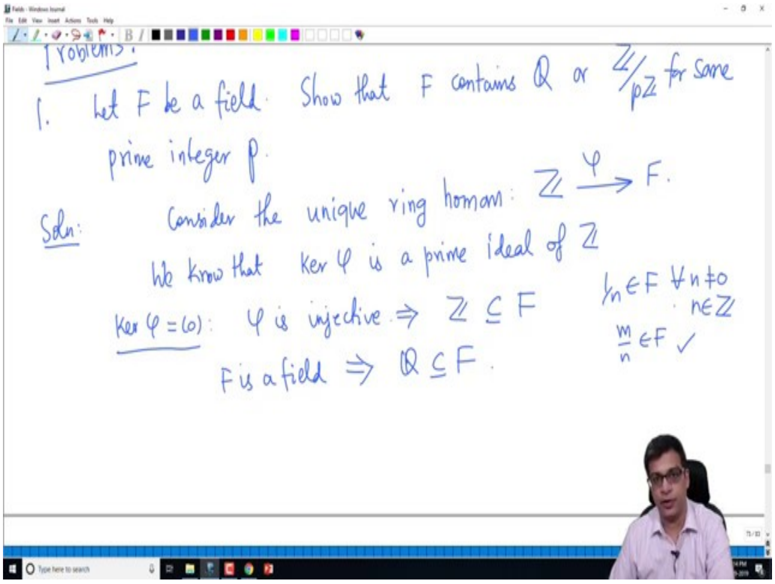
Introduction to Rings and Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 43
Problems 10

(Refer Slide Time: 00:16)



Problems:

1. Let F be a field. Show that F contains $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime integer p.

Soln: Consider the unique ring homom: $\mathbb{Z} \xrightarrow{\varphi} F$.

We know that $\ker \varphi$ is a prime ideal of $\mathbb{Z}$

$\ker \varphi = (0)$: φ is injective $\Rightarrow \mathbb{Z} \subseteq F$ $\quad$ $1/n \in F$ $\forall n \neq 0$, $n \in \mathbb{Z}$

F is a field $\Rightarrow \mathbb{Q} \subseteq F$. $\quad$ $\frac{m}{n} \in F$ ✓

Let us do some problems on field theory, so that we understand all the theory that we have developed in the previous videos. So let me start with some simpler problems. So, let F be any field show that F contains Q or Z mod p Z for some p ok, so this is actually not really a problem, I just wanted to start with this. Because, it captures the main starting point for field theory for some prime p I should say prime integer p.

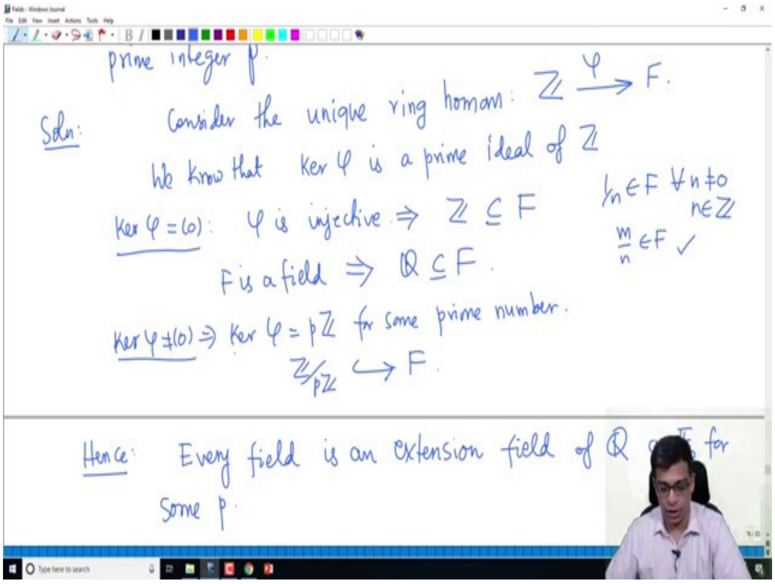
Let F be a field show that it contains either Q or Z mod p Z, so this solution is very easy as I said we have multiple times discussed this. So, consider the unique ring homomorphism from Q or rather Z to F, for every ring, commutative ring with unity there is a unique map from the ring of integers to it.

So, consider the ring unique ring homomorphism from Z to F, we know that by the argument that a sub ring of an integral domain is an integral domain and the first isomorphism theorem. We know that kernel phi is a prime ideal of Z, this came up in when we discussed finite fields also it is a prime ideal of Z.

So, there are two cases if kernel phi is 0 then phi is injective, what are the prime ideals of Z these are ideals, either the 0 ideal or generated by a prime number. So, if it is 0 ideal it is injective; that means, Z is contained in F by abuse of notation I can think of Z actually as a sub ring of F because, Z has an isomorphic copy of itself in F by treating that isomorphic copy as Z I can think of Z as F.

But, how can you get Q then, but because F is a field every integer positive integer, every non negative integer n rather every nonzero integer n has an inverse in F. So, Q itself is contained in F right, because 1 by n is there for all nonzero n, once 1 by n is there m by n is there ok, so every rational number will be there. So, Q itself is contained in F.

(Refer Slide Time: 03:02)



prime integer p.

Soln: Consider the unique ring homom: $\mathbb{Z} \xrightarrow{\varphi} F$.

We know that $\operatorname{Ker}\varphi$ is a prime ideal of $\mathbb{Z}$

$\operatorname{Ker}\varphi = (0)$: φ is injective $\Rightarrow \mathbb{Z} \subseteq F$

F is a field $\Rightarrow \mathbb{Q} \subseteq F$.

$1/n \in F \ \forall n \neq 0, n \in \mathbb{Z}$

$\frac{m}{n} \in F$ ✓

$\operatorname{Ker}\varphi \neq (0) \Rightarrow \operatorname{Ker}\varphi = p\mathbb{Z}$ for some prime number.

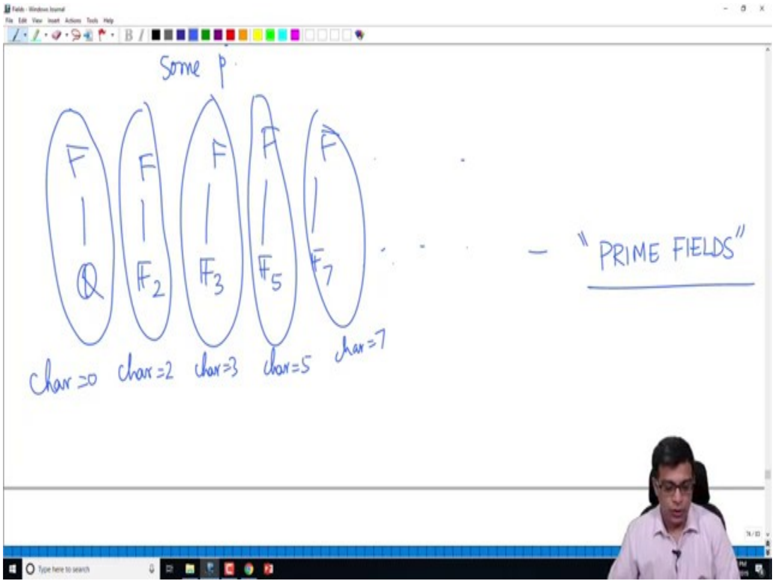
$\mathbb{Z}/p\mathbb{Z} \hookrightarrow F$.

Hence: Every field is an extension field of $\mathbb{Q}$ or $\mathbb{F}_p$ for some p.

So, that is one case; if kernel phi is nonzero this means kernel phi is equal to p Z for some prime number. In this case Z mod p Z is contained in F by the first isomorphism theorem, Z mod kernel is isomorphic to it is image which I am thinking of Z mod p z. So, Z mod p Z is contained in F, so F contains Q in case 1 and F contains Z mod p Z in case 2.

So, that finishes the solution, in other words what we want to remember is hence, every field that you can work with is an extension field of Q or F p for some p. And remember, it has to be exactly one of them as this solution shows if it contains Q it cannot contain F p if it contains F p, it cannot contain F q for some other prime Q ok, so it is exactly one.

(Refer Slide Time: 04:11)

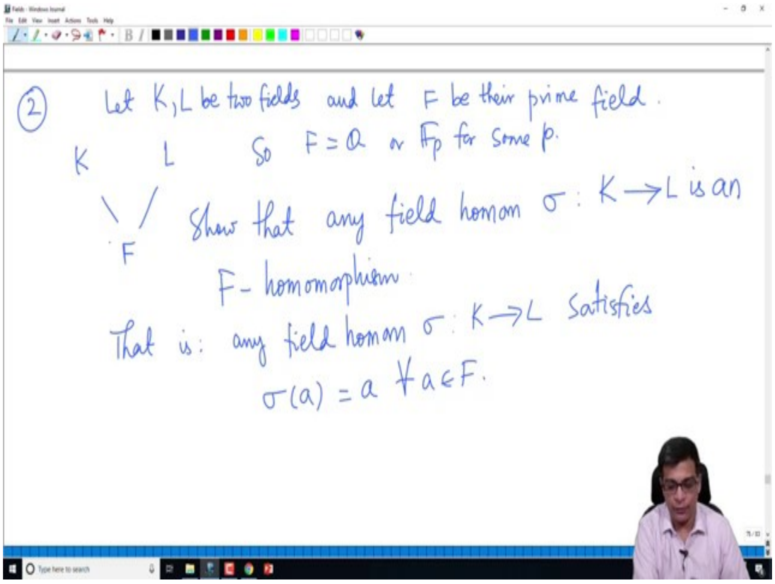


So, basically the world of fields sits above either Q or F 2 or F 3, F 5, F 7 and so on, so you have a fields here, you have a fields above this, you have a fields above this and above this above this and so on. So, every field is above either Q or F 2 or F 3 and it is unique, so there is no connection between this, these are all disconnected.

In this case we say characteristic is 0, in this case we say characteristic is 2, in this case we say characteristics is 3, in this case we say characteristic is 5, in this case we say characteristic is 7 and so on, right. So, characteristic 0 fields are all living above Q characteristic 2 fields are all living above F 2 and so on.

So, these bottom things are called prime fields, so prime fields are those that are at the base of every field; so, either Q so, prime field of a characteristic 0 field is like is Q, prime field of a characteristic 2 field is 2 F 2, prime field of a characteristic 11 field is F 11 and so on. So, every field is an extension of this, so that is the first exercise, so we have every field is like this.

(Refer Slide Time: 05:38)



② Let K, L be two fields and let F be their prime field.

So $F = \mathbb{Q}$ or $\mathbb{F}_p$ for some p.

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

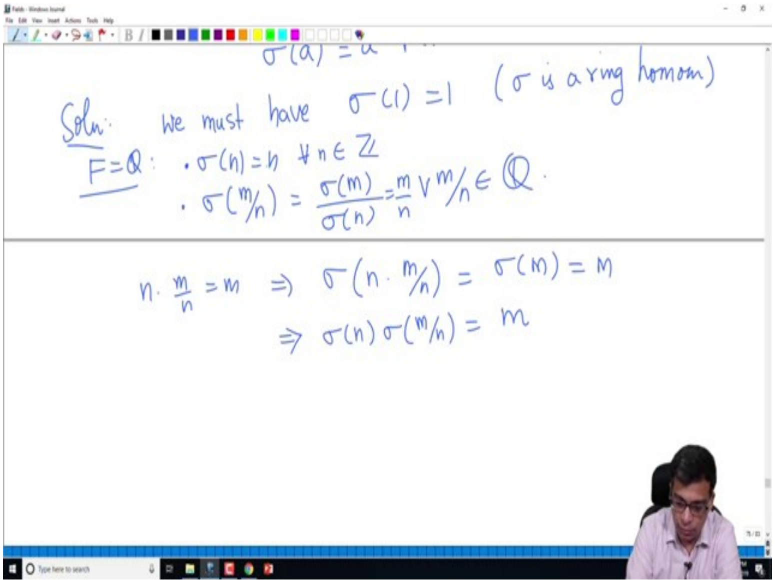
Show that any field homom $\sigma : K \to L$ is an F-homomorphism.

That is: any field homom $\sigma : K \to L$ satisfies $\sigma(a) = a \ \forall a \in F$.

So, second exercise; let K be a field and let F be it is prime field, remember there is a uniquely determined prime field. Let K and L be two fields I should say and let F be their prime field, so what we have is K is here, L is here and they are both over F. So, F is in fact, so F is Q or F p for some p right, so F is Q or F p, so I want to do an exercise which is not dependent on which case we are dealing with.

So, F is an arbitrary prime field it is either one of those and K and L are two fields then show that. So, this K map when we talked about field homomorphisms, so show that any field homomorphism sigma from K to L is an F-homomorphism right. So, in other words that is any field homomorphism fixes any field homomorphism sigma from K to L satisfies sigma of a is equal to a for all a in F. That means, it fixes every element of F this is not true remember if you take an arbitrary field extension. If F is arbitrary and K and L are two arbitrary field extensions of F not every homomorphism is necessarily an F homomorphism, this is only a statement for prime fields, ok.

(Refer Slide Time: 07:41)



$\sigma(a) = a$

Soln: We must have $\sigma(1) = 1$ (σ is a ring homom)

$F = \mathbb{Q}$:
- $\sigma(n) = n \ \forall n \in \mathbb{Z}$
- $\sigma(m/n) = \frac{\sigma(m)}{\sigma(n)} = \frac{m}{n} \ \forall m/n \in \mathbb{Q}$.

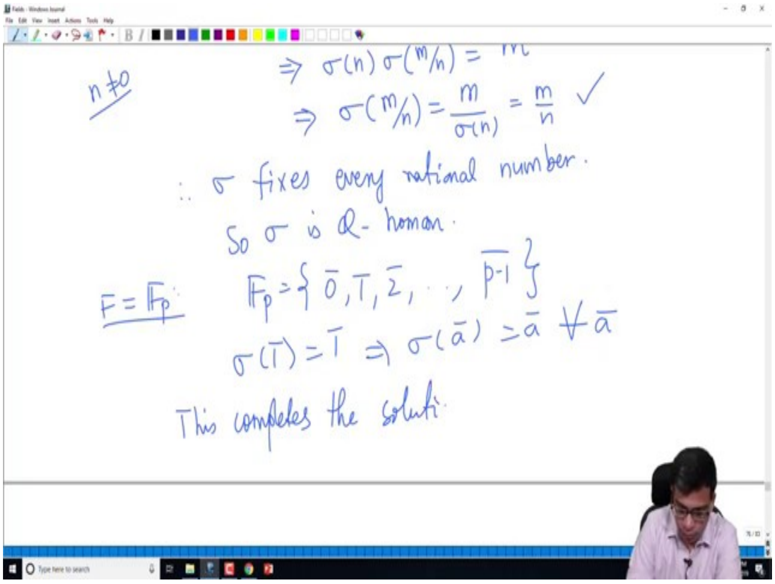
$$n \cdot \frac{m}{n} = m \Rightarrow \sigma(n \cdot m/n) = \sigma(m) = m$$
$$\Rightarrow \sigma(n)\sigma(m/n) = m$$

So, I will quickly do this, this is not difficult and I will start the solution and leave the actual solution to you, the detailed solution to you. So, the point is we must have sigma 1 is 1, so this is ok, this is forced for us because sigma is a ring homomorphism. Any ring homomorphism sends 1 to 1 and a field homomorphism is actually just a ring homomorphism.

So, 1 sigma 1 is 1, so sigma n is n, so I am going to first consider the case F equal to Q, sigma n is equal to n for all n in Z. Because, sigma 2 is sigma 1 plus sigma 1 which is 2, and 1 sigma n is n sigma right, sigma m by n is equal to sigma m by sigma n for all m by n in Q. So, this is because the first power condition is clear, for the second condition what we have is n times m by n is m, right.

So, this implies sigma n times m by n is equal to sigma m which is m. You have already showed that sigma of integers are those integers itself sigma fixes integers. This is clear because sigma 1 is 1, but this means sigma is a field homomorphism, so this means sigma of n times sigma of m by n is equal to m, ok. So, actually what I should really write is m by n. So, sigma of m is m sigma of n is n.

(Refer Slide Time: 09:32)



$n \neq 0$

$\Rightarrow \sigma(n)\,\sigma(m/n) = m$

$\Rightarrow \sigma(m/n) = \dfrac{m}{\sigma(n)} = \dfrac{m}{n}$ ✓

$\therefore$ σ fixes every rational number.

So σ is $\mathbb{Q}$- homom.

$\underline{F = \mathbb{F}_p}$: $\mathbb{F}_p = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{p-1}\}$

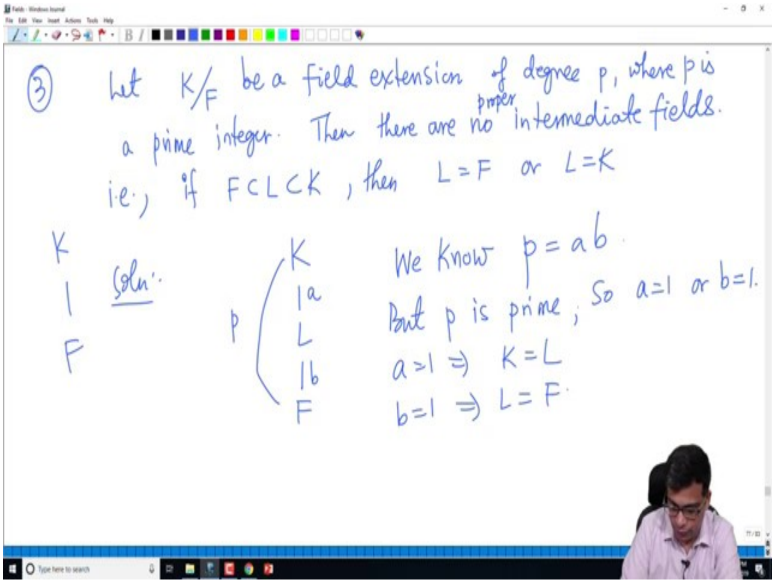
$\sigma(\bar{1}) = \bar{1} \Rightarrow \sigma(\bar{a}) = \bar{a} \ \forall \bar{a}$

This completes the soluti

So, sigma of n times sigma of n by n is m, so sigma of m by n is equal to m by sigma of n which is, so I am assuming of course, n is non-zero here which is m by n ok. So, sigma fixes every rational number; so, sigma is a Q homomorphism. The argument is even easier for F p, because F p is actually nothing but 0 bar, 1 bar, 2 bar up to p minus 1 bar, right.

So, sigma of 1 bar is 1, because 1 multiplicative identity goes to itself, so sigma of a bar is a bar for all a bar, because each of them is one added to itself that many times; so, this finishes the solution, right. So, any homomorphism of extensions is in field extensions is in fact, a homomorphism over the prime field; here very important point is that F has to be Q or Z mod p Z otherwise it is not true So, that is a nice thing to know you do not need to separately check that it fixes Q or it fixes F p point wise.

(Refer Slide Time: 11:05)



③ Let K/F be a field extension of degree p, where p is a prime integer. Then there are no proper intermediate fields.

i.e., if $F \subset L \subset K$, then $L = F$ or $L = K$

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

Soln:

$$\begin{tikzcd} K \arrow[d, dash, "a"] \arrow[dd, dash, bend right, "p"'] \\ L \arrow[d, dash, "b"] \\ F \end{tikzcd}$$

We know $p = ab$.

But p is prime; So $a=1$ or $b=1$.

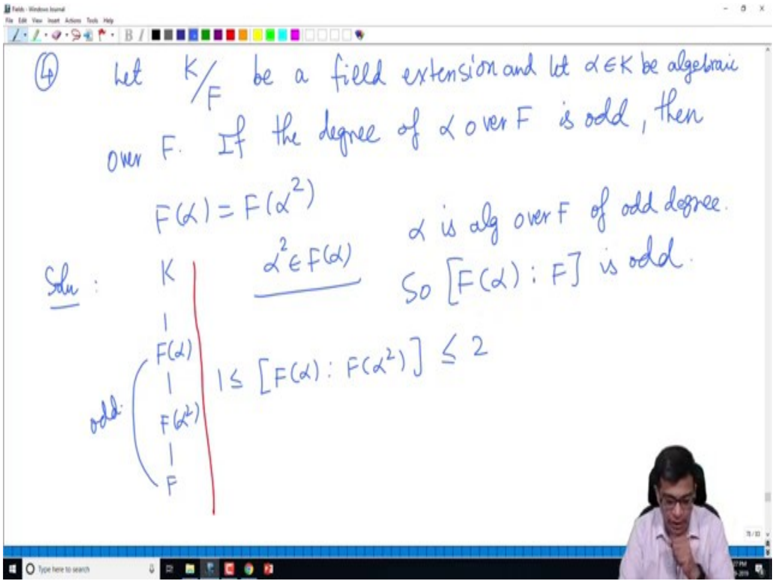
$a=1 \Rightarrow K=L$

$b=1 \Rightarrow L=F$.

So, the third exercise which is also very simple, so let K over F be a field extension of degree p where p is a prime integer. Then there are no intermediate fields, what I mean is that is, if F is contained in L is contained in K then L is equal to F or L equal to K, so what I really mean is that there are no proper intermediate fields.

So, K is here, F is here there is nothing in between other than K and F of course, this is also very simple, because if K F L is in between this we know is p, let us say this is a, this is b we know p is equal to a b, right. So, we know p is equal to a b, but p is prime; so, a is equal to 1 or b equal to 1 any prime number cannot factor non-trivially. So, if a is equal to 1, that means, K is equal to L; if b equal to 1; that means, L is equal to F.

(Refer Slide Time: 12:38)



(4) Let K/F be a field extension and let $\alpha \in K$ be algebraic over F. If the degree of α over F is odd, then

$F(\alpha) = F(\alpha^2)$

Soln:

$$\begin{tikzcd} K \arrow[d, dash] \\ F(\alpha) \arrow[d, dash] \\ F(\alpha^2) \arrow[d, dash] \\ F \end{tikzcd}$$

odd

$\underline{\alpha^2 \in F(\alpha)}$

α is alg over F of odd degree.

So $[F(\alpha):F]$ is odd.

$1 \leq [F(\alpha):F(\alpha^2)] \leq 2$

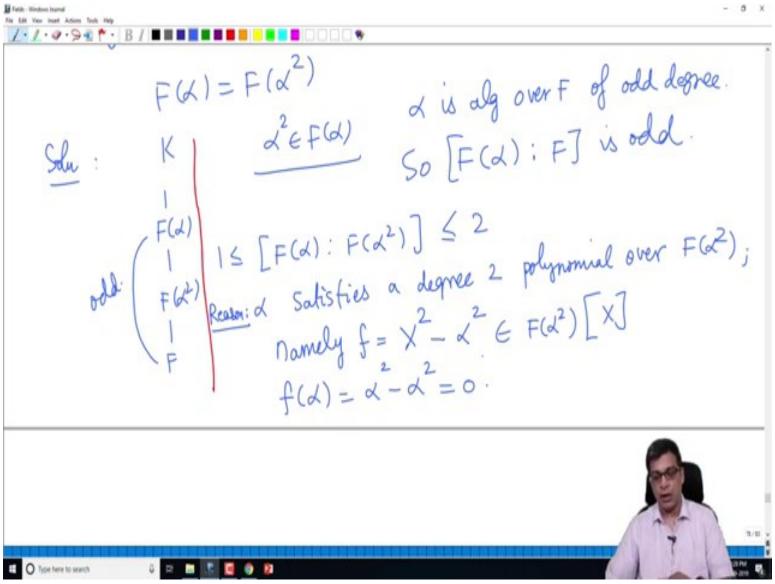
So, that also finishes the solution of this problem, so if you have a prime degree extension there are no proper intermediate fields, so let me do one more example in a similar flavor: let K over F be a field extension. So, the previous problem and this problem are characteristic independent I am not assuming anything about what the prime field is, it works for any prime field. Let K over F be a field extension and let alpha in K be algebraic over F.

If the degree of alpha over capital F is odd then what we can say is that F alpha is equal to F alpha squared. This is also really a consequence of multiplicativity of degree, but in a slightly different way, so let us do this. So, we have K which is actually not relevant we are really interested in F alpha, F alpha squared, F alpha, F.

So, remember alpha squared certainly contains F alpha is contained in F alpha because, alpha squared is here, alpha squared is a polynomial in alpha with coefficients in F namely it is one times alpha squared. So, it is there, so F alpha squared is a subfield, what do we know? We know that alpha is algebraic over F of odd degree.

So, F alpha colon F is odd right, because again remember degree of an algebraic extension generated by a single element alpha is equal to the degree of the element itself, so this is odd. On the other hand I claim that the degree of extension F alpha over F alpha squared is less than or equal to 2, so of course, it is greater than equal to 1. Any degree of a field extension will have positive degree, it cannot have degree less than one right, so it is either it is at least one, I claim that it is at most 2 here.

(Refer Slide Time: 15:25)



$F(\alpha) = F(\alpha^2)$

α is alg over F of odd degree.

$\underline{\alpha^2 \in F(\alpha)}$

So $[F(\alpha) : F]$ is odd.

Soln :

$$\begin{tikzcd}
K \arrow[d, dash] \\
F(\alpha) \arrow[d, dash] \\
F(\alpha^2) \arrow[d, dash] \\
F
\end{tikzcd}$$

odd.

$1 \leq [F(\alpha) : F(\alpha^2)] \leq 2$

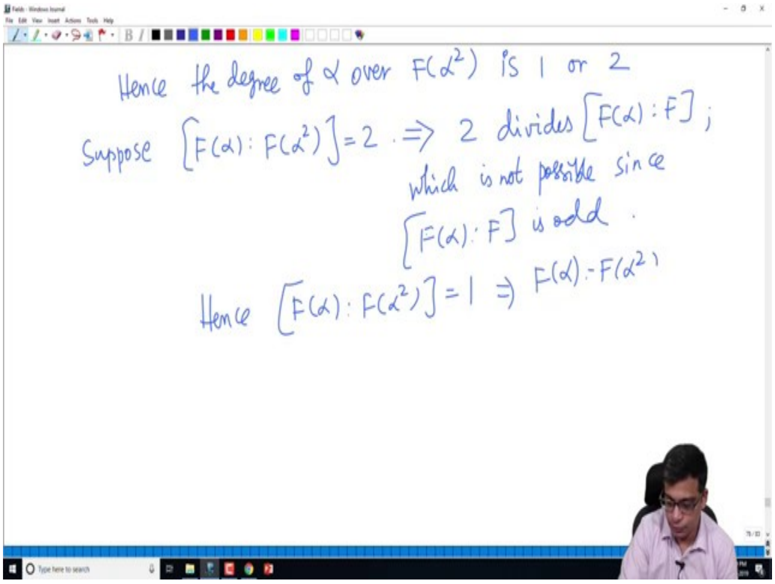
Reason: α satisfies a degree 2 polynomial over $F(\alpha^2)$;

Namely $f = X^2 - \alpha^2 \in F(\alpha^2)[X]$

$f(\alpha) = \alpha^2 - \alpha^2 = 0$.

This is because alpha satisfies a degree 2 polynomial, so the reason is this. The reason for the upper bound is that alpha satisfies a degree 2 polynomial over F alpha square. Namely, X squared minus alpha squared, this is a polynomial in over the ring over the field F alpha squared right, because alpha squared is an element of F alpha squared. So, this is a polynomial of degree 2 over this, so if you take F equal to this, what is F alpha this is alpha squared minus alpha squared which is 0, so alpha satisfies a degree 2 polynomial.

(Refer Slide Time: 16:18)



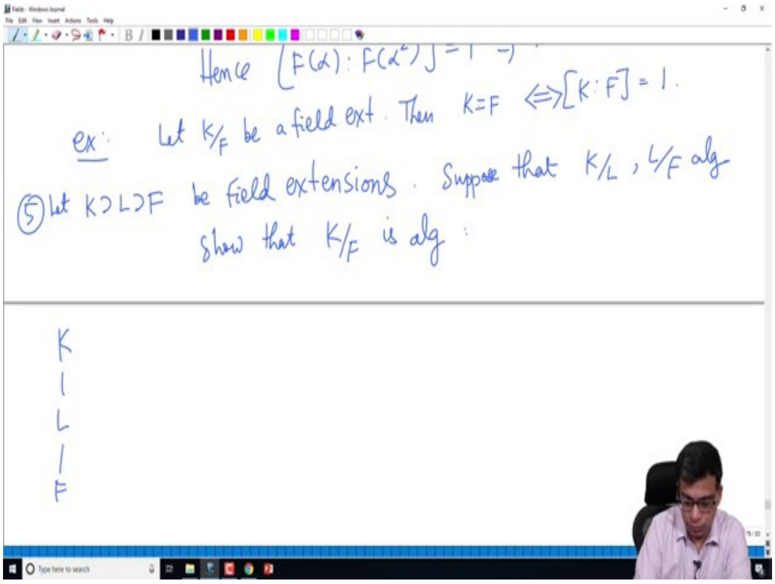
Hence the degree of α over $F(\alpha^2)$ is 1 or 2

Suppose $[F(\alpha):F(\alpha^2)]=2 \Rightarrow 2$ divides $[F(\alpha):F]$; which is not possible since $[F(\alpha):F]$ is odd.

Hence $[F(\alpha):F(\alpha^2)]=1 \Rightarrow F(\alpha)=F(\alpha^2)$

Hence, the degree of alpha over F alpha square is 1 or 2; it may not be 2 right, because maybe as alpha itself is in F alpha squared. So, it can be 1, but it cannot be more than 2 because it satisfies a degree 2 polynomial, but suppose it is 2. That means, F alpha colon F alpha squared is 2, but this is not possible right because then 2 divides the degree of F alpha over F which is not possible because since F alpha colon F is odd. Hence, F alpha colon F alpha squared is 1; it is either 1 or 2, it cannot be 2, so it has to be 1; that means, F alpha is equal to F alpha squared, right.

(Refer Slide Time: 17:28)



Hence $[F(\alpha):F(\alpha^2)]=1 \Rightarrow$

ex: Let K/F be a field ext. Then $K=F \Leftrightarrow [K:F]=1$.

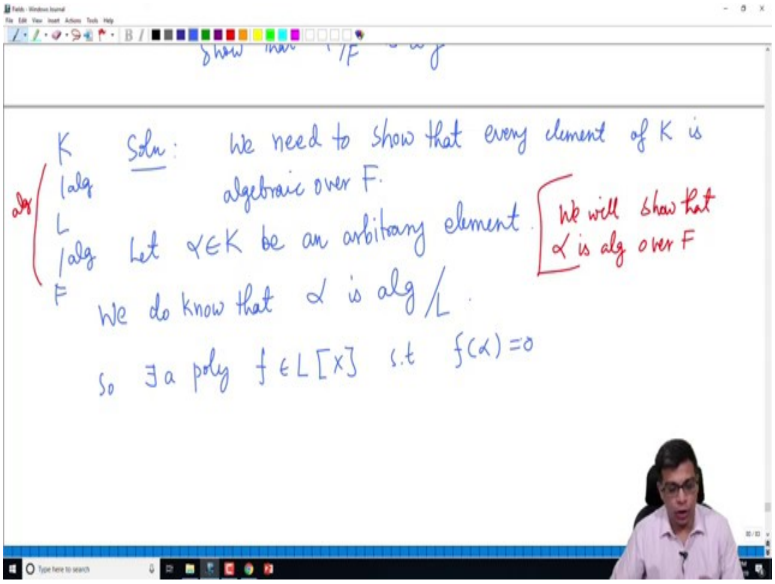
(5) Let $K \supset L \supset F$ be field extensions. Suppose that K/L, L/F alg. Show that K/F is alg.

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

There is a small observation here which is that if you have a field extension this I have used multiple times let K over F be a field extension; that means, K is a field containing another field F then K is equal to F if and only if K colon F is 1, the degree is 1. So, F alpha colon F alpha squared is 1; that means, F alpha is equal to F alpha squared, so what we have is that this is equal. So, this is a nice convenient statement sometimes that is useful to you, if you have an algebraic element whose degree is even sorry, whose degree is odd then if you take the field generated by the square of it is the same field.

So, now, let us continue with some more problems, so this is 4th problem, so let us do 5th problem. So, what I want to do now is let us take three fields let us say K containing L containing F are algebraic field extensions. So, what we have is that K over L, so I will write it here K over L over F, suppose that K over L and L over F are algebraic show that K over F is algebraic, ok.

(Refer Slide Time: 19:13)



K
|alg
L
|alg
F

alg

Soln: We need to show that every element of K is algebraic over F.

Let $\alpha \in K$ be an arbitrary element. We will show that α is alg over F

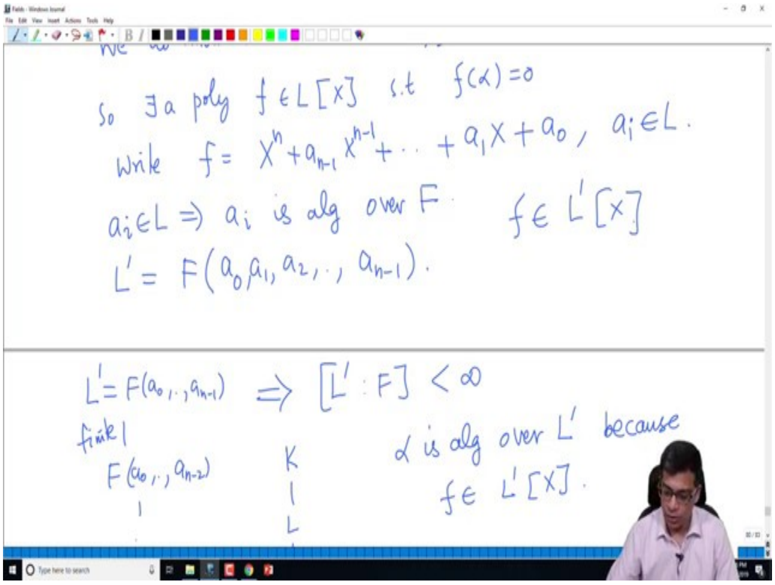
We do know that α is alg $/L$.

So $\exists$ a poly $f \in L[x]$ s.t $f(\alpha)=0$

So, what I am saying is that this is algebraic; this is algebraic show that this is algebraic. So, the two intermediate extensions are algebraic show that the bigger extension is algebraic. So, this is also easy, this uses something that we have done in the in one of the previous videos. So, we need to show that, what is an algebraic extension, it is an extension that every element is algebraic we need to show that every element of K is algebraic over F.

So, let us take an arbitrary element, so let alpha in K be an arbitrary element we want to show that it is algebraic over F, we will show that alpha is algebraic over F, that is what our goal is. We do know that that alpha is algebraic over L right, because K is algebraic over L; that means, every element of K is algebraic over L. So, there exists a polynomial f in L X such that f alpha is 0, so there is a polynomial with coefficients in L which has alpha as a root.

(Refer Slide Time: 20:43)



So $\exists$ a poly $f \in L[X]$ s.t $f(\alpha) = 0$

Write $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, $a_i \in L$.

$a_i \in L \Rightarrow a_i$ is alg over F. $f \in L'[X]$

$L' = F(a_0, a_1, a_2, \ldots, a_{n-1})$.

$L' = F(a_0, \ldots, a_{n-1}) \Rightarrow [L' : F] < \infty$

finite

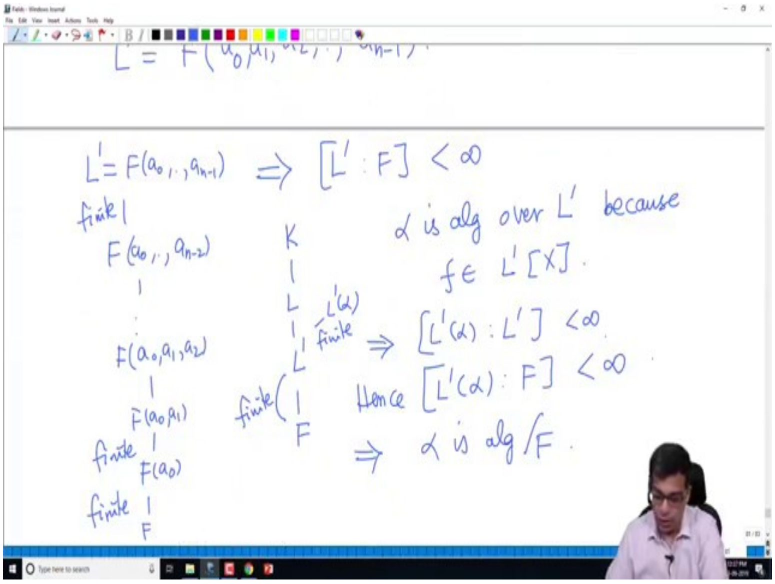
$F(a_0, \ldots, a_{n-2})$

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

α is alg over L' because $f \in L'[X]$.

So, suppose we have f as X power n, a n minus 1 X power n minus 1, a 1 X plus a 0 and remember ai’s are in L. Since ai’s are in L each a i is algebraic over capital F because L is algebraic over capital F; that means, every element of L is algebraic over capital F. Now, let us consider the new field let us call it L prime to be F adjoined a 1or another a 0, a 1, a 2 up to a n minus 1; I claim that this is algebraic over F.

(Refer Slide Time: 21:37)



$L = F(a_0, a_1, a_2, \ldots, a_{n-1})$

$L' = F(a_0, \ldots, a_{n-1}) \Rightarrow [L' : F] < \infty$

$$\begin{tikzcd}[column sep=small] L' \arrow[d, dash, "\text{finite}"'] \\ F(a_0, \ldots, a_{n-2}) \arrow[d, dash] \\ \vdots \\ F(a_0, a_1, a_2) \arrow[d, dash] \\ F(a_0, a_1) \arrow[d, dash, "\text{finite}"'] \\ F(a_0) \arrow[d, dash, "\text{finite}"'] \\ F \end{tikzcd} \qquad \begin{tikzcd}[column sep=small] K \arrow[d, dash] & \\ L \arrow[d, dash] & L'(\alpha) \arrow[dl, dash, "\text{finite}"] \\ L' \arrow[d, dash, "\text{finite}"'] & \\ F & \end{tikzcd}$$

α is alg over L' because $f \in L'[X]$.

$\Rightarrow [L'(\alpha) : L'] < \infty$

Hence $[L'(\alpha) : F] < \infty$

$\Rightarrow \alpha$ is alg $/F$.

So, what is L prime? L prime is F this we have done actually in one of the previous videos, so L prime is F adjoined a 0 a n minus 1, but each of them is an algebraic element, so you can actually 1 by 1 attach this, ok. So, you have these; this is algebraic because a 0 is algebraic over F, a 0 being an element of L and L is an algebraic extension of F, a 0 is algebraic over F. It is algebraic hence it is finite an algebraic extension generated by a single element is finite.

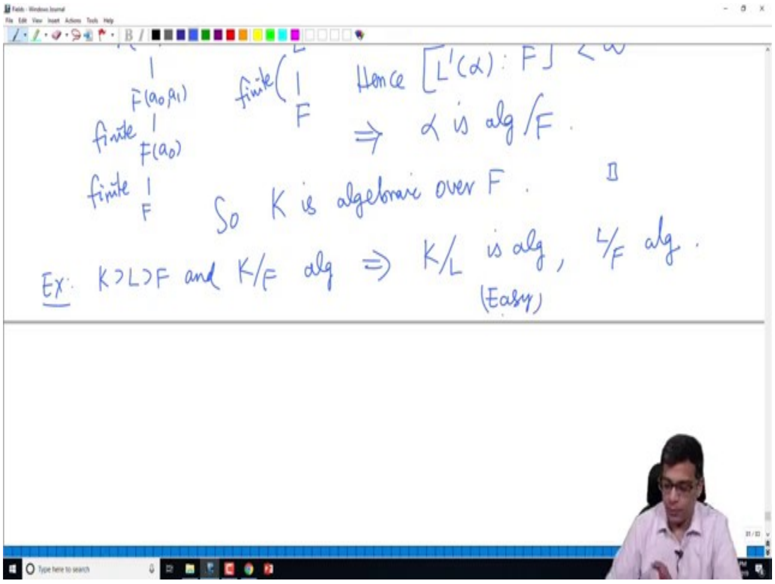
Similarly, a 1 is algebraic over F certainly a 1 then is algebraic over F a 0, so this is finite everything here is finite, so L prime over F is finite, but a finite extension is algebraic, ok. So, what I want to say is that it is finite, now so let us keep that aside what we have is K actually what we have is K, L prime and F, L prime contains L.

So, the full picture is like this K, L, L prime over F; remember L prime is only generated L prime does not include all elements of L it only includes these coefficients of this particular small F, what we have shown is that this is finite. Now, I claim that alpha is algebraic over L prime; alpha is algebraic over L that we know, but it is in fact, algebraic over L prime because, the polynomial that alpha satisfies. In fact, lives over alpha L prime right, because L prime was constructed.

So, that this F that we have here whose coefficients are a priori in L are in fact, over L prime because, a 0, a 1, a 2, a n minus 1 are all in L prime, so it is algebraic over L prime and hence L prime alpha over L is a finite extension. So, I will write it like this L prime alpha over L prime is finite, so what I have is L prime alpha is finite. Because, again it is finite, it is an algebraic extension generated by a single element, so it is the degree of alpha itself, so it is finite.

So, now, this is finite this is finite; hence, L prime alpha over F itself is finite because, L prime alpha over F is L prime F dot L prime alpha over L prime, so this times this is L prime alpha over F. So, if L prime alpha over F is finite; that means, alpha is algebraic over F right, because the field generated by and L prime alpha is actually nothing but yeah, so it is a finite extension, so it is algebraic over F. So; that means, what we have shown is that it is contained in a finite extension; that means, it is algebraic and remember alpha was an arbitrary element and we have shown that it is algebraic over F.

(Refer Slide Time: 25:32)



$F(a_0, a_1)$

finite

$F(a_0)$

finite

F

finite

F

Hence $[L'(\alpha) : F] < \infty$

$\Rightarrow \alpha$ is alg $/F$.

So K is algebraic over F. ▯

Ex: $K \supset L \supset F$ and K/F alg $\Rightarrow K/L$ is alg, L/F alg.

(Easy)

So, K is algebraic over F ok, so that finishes the solution of that problem, what we have shown is that if you have two field extensions intermediate ones are finite sorry, intermediate ones are algebraic, the bigger one is algebraic. Of course, the; I mean if the whole thing is algebraic it is a trivial fact that both intermediate things are also algebraic.

So, if you have K containing L containing F and K over F is algebraic this is very easy K over L is algebraic and L over F is algebraic. Because K site, every element of K satisfies a polynomial relation over capital F, so it automatically satisfies a polynomial relation over capital L. Similarly, every element of L is an element of K it satisfies a polynomial relation over F, so this is also algebraic, so this is easy.

The converse is what the problem asked you to do; so, but altogether you can now remember this as saying if you have three fields and they form a tower, the full thing is algebraic if and only if both the intermediate things are algebraic.

So, so far we have done some of the problems, so I am going to stop this video here; in the next video we will continue and discuss some more problems

Thank you.