# Introduction To Rings And Fields

Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

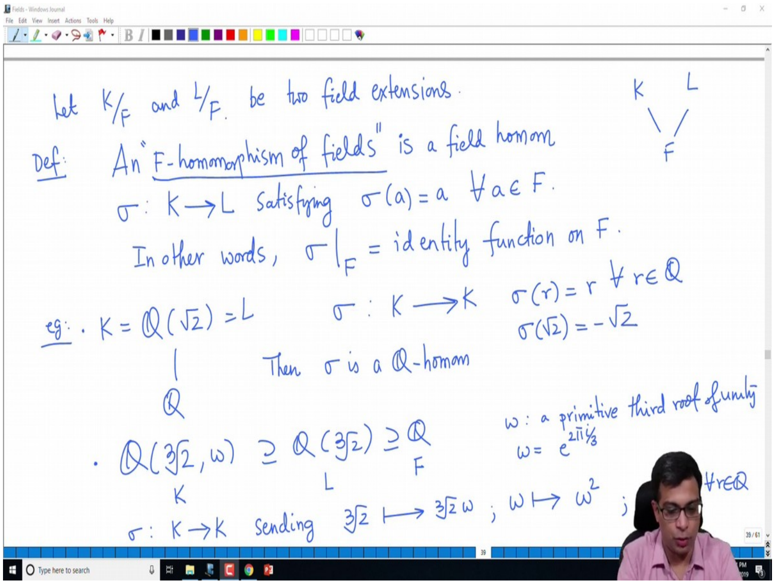
## Lecture - 38
## Field homomorphisms

Let us continue now our study of fields. So, far we defined what field extensions are and we learned that those are the main objects of studying field theory. We learned what algebraic and transcendental extensions are. If an element is algebraic, we learned what its degree over the base field is; we also learned what the degree of a field extension is.

This is just the dimension of the bigger field when it is considered as a vector space over the smaller field. We learned that the degree is multiplicative; we learned that finite extensions are algebraic. We also learned that if you have a field extension the elements in the bigger field that are algebraic over the base field are a subfield of the bigger field.

Today, we are going to continue to study a very important notion called homomorphism of field over a fixed based field. So, I have written some of these things already. So, let me just go through this carefully.

(Refer Slide Time 01:07)



Let $K/F$ and $L/F$ be two field extensions.

$$\begin{tikzcd} K \arrow[dr, dash] & & L \arrow[dl, dash] \\ & F & \end{tikzcd}$$

Def: An "F-homomorphism of fields" is a field homom $\sigma : K \to L$ satisfying $\sigma(a) = a \ \forall a \in F$.

In other words, $\sigma|_F$ = identity function on F.

eg: . $K = \mathbb{Q}(\sqrt{2}) = L$ $\sigma : K \longrightarrow K$ $\sigma(r) = r \ \forall r \in \mathbb{Q}$
$\sigma(\sqrt{2}) = -\sqrt{2}$

$$\begin{tikzcd} \mathbb{Q}(\sqrt{2}) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

Then $\sigma$ is a $\mathbb{Q}$-homom

. $\underset{K}{\mathbb{Q}(\sqrt[3]{2}, \omega)} \supseteq \underset{L}{\mathbb{Q}(\sqrt[3]{2})} \supseteq \underset{F}{\mathbb{Q}}$ $\omega$ : a primitive third root of unity
$\omega = e^{2\pi i/3}$

$\sigma : K \to K$ sending $\sqrt[3]{2} \longmapsto \sqrt[3]{2}\omega$ ; $\omega \mapsto \omega^2$ ; $\forall r \in \mathbb{Q}$

So, let us take two field extensions K over F and L over F. So, the base field is the same. And we have two fields above it K and L. There is no containment among K and L. So, K and L are just field extensions of F. An F-homomorphism of fields between K and L is a field homomorphism, it is not merely a field homomorphism, but it has an additional property that it fixes every element of F, ok.

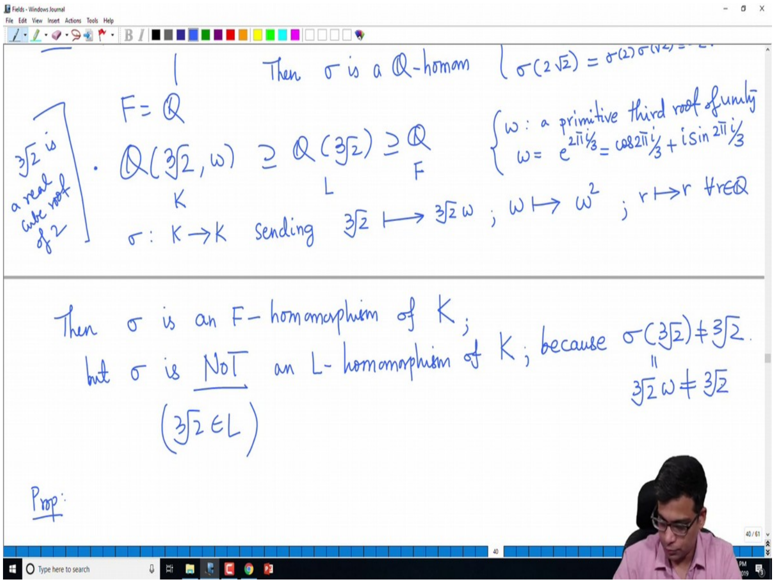
So, remember what a field homomorphism is, it is any ring homomorphism that is all, there is no additional property for a field homomorphism. But an F-homomorphism, so this F is important here, it is more than a field homomorphism. This F refers to the base field for both K and L. It is an F-homomorphism, if it fixes F point wise, or in other words, sigma restricted to F is the identity function on F, ok.

So, it simply means that sigma of every element of F is itself; it is not allowed to change elements of F. So, a couple of quick examples, you take the field Q adjoined root 2 over Q ok. So, take that to be K and L. And F is K, F is Q. And look at the homomorphism, it is sends rational numbers to rational numbers rational numbers to itself every rational goes to itself, but root 2 maps to minus root 2 remember that every element of K is a polynomial in root 2 with coefficients in Q.

So, if I tell you what the image of R is for every rational number R, and what image of root 2 is it suffices to completely and uniquely determine what the image of every element of K is, because sigma is a field homomorphism. It should send 2 times root 2 to I do not need to separately say what it is. It should be 2 times, it should be a sigma of 2 times sigma of root 2, that means, it should be minus 2 root 2.

Similarly, sigma of 3 times root 2 plus 5 and so on. And I claim that that is a Q homomorphism that is because it fixes R by definition every element of Q is fixed. So, as an exercise later we will do this, and you should think about this before that. Any homomorphism of an extension field of Q is automatically Q, Q-homomorphism. So, in other words Q is automatically fixed by a field homomorphism; you do not need to ask for it separately. On the other hand, let us look at another example.

(Refer Slide Time 03:49)



Then $\sigma$ is a $\mathbb{Q}$-homom ( $\sigma(2\sqrt{2}) = \sigma(2)\sigma(\sqrt{2})$

$F = \mathbb{Q}$

$\sqrt[3]{2}$ is a real cube root of 2 . $\underset{K}{\mathbb{Q}(\sqrt[3]{2}, \omega)} \supseteq \underset{L}{\mathbb{Q}(\sqrt[3]{2})} \supseteq \underset{F}{\mathbb{Q}}$

$\begin{cases} \omega : \text{a primitive third root of unity} \\ \omega = e^{2\pi i/3} = \cos 2\pi i/3 + i \sin 2\pi i/3 \end{cases}$

$\sigma : K \to K$ sending $\sqrt[3]{2} \longmapsto \sqrt[3]{2}\,\omega$ ; $\omega \mapsto \omega^2$ ; $r \mapsto r \ \forall r \in \mathbb{Q}$

Then $\sigma$ is an F-homomorphism of K;

but $\sigma$ is $\underline{\text{NOT}}$ an L-homomorphism of K; because $\sigma(\sqrt[3]{2}) \neq \sqrt[3]{2}$.

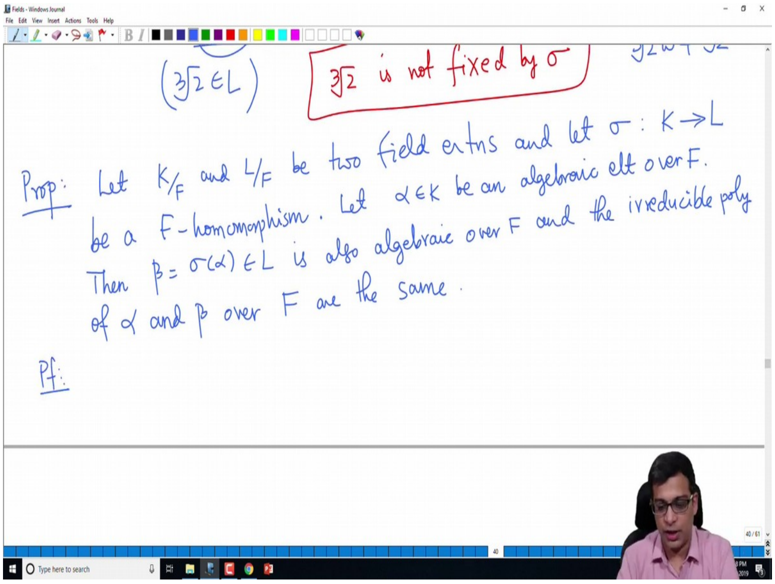
$(\sqrt[3]{2} \in L)$ $\quad \sigma(\sqrt[3]{2}) = \sqrt[3]{2}\,\omega \neq \sqrt[3]{2}$

Prop:

Let us look at the field Q adjoined cube root of 2 and omega, where cube root of 2; cube root of 2 is a real cube root of 2. There are 3 cube roots of 2, let us take the real one and adjoin omega which is a primitive third root of unity. And if you recall that just e over 2 pi i by 3. This is just cosine 2 pi i by 3 plus i sin 2 pi i by 3. And then let us call this will K, L and F respectively. And let us look at the function from K to K with sends cube root of 2 to cube root of 2 omega, omega to omega squared and R rational number to itself.

So, later on you will see why I have chosen these particular images. And just like in the previous example, it suffices to describe the images of these generators cube root of omega, and tell what the image is of rational numbers are, to uniquely determine the entire homomorphism. Then if you think about it, sigma is an F-homomorphism of K, F being the rational numbers because rational numbers are fixed, but it is not an L-homomorphism of K, because cube root of 2 is in L and cube root of 2 does not go to itself right. Cube root of 2 in fact goes to cube root of 2 omega which is not cube root of 2 ok. So, cube root of 2 is not fixed by sigma that is the notation we language we want to use.

(Refer Slide Time 05:23)



$(\sqrt[3]{2} \in L)$

$\boxed{\sqrt[3]{2} \text{ is not fixed by } \sigma}$

**Prop:** Let $K/F$ and $L/F$ be two field extns and let $\sigma : K \to L$ be a F-homomorphism. Let $\alpha \in K$ be an algebraic elt over F. Then $\beta = \sigma(\alpha) \in L$ is also algebraic over F and the irreducible poly of $\alpha$ and $\beta$ over F are the same.

**Pf:**

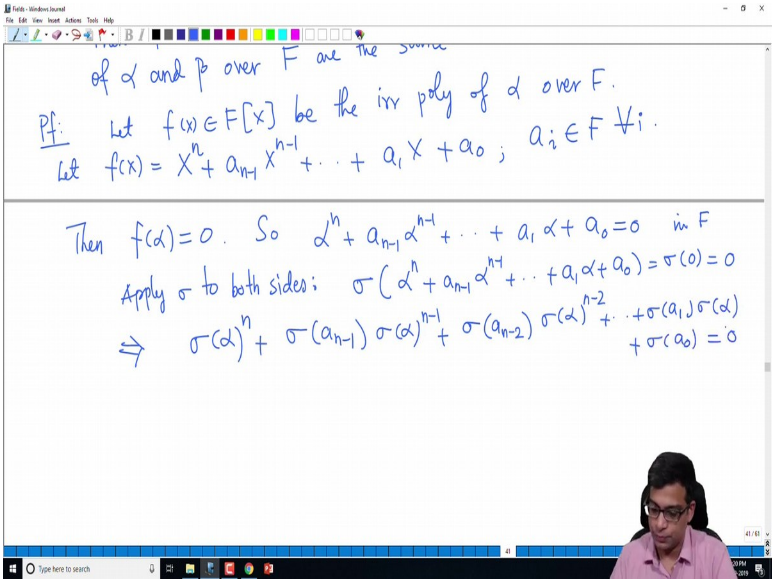
So, cube root of 2 is not fixed by sigma. So, in order to be an L-homomorphism every element of L has to be fixed by sigma. In this case, it is not so, it is not L L-homomorphism nevertheless it is a K-homomorphism. So, now, I am going to do a very important proposition which will describe to us what are the possible images of elements are for an F-homomorphism and that it also explain why I have chosen these particular images for cube root of 2 and omega.

So, let us take the following statement: let K over F and L over F be two field extensions, and let sigma from K to L be a field or rather F-homomorphism. So, in particular, it is a homomorphism of fields which fixes every element of F. Then let alpha be in K and let beta be equal to sigma alpha there is of course in L. Then the proposition says the irreducible polynomials, ok. So, I am actually, I should write here, let alpha be an irreducible element, sorry let alpha be an algebraic element over F.

Let us take an algebraic element. I am working in general with an arbitrary field extension which may not be algebraic, but alpha needs to be algebraic. Then beta which is sigma alpha and which is an L is also algebraic over F, so image of an algebraic element is algebraic and moreover the irreducible polynomials of alpha and beta over capital F are the same.

So, this is a very large restriction on what can be the possible image of an element in capital K, as long as it is algebraic that restriction applies. So, let us prove this. So, what we are saying is that image of an algebraic element is algebraic and moreover its irreducible element must be the same as irreducible element of, sorry it is irreducible polynomial is same as irreducible polynomial of alpha.

(Refer Slide Time 08:14)



of $\alpha$ and $\beta$ over F are the same

Pf: Let $f(x) \in F[x]$ be the irr poly of $\alpha$ over F.

Let $f(x) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ ; $a_i \in F \ \forall i$.

Then $f(\alpha) = 0$. So $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ in F

Apply $\sigma$ to both sides: $\sigma(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) = \sigma(0) = 0$

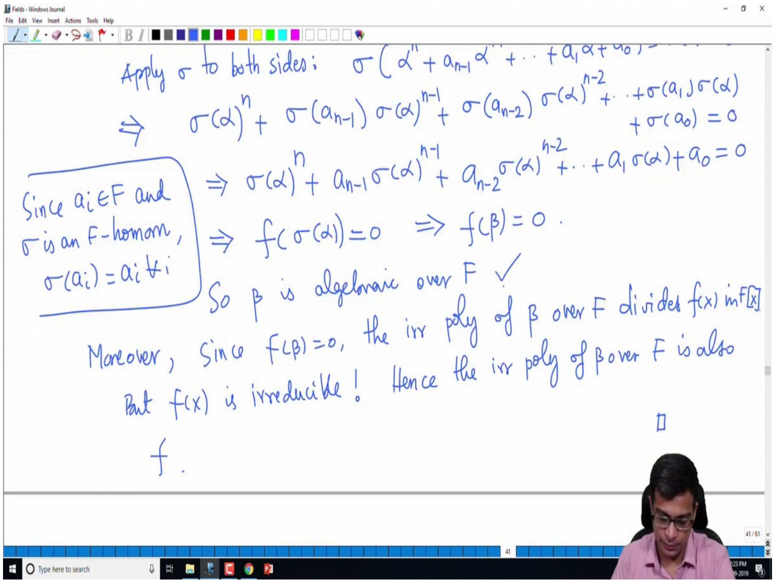
$$\Rightarrow \sigma(\alpha)^n + \sigma(a_{n-1})\sigma(\alpha)^{n-1} + \sigma(a_{n-2})\sigma(\alpha)^{n-2} + \cdots + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) = 0$$

And the proof is very simple. So, let f X be the irreducible polynomial of alpha over F. So, what do we know we know that we write f X as a monic right irreducible polynomial is by definition monic. So, we can write it like this a X n a n minus 1 X n minus 1 plus dot dot dot a 1 X plus a 0. And what do we know about a i's there in F for all i right, because it is the irreducible polynomial over capital F. So, x a i's for an capital F.

So, then we know f alpha is 0, because it is irreducible polynomial of alpha that means, alpha is a root. So, alpha power n plus a n minus 1 alpha power n minus 1 plus dot dot dot plus a 1 alpha plus a 0 is 0. So, this is a inequality in capital F. Now, we will apply sigma to both sides.

If we apply sigma to both sides, what do we get sigma of alpha power n a n minus 1 alpha power n minus 1, a 1 alpha plus a 0 is sigma of 0. Sigma being a field homomorphism which is a ring homomorphism sends 0 to 0. This means and also because sigma is a homomorphism, you can put it inside the bracket and write this as sigma alpha power n sigma a n minus 1 sigma alpha power n minus 1 plus I will write one more term sigma a n minus 2 sigma alpha n minus 2 plus plus plus dot dot dot sigma a 1 sigma alpha plus sigma a 0 equal to 0.

(Refer Slide Time 10:16)



Apply $\sigma$ to both sides: $\sigma(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0)$

$$\Rightarrow \sigma(\alpha)^n + \sigma(a_{n-1})\sigma(\alpha)^{n-1} + \sigma(a_{n-2})\sigma(\alpha)^{n-2} + \cdots + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) = 0$$

Since $a_i \in F$ and $\sigma$ is an $F$-homom, $\sigma(a_i) = a_i \; \forall i$

$$\Rightarrow \sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + a_{n-2}\sigma(\alpha)^{n-2} + \cdots + a_1\sigma(\alpha) + a_0 = 0$$

$$\Rightarrow f(\sigma(\alpha)) = 0 \Rightarrow f(\beta) = 0.$$

So $\beta$ is algebraic over $F$ ✓

Moreover, Since $f(\beta) = 0$, the irr poly of $\beta$ over $F$ divides $f(x)$ in $F[x]$

But $f(x)$ is irreducible! Hence the irr poly of $\beta$ over $F$ is also $f$.

□

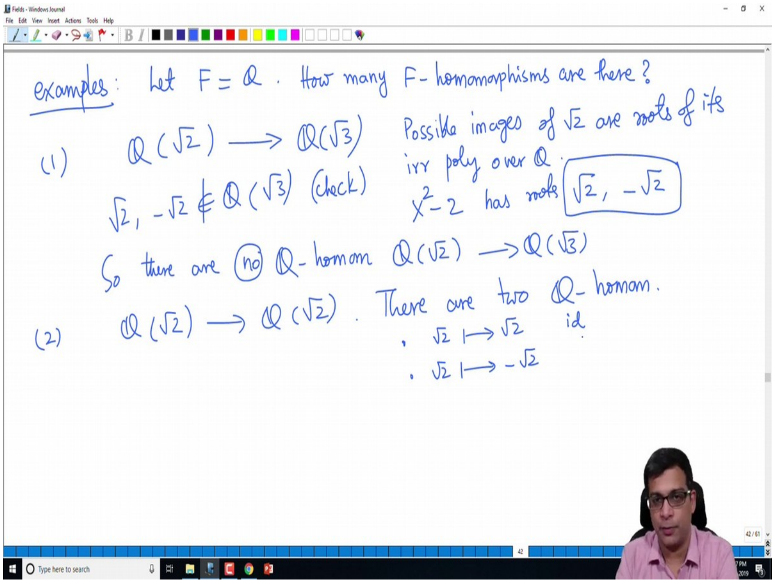
Now, what do (Refer Time: 10:14) about sigma a i’s since a i is in capital F and sigma is an F-homomorphism, what is an F-homomorphis, it fixes every element of F right a i's or n f sigma is an F-homomorphism. So, it fixes every element of F in particular it fixes a i. So, now, I can rewrite this as sigma alpha power n plus a n minus 1 sigma alpha power n minus 1 a n minus 2 sigma alpha n minus 2 plus a 1 sigma alpha plus a 0 equal to 0.

So, I have just written sigma n minus 1 as a n minus 1, sigma n minus 2 as n minus 1 n minus 2 here, sigma a 1 as a 1 sigma a 0 as a 0. This is a very simple proof, but it is an extremely important proposition, this means f of sigma alpha is 0, but what is sigma alpha, I have called it beta. So, f of beta is 0. So, immediately we see that beta is algebraic over F.

The first statement is now clear right, because f is a polynomial in capital F X and beta is a root of it. So, it is algebraic over this. Moreover, since f beta is 0, the irreducible polynomial of beta over capital F divides f X in capital F X right, because it is the irreducible f beta is 0, that means, beta is a root of f. And irreducible polynomial of beta divides every polynomial which has beta as root. So, it divides f X also. But what is f X? f X is irreducible, because it is the irreducible polynomial of alpha. So, it is irreducible, that means, the irreducible polynomial of alpha of beta over F is also f, that completes the proof, ok.

So, the proposition is saying that if you have an F-homomorphism from K to L an algebraic element goes to an algebraic element, and the irreducible polynomial of both elements are same and that is a reason why I cannot arbitrarily choose anything I want as a image of cube root 2 in this example. Because, what is irreducible polynomial of cube root of 2, I will come back to this and write it again, but it is X cube minus 2; so, image of cube root of 2 has to be another root of that polynomial. Similarly, image of omega has to be another root of its irreducible polynomial and so omega squared is a possibility, ok.

(Refer Slide Time 13:22)



examples: Let $F = \mathbb{Q}$. How many F-homomorphisms are there?

(1) $\mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{3})$ Possible images of $\sqrt{2}$ are roots of its irr poly over $\mathbb{Q}$.

$\sqrt{2}, -\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$ (check) $X^2 - 2$ has roots $\boxed{\sqrt{2}, -\sqrt{2}}$

So there are no $\mathbb{Q}$-homom $\mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{3})$

(2) $\mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})$. There are two $\mathbb{Q}$-homom.

- $\sqrt{2} \longmapsto \sqrt{2}$ id.
- $\sqrt{2} \longmapsto -\sqrt{2}$

So, as examples to illustrate this how limited a field homomorphism are; F-homomorphisms are, because of this very strong restriction on what the image of an element is. So, let me do a few examples. First one is let us list all; so, every example here is for extensions of Q. So, in these examples, I want to determine how many F-homomorphisms are there. So, I will give you two extensions of Q. And in each case, I want to determine how many F homomorphisms are there. For example, let us take cube root of 2 to let us make take square root of 2 square root of 3, ok.

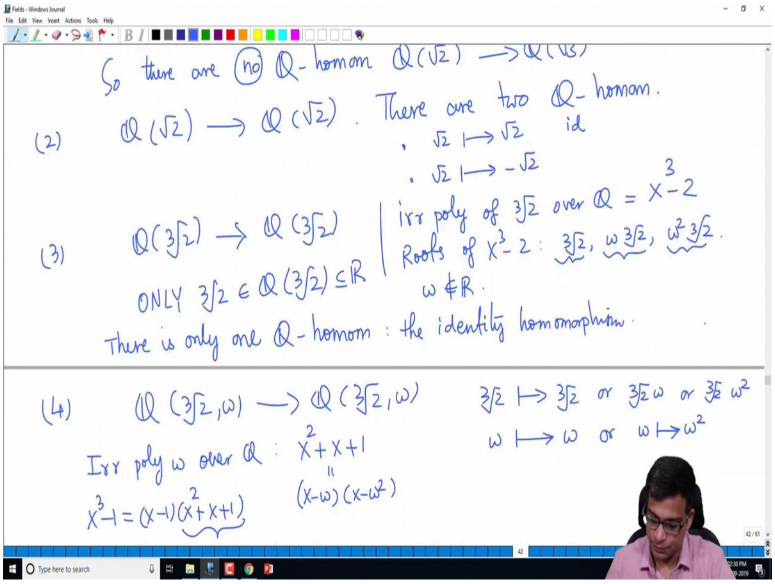
So, remember it is supposed to be a Q-homomorphism. So, Q must go to Q by identity map, it fixes Q in other words. Root 2 can go to something, possibly images of root 2 are roots of its irreducible polynomial; remember root 2 is algebraic. So, we can apply the previous proposition irreducible polynomial over Q. What is the irreducible polynomial of root 2 over Q, it is X squared minus 2, this we know, because it is a root of this and clearly this is irreducible because it has no roots in Q.

So, what are roots of this? It has two roots right, minus root 2 and root 2. So, only possible images of root 2 are root 2 and minus root 2, are any of them available here, no, both root 2 and minus root 2 are not in Q adjoined root 3. Get this requires a little check to be precise. We have to check this because Q root 3 is all polynomials in root 3 of degree 1. So, it is a plus b root 3, where a and b are rational numbers. There is no a and b rational numbers such that a plus b root 3 is either equal to root 2 or minus root 2.

So, this I will leave as an exercise for you check this. So, that means, there are no possible images for root 2 in this field. So, there are no Q-homomorphism from Q root 2 to Q root 3 that is all. There are no homomorphisms, because root 2 can go to either root to or minus root 2 and neither of them is in Q root 3 ok, so that means, there is no homomorphism. So, the number of homomorphisms is 0 in the first example.

What about root 2 to root 2; here there are two Q homomorphisms right; one sending root 2 to root 2, the other sending root 2 to minus root 2. As a previous example shows the possible images are root 2 and minus root 2; in the first example root 2 and minus root 2 are not here; in the second example they are there. So, I can send it to this. So, this is the identity map and this is another map. Remember I am not specifying what images of Q are, because they are supposed to be fixed. So, all I need to say is what is the image of root 2.

(Refer Slide Time 17:04)



So there are $\boxed{\text{no}}$ $\mathbb{Q}$-homom $\mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{3})$

(2) $\mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})$. There are two $\mathbb{Q}$-homom.

- $\sqrt{2} \longmapsto \sqrt{2}$ id
- $\sqrt{2} \longmapsto -\sqrt{2}$

(3) $\mathbb{Q}(\sqrt[3]{2}) \rightarrow \mathbb{Q}(\sqrt[3]{2})$ | irr poly of $\sqrt[3]{2}$ over $\mathbb{Q}$ = $X^3 - 2$

Roots of $X^3 - 2$ : $\underbrace{\sqrt[3]{2}}$, $\underbrace{\omega \sqrt[3]{2}}$, $\underbrace{\omega^2 \sqrt[3]{2}}$.

ONLY $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ | $\omega \notin \mathbb{R}$.

There is only one $\mathbb{Q}$-homom : the identity homomorphism.

(4) $\mathbb{Q}(\sqrt[3]{2}, \omega) \longrightarrow \mathbb{Q}(\sqrt[3]{2}, \omega)$ $\quad$ $\sqrt[3]{2} \longmapsto \sqrt[3]{2}$ or $\sqrt[3]{2}\omega$ or $\sqrt[3]{2}\omega^2$

$\omega \longmapsto \omega$ or $\omega \longmapsto \omega^2$

Irr poly $\omega$ over $\mathbb{Q}$ : $X^2 + X + 1$ $= (X-\omega)(X-\omega^2)$

$X^3 - 1 = (X-1)\underbrace{(X^2+X+1)}$

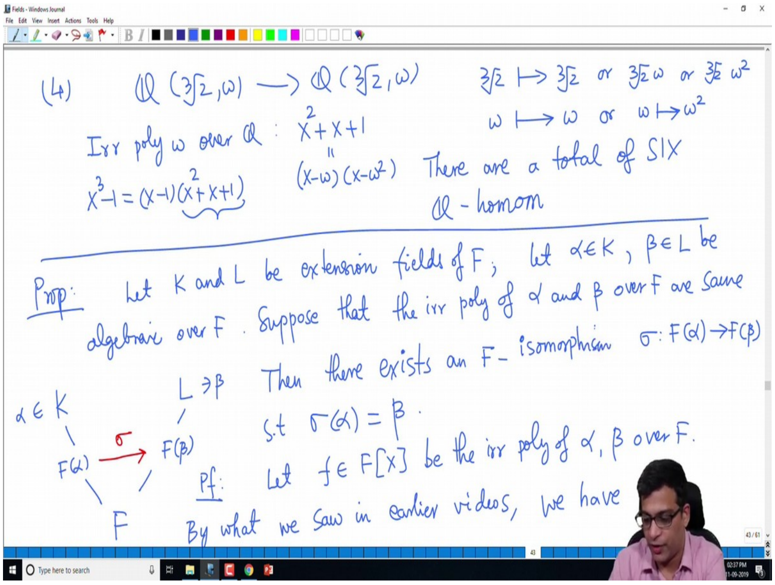
The third example is: let us take cube root of 2 to cube root of 2. So, there is example that we considered earlier. Cube root of 2 has irreducible polynomial. So, again this is the mantra to determine images of possible images of an element. Look at its irreducible polynomial, find out its roots and see what are the possible elements that you have in the target field. So, irreducible polynomial of cube root of 2 over Q, it is very easy to check again is X cubed minus 2. What are the roots of X cubed minus 2 in some large field right and see for example, R cube root of 2 omega cube of 2 omega squared cube root of 2. These are the three roots of this polynomial, because cube root of 2 is a real number omega is cube root of unity. So, this cube root is also two this cube root is also 2.

So, each of them this cube is 2, this cube is 2, this cube is 2. So, these are the roots. But how many are there in this field only cube root of 2 is in cube root of Q adjoined cube root of 2, because we know that this is a real field. This is contained in R, whereas omega is not in R right, omega is a purely imaginary number, purely complex number, it is not in R. So, there is only one possible image for cube root of 2, there is only one Q-homomorphism which sends root 2 cube root of 2 to cube root of 2. This is the identity map, because Q is fixed and cube root of 2 goes to cube root of 2. So, this is the identity homomorphism.

And one final example I will do is that Q adjoined cube root of 2 comma omega to cube root of 2 comma omega. So, here I do have other possibilities. So, cube root of 2 can go to cube root of 2 or cube root of 2 omega or cube root of 2 omega squared. And what is the irreducible polynomial of omega over Q, I claimed that this is X squared plus X plus 1 because it satisfies X cube minus 1 right, which it is a cube root of 1. So, it is it is a root of X cube minus 1 which is not irreducible in you can factor it like this. This must be the irreducible polynomial because X minus 1 clearly does not have omega is a root.

And what are its roots; it is actually omega 1 omega minus omega squared. So, omega has two possibilities; cube root of 2 has three possibilities. Omega can go to omega or omega can go to omega squared and these are independent. What you choose for the first one namely cube root of 2 is independent of what you choose for omega. In the example that I wrote earlier in this video, I chose one such thing cube root 2 goes to cube root of 2 omega, omega goes to omega squared, you have any number of such things here.

(Refer Slide Time 20:26)



(4) $\mathbb{Q}(\sqrt[3]{2}, \omega) \longrightarrow \mathbb{Q}(\sqrt[3]{2}, \omega)$ $\quad \sqrt[3]{2} \longmapsto \sqrt[3]{2}$ or $\sqrt[3]{2}\omega$ or $\sqrt[3]{2}\omega^2$

$\omega \longmapsto \omega$ or $\omega \longmapsto \omega^2$

Irr poly $\omega$ over $\mathbb{Q}$ : $X^2+X+1 \overset{\shortparallel}{} (X-\omega)(X-\omega^2)$

$X^3-1 = (X-1)\underbrace{(X^2+X+1)}$

There are a total of SIX $\mathbb{Q}$ - homom

Prop: Let $K$ and $L$ be extension fields of $F$; let $\alpha \in K$, $\beta \in L$ be algebraic over $F$. Suppose that the irr poly of $\alpha$ and $\beta$ over $F$ are same. Then there exists an $F$- isomorphism $\sigma : F(\alpha) \to F(\beta)$ s.t $\sigma(\alpha) = \beta$.

$$\begin{tikzcd}
\alpha \in K \arrow[d, dash] & & L \ni \beta \arrow[d, dash] \\
F(\alpha) \arrow[rr, "\sigma"] \arrow[dr, dash] & & F(\beta) \arrow[dl, dash] \\
& F &
\end{tikzcd}$$

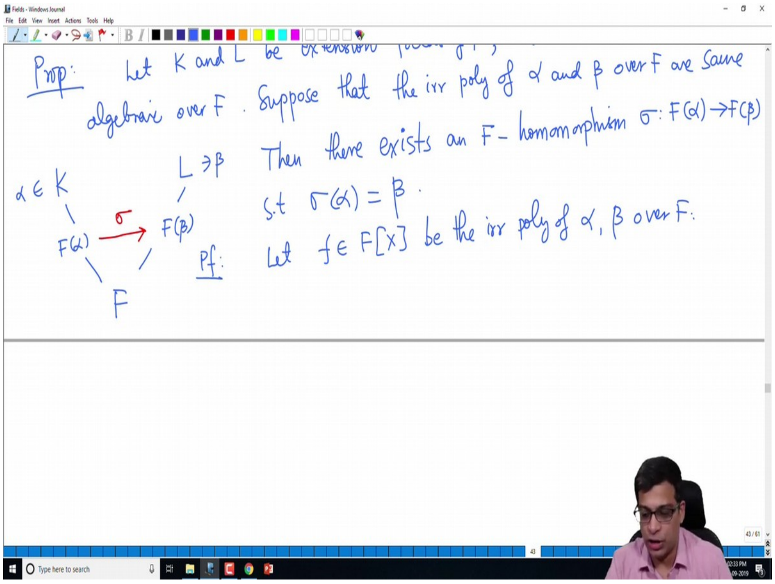
Pf: Let $f \in F[X]$ be the irr poly of $\alpha, \beta$ over $F$.

By what we saw in earlier videos, we have

So, there are a total of because these are independent and first element has three choices; second element has two choices there are total of six Q-homomorphisms here, ok. So, this tells you how, what are the possible images of algebraic elements are. So, now, let me do another proposition which illustrates when can you construct homomorphism, it is all right to say that alpha can only go to roots of its irreducible polynomial, but can there be a homomorphism by just sending alpha to any root of irreducible polynomial which is sort of what I did in this example. So, I am going to formalize this in this statement in this proposition.

So, let K and L be extension fields of F; let K and L be extension fields of F, let us choose two elements alpha and K, beta and L be both algebraic over F. Suppose that the irreducible polynomials of alpha and beta over capital F are same, ok.

(Refer Slide Time 22:06)



Prop: Let K and L be extension

algebraic over F. Suppose that the irr poly of $\alpha$ and $\beta$ over F are Same

Then there exists an F- homomorphism $\sigma : F(\alpha) \to F(\beta)$

s.t $\sigma(\alpha) = \beta$.

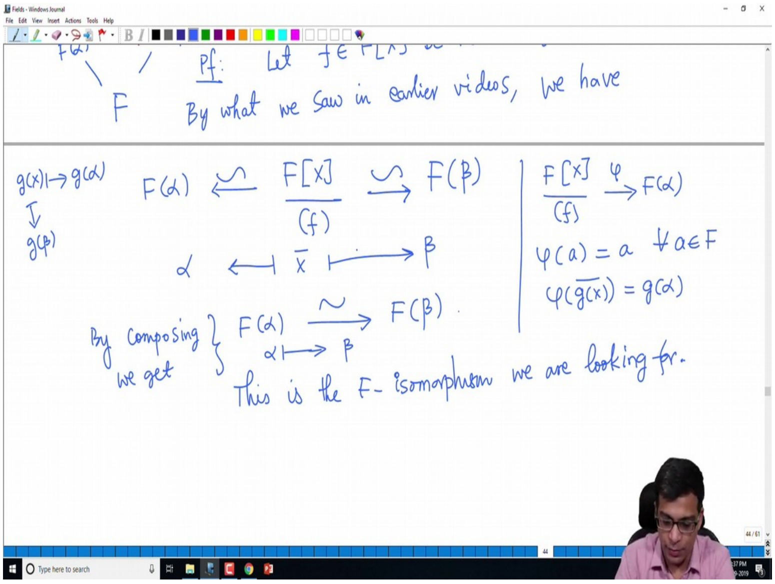
$$\begin{tikzcd}
\alpha \in K \arrow[d, dash] & & L \ni \beta \arrow[d, dash] \\
F(\alpha) \arrow[rr, "\sigma"] \arrow[dr, dash] & & F(\beta) \arrow[dl, dash] \\
& F &
\end{tikzcd}$$

Pf: Let $f \in F[x]$ be the irr poly of $\alpha, \beta$ over F.

So, you have this is the picture. K is here, L is here, F is here, F alpha is here, F beta is here right, because alpha is here, beta is here. K and L are not necessarily algebraic extensions. The elements alpha and beta are algebraic and their irreducible polynomial is the same then there exist. So, this is a, this completes the previous proposition together these two proposition are very important for us. Then there exists an F-homomorphism sigma from F alpha to F beta such that sigma alpha is equal to beta.

So, what I am now saying is that there is a map like this sigma which is an F-homomorphism that means, it fixes F every element of F is fixed by sigma and it sends alpha to beta. So, this is very easy and let me quickly prove this. Let f in capital F X be the irreducible polynomial of alpha beta over capital F right. Hypothesis is that both alpha and beta of the same irreducible polynomial, let us call that f.

(Refer Slide Time 23:36)



$F(\alpha)$ \ / $F$

<u>Pf:</u> Let $f \in F[X]$

By what we saw in earlier videos, we have

$g(x) \mapsto g(\alpha)$
$\downarrow$
$g(\beta)$

$$F(\alpha) \xleftarrow{\sim} \frac{F[X]}{(f)} \xrightarrow{\sim} F(\beta)$$

$$\alpha \longleftarrow\!\shortmid\ \bar{X} \longmapsto \beta$$

$$\frac{F[X]}{(f)} \xrightarrow{\varphi} F(\alpha)$$

$\varphi(a) = a \ \forall a \in F$

$\varphi(\overline{g(x)}) = g(\alpha)$

By composing we get $\left.\right\}$ $F(\alpha) \xrightarrow{\sim} F(\beta)$.
$\alpha \mapsto \beta$

This is the F- isomorphism we are looking for.

Then by what we saw earlier, we know that F alpha is isomorphic to the polynomial ring F X modulo the maximal ideal generated by f. Capital F X is a UFD right, in fact, it is a PID being a polynomial ring in one variable over a field F. Small f is an irreducible polynomial, so it generates a maximal ideal, and that is in fact the field f round bracket alpha. At the same time, we have F X mod f is also isomorphic to f beta by what we saw in earlier videos we have this.

And what is this isomorphism, here remember X goes to alpha here, here X goes to beta because this map sends f X any polynomial you sent to its evaluation at alpha. This map if you remember g x under these maps g x goes to g alpha on the one hand g beta on the other hand. So, X bar is what I am writing in the residue quotient ring, but its image is just the polynomial X evaluated at alpha that is just alpha. Here the image is the polynomial X evaluated at beta that is beta. So, now, we are done and not only that this map, this homomorphism.

Let us call this phi, phi of an element of a is a, phi of an element F is itself, because again this map sends g x to g alpha. So, if g x is a constant polynomial there is no way no nothing to substitute alpha for it sends that constant polynomial to itself; that means, if you now compose this. So, I will not by and these are inverses right by composing the inverse. These are isomorphisms right so, there is a map like this, and there is a map like this. So, I can compose the inverse of the first map with the second map to get we get F alpha. In fact, it is a field isomorphism. And by composing we get and this is the F-homomorphism, in fact, I will write F isomorphism we are looking for.

So, what I am trying to say is that, so let me actually amend this sentence here, the proposition is better than this there is an F-isomorphism. I have not technically talked about F-isomorphisms yet before, but this is exactly the same concept as a F-homomorphism F-homomorphism is a field homomorphism which fixes F point wise F-isomorphism is simply a field isomorphism, that means, it is an isomorphism of rings which fixes F point wise. So, this is the F-isomorphism we are looking for right that is clear. Because this is an isomorphism of rings, it sends alpha to beta because under this inverse alpha goes to X bar, X bar goes to beta.

So, alpha goes to beta and every element of F is fixed, so that is a proof ok. And implicitly I have used this proposition to say that there are 6 homomorphisms in this example Q adjoined cube root of 2 omega to Q adjoined cube root of 2 omega. Because I need these propositions to say that I can send cube root of 2 to any other roots its irreducible polynomial and I can construct a valid field homomorphism, ok.

So, in this video we have looked at a very important notion which describe to us when you have two fields above the same base field F, what is the notion of F-homomorphism? And once you have F-homomorphism, what are the possible images of algebraic elements. So, let me end this video here. In the next video, we are going to talk about adjoining roots of a polynomial, and how to construct splitting fields of polynomials.

Thank you.