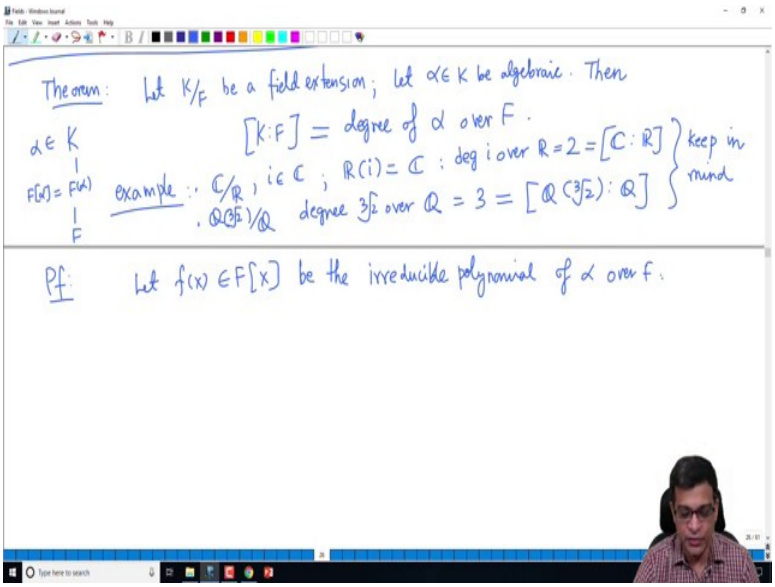
**Introduction To Rings And Fields**
**Prof. Krishna Hanumanthu**
**Department of Mathematics**
**Chennai Mathematical Institute**

**Lecture – 36**
**Degree of a field extension 2**

In the last video, when we considered field extensions we defined two important notions. We defined the degree of an element and we also defined the degree of an extension. So, the degree of an element was defined when alpha is algebraic and it was defined to be simply the degree of its irreducible polynomial. And degree of the field extension was defined when we view K as a vector space over the base field F, and hence we can ask for its dimension and we call that dimension the degree of the extension. So, there are two numbers degree of an element and degree of the extension, and we looked at some examples.

And today we will start with the theorem which connects the two notions, ok.

(Refer Slide Time: 00:59)




This is how we will say, how we explained that we can explain why the same word degree is used. So, let us say K over F is a field extension; as always remember our objects of study in this field theory part is field extensions. So, let K over F be a field extension, let alpha be an element of K. So, we are going to consider the sub field F alpha, let this be algebraic.

Suppose, K over F is the given extension and you have an intermediate field which I call, which I denote by alpha, F alpha. Remember F round bracket alpha is actually same as F square bracket alpha because alpha is algebraic and it is the smallest field that contains both F and alpha. So, let K be, let alpha be algebraic, then the two numbers K colon F which is the degree of F K over F is equal to the degree of alpha over F, ok.

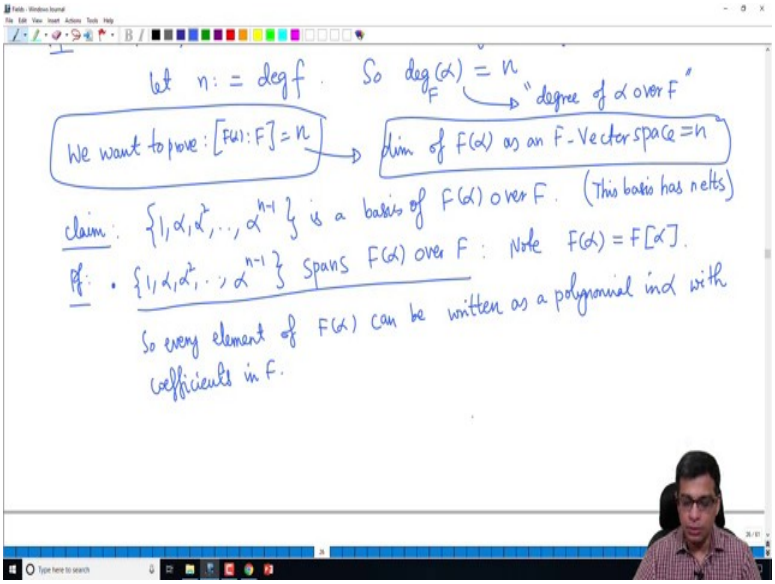
So, I am going to prove this. This is a very useful a result for us. And example to keep in mind, I will give you two examples. If you look at C over R, the field extension and you take i and C, then R adjoined I is actually nothing but C. And in this case we have degree of i over R is 2, which is also same as C colon R, ok. So, last video I said that 1 comma i is a basis for this.

Another example you can take is Q adjoined root 2 over Q then degree of root 2 over Q. Let me take cube root of 2 just for variety. So, cube root of 2, degree of this over Q is actually 3, one can prove this because x cubed minus 2 is an irreducible element, x cubed minus 2 is the irreducible polynomial of this element over Q and this is also Q adjoined cube root of 2 colon Q the degree of the field extension itself.

So, I am going to prove this equality as part of the proof of the theorem, ok. So, perhaps I did not do this example last time, but we are going to do this. So, the two examples to keep in mind are these, among many other examples as we are doing this you might want to think about these examples, ok. So, let us prove this. This is not difficult at all.

So, let alpha, let F be; let F in capital F x be the irreducible polynomial of alpha over F. Remember, this is the smallest degree polynomial which has alpha as a root, smallest degree polynomial with coefficients in capital F which has alpha as a root.

(Refer Slide Time: 04:18)



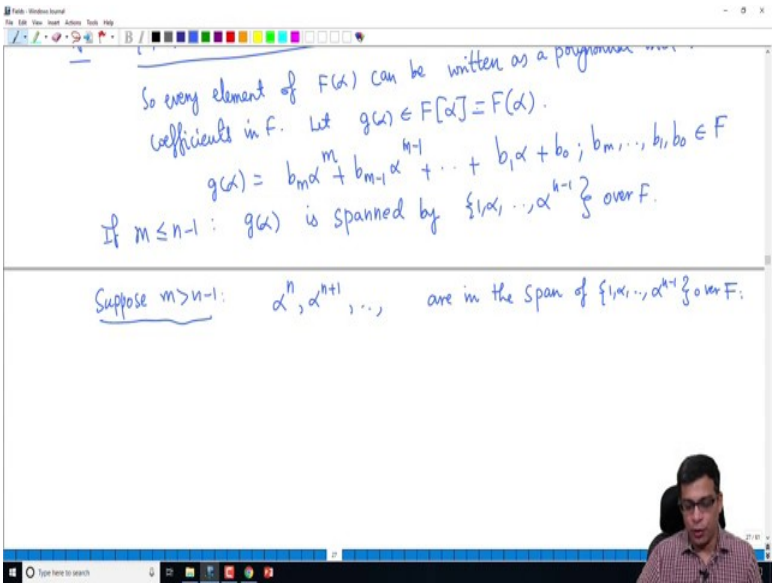

So, let the degree of this polynomial be F n. So, degree of alpha, I will write it like this for simplicity is n. So, this symbol here stands for degree of alpha over F, it is a convenient way of writing that. So, we want to prove what? We want to prove that the, so we want to prove the degree of the field extension is also n, right. We are trying to show the degree of sorry not K F, remember I am not saying that. Actually, I go back here and make a correction this is completely wrong what I wrote. I can only say that I should only say that the degree on the extension F alpha over F is degree of alpha. K can be much bigger, so that was wrong, so please correct that.

So, what we want to prove is the degree of the field extension F alpha over F is n, ok. So, this is what we want to prove. And remember this means, the dimension of F alpha as an F vector space is equal to n that is in other words, that is what we are supposed to prove, ok. So, now, let us go ahead and prove this.

So, basically, I will directly exhibit a basis. So, claim that the set 1, alpha, alpha squared up to alpha n minus 1 is a basis of F alpha over F. If I show this it will follow that F alpha has dimension n, right because there are n elements. This basis has n elements. Because this basis has n elements dimension is going to be n. Remember, definition of dimension is, it is the cardinality of any basis and if I exhibit a particular basis and show that it has n elements n elements it is enough, because any two bases have same number of elements. So, that is all we need to show that is a basis.

So, there are two things to prove and we are trying to prove something as a basis. First is that it spans, it spans F alpha over F. So, let me prove this first, ok. So, for this we note that, we recall that the field F round bracket alpha is actually same as F squared bracket alpha. So, every element of F alpha can be written as a polynomial in alpha with coefficients in F. This is by definition; this has nothing to do with F, the irreducible polynomial of alpha. F square bracket alpha is the polynomial ring over alpha, over F in alpha; that means, elements are polynomials in alpha with coefficients in F. So, every element can be written like that, but we are trying to show that this particular set spans it.

(Refer Slide Time: 08:00)



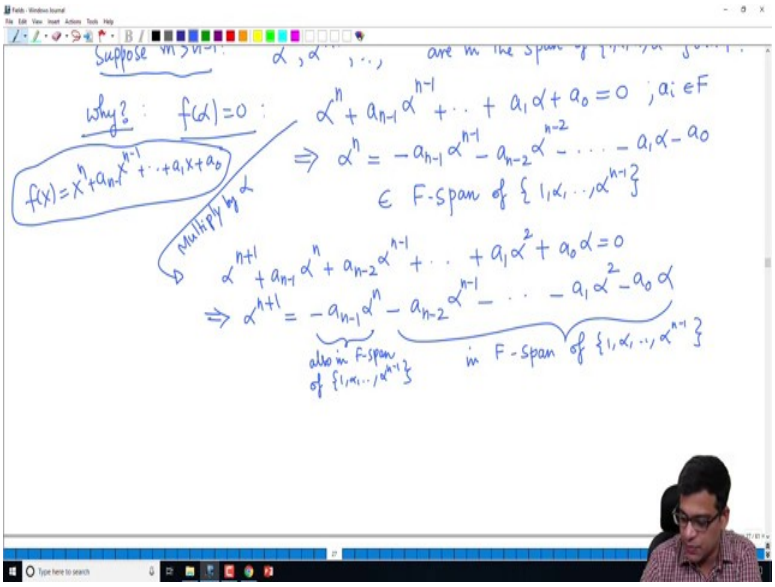

So, a priori maybe a larger power than n, may be required to express elements of F round bracket alpha which is same as F squared bracket alpha. But, because small f of alpha is 0 we can get rid of the all terms with the degree greater than equal to n, ok. So, let us take an arbitrary element of F alpha.

So, let it is a g alpha be an element of F alpha which I keep reminding you is same as round bracket alpha. So, g alpha can be written as some b m X m b m minus 1 X m minus 1 b 1 sorry x after evaluating, right, so it should be alpha b 1 alpha plus b 0, where b m, b 1, b 0 are all in F. This is the important point. If m is less than or equal to n minus 1 g alpha is spanned by the set we are trying to show is a basis, right. If m is less than equal to n minus 1 g alpha is spanned by that is it because all the exponents of alpha here

are less than equal to n minus 1, the coefficients are over F. So, this is spanned by the set over F. But of course, m could be greater than n minus 1. We have to also deal with this.

And here, the polynomial, irreducible polynomial of alpha comes to our rescue. So, what I will show is I will show you how to express alpha power n, alpha power n plus 1 and so on are in the span of 1, alpha, alpha n minus 1 over F. So, if I show this, if I show that all powers of alpha are in the span of this set we are done because every polynomial is written in terms of some powers.

(Refer Slide Time: 10:14)




So, this the reason is, why is this true? The reason is we will just do one by one. We know that F alpha is 0, right and F number is a monic, polynomial of degree n, so that means, it looks like this alpha power n. So, I did not specify what F was earlier. So, let us say we have this, right.

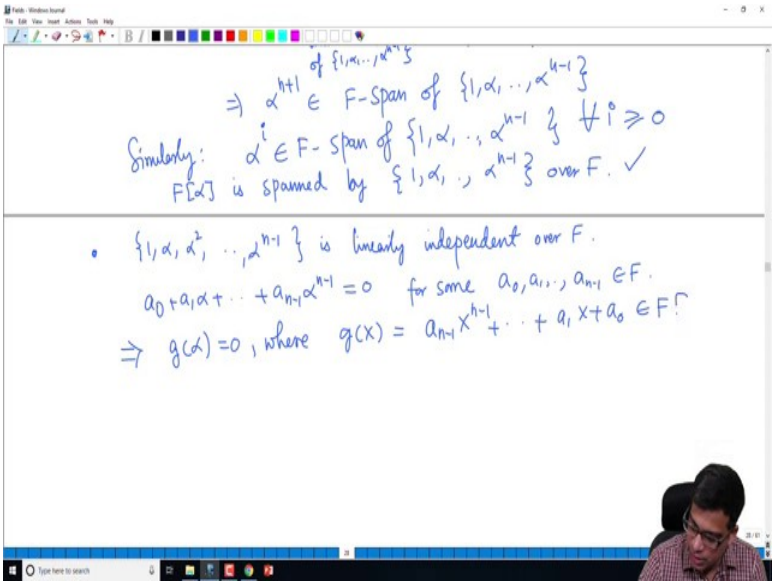
So, in other words what I am assuming is that the F x is x power n a n minus 1 x power n minus 1 and so on up to a 1 x plus a 0. F alpha is 0 means this is 0. This implies alpha power n is equal to minus an minus 1 alpha power n minus 1 minus an minus 2 minus 2 alpha power n minus 2 minus dot dot dot minus a 1 alpha minus a 0. But this is obviously, in the span of I will write F span of the set 1, alpha, alpha power n minus 1, right, because only powers of alpha that you see here are alpha n minus 1, alpha n minus 2, alpha, alpha power 0 and the coefficients are all in of course, that is an important part, the

coefficients are all in F. So, this is inside F span of this. So, alpha power n can be actually written as a linear combination of 1, alpha, alpha power n minus 1.

What about alpha power n plus 1? That is also easy. We can multiply this equation here by alpha. We get alpha power n plus 1 plus a n minus 1 alpha power n plus a n minus 2 alpha power n minus 1, a 1 alpha squared, a 0 alpha is equal to 0. So, we are just multiplying by alpha, but that means, alpha power n plus 1 can be written as minus an minus 1 alpha power n minus an minus 2 alpha power n minus 1 minus a 1 alpha squared minus a 0 alpha.

Now, look at this, these terms here are already in the span of by just the definition there in the span of a 1, alpha, alpha power n minus 1, right, because only powers there are up to alpha power n minus 1 the coefficients are already in F. This a priori is not there, but we just proved that remember. Alpha power n is in is in span of this. So, this is also in F span of our set. So, this the first term is in F span of 1, alpha, alpha power n minus 1, this remaining terms are also in the span of this. So that means, alpha power n plus 1 is in F span of 1, alpha, alpha power n minus 1.

(Refer Slide Time: 13:09)




And similarly, alpha power i is in F span of 1, alpha, alpha power n minus 1 for all i greater than equal to 0, ok. So, I can put everything together. Now, because alpha power 0 is 1, is in the F span alpha is there, alpha power n minus 1 is there. For the first n minus

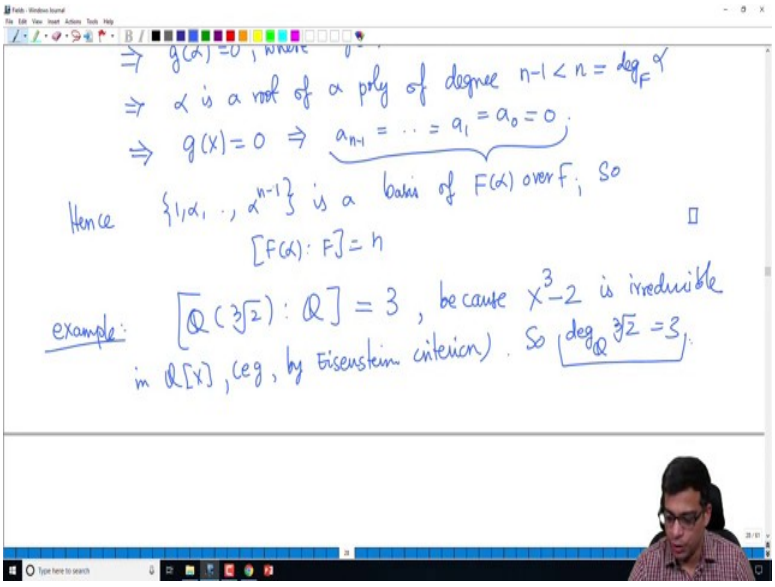
1 or first n actually there is it is immediately clear, because they are all already in this set, but for higher powers we argued here that they are all in the span of this.

That means, F square bracket alpha is spanned by this set over F. So, this is the first part. We are trying to show that set is a basis; we just showed that it is a spanning set. What is the second part? We want to show that alpha, alpha squared, 1, alpha, alpha squared up to alpha n minus 1 is an F basis of F alpha is what we want to show. And the this is easy.

Suppose, what is linearly, so actually sorry I will write it as is linearly independent over capital F. It is also an F basis, but we are trying to show both the parts that constitute a basis. We showed that its spans and now we are showing that it is linearly independent. So, let us take a linear combination. And we want to show that if that linear combination is 0 each coefficient is 0.

Suppose, a 1, a 0 plus a 1 alpha plus a n minus 1 alpha n minus 1 is 0 for some a 0, a 1 up to a n minus 1 in capital F. But that means, g of alpha is 0 where g of x is a polynomial given by a n minus 1 x n minus 1, a 1 x plus a 0 this of course, in is in capital F X.

(Refer Slide Time: 15:38)




But, this implies alpha is a root of a polynomial of degree n minus 1, right which is strictly less than n. Remember n was the degree of alpha over F; that means, n is the degree of the smallest nonzero polynomial. Remember, irreducible polynomial is supposed to be nonzero. So, it is a degree of the smallest nonzero polynomial that has alpha as a

root, but here we are producing a polynomial which is degree n minus 1 and smaller than n yet which has alpha as a root that means, g of x is 0 because there is by definition n is the smallest degree of an irreducible polynomial or smallest degree of a nonzero polynomial that as alpha as a root; g is apparently a polynomial of degree n minus 1 which has alpha as a root, but that violates the minimality of n.

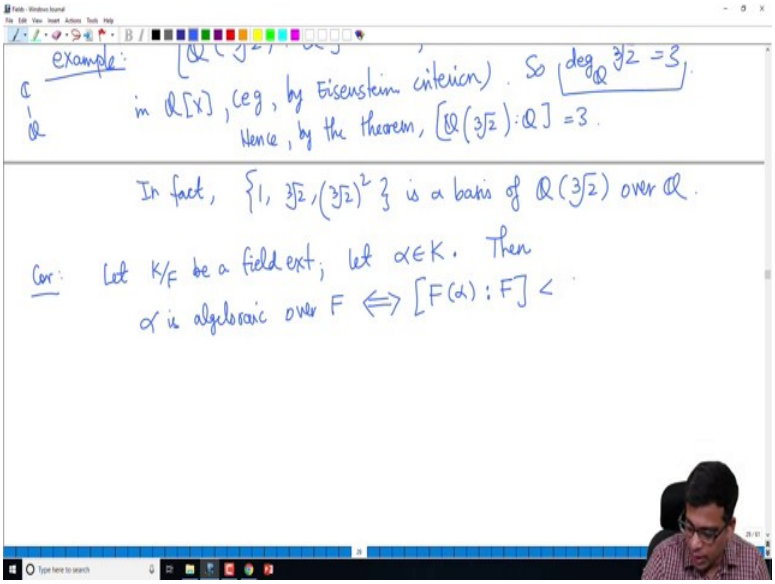
So, the only solution to this is that g is 0. But that means, if a polynomial is 0 all its coefficients are 0, right. So, this is what we wanted to show. We started with the linear dependence relation and showed that all the coefficients are 0. Hence, 1 alpha up to alpha n minus 1 is a basis of F alpha over F, so degree of F alpha over F is n. So, this proves the theorem that I wrote.

And I will do now one or two examples and corollaries to illustrate why this is such a very useful statement. Immediately, let us go back to one of the examples that I wrote. I can conclude that the degree of the field extension Q added adjoined cubed root of 2 to Q is 3 because, I will write it like this X cube minus 2 is irreducible in Q X, ok. So, we can check that this is irreducible for example, by Eisenstein criterion, right.

Remember, in our a ring theory part we discussed Eisenstein criterion to check that these are irreducible, we need to find a prime which divides all the coefficients except the leading coefficient and such that are square of that prime does not divide the constant. Here we have that, 2 divides all the questions except the leading coefficient and 2 square does not divide 2. So, this is irreducible.

So, degree of cube root of 2 over Q is 3. This is the crucial observation. Because x cubed minus 2 is a polynomial which has alpha is a root and it is already irreducible and monic, it must be irreducible polynomial of cube root of 2 over Q and it is degrees 3, so degree of cube root of 2 over Q is 3.

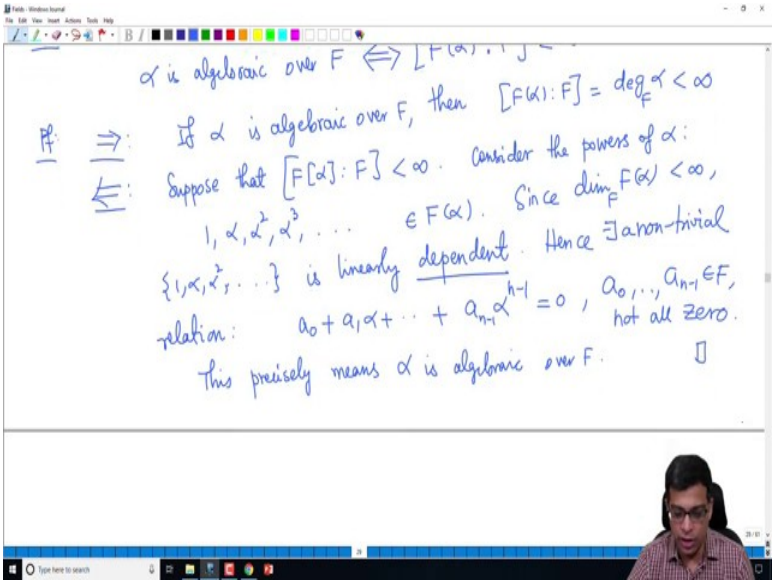
(Refer Slide Time: 18:57)




And hence by the theorem, the degree of the extension is 3. We can also directly write a basis. In fact, from the proof of the theorem 1 cube root of 2, cube root of 2 whole squared is a basis of Q adjoined cube root of 2 over Q. So, this says that cube root of if you add a cube root of 2 and consider the smallest field containing Q and cube root of 2, these all happening inside complex numbers let us say. So, we can for example, fix the ambient field to be the bigger field to be C. The smallest field in C that contains Q and cube root of 2 is denoted by Q adjoined cube root of 2 and the degree of that over Q is 3; that means, the dimension of this as a Q vector space is 3, ok.

So, now immediately we can do a few nice corollaries and these are extremely useful for us, ok. So, what I will show is that let K be field extension over F and let alpha be in K and suppose its algebraic over F, sorry I will not say that let alpha be in K. What I will say is that, then alpha is algebraic over F if and only if the field extension F alpha over F has finite degree, ok.

(Refer Slide Time: 20:50)




So, I am going to prove this. This is a very simple corollary of the theorem we proved, but it is an extremely, it is an extremely useful way of checking whether something is algebraic or not. So, actually this is easy to prove whether you have the theorem or not. So, let us anyway prove this. So, in this direction alpha is, suppose alpha is algebraic, if alpha is algebraic over capital F then by the theorem the degree of the field extension is the degree of the element over F which of course is a finite number, right because what is if alpha is an algebraic element its degrees, the degree of irreducible polynomial which is actually a number. So, it is a finite number which is the degree of this. So, this is ok, this is an immediate corollary of the theorem.

Now, suppose that the degree of the extension is finite. We want to show that alpha is algebraic and this uses the proof of the theorem. So, in this case what we do is consider the powers of alpha. In other words, I consider alpha 1, alpha power 0 is 1, alpha, alpha squared alpha cubed and so on, right these are all in F alpha. Since, dimension of F alpha as an F vector space is finite, this set is not linearly independent.

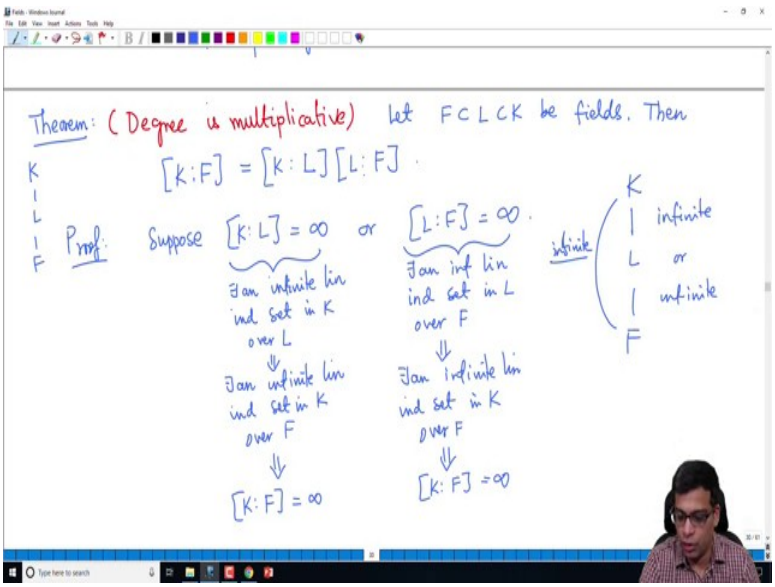
In other words, this set is linearly dependent, right, because you have an infinite set here in a finite dimensional vector space, that infinite set cannot be linearly independent. Remember, if dimension is hundred any set containing more than 100 elements has to be linearly dependent because if it is linearly independent you have a linearly independent set which has more elements than a basis which is not possible. So, this is linearly depen-

dent. Hence, there exist a nontrivial relation; this is what it means for the set to be linearly dependent. So, we can write it as a 0, a 1 alpha, a n or a n minus 1 alpha n minus 1 is 0 for sum a 0 an minus 1 in F not all 0 that is the whole point, right. There is a dependence relation. There is a nontrivial relation; that means, there is a tuple of elements of the field capital F which are not all 0s such that this happens.

But, this exactly means alpha is algebraic over F, right we have exhibited a polynomial relation that it is satisfies. So, it is algebraic. So, this is very simple, right. So, we have started with the assumption that degree is finite and concluded that it is algebraic. So, this is a very convenient way of checking that an element is algebraic or base field or not we look at the degree of field extension of the field obtained by adding that element to the base field.

Now, I will do one more theorem here together with that theorem and this corollary we can actually conclude lot of nice things about algebraic elements.

(Refer Slide Time: 24:33)




So, let me prove this theorem this says that degree is multiplicative. So, this theorem you should remember as saying degree is multiplicative. What I mean by this I will explain.

So, let F in L in K be fields, ok. So, what we have is K, L and F, 3 fields; one sitting on top of the other, K sitting on top of L, L sitting on top of F. So, they are all field extensions. Then what we can say is K colon L or K colon F, the degree of the largest field

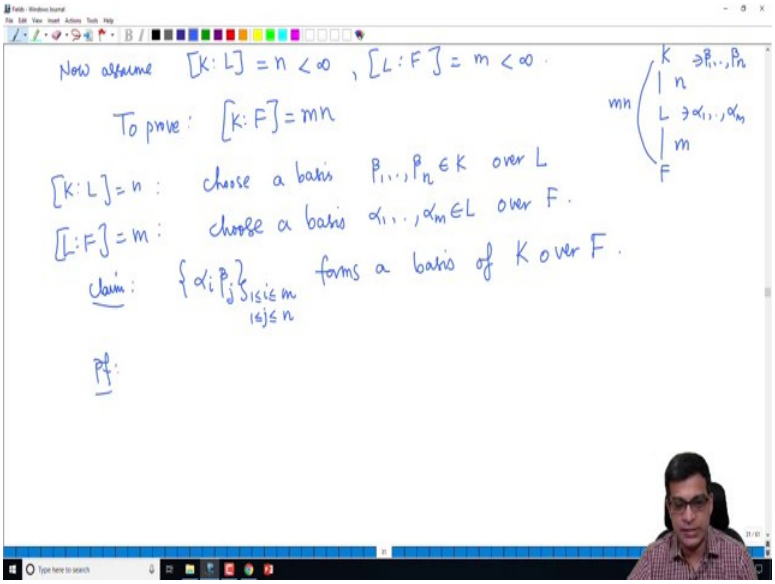
over the smallest field is the product K colon L and L colon F, and I am also including the possibility that they are infinite here. So, I will prove that also as part of the statement. In particular what we are saying is that if either of these numbers K colon L or L colon F is infinite, K colon F is also infinite with the convention that infinity times anything is infinity. So, let us first clear settle that case. Suppose, K colon L is infinity or L colon F is infinity.

Suppose, that we have either this is infinity, L colon F is infinity or K colon F is infinity, at least one of them is infinity. Then what happens? In this case there exists an infinite linearly independent set in K over F, right. And in this case there exists an infinite linearly independent set in L over F. So, here of course, I should write L over K over L. So, K colon is in F, K colon L is infinity means the dimension of K as an L vector space is infinity; that means, there is an infinite collection of vectors in K which are linearly independent over L. Similarly, if L colon F is infinity there is an infinite collection of vectors which are linearly independent over F.

But that means, there exists an infinite linearly independent set in K over F also, in the first situation. Because if the collection of vectors is linearly independent over L, they will be also linearly independent over a smaller field because if some linear combination with coefficients in F gives you 0; that means, those elements those coefficients in F are also in the field L. So, that means, that is an L linear combination, but then there cannot be a non-trivial L linear combination. So, there is an infinite linear independent set in K over F.

In this case also, there exists an infinite linearly independent set in K over F. Here the point is the original vectors we started with or in L, right, but L is a subfield of K, it is a sub vectors a space of K if you wish. So, if L itself has infinitely many independent F vectors or F independent vectors those vectors are already in K; that means, K itself admits the infinity set of F independent vectors. In either case we have K colon F is infinity. So, what we are saying is that if one of these, so we have K, L, F, this is infinity or this is infinity implies this is infinity, ok. So, this is the first a simple case when either of these two numbers K colon L or L colon F is infinity then K colon F is also infinity.

(Refer Slide Time: 28:52)



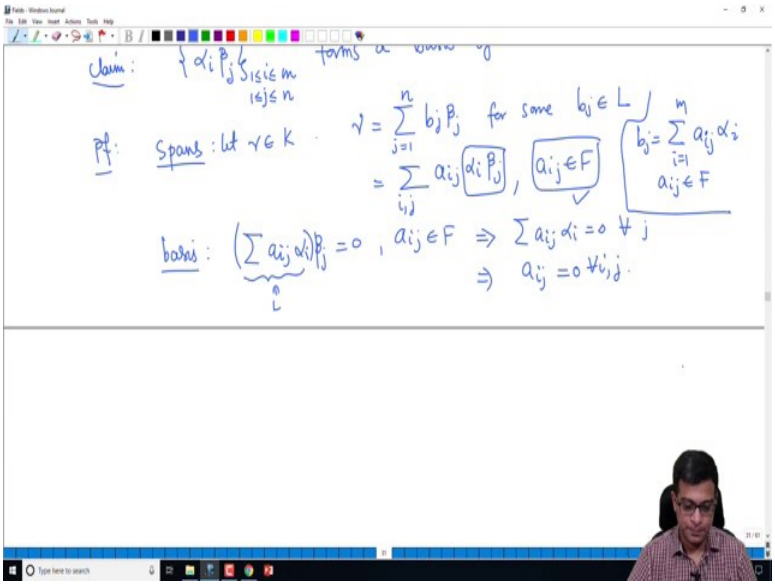

Now, assume that both K colon L and L colon F are finite and let us call them n and m respectively. So, you have K colon L is n. So, you have K, L, F. So, usually it is the degrees are denoted by just writing the number next to the vertical bar, bar which represents the field extension. So, this is n and this is m. So, we want to prove K colon F is m n, ok. This is actually very simple, but very useful observation that constantly we use in rest of the field theory course or any problems that you solve in field theory it is a very important observation, ok.

So, this is as I said not difficult at all. So, what do we do? Since, K column L is equal to n, choose a basis which I will call beta 1 beta n over L, right. So, K as an L vector space as dimension n, so I can choose n vectors which form basis. L colon F is m, so similarly we can choose a basis, alpha 1 through alpha m of L over F. So, just to simply keep track of what we are doing, I have beta 1 through beta n here alpha 1 through alpha m here, right. Beta 1 through beta m form a basis of K over L, alpha 1 through alpha m form a basis of L over F. Now, the claim that will prove the statement that K colon F is m n is the following.

The set of products alpha i beta j, 1 less than i less than n over m, 1 less than j less then n form say basis of L or rather K over F. So, it is fairly easy to conclude that this is actually a set of m n distinct elements. So, I will make that remark after approving this claim, because beta is a different, alpha is a mutually different, the products cannot equal for

different indices. So, we have a basis consisting of m n elements so that means, dimension is m n. So, this is very easy.

(Refer Slide Time: 31:38)



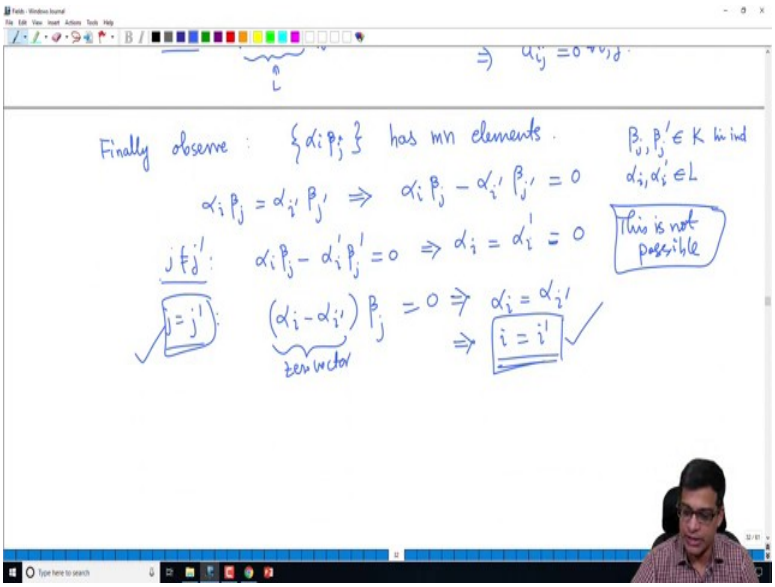

This spans you can check. Again, remember as in the earlier theorem of this video basis means its spans and is linearly independent. So, to prove that it spans let us choose an arbitrary element gamma in K, we can write gamma. So, I will I will quickly do this it is not difficult at all. So, gamma is in K and K has a basis beta 1 through beta n over alpha. So, this can be written as beta b j b beta j for some b j in L, right j equal to 1 to n. This is because capital K has a basis beta j's over capital L. So, b small b j are in L.

But that because b j's are in L, b j can be written as summation a ij alpha I, i equal to 1 to m and a ij in F. So, because b j are in L and alpha 1 through alpha m are F basis of L each b j can be written as a linear combination of alpha i's. So, I am going to write both of them together and write this as a ij alpha i beta j, right. So, gamma can be written as a linear combination of alpha i beta j with coefficients in F that is the whole point. These are the; supposed basis elements, so we have expressed any arbitrary element as a linear combination of this with coefficients in F.

Basis is also equally easy suppose a ij alpha i beta j is 0 with a ij in F of course. But that means, we can first conclude that because beta j are linearly independent over capital L and these coefficients are in capital L summation a ij alpha i is 0 for all j. But again alpha is the linearly independent so; that means, a ij is 0 for all i and j, ok. So, this is a very

easy proof actually let me not complete the proof yet, but you hopefully followed this. We have shown that its spans and forms a basis. So, it proves a claim at least that it is a basis.

(Refer Slide Time: 34:15)




Now, final comment is alpha i beta j has n elements or m n elements. In other words, certainly we have m n choices for ij, but I am now saying that they cannot become equal for different i and different j. Why is this? Because if alpha i beta j is equal to alpha i prime beta j prime what we have is; so, what we have is, so if alpha i beta j is equal to alpha i prime beta j prime we rewrite this as alpha i beta j minus alpha i prime beta j prime, ok. So, now, this is 0 and remember beta j, beta j prime are in what did we choose them K and alpha i, alpha i prime are in a L.

Now, remember that beta j and beta j prime are linearly independent because they are part of the basis, so beta 1 through beta n are a basis over L and here we are just taking two of them they form a linearly independent set. Now, we have two possibilities, if j is equal to, if j is not equal to j prime then alpha i beta j, alpha i prime beta j prime is 0 with alpha i and alpha i prime in the base field L implies that alpha i equals alpha i prime equal to 0, right, because we have a linear relation between two different independent vectors; that means, the coefficient must be 0, but this is not possible.

Why is it not possible? This is not possible because alpha is are also basis elements, right. So, they cannot be 0. So, this implies that j cannot be equal; j has to be equal to j

prime. If j is equal to j prime what we have is alpha i, minus alpha i prime is equal to beta j. But, beta j remember is a linearly independent vector; that means, it is nonzero. This in particular means that alpha i is equal to alpha i prime, i prime it should be. Alpha i is equal to alpha i prime because these are this must be the 0 vector. Any nonzero vector times a scalar is 0 means that scalar is 0. This means i must be equal to i prime, right again invoking the fact that alpha i is form a basis, if two of them are equal, no two of them are equal actually. So, the only possibilities i equal to i prime, so j is equal to j prime and i is equal to i prime. So, we do have m n distinct elements.

So, please think about this last part carefully. So, we have shown that these are linearly independent and we have shown that they are different elements. Strictly speaking fact that they are linearly independent already shows that they are different, but if that point is not clear in the linear independence part, I wanted to do this explicitly again. So, now this does complete the theorem.

We have shown that the degree is multiplicative. If you have three fields and it is a tower of fields, this is called tower of fields or field extensions rather. Then, the degree of the largest extension is the product of the middle two extensions, and we also proved in this video the theorem about the degree of an element being equal to the degree of the field extension itself, ok. Together these two are very useful for us. And let me stop this video here. In the next video, we will do corollaries of these two very important results.

Thank you.