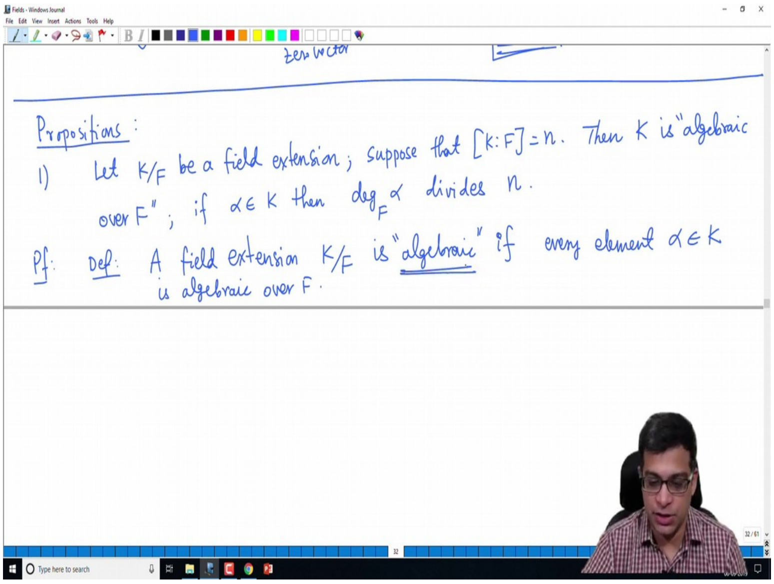
Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture – 37
Algebraic elements form a field

Let us continue now. In the last video we proved that degree of an element is equal to the degree of the field generated by that element loosely speaking and also we showed that the degree is multiplicative for field extensions.

(Refer Slide Time: 00:31)

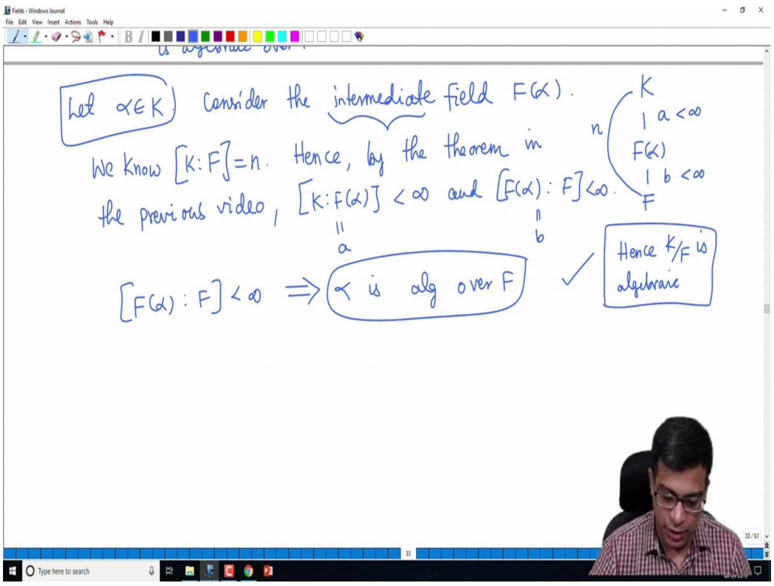


So, we are going to exploit those two facts and to make some nice observations today ok. So, let me go ahead and prove the propositions one by one, so the first one I want to say is let K be a field extension over F. Let K over F be a field extension and suppose that the degree of the extension is n.

Then K is algebraic over F ok, so I do not recall if I defined what it means for a field to be algebraic over a base field, if not I will just quickly do this when I do the proof K is algebraic over F. If further if alpha is in K, then the degree of alpha over F divides n ok. So, let me prove this proposition before we come to the other proposition later.

So, let me first say what is the definition of a field extension being algebraic, a field extension it is a very simple definition. A field extension K over F is algebraic if every element of K is algebraic over F that is all, very simple. So, an algebraic extension is one where every element is algebraic we have already defined the meaning for an element to be algebraic. So, to prove K is algebraic over F all we need to show is that every element of K is algebraic over F ok, so now this is very easy.

(Refer Slide Time: 02:31)



So, what we have is an arbitrary element in K, we are going to prove both statements of the proposition in one shot, consider the intermediate field F alpha. So, the intermediate field the word intermediate refers to the fact that you have F alpha between K and F. So, it is an intermediate field it is between these two what do we know now we are given that this is n. And suppose, so we know by hypothesis that K colon F is n.

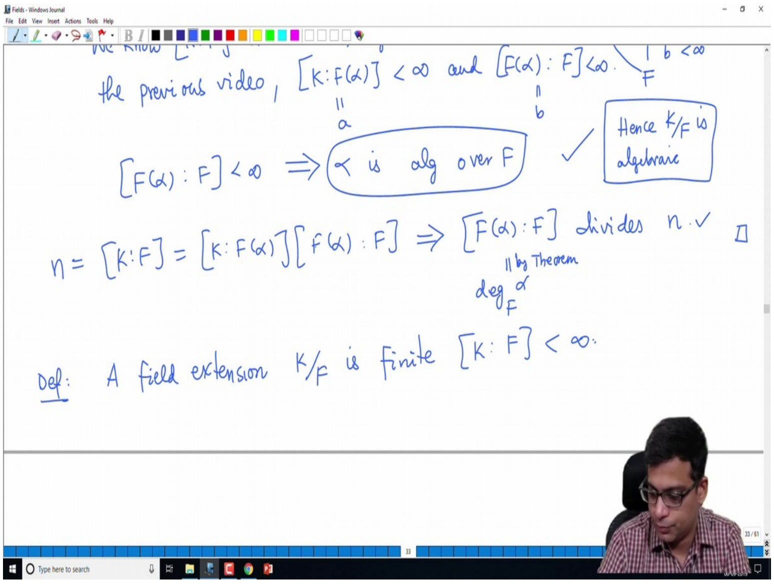
So, immediately hence by the theorem above in the previous video the multiplicativity of the degree, remember K colon F alpha is less than infinity. And F alpha colon F is also less then infinity, why is this? Because if either of them infinity either K colon F alpha is infinity or F alpha over F is infinity there product remember will be the product degree of K colon F.

We have shown in part of the first case of the proof of that theorem if the K colon F alpha is infinity or F alpha over F is infinity K colon F is also infinity. But we are given that it is a finite degree I mean when I say n of course, I mean that it is a it is an integer; that means, it is not infinite. That means, this let us call that a, let us call this b and both are infinity, so this is those are finite, so a and b are finite things and a b is equal to n.

So, first of all we already know that F alpha colon F is infinity implies alpha is algebraic over ok. So, this is the first part right, we are trying to show that alpha is algebraic, we started with an arbitrary element and we concluded that it is algebraic.

Hence, K over F is algebraic what is an algebraic extension? I wrote here it means every element is algebraic I started with an arbitrary element nothing special about alpha. Alpha is any element and I concluded that it is algebraic over F, so the extension itself is algebraic, so this is the first part.

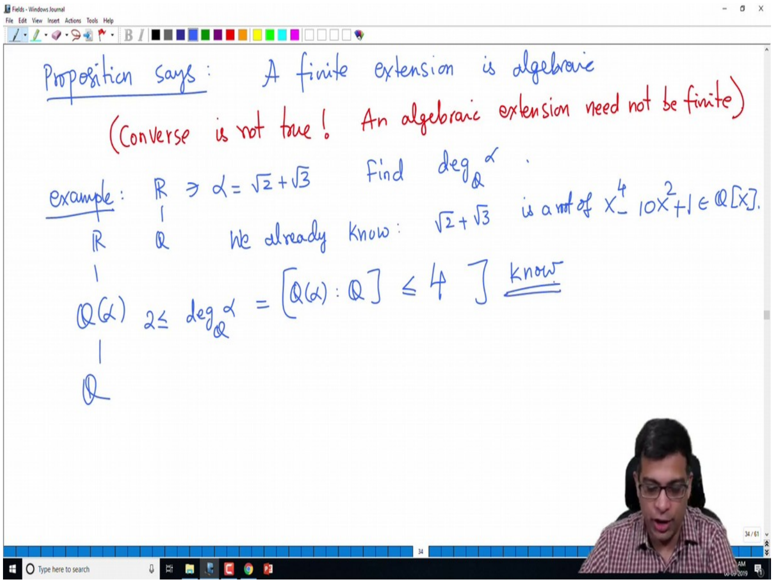
(Refer Slide Time: 05:07)



But we also have the second part, because we know that K colon F is equal to K colon F alpha times F alpha colon K or F alpha colon F and this is n. So, F alpha colon F divides n, but remember the crucial theorem that we proved in the previous video is that this is exactly equal to degree of alpha over F right, this is by theorem.

The first theorem of the last video, by that theorem the degree of F alpha over F is equal to degree of alpha over F, so that divides n, so this is the second statement, so, we get what we want ok. So, this says that if you have a finite extension ok, so also let me define this formally, so that we can refer to this without any confusion. A field extension K over F is called finite very simple if K colon F is finite ok, so field extension is finite, its degree is finite.

(Refer Slide Time: 06:23)



So, what we have, the theorem proposition really said? Proposition says, a finite extension is algebraic, what we have said the first part of the proposition said a finite extension is algebraic. All we assumed was that it is a finite extension and we showed that algebraic. More over we in fact, have that degree of any element in the field K over capital F in fact, divides the degree. But, this is a useful statement to remember and I will remind you or actually tell you and we will come back to this later converse is not true.

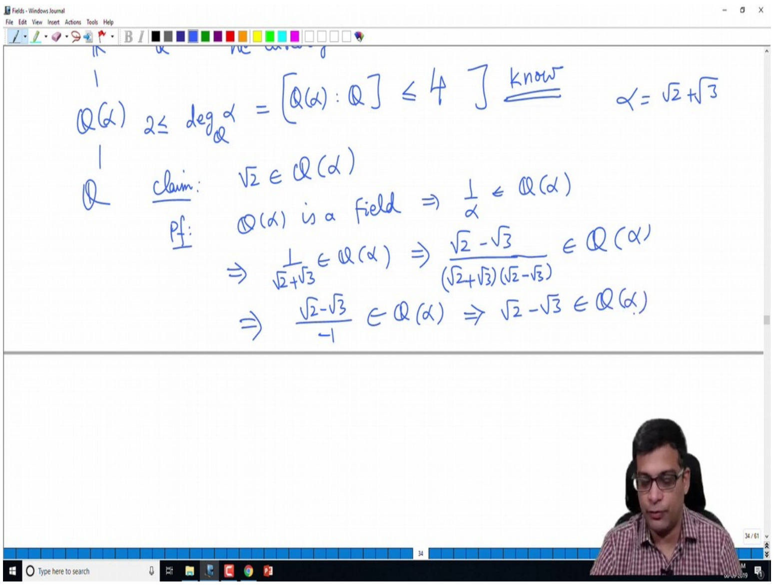
So, that is, an algebraic extension need not be finite, algebraic extension need not be finite, so this is for later, but a finite extension is algebraic. So, as an example of this let me go quickly tell you something that we did in a previous video. So, we considered the field for example, R over Q the field extension and we looked at alpha in R to be root 2 plus root 3.

If you looked at this element and we want to find degree of alpha over Q, so that was the question. So, we observed last time that we already know that root 2 plus root 3 satisfies ok. So, I am going to recall I do not the polynomial, so let me look it up, so X power 4 minus 10 X squared plus 1 or rather I will write like this is a root of this polynomial is a roots right.

So, it is a root of this that we have shown by if you check that video you will see that we wrote alpha is equal to root 2 plus root 3, then wrote alpha minus root 2 is equal to root 3 and squared and then we did another squaring later on to get this. So; that means, now I am going to consider this extension forget R my goal is to consider this extension of course, this is an R.

But I am mainly interested in this extension, to find the degree of this, all we need to find is the degree of the filed extension we typically write round bracket alpha though we can also write square bracket alpha here. Degree of alpha this; this we know, what we can definitely say is that this is less than or equal to 4 and we also said this is at list 2, so this we know right. So, what I now want to do is to determine whether it is 2, 3 or 4, so let us look at this.

(Refer Slide Time: 09:27)

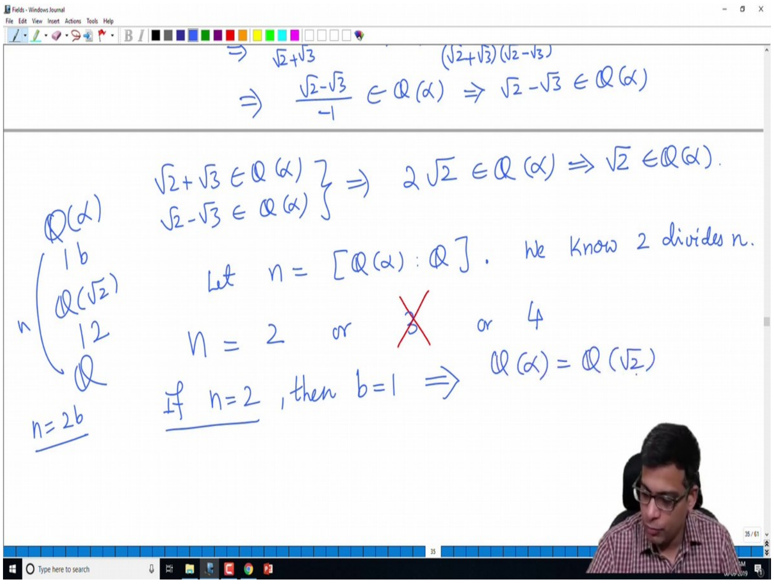


So, first I claim that a simple fact root 2 and root 3 both belong to or actually I will just say root 2 belongs to Q alpha, of course, than root 3 also belongs to it, but I do not need that, so I claim root 2 belongs to this. This is a nice argument what we have saying is that root 2 can written as a polynomial and root 2 plus root 3 which is not a priori clear, but we can do this.

So, what do we do, since Q alpha is a field 1 by alpha is in Q alpha remember Q alpha is a field. So, alpha is a nonzero element, so it is inverse is there; that means, 1 by root 2 plus root 3 is in Q alpha because alpha remember is just root 2 plus root 3. I am just writing that as alpha for simplicity; this means I multiply both's numerator and denominator by root 2 minus root 3 ok.

So, what I get is root 2 minus root 3 in the numerator, and root 2 plus root 3 times root 2 minus root 3 in the denominator. This belongs to Q alpha because I have not changed anything, multiplied both the thing numerator and denominator by root 2 minus root 3. So, what do I get is root 2 minus root 3, but what is root 2 plus root 3 times root 2 minus root 3? That is actually minus 1 this is in Q alpha right. So; that means, root 2 minus root 3 is in Q alpha, because that negative of root 2 minus 3 is there means root 2 minus root 3 is there.

(Refer Slide Time: 11:03)

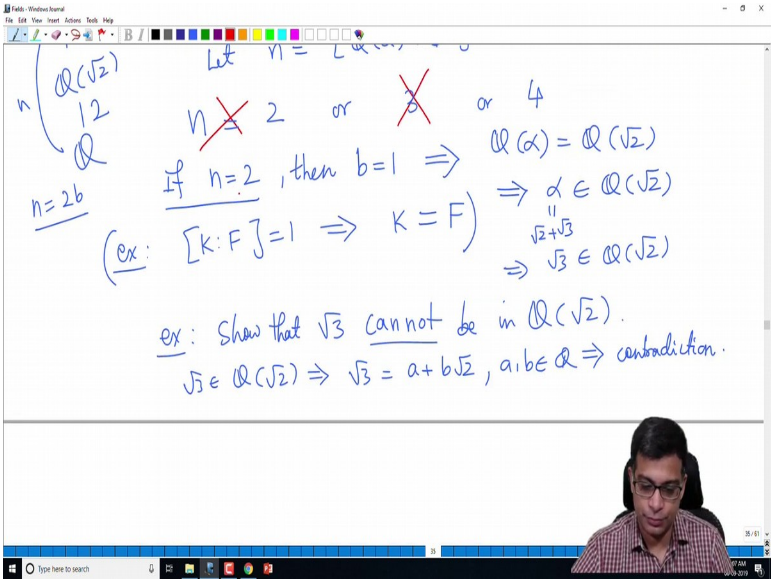


On the other hand, root 2 plus root 3 is also in Q alpha root 2 minus root 3 in Q alpha together these two imply there sum is in Q alpha. Because Q alpha is a field two elements are there means their sum is there, again using the fact that Q alpha is a field we can divide by 2; that means, root 2 is an Q alpha very good, so root 2 is there.

So, our field extension now has this shape, Q alpha Q root 2, Q ok. So now, let us use a of degrees this we know is 2 that is easy to show because root 2 satisfies x squared minus 2 which you know is irreducible for example, by Eisenstein's criteria. So, now let n be the degree of the field extension Q alpha over Q what we know is that we now know 2 divides n, because if this is b let us say then and this is n we know that n is equal to 2 b.

So, remember earlier we said l is n is 2 or 3 or 4 in the previous video when we talk about this, these were the three possibilities we ruled out 1 and we know that it is less than or equal to 4. Now, we can rule out 3 right, because 3 is not divisible by 2, so now, it is either 2 or 4. If n is equal to 2, then b is equal to 1 right, because 2 times b is n; n is 2; that means, b is equal to 1. But, if b is equal to 1 Q alpha equal to Q root 2 ok, so this is a simple exercise for you.

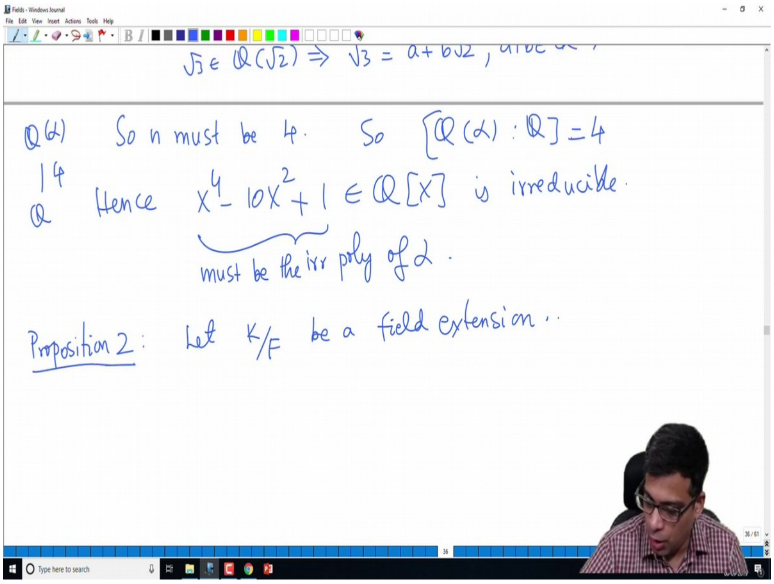
(Refer Slide Time: 13:01)



If you have a field extension with degree 1 you should do this; that means, K is equal to F, if the degree of the field extension is 1 K is equal to F. So, Q alpha is equal to Q root 2, so let me continue that here Q alpha is equal to root Q root 2; that means, alpha is in Q root 2. So, what we have is that this top extension is trivial, if alpha is in Q root 2 alpha remember is root 2 plus root 3. If root 2 plus root 3 is in Q root 2 then Q root Q root 3 is in Q root 2 because it is root 2 plus root 3 minus root 2. So, root 3 is in Q root 2 and this is another exercise I will leave it for you show that root 2 root 3 cannot be in Q root 2 this is very easy.

Because if it is there I will I will just start the proof and leave you the details: root 3 can be written as a plus b root 2 where a and b are recall what is the basis of Q root 2 over 2, it is 2 and root 2 and this leads to a contradiction. Root 2 cannot be written as a linear combination of a rational number plus another rational number turns root 2, so; that means, that n cannot be 2.

(Refer Slide Time: 14:37)

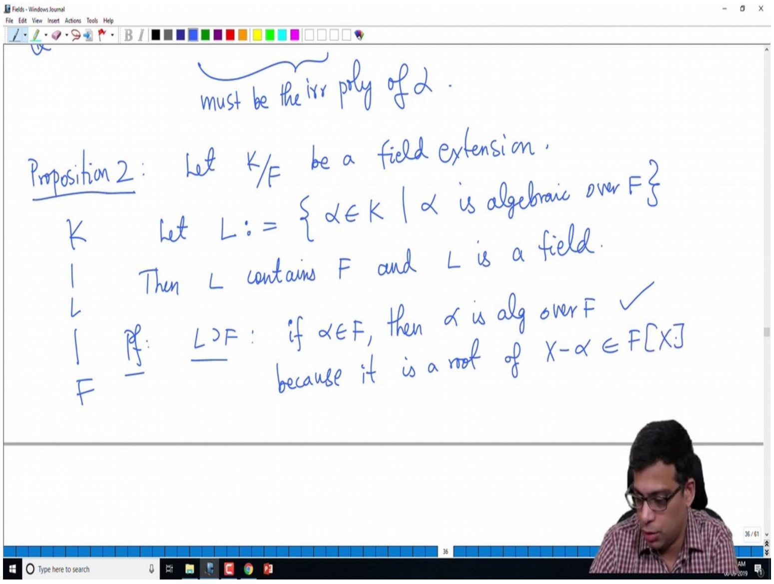


So that means, n can also not be 2, so n has to be 4, so Q alpha colon Q is 4 very good this is what I said in that video. In fact, we now can say hence X power 4 minus 10 X squared plus 1 in Q X is irreducible also we can say this, see we have no direct way of checking that this polynomial is irreducible. But, indirectly we have checked that it is irreducible why is that, that is the polynomial right why is this irreducible.

We know that Q alpha over Q has degree 4; that means, 4 is the smallest degree of any of a polynomial that divides that has alpha is a root. This polynomial has alpha is root nothing smaller has alpha as a root, so this must be irreducible polynomial of alpha right. There is no other choice it is a monic polynomial of the smallest degree that possible for a polynomial which has alpha as a root because this is 4, so this is a irreducible.

So, this is nice right? We have, we cannot directly show because just playing with polynomials and writing factors and so on, it is very complicated to show this is irreducible, but using this field theory we have shown that it is irreducible. So, now, let me do the second proposition that I want to do in this video which is very a nice statement also and it uses the previous videos or results in the previous video.

(Refer Slide Time: 16:33)

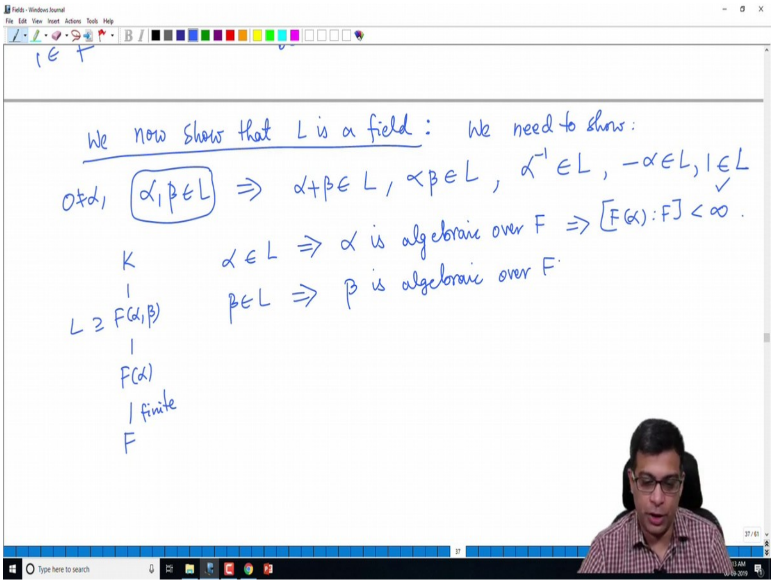


So, let K over F be a field extension any field extension. Now, I am going to define a subset of K and which contains F, so let L be all elements in K that are algebraic over F all elements in L K which are algebraic over F. So, we have K and F are given and I have defined L here the statement is then L contains F and L is in fact, of field.

So, let me prove this, so L is a field, so in fact, the picture is L is here and F is that ok. So, the proof is first part, so as of now L is a subset only L is a subset of F a L is a subset of K, so first part is show that L contains F this is very easy. Because, if alpha is in F then certainly alpha is algebraic over F right, because it is satisfies this is very easy let me just specify it.

Because it satisfies or it is a root of X minus alpha which is a polynomial over F. So, every element in the field is algebraic over itself that is very trivial right, so L contains F that is fine. It is a subset of K that contains F, so it is sits in between the crucial thing is, so the two statements I am making here the first one is trivial, but the second one is a crucial thing.

(Refer Slide Time: 18:19)



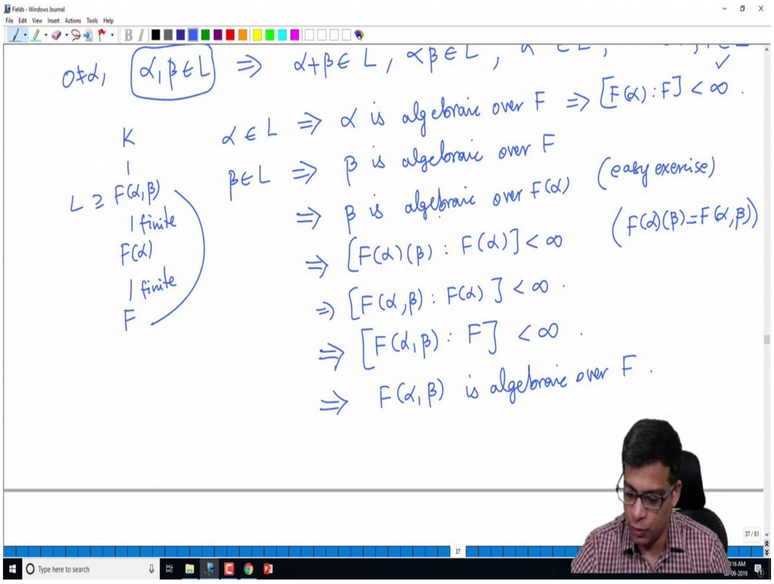
So, now we show that L is a field, so it is it contains F is trivial now we show that it is a field; what do we have to show that it is a field. We have to show that we need to show if alpha and beta are in L then various combinations that you can construct with alpha or also in L. That means, alpha, beta, alpha plus beta is an L, alpha beta is in L and if alpha is nonzero alpha inverses in L right and minus alpha is in L and so on.

So, it is already a subset of K to be a field it must be closed under addition, it must be closed under multiplication, it must contain one, it must contain inverses of any non zero thing there and so on ok. So, all these are to be proved 1 is certainly there because. 1 is an F remember these are all sub fields, so 1 is already here. So, 1 is there that is not a problem, because F is contained in L, but if alpha and beta are there why are all these combinations there, and this is where we use the multiplicativiy of the degree.

So, what we have now is K is there and, so we take alpha and beta in L; we consider the field generated by F alpha beta. So, when I write this remember we already understand what is F bracket one element we also understand what is F bracket 2 elements. Because, these are all ratios of polynomials in alpha and beta in two variables and you plug in alpha and beta with coefficients in F ok.

So, now, we have F, so of course, this whole thing is in L, that is a separate fact, but L is not yet a field, but these are fields. Now, the point is we have this is F alpha and this is F, so this is the tower that we will consider. Since alpha is in L alpha is algebraic over by definition right, alpha is algebra over F; that means, F alpha colon F is finite, so this is finite. Now, beta is also in L; that means, beta is algebraic over F by definition, because L consists of algebraic elements over F, so beta is an l; that means, beta is algebraic over F.

(Refer Slide Time: 21:11)



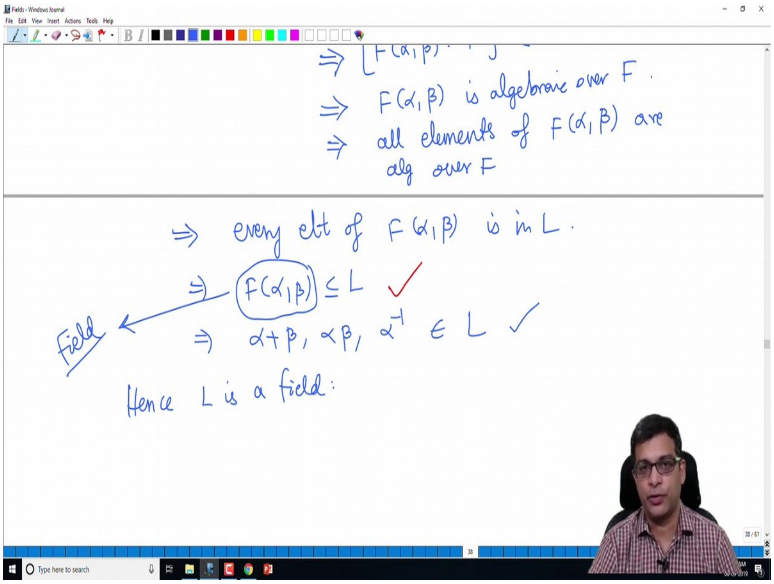
Now, I am going to make a very nice observation, very easy and nice observation is that beta is actually algebraic over F alpha also right. So, beta is algebraic over the smaller field F; that means, beta satisfies a polynomial with coefficients in capital F; that means, that same polynomial will be also a polynomial over F non bracket alpha.

So, certainly beta is algebraic over F alpha, so this is easy exercise I actually said this in words please think about this and go back to that part if you want. But if beta is algebraic over F it satisfies a polynomial over F that polynomial actually leaves over F alpha, so it is algebraic over F alpha. That means, F alpha, beta colon F alpha is finite right, this is the same statement alpha is algebraic over F means F alpha colon F is finite.

Beta is algebraic over F alpha means F alpha bracket beta colon F alpha is finite, but; that means and this is something also as an easy exercise F alpha bracket beta is just F alpha beta ok. This is also a similar to polynomial rings that we considered polynomial ring in one variable, or a polynomial ring in one variable is just a polynomial ring in two variables ok. So, let me not say anything about this can be easily checked right down typically elements on both sides and you will see that their same sense. So; that means, F alpha beta colon F alpha is finite, so this is also finite, so F alpha beta or F alpha is finite F alpha over F is finite.

That means, by the product rule for degrees F alpha beta over F is finite, because this is just the product. So, this is finite; that means, by the first proposition that we did F alpha beta is algebraic over F, nice right F alpha beta colon F is finite. Every finite extension is an algebraic extension that is what we proved in the beginning of this video a finite extension is algebraic.

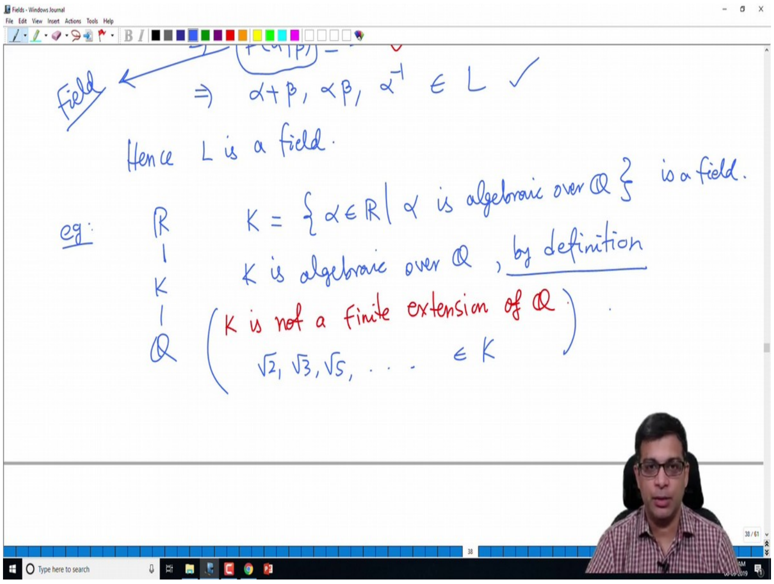
(Refer Slide Time: 23:47)



So, F alpha beta is algebraic over F; that means, at one shot you get that all elements of this are algebraic over F; that means, every element of F alpha beta is in L right. Because, in other words F alpha beta is contained in L, so I should not have written this ah, because I was going to show this right F is there alpha and beta are there that does not mean a priori at F alpha beta is in L.

Now, we can say that it is in L; that means, alpha plus beta is there, alpha beta is there, alpha inverse is there, if alpha is nonzero right. Because, F alpha beta is a field this is a field and if two elements are there sum is there the product is there inverses are there everything is there, so hence L is a field. So, this is a nice argument it might seem somewhat tricky initially, but please carefully listen to this again watch the video and make sure that you understand this. This is a very typical and a beautiful argument to prove that all algebraic elements form a subfield of K.

(Refer Slide Time: 25:07)



So, as an example if you take R over Q and consider K to be all alpha in R all real numbers which are the algebraic over Q, so that will sit inside R and we will contain Q is F field. So, this is what we call an algebraic closure of Q a this is something I will mention later just terminology I am giving now it is an algebraic closure of Q actually in R, so I should not say that I should also include c, so let me just take that back.

So, it is algebraic over it is a field and K is algebraic over Q that is what I would say, it is not an algebraic closure, because for example, it does not contain I is supposed to be in the algebra closure of Q, if you replace R by C then you get that. So, K is algebraic over Q by definition right, because every element of K is by definition algebraic over Q which means K is algebraic over Q by definition. And this maybe I will do this later K is not a finite extension of you might want to think about this also because it contains root 2, root 3, root 5 and so on.

So, root 2, root 3 it requires a bit of a proof, all are in K and they cannot be linearly dependent ok, so this is for later. So, this is a construction a priori we do not know that sum of algebraic elements is algebraic and product of algebraic elements as an algebraic and so on, because if you directly try to prove it from the definition of being algebraic. That means, it satisfies a polynomial, things get very very tricky. So, you, it is not always possible to write the polynomials with satisfied alpha plus beta or alpha beta and so, on.

But using this trick about finite extensions being algebraic we get the result, so every, all algebraic elements form a subfield. So, let me stop this video here; in this video we have looked at two important things which say that a finite extensions is algebraic. And we also showed that if you take a field extension and take all algebraic elements of the bigger field over the smaller field they form a field.

Thank you.