2$ , say, let us just remember our  $\alpha$ 's if necessary, and say  $\alpha_2$  is not in  $K$ . So  $\alpha_1$  is in  $K$ , but  $\alpha_2$  is not in  $K$ . And that is somehow the the key point here. So, I have  $L, K, F$ . And the situation is I have one root in  $K$ . And I find another root, which is not in  $K$ , but, you know, sort of outside  $K$ , it is only in  $L$ , for example, whatever it is, it is not in  $K$ , it is outside is what I meant.

Now, this is going to be what we will use in order to get a contradiction, we will contradict the hypothesis 2, and what did the hypothesis say? It said that every homomorphism, let us go back and see every homomorphism or automorphism of  $L$ , which preserves  $F$  pointwise must map  $K$  to itself. Now, because we now have  $\alpha_1$  in  $K$ , and  $\alpha_2$ , which is not in  $K$ , let us sort of use these two  $\alpha$ 's to define a homomorphism. So, the idea is to try and define a homomorphism, which will map  $\alpha_1$  to  $\alpha_2$ . If you can do that, then we would have somehow gotten a contradiction to 2. So that is what we will try and do now.

(Refer Slide Time: 25:02)

Recall: (1) Since  $\alpha_1$  and  $\alpha_2$  have the same minimal poly over  $F$ ,  $\exists$  an isomorphism

$m_\alpha(x)$   
 $(\approx \frac{F[x]}{(m_\alpha(x))})$

$\varphi: F(\alpha_1) \rightarrow F(\alpha_2)$   
 with  $\varphi(\alpha_1) = \alpha_2$ .

$$\begin{array}{ccc}
 L & & L \\
 | & & | \\
 F(\alpha_1) & \xrightarrow{\varphi} & F(\alpha_2) \\
 | & & | \\
 F & \xrightarrow{id} & F
 \end{array}$$

(2)



So, again recall from the previous or initial discussions on adjoining symbolic adjunction of roots and so on, that if  $\alpha_1$ , so, since  $\alpha_1$  and  $\alpha_2$  are both roots, they both have the same minimal polynomial over  $F$ . Because of course, what is the minimal polynomial? That is what we call  $m_\alpha$  of  $x$ , both of them are roots of that and  $m_\alpha$  is irreducible.


So, it must be the minimal polynomial of  $\alpha_2$  as well. So, since they both have the same minimal polynomial, we know that there exists an isomorphism of fields, from where to where? From  $F$  adjoined  $\alpha_1$  to the field  $F$  adjoined  $\alpha_2$ .

And you can, you can either think of this symbolically, so what is, so I want to say, think of all these sitting inside  $L$  for example, for the moment forget  $K$ . So, there is  $F$  here. So, we will bring  $K$  back into the picture afterwards. But for now, just look at  $F$  adjoined  $\alpha_1$  and  $F$  adjoined  $\alpha_2$ , what we know is that there is an isomorphism between  $F$  adjoined  $\alpha_1$  and  $F$  adjoined  $\alpha_2$ , which is identity on  $F$ . So, there is an  $F$  isomorphism, it is called this map  $\phi$ , there exists an isomorphism  $\phi$  from  $F$  adjoined  $\alpha_1$  to  $F$  adjoined  $\alpha_2$ .

So, recall this this statement. So, recall from the initial discussion on adjunction and so on, and if you quickly recall why this was the case, because, in fact, both of these fields are, abstractly isomorphic to the field  $F[x]$  the polynomial ring modulo the ideal generated by  $m$  adjoined  $x$ .  $m$  adjoined  $x$  is the maximal ideal here. And so, these both these guys are actually isomorphic to this abstract field  $F[x]$  modulo  $m$  adjoined  $x$ .

So that is, that is how one sort of deduce that. So, there is an isomorphism, further with an additional property such that it maps  $\alpha_1$  to  $\alpha_2$  with  $\phi$  of  $\alpha_1$  equals  $\alpha_2$ . So, this is the key property that we will use now. So, I am guaranteed that such a such a map exists. Now, so this is sort of the first statement to recall.

(Refer Slide Time: 28:12)

Given an isomorphism  $\varphi: F(\alpha_1) \rightarrow F(\alpha_2)$ ,  $\exists \tilde{\varphi}: L \rightarrow L$  

$$\begin{array}{ccc} L & \xrightarrow{\tilde{\varphi}} & L \\ | & & | \\ F(\alpha_1) & \xrightarrow{\varphi} & F(\alpha_2) \end{array} \quad \text{st} \quad \tilde{\varphi}|_{F(\alpha_1)} = \varphi.$$

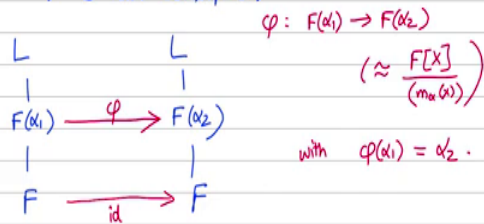
Observe  $\tilde{\varphi}: L \rightarrow L$   $\tilde{\varphi}(\alpha_1) = \varphi(\alpha_1) = \alpha_2$

Our Assumption  $\alpha_1 \in K$   $\alpha_2 \notin K$

$\Rightarrow \tilde{\varphi}(K) \neq K$ . Contradicts (2) ■



Recall: (1) Since  $\alpha_1$  and  $\alpha_2$  have the same minimal poly over  $F$ ,  $\exists$  an isomorphism



(2)

we have  $\varphi(K) = K$ .

(3)  $\forall \alpha \in K$ , the min poly  $m_{\alpha}(x) \in F[X]$  of  $\alpha$  over  $F$  splits completely over  $K$ .

Proof: (3)  $\Rightarrow$  (1): Consider  $\{m_{\alpha}(x) : \alpha \in K\} \subseteq F[X]$ .

Clearly, (3)  $\Rightarrow K$  is the splitting field of this collection.

(1)  $\Rightarrow$  (2) Let  $\{f_i(x) : i \in I\} \subseteq F[X]$  be such that  $K$  is its splitting field.

Now, the second statement, given an isomorphism. So, given an isomorphism from one field to another, this case,  $F \alpha_1$  to  $F \alpha_2$ , so, I am given an isomorphism of fields, then it extends to an isomorphism of their algebraic closures. Now, in this case,  $L$  is the algebraic closure of both  $F \alpha_1$  and  $F \alpha_2$ . So, the universal property says that  $\varphi$  extends to an isomorphism of  $L$ , to an automorphism of  $L$  if you wish.

Well, in this case, I have taken  $L$  to be the universal, to be the algebraic closure on both sides. So, given an isomorphism  $\varphi$  from  $F \alpha_1$  to  $F \alpha_2$  there exists  $\tilde{\varphi}$  from  $L$  to  $L$ , such that  $\tilde{\varphi}$  when you restrict it to  $F \alpha_1$ , it coincides with the map  $\varphi$ . So, this is the other property that we need to recall in the construction of algebraic closures. But now observe that this exactly contradicts, the hypothesis 2.

So now observe that this map  $\tilde{\phi}$  from  $L$  to  $L$ , it is an automorphism of  $L$  does the following, it maps well it it coincides with  $\phi$  on  $F$   $\alpha_1$ , so this just does whatever  $\phi$  does to  $\alpha_1$ . And remember that is the special property of  $\phi$  that we talked about is that it maps  $\alpha_1$  to  $\alpha_2$ . So,  $\tilde{\phi}$  maps  $\alpha_1$  to  $\alpha_2$  in particular, recall, we assumed that  $\alpha_1$  was an element of  $K$  and  $\alpha_2$  was not an element of  $K$ . This was our assumption. So, this is what we had assumed. So, our assumption was that this happens.

So, what does this mean? This says that  $\tilde{\phi}$  of  $K$  is not  $K$ , it is mapping one element of  $K$  to an element that is outside  $K$ . And so, this contradicts our hypothesis 2 and completes the proof of this proposition. So normal extensions are, well, they can be thought of as splitting fields of collections of polynomials. But in terms of homomorphisms, they are also sort of the extensions with the property that automorphisms of the algebraic closure always leave, normal extensions, stable, they fix them, automorphisms which are identity on the base field.

And so, in some sense, the remarkable point, one other little remark here, is that this last point here is also rather remarkable, it says that, if your extension is normal, so it is the splitting field of a collection of polynomials, then every  $\alpha$  in in the field has a minimal polynomial, which also splits completely, which means that if one root I mean  $\alpha$  is of course, one root of its minimal polynomial, what we are saying is that all the roots of that minimal polynomial must actually belong to the, the field  $K$ . And so that is somewhat remarkable.

(Refer Slide Time: 31:35)

Eg  $K = \mathbb{Q}(\sqrt{2}, i)$   $\alpha = 1 + \sqrt{2} + 3i \in K$

|

$\mathbb{Q}$

$m_\alpha(x)$  over  $\mathbb{Q}$

All roots of  $m_\alpha(x)$  lie in  $K$ .

So, for example, if you recall the example of a normal extension we gave, if you take the field  $\mathbb{Q}$  and adjoin both  $\sqrt{2}$  and  $i$  to it. I think of it as a normal extension of  $\mathbb{Q}$ . So of course, you know, we exhibited those two special polynomials for which this is the splitting field, but the third equivalent property of this proposition says you can in fact take any  $\alpha$  you want in this field  $K$ . For example, I can take  $\alpha$  to be  $\sqrt{2} + 3i$ , this is an element of  $K$  or in fact, more general combinations, if you wish, say  $1 + \sqrt{2} + 3i$  is another element.

So, suppose I pick this element  $\alpha$  in my field  $K$ , then what it says is, you look at its minimal polynomial  $m_\alpha(x)$  over  $\mathbb{Q}$ . So, this is the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$ , then all roots of this minimal polynomial will also lie in this field  $K$ . So, all roots of  $m_\alpha(x)$  lie in  $K$ . So, it or in other words the minimal polynomial splits completely over  $K$ , that is what it means. Well, it is somewhat remarkable because what it says that the other roots are the, sometimes we call it the other conjugates of  $\alpha$ , the other roots of its minimum polynomial are also somehow combinations of  $\sqrt{2}$  and  $i$  e for example, that is what this proposition is saying.