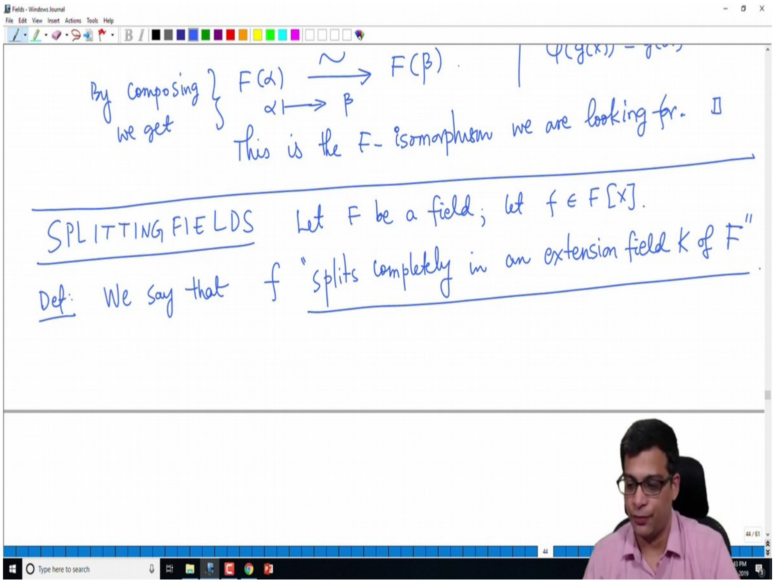
Introduction to Rings and Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 39
Splitting fields

Let us continue now, in this video I am going to introduce a very important notion called Splitting fields. So, what I will do now is.

(Refer Slide Time: 00:24)



By composing we get } $F(\alpha) \xrightarrow{\sim} F(\beta)$. | $\varphi(g(x)) =$

$\alpha \longmapsto \beta$

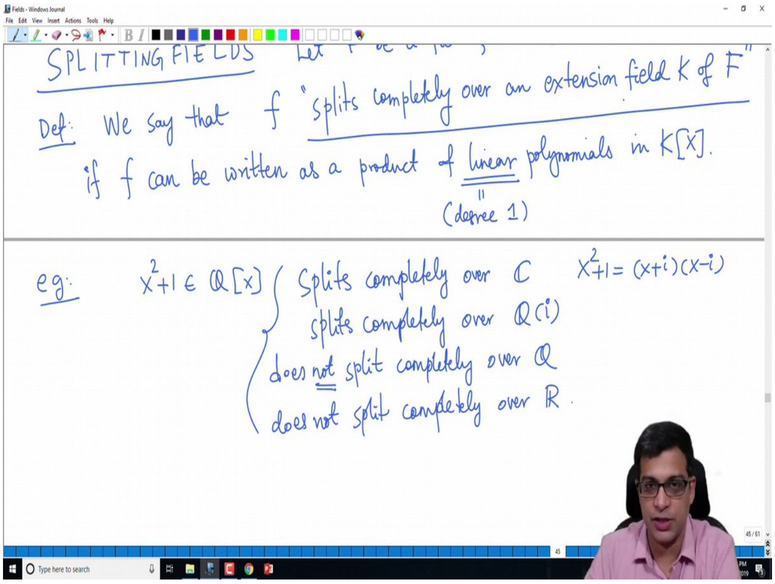
This is the F- isomorphism we are looking for. □

SPLITTING FIELDS Let F be a field; let $f \in F[x]$.

Def: We say that f "splits completely in an extension field K of F".

Let F be some field and let us choose a polynomial f in the polynomial ring over capital F. Let f be a polynomial in capital F X. We say that so, this is an important definition, we say that f splits completely in an extension field K of F, in an extension field K of F so, this is the terminology, we say that it splits completely in an extension field K of F.

(Refer Slide Time: 01:14)



SPLITTING FIELDS   Let

Def: We say that f "splits completely over an extension field K of F"
if f can be written as a product of linear polynomials in K[X].
$\overset{\shortparallel}{\text{(degree 1)}}$

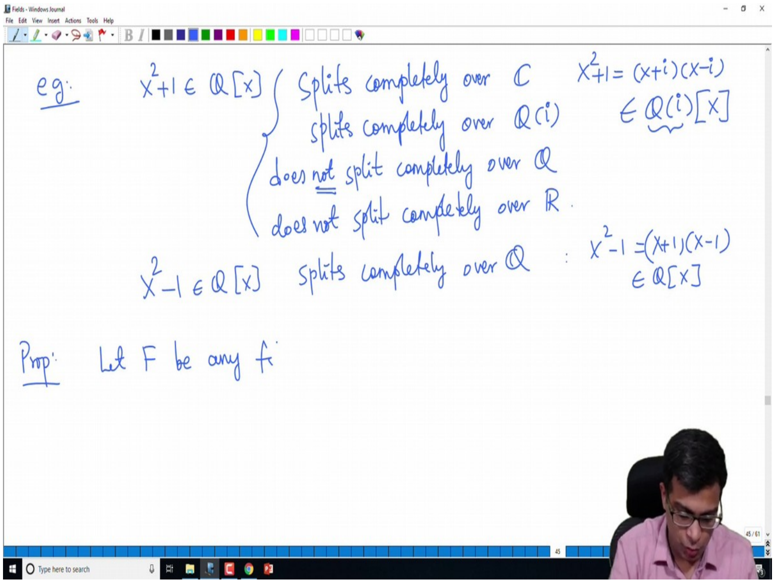
eg: $X^2+1 \in \mathbb{Q}[X]$
Splits completely over $\mathbb{C}$ $X^2+1=(X+i)(X-i)$
splits completely over $\mathbb{Q}(i)$
does not split completely over $\mathbb{Q}$
does not split completely over $\mathbb{R}$.

If f can be written as a product of linear or degree 1 polynomials in the polynomial ring over the bigger field, linear means degree 1; linear polynomials means degree 1 polynomials, ok.

So, we say that it splits completely; that means, all the way up to degree 1. So, for example, X squared plus 1 which is a polynomial in rational numbers does not or let us say splits completely in C right because, X squared plus 1 can be written as X plus i times X minus i where, i is in C. It is also splits completely or rather I will right over C over; so, I should just slightly modify this, splits completely over an extension field capital K, if that happens splits completely over Q adjoined i also. Because, we do not need all of complex numbers right for the splitting, we just need i.

On the other hand, it does not split completely over Q, because it is not a product of linear polynomials over Q, it is irreducible and you cannot factor it into linear polynomials. It does not even split completely over R also, right. So, the base field is extremely important, it is over the base fields are splitting completely or not make sense.

(Refer Slide Time: 03:18)



eg: $X^2+1 \in \mathbb{Q}[X]$ $\left\{\begin{array}{l}\text{Splits completely over } \mathbb{C} \\ \text{splits completely over } \mathbb{Q}(i) \\ \text{does } \underline{\underline{\text{not}}} \text{ split completely over } \mathbb{Q} \\ \text{does not split completely over } \mathbb{R}.\end{array}\right.$ $X^2+1 = (X+i)(X-i) \in \underline{\mathbb{Q}(i)}[X]$

$X^2-1 \in \mathbb{Q}[X]$ splits completely over $\mathbb{Q}$: $X^2-1 = (X+1)(X-1) \in \mathbb{Q}[X]$

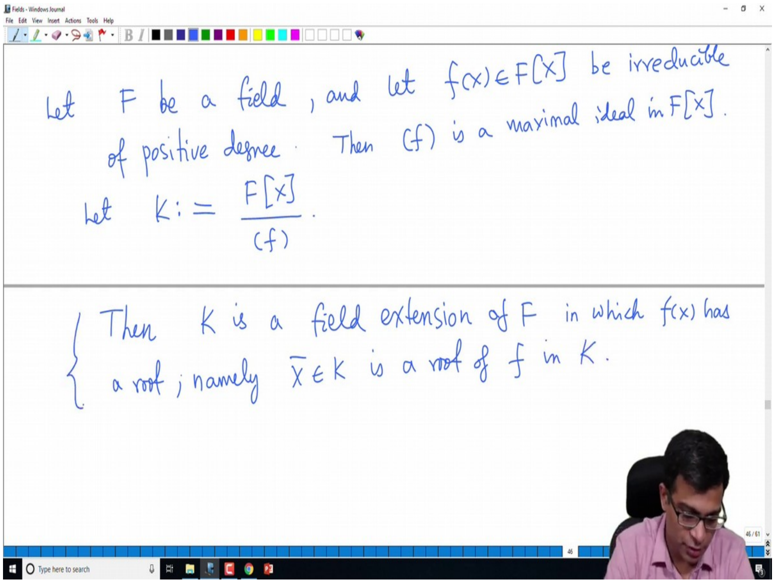
Prop: Let F be any fi

On the other hand, X squared minus 1 which is a rational polynomial splits completely over Q itself right, because X squared minus 1 is X plus 1 times X minus 1 right and this is actually a splitting in the polynomial ring over Q here this is the splitting over the polynomial ring over Q i, ok.

So, splitting completely means, splitting as a product of linear factors in other words, what we are saying is that f has all the roots in that field. Here X squared plus 1 has 2 roots but, not in Q only in Q i, you have to go at least Q i. So, it is a field, we say that a polynomial splits over some field, if it has all the roots there, we have to be careful about what all the roots means what we really mean is that it is written as a product of linear polynomials ok.

So, what I want to start with is we want to say that it always; there is such a field always. So, proposition, let F be any field yeah; so, actually before I read the proposition, let me do the main case of this as a separate remark.

(Refer Slide Time: 04:40)



Let F be a field, and let $f(x) \in F[X]$ be irreducible of positive degree. Then (f) is a maximal ideal in $F[X]$.

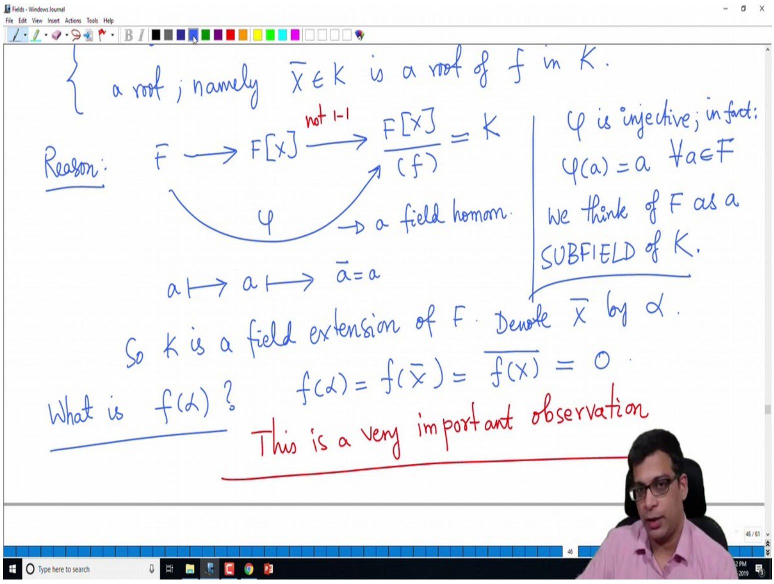
Let $K := \frac{F[X]}{(f)}$.

Then K is a field extension of F in which $f(x)$ has a root; namely $\bar{X} \in K$ is a root of f in K.

So, let us say F is a field and let f X be in capital F X be an irreducible polynomial that is irreducible of positive degree. So, degree f is positive. Then, f is a maximal ideal in F X, right. This is something that we have seen many times before, if you have the polynomial ring over one in one variable or a field, the ideal generated by a irreducible polynomial is a maximal ideal.

So, let K be the field F X modulo f then, what we want to say is that there is a very simple point but, it is an extremely important point then, K is a field extension of F; K is a field extension of capital F, in which f X has a root namely X bar, ok. So, let me explain this, what is the explanation for this.

(Refer Slide Time: 06:17)



{ a root ; namely $\bar{X} \in K$ is a root of f in K.

Reason:

$$\begin{tikzcd} F \arrow[r] \arrow[rr, bend right, "\varphi"'] & F[X] \arrow[r, "\text{not 1-1}"] & \frac{F[X]}{(f)} = K \end{tikzcd}$$

$\to$ a field homom.

$a \longmapsto a \longmapsto \bar{a} = a$

φ is injective; in fact: $\varphi(a) = a \;\forall a \in F$

We think of F as a SUBFIELD of K.

So K is a field extension of F. Denote $\bar{X}$ by α.

What is $f(\alpha)$? $\quad f(\alpha) = f(\bar{X}) = \overline{f(X)} = 0$.

This is a very important observation

So, the reason so, this might not look like a field extension a priori but, it is in fact, a field extension, that is because remember F always sits inside F X, right. So, there is an injective map from F to F X and now what we are doing is F X mod the polynomial the ideal generated by the polynomial f and that is K.

This of course, is not injective, not 1-1 right that is because, the polynomial f goes to 0 here. So, that is not injective but, the composition this is a field homomorphism right, this is a field homomorphism. Because, the first one is a ring homomorphism, the second one is a ring homomorphism; the composition is a ring homomorphism. A field homomorphism is really nothing but, a ring homomorphism between two fields. F and K are fields, it is a field homomorphism.

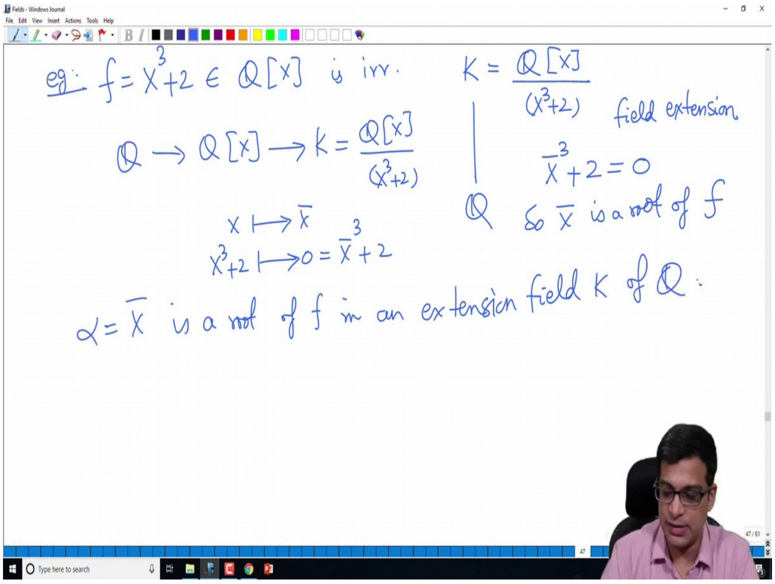
And, as such if you call this phi, phi is injective right. In fact, phi can phi of a is actually a for all a and k, all a in F. In fact, phi of a is equal to a for all a in F, because where does so, if you just tress the maps here, small a goes to small a right. It goes to itself as a constant and then this goes to a bar but, I am going to identify that with a.

So, we think of F as a sub field of K. Really very to be very precise F is isomorphic as a field to the image which is a sub field of K and we are identifying F with that image. So, we can think of F as a subfield of K. So, K is a field extension in other words right. What is a field extension? It is simply as field containing this field that is the first statement, it is a field extension of K F in which f X has a root.

Now, what is X bar? Just to be more familiar to you, I am going to think of the image of X as alpha. So, denote X bar by alpha. So, then what is f alpha? What is f alpha, f alpha I claim is 0 because, f alpha is equal to f of X bar but, then this is same as f of X whole bar. Because, thus the map here sends the second map takes a polynomial and sends it to its residue, which is simply replacing X by X bar but, f X bar is 0 ok. So, this is extremely important, this is a very important observation, ok.

So, in some sense there is a god given procedure to obtain a bigger field where any reducible polynomial has a root. All you need to do is go modulo the ideal generated by that irreducible polynomial, because that ideal is a maximal ideal, the quotient ring is in fact a field and the residue of X is a root of the polynomial.

(Refer Slide Time: 10:24)



eg: $f = X^3+2 \in \mathbb{Q}[X]$ is irr.

$$\mathbb{Q} \to \mathbb{Q}[X] \to K = \frac{\mathbb{Q}[X]}{(X^3+2)}$$

$$X \mapsto \bar{X}$$
$$X^3+2 \mapsto 0 = \bar{X}^3+2$$

$$\begin{tikzcd} K = \frac{\mathbb{Q}[X]}{(X^3+2)} \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

field extension

$\bar{X}^3+2=0$

So $\bar{X}$ is a root of f

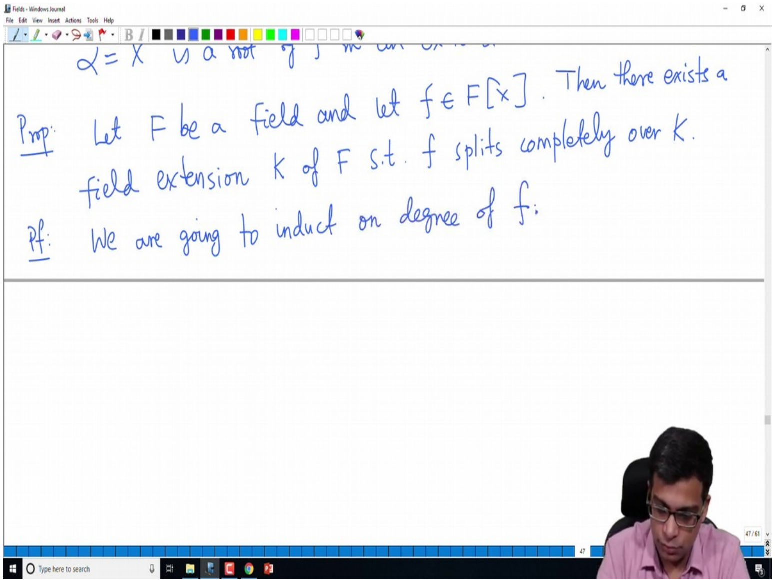
$\alpha = \bar{X}$ is a root of f in an extension field K of $\mathbb{Q}$.

So, to illustrate this what we do; let us for example, consider X cubed plus 2, ok. This is irreducible, this is for you can see this in many ways for example, Eisenstein criterion shows this. So, what do we do, we take Q K to be, Q adjoined X cube plus 2 right, this by the observation I made earlier is a field extension. Because, rational numbers are not really disturbed in K, only X becomes X bar but, rational numbers under this composition of these maps are unchanged.

So, these are field extension and X bar here satisfies right because, if you think about this, K is Q X modulo X cube plus 2. So; that means, image of X here is X bar but, X bar cubed plus 2 goes to 0, this is X bar cubed plus 2. X cube plus 2 goes to 0, which is X bar cube plus 2; that means, X bar is a root of f, which was the polynomial I started with, it is a root of f, f is X cube plus 2. So, X bar is a root of f.

So, then we forget all this and think of X bar as alpha and we say that is a root of f in an extension field K of Q, ok. This is the illustration of the procedure that I described here. So, the upshot is for every irreducible polynomial there is a natural field extension in which the irreducible polynomial we started with has roots. Now, this process can be generalized to show that there is always a large enough field where every polynomial has all the roots, more precisely every polynomials splits completely.

(Refer Slide Time: 12:44)



$\alpha = X$ is a root of f in an

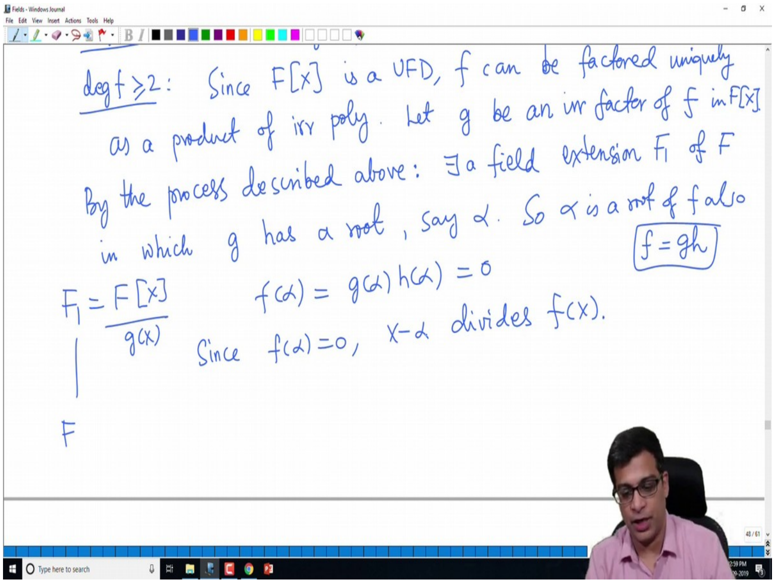
Prop: Let F be a field and let $f \in F[x]$. Then there exists a field extension K of F s.t. f splits completely over K.

Pf: We are going to induct on degree of f:

So, now let me write the proposition that I was writing earlier. The proposition says, let F be a field and let small f be a polynomial over capital F and no longer assuming it is irreducible, then there exists a field extension K of f, sorry K of capital F, such that small f splits completely over K.

Remember, I defined the notion of splitting completely in an extension field; that means, the polynomial splits or written is written as a product of linear polynomials, the remark above this proposition showed that for every irreducible polynomial there is an extension field, where the irreducible polynomial has a root. Now, I am saying that for every polynomial you can construct a large enough field where the polynomial splits completely. The idea is that we are going to induct on the degree of f, small f, ok.

(Refer Slide Time: 14:09)



deg $f \geq 2$: Since $F[x]$ is a UFD, f can be factored uniquely as a product of irr poly. Let g be an irr factor of f in $F[x]$. By the process described above: $\exists$ a field extension F_1 of F in which g has a root, say α. So α is a root of f also

$\boxed{f = gh}$

$F_1 = \frac{F[x]}{g(x)}$

$f(\alpha) = g(\alpha) h(\alpha) = 0$

Since $f(\alpha) = 0$, $x - \alpha$ divides $f(x)$.

F

So, degree of f is 1 means what; that means, f already splits completely; f is already a linear polynomial; that means, it splits completely over capital F itself. So, take K equal to F. The goal of the proposition is to exhibit a field extension over which f small f splits completely, if degree 1 then, all we can just take it to be the best field itself.

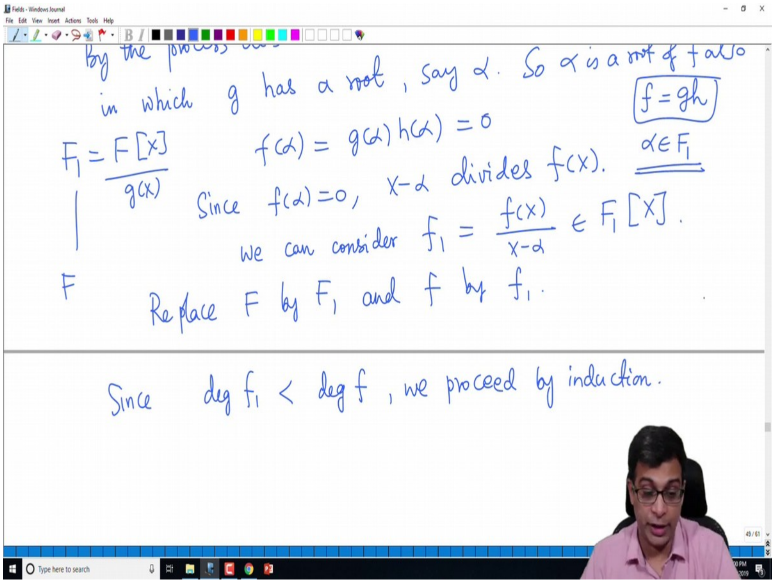
Now, let us say degree f is at least 2; now, we know since F X is a UFD, f small f can be factored, uniquely has a product of irreducible polynomials right, this is the consequence of F X being a UFD. So, what we can do is let g be an irreducible factor of f, in capital F X. Let it be an irreducible factor of f in capital F X. So, now, by the process described above, there exists a field extension K of F, let us say F 1 of F, I want to keep K as the final field I get. So, I call this now F 1, there exists a field F 1, field extension F 1 of F in which g has a root, say alpha.

So, just to recall how do we construct such an extension field? We simply take F 1 to be F X modulo g X, it is an extension field of F and X bar is a root of g because, g is a irreducible polynomial F 1 is a field. So, alpha is a root of f also right, this is clear because, f of alpha is g of alpha times h of alpha right, g is a factor of f, so; that means, f is g h. So, f alpha is g alpha times h alpha which is 0 because, g alpha is 0.

So, now, we can write we can so, note that since f alpha is 0, X minus alpha divides ok, this is something I have done earlier when I talked about rings, ring theory part of the course. If you have f alpha is a 0, f alpha is 0; that means, alpha is a root of a polynomial;

that means, X minus alpha is a factor of f x. Because, you can always divide by X minus alpha and the remainder is a constant because, X minus alpha has degree 1, but, when you plug in alpha, f alpha becomes 0, x minus alpha becomes 0 so, the remainder is 0.

(Refer Slide Time: 17:35)



By the process

in which g has a root, say α. So α is a root of f also $\boxed{f = gh}$

$F_1 = \frac{F[x]}{g(x)}$

$|$

F

$f(\alpha) = g(\alpha)h(\alpha) = 0$

$\underline{\underline{\alpha \in F_1}}$

Since $f(\alpha) = 0$, $X - \alpha$ divides $f(x)$.

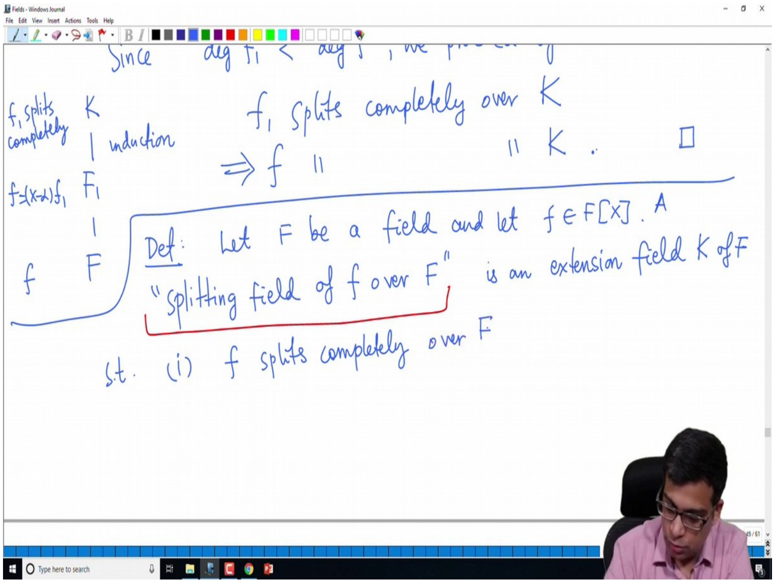
we can consider $f_1 = \frac{f(x)}{X-\alpha} \in F_1[X]$.

Replace F by F_1 and f by f_1.

Since $\deg f_1 < \deg f$, we proceed by induction.

So, we can now consider F 1 to be F X divided by X minus alpha, this is in F X. F 1 X rather because, alpha is only in capital F 1 right, this division is not necessarily true in capital F X but, it is true in capital F 1 X. So, replace F by F 1 and small f by small f 1. Since, degree of small f 1 is strictly less than degree of small f, we proceed by induction, remember we are inducting on the degree. So that means, for any polynomial whose degree is less than degree of f over any field you can construct a large enough field in which the polynomial splits completely.

(Refer Slide Time: 18:44)



Since deg f_1 < deg f, we

f_1 splits completely   K

| induction

$f=(x-\alpha)f_1$ F_1

|

f F

f_1 splits completely over K

$\Rightarrow f$ " " K. □

Def: Let F be a field and let $f \in F[X]$. A "splitting field of f over F" is an extension field K of F

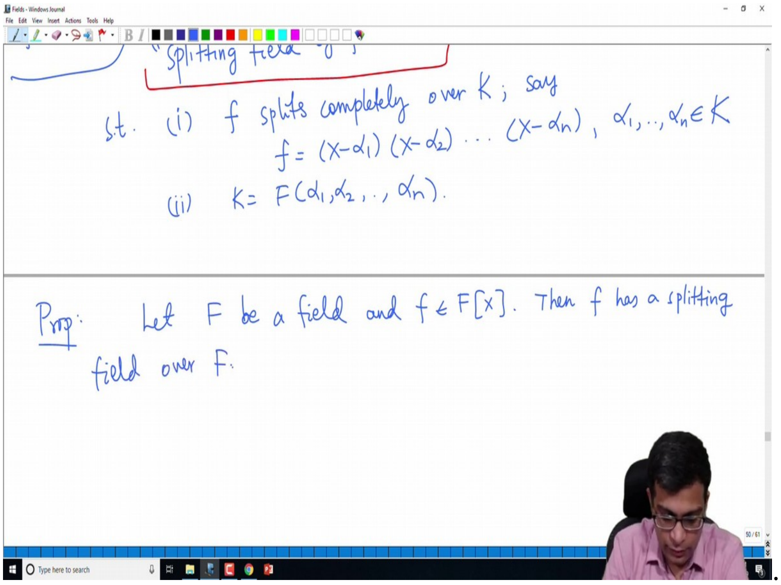
s.t. (i) f splits completely over F

So, we can go from F to F 1, here we have F, here you have f equals X minus alpha times f 1 and finally, we get from this is induction step f 1 splits completely. So, f 1 splits completely in over capital F, capital K rather this means, f splits completely over capital K right because, what is f? f is just X minus alpha times f 1. So, the additional term in f is already linear. So, if the f 1 is the product of linear polynomials over capital K so, is small f.

So, f is also going to split completely over capital K. So; that means, we have constructed a polynomial a larger field over which you have the polynomials splitting completely ok. This is a very useful construction for us, this tells us that a given polynomial may not have roots over a base field, lots of polynomials do not have roots in Q. But, you can always construct a bigger field, where the polynomial will have roots, not only will it have roots but, it will split completely as a product of linear polynomials.

So, now, let me define this very important notion and there is a point of this video, let capital F be a field and let small f be a polynomial over capital F. A splitting field; a spitting field of small f over capital F, again this entire phrase is important for us. A splitting field of small f over capital F is an extension field K of F such that two conditions, f splits completely over the bigger field over capital K.

(Refer Slide Time: 21:06)



"splitting field" of f

s.t. (i) f splits completely over K; say

$f = (X-\alpha_1)(X-\alpha_2)\dots(X-\alpha_n)$, $\alpha_1,..,\alpha_n \in K$

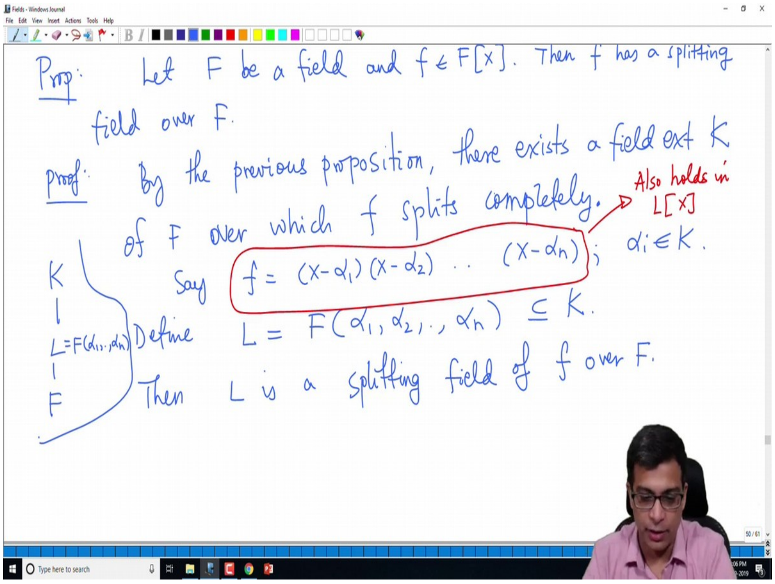
(ii) $K = F(\alpha_1,\alpha_2,..,\alpha_n)$.

Prop: Let F be a field and $f \in F[X]$. Then f has a splitting field over F.

Say f can be written as X minus alpha 1, X minus alpha 2 remember splitting completely means, it is a product of linear polynomials and they are all in capital K. So, it is a product of linear polynomials over capital K and capital K must be generated by these roots, it should not have any unnecessary elements, ok. So, it is exactly the splitting field.

So, now, the definition is now the proposition is every polynomial has a splitting field, let F be a field and let small f be a polynomial over capital F, capital F then small f has the splitting field over capital F, what is the proof?

(Refer Slide Time: 22:06).



Prop: Let F be a field and $f \in F[X]$. Then f has a splitting field over F.

Proof: By the previous proposition, there exists a field ext K of F over which f splits completely.

Say $\boxed{f = (X-\alpha_1)(X-\alpha_2)\dots(X-\alpha_n)}$; $\alpha_i \in K$.

Also holds in $L[X]$

Define $L = F(\alpha_1,\alpha_2,..,\alpha_n) \subseteq K$.

Then L is a splitting field of f over F.

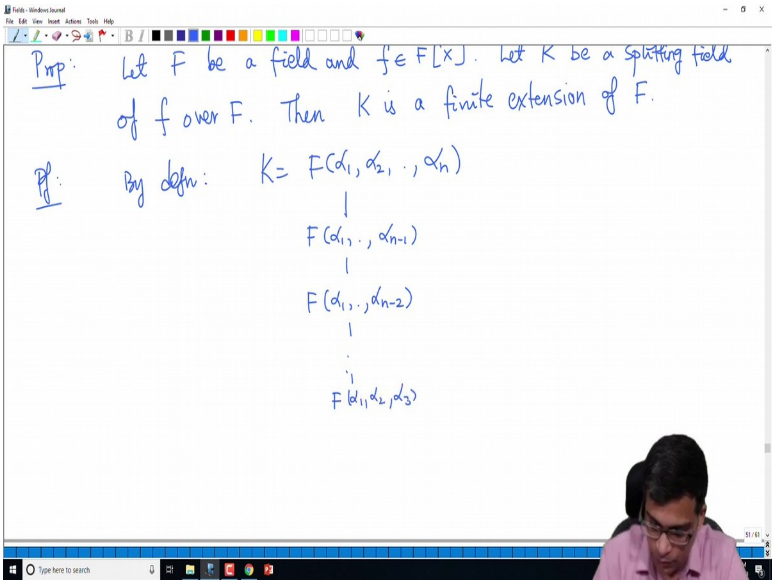
$$\begin{tikzcd} K \arrow[d, dash] \\ L=F(\alpha_1,..,\alpha_n) \arrow[d, dash] \\ F \end{tikzcd}$$

By the previous proposition, there exists a field extension K of F over which f splits completely, right. So, this is the first condition for the splitting field, small f should split completely over the bigger field but, there is also the second condition. So, now, in the previous proposition we did not take care of the second condition.

Now, we are going to do that so, say small f is it splits completely right. So, we take X minus alpha 1 times X minus alpha 2 times X minus alpha n with alpha i in capital K. It is not true that capital K is the splitting field of small f because, the second condition may not be satisfied but, no problem it is very simple to get a splitting field. Simply is define L to be capital F adjoined alpha 1, alpha 2, alpha n, this is of course in K. So, we have constructed a field in the previous proposition K and F is our base field and now I am defining a new field only using the required elements alpha 1 to alpha n. So, then L is a splitting field of small f over capital F, right.

Now, this is clear because, f splits over L also, small f splits over L also because, this factorization which was apriori defined over capital K X also holds in L X right. Because, what is the meaning of this holding in L X, all we want is that the coefficients of this polynomial are in L but, it was constructed so that, all the alpha is are in L. So, this holds in L x; that means, small f splits over capital L and by construction the second condition holds, L is equal to f alpha 1 to alpha n. So, L is a splitting field of small f over capital F. Let me write another nice proposition, before doing some examples.

(Refer Slide Time: 24:47)



Prop: Let F be a field and $f \in F[X]$. Let K be a splitting field of f over F. Then K is a finite extension of F.

Pf: By defn: $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$

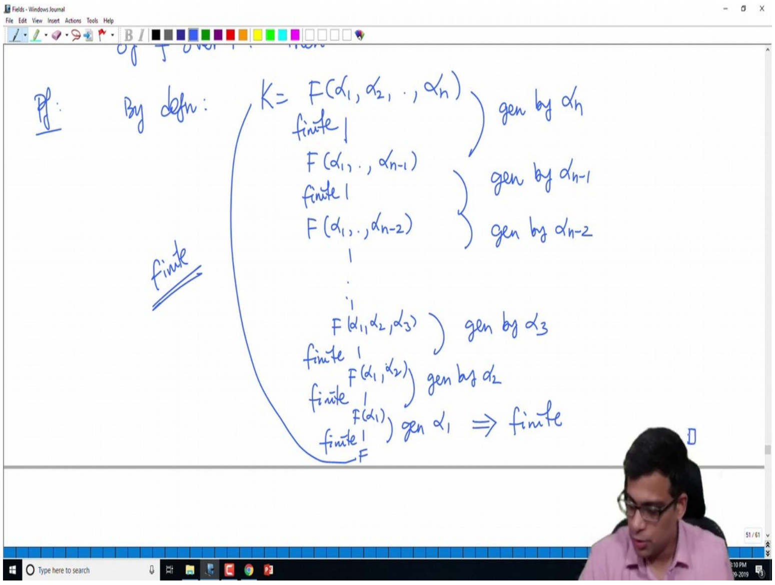
$$\begin{tikzcd}
F(\alpha_1, \alpha_2, \ldots, \alpha_n) \arrow[d, dash] \\
F(\alpha_1, \ldots, \alpha_{n-1}) \arrow[d, dash] \\
F(\alpha_1, \ldots, \alpha_{n-2}) \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
F(\alpha_1, \alpha_2, \alpha_3)
\end{tikzcd}$$

Let capital F be a field and let small f be a polynomial over that field. Let K be a splitting field of small f over capital F. A quick remark here which I will not write and I will not use this much but, splitting field is essentially unique. Meaning, if you have two splitting fields of the same polynomial over the same base field, you can exhibit an isomorphism of the two splitting fields over the base field.

So, often when you read books, they talk about these splitting field and that is a statement which is valid up to isomorphism, but I am not going to use that a lot. So, I am going to keep calling this a splitting field of small f over capital F. Then K is a finite extension of capital F.

So, splitting fields are automatically finite extensions. So, this is very simple because, by definition K is F alpha 1, alpha 2, alpha n right. So, this sits inside a tower like this. So, this is generated by alpha n over this, this is generated by alpha n minus 1 over this and all the way up to F alpha 1 let us say alpha 2 alpha 3 to F alpha 1 alpha 2, F alpha 1 to F.

(Refer Slide Time: 26:26)



Pf: By defn: $K = F(\alpha_1, \alpha_2, .., \alpha_n)$ gen by α_n

finite

$F(\alpha_1, .., \alpha_{n-1})$ gen by α_{n-1}

finite

$F(\alpha_1, .., \alpha_{n-2})$ gen by α_{n-2}

$F(\alpha_1, \alpha_2, \alpha_3)$ gen by α_3

finite

$F(\alpha_1, \alpha_2)$ gen by α_2

finite

$F(\alpha_1)$ gen α_1 $\Rightarrow$ finite

finite

F

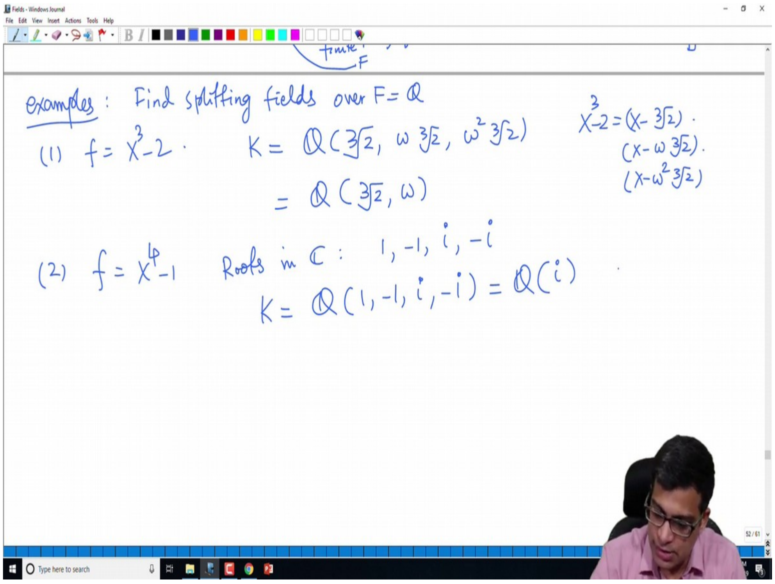
finite

So, I have broken up this into a series of field extensions, where each one is generated by a single thing. So, this is generated by alpha n, this is generated by alpha n minus 1, the next one is generated by alpha n minus 2. This is generated by alpha 3, this is generated by alpha 2, this is generated by alpha 1.

But, now by what we did in a previous video, if you have an algebraic element and you have an extension generated by this, this is finite right, this is finite, similarly this is finite, this is finite. Everything in this tower is finite, right. So, everything is finite, the entire thing in other words because of the multiplicative property of degree of field extensions, K over F the degree will be product of this times, this times, this times, this times, this. So, this is finite. So, that is the proof ok.

So, I have done this pictorially but, I hope it is clear, if you have a splitting field, it is automatically a finite extension. Let me now do a few examples to end the video and we will continue from the next video.

(Refer Slide Time: 27:55)



examples : Find splitting fields over $F = \mathbb{Q}$

(1) $f = X^3 - 2$. $K = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$

$= \mathbb{Q}(\sqrt[3]{2}, \omega)$

$X^3 - 2 = (X - \sqrt[3]{2}) \cdot (X - \omega\sqrt[3]{2}) \cdot (X - \omega^2\sqrt[3]{2})$

(2) $f = X^4 - 1$ Roots in $\mathbb{C}$: $1, -1, i, -i$

$K = \mathbb{Q}(1, -1, i, -i) = \mathbb{Q}(i)$

So, just I will do three examples. What is the splitting field of so, the question is to find splitting fields. So, I will give three examples, find splitting fields. So, let us take capital F to be Q and small f, in all examples actually F is Q. So, I will change the polynomial only. So, X cube minus 2, what is the splitting field here? So, here K can be taken as Q adjoined cube root of 2 and omega.

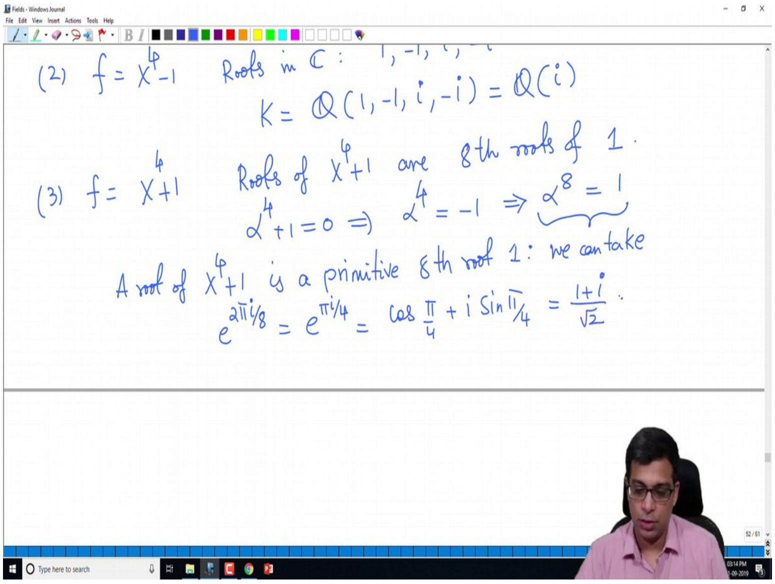
This is something that came up before, there are 3 roots here, actually it can be written as it has to be written as because, these are the 3 roots and this polynomial does split completely over this right because, it is X minus cube root of 2, times X minus omega cube root of 2, times X minus omega squared cube root of 2.

But, it is not necessary to list all 3 elements here because, if cube root of 2 and omega cube root of 2 are there in this field, their ratio is going to be there; that means, omega is there but, once omega is there and cube root of 2 is there, omega cube root of 2 is there, omega squared cube root of 2 is there. So, this is sort of a minimal generating set. So, I can describe this as the splitting field and what is its degree. So, let me not, ok.

So, I will postpone that degree calculation to later, let me do one more example, X power 4 minus 1, what is the splitting field? Here what are the roots, let us say in C. So, we have to see for Q, there is a god given field over which all polynomials have roots, that is related to the fact that C is algebraically closed, which I will formally mention in a later video. So, what are the roots in C, they are 1 minus 1, i minus i.

So, the splitting field is simply given by Q adjoined, 1 minus 1 i minus i because, you have to add all the roots, but of course, it is not necessary to add 1, minus 1 that are already in Q that is silly to write like that and in fact you also do not need to write minus i, because, minus i is already there, if once i is there. So, this is the splitting field you adjoined one of them, that is enough.

(Refer Slide Time: 30:30)



(2) $f = X^4 - 1$ Roots in $\mathbb{C}$: $1, -1, i, -i$

$K = \mathbb{Q}(1, -1, i, -i) = \mathbb{Q}(i)$

(3) $f = X^4 + 1$ Roots of $X^4 + 1$ are 8th roots of 1.

$\alpha^4 + 1 = 0 \Rightarrow \alpha^4 = -1 \Rightarrow \underbrace{\alpha^8 = 1}$

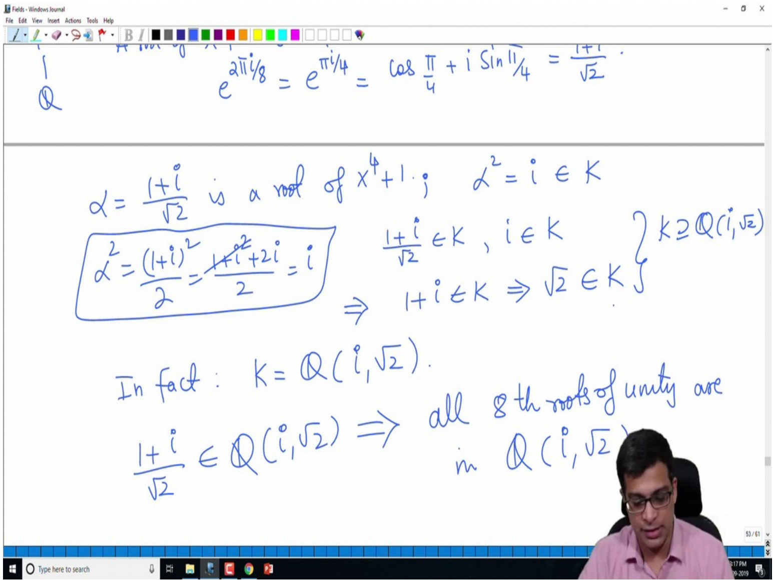
A root of $X^4 + 1$ is a primitive 8th root 1: we can take

$e^{2\pi i/8} = e^{\pi i/4} = \cos\frac{\pi}{4} + i \sin \pi/4 = \frac{1+i}{\sqrt{2}}$.

In the first example you have to adjoin two elements to Q to get a splitting field; here you have to adjoin only 1; final example for this video, X power 4 plus 1. So, note that, roots here are roots of X power 4 plus 1 are 8th roots of 1 because, remember if alpha power 4 plus 1 equal to 0; that means, alpha power 4 equal to minus 1; that means, alpha power 8 is equal to 1.

So, alpha power 8 is 1 and alpha power all the roots must satisfy this condition but, some root cannot be a fourth root of unity, there must be a primitive 8th root of unity which is a root of this. So, a root of X power 4 plus 1 is a primitive 8th root of 1. So, for example, we can take this to be a e power 2 pi i by 8, which is e power pi i by 4, which is cosine pi by 4 plus i sin pi by 4. So, this is 1 plus i root 2, right.

(Refer Slide Time: 32:16)



$\mathbb{Q}$ $\quad e^{2\pi i/8} = e^{\pi i/4} = \cos\frac{\pi}{4} + i \sin \pi/4 = \frac{1+i}{\sqrt{2}}$.

$\alpha = \frac{1+i}{\sqrt{2}}$ is a root of x^4+1. ; $\alpha^2 = i \in K$

$\boxed{\alpha^2 = \frac{(1+i)^2}{2} = \frac{\cancel{1+i^2}+2i}{2} = i}$

$\left.\begin{array}{l}\frac{1+i}{\sqrt{2}} \in K,\ i \in K \\ \Rightarrow 1+i \in K \Rightarrow \sqrt{2} \in K\end{array}\right\} K \supseteq \mathbb{Q}(i,\sqrt{2})$

In fact : $K = \mathbb{Q}(i,\sqrt{2})$.

$\frac{1+i}{\sqrt{2}} \in \mathbb{Q}(i,\sqrt{2}) \Rightarrow$ all 8 th roots of unity are in $\mathbb{Q}(i,\sqrt{2})$

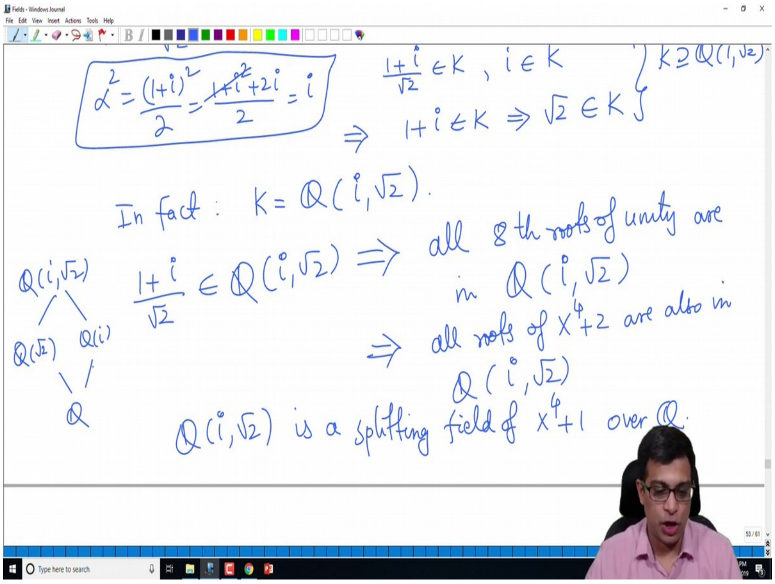
So, this is a root of 1 plus i by root 2 is a root of X power 4 plus 1, what is another root? i is also a root. That is clear right because, oh sorry i is not a root. So, this is a root, so all the roots are primitive roots of unity and one of those primitive roots of unity is this, primitive 8th root of unity.

Let us call this alpha then, what is alpha squared, alpha squared is actually i because, you can check that by multiplying this because, alpha squared is 1 plus i whole squared by 2, this is a 1 plus i squared plus 2 i by 2. So, this is this will cancel and you get i ok. Also it follows from the fact that, e power 2 pi i by 8 whole squared is e power 4 pi i by 8, which is e power pi i by 2. So, which is i.

So, alpha squared is in K, whatever is our potential splitting field contains i and it contains i plus 1 plus i over root 2. So, 1 plus i by root 2 is there, i is in there; that means, 1 plus i is also there right because say K certainly contains Q. So, we are looking at extensions of Q, 1 is there, i is there, 1 plus i is there; that means, the ratio of these two is there, 2 2 is there. So, what I want to say is that K is in fact, equal to; so, certainly these two together imply that K contains Q adjoined i comma root 2 right. But, in fact K is equal to Q adjoined right that is because, 1 plus i by root 2 is already in Q adjoined i comma root 2, this means all 8th roots of unity are in Q adjoined i comma root 2.

See the roots of unity from a cyclic group, under multiplication and a primitive root of unity is a generator of it. So, once one of those things generators is there, its powers will be there; that means, all other roots are also there.

(Refer Slide Time: 35:08)



$$\boxed{\alpha^2 = \frac{(1+i)^2}{2} = \frac{\cancel{1+i^2}+2i}{2} = i}$$

$\frac{1+i}{\sqrt{2}} \in K$, $i \in K$

$\Rightarrow 1+i \in K \Rightarrow \sqrt{2} \in K$ $\Big\}$ $K \supseteq Q(i,\sqrt{2})$.

In fact : $K = Q(i,\sqrt{2})$.

$\frac{1+i}{\sqrt{2}} \in Q(i,\sqrt{2}) \Rightarrow$ all 8 th roots of unity are in $Q(i,\sqrt{2})$

$\Rightarrow$ all roots of X^4+2 are also in $Q(i,\sqrt{2})$

$Q(i,\sqrt{2})$ is a splitting field of X^4+1 over Q.

So, once all roots are there, all 8th roots of unity are there; that means all roots of X power 4 plus 2 are also in Q adjoined i comma root 2, ok. So; that means, Q adjoined i comma root 2 is a splitting field of X power 4 plus 1 over Q, ok. What I have said here just to summarize quickly, I am interested in the splitting field of X power 4 plus 1. We first observed that all roots of X power 4 plus 1 are roots of 8th roots of 1 and one of them has to be primitive 8th root of 1.

So, I am taking that to be 1 plus i over root 2, that must be a root, and what I noted is i and root 2 must be in the field but, once you put i and root 2 every other root automatically can be expressed as a rational polynomial in i and root 2; that means, it contains all the roots. And if you remove either of i or root 2, you will not get all the roots. So, Q adjoined i and root 2 is a splitting field of X power 4 plus 1 over Q.

So, our picture is Q adjoined i comma root 2 containing Q i of course, it contains two fields, Q root 2, Q i and both are extensions of Q. This is a splitting field of X power 4 minus 1; this entire thing is a splitting field of X power 4 plus 1. So, let me stop the video here, the last example I went over fast but, please watch the video again if you need to and ask questions in the discussion forum, if you have any doubts.

Thank you.