Introduction To Rings And Fields

Prof. Krishna Hanumanthu

Department of Mathematics

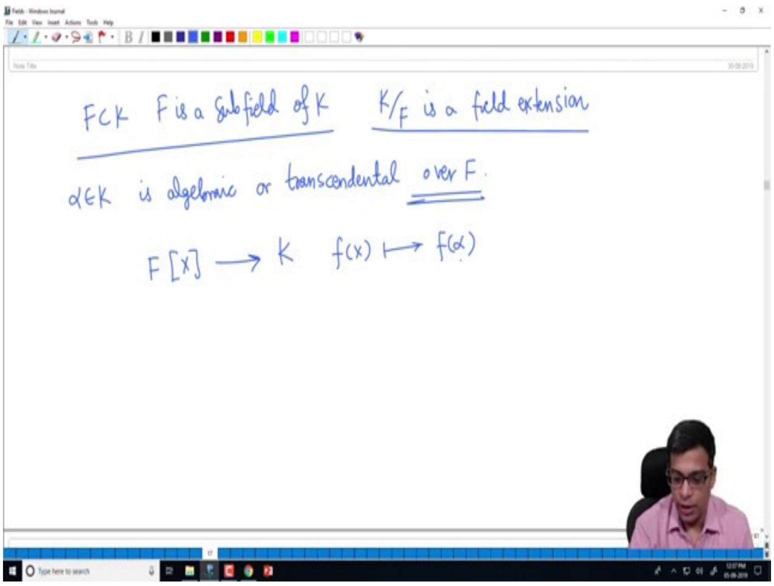
Chennai Mathematical Institute

Lecture - 35

Degree of a field extension 1

Let us continue now with Field Theory; in the last two videos we defined, fields we looked at Field Extensions which I told you are the primary objects of study in field theory.

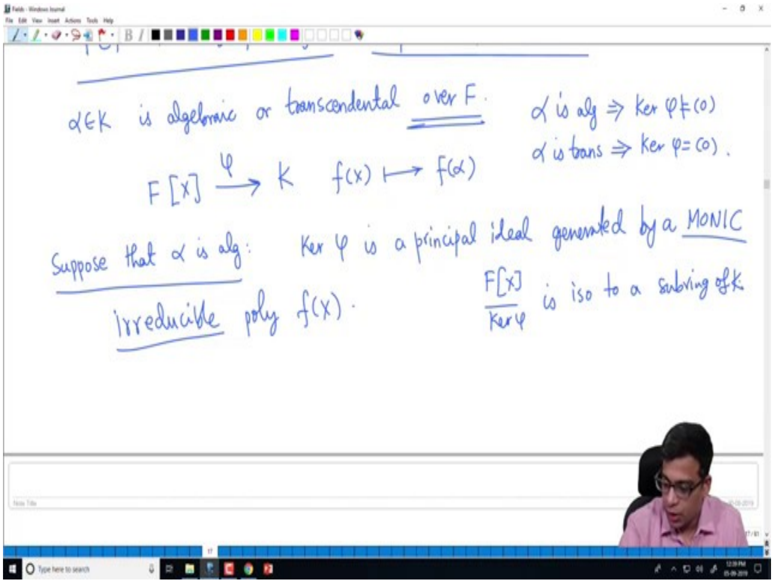
(Refer Slide Time: 00:33)



So, unlike in the rings case we usually considered fields when in this fashion. So, we are going to look at F is a subfield of K, so that is our main case. So, we say that K over F is a field extension right. So, this is the primary objective of study and I talked about when an element of alpha, when an element alpha of K is algebraic over F or transcendental over F we define these two notions and I emphasize the fact that over F is very important. So, let us continue this study today and I am going to assume that I am dealing with the field extension and alpha is an element of the bigger field.

So, remember we consider this ring homomorphism which sends F x to F alpha and whether alpha is algebraic or not is readable from this homomorphism.

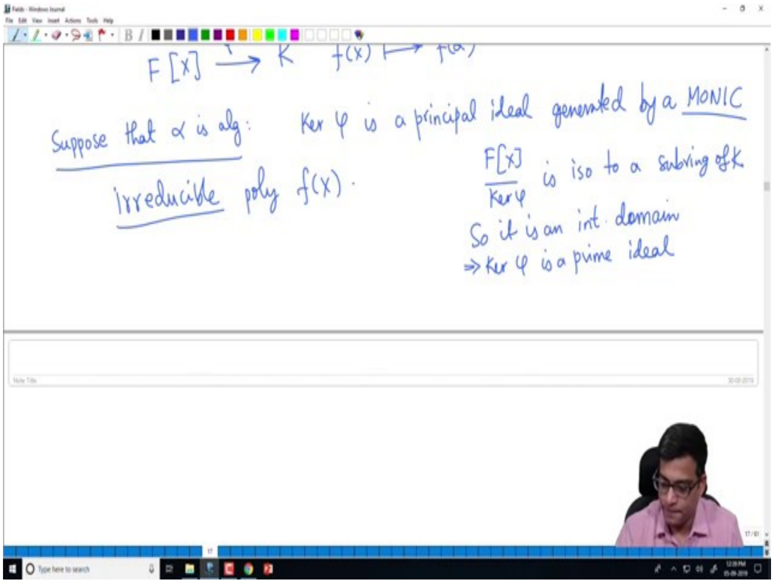
(Refer Slide Time: 01:42)



If alpha is algebraic this implies if this map is kern phi kernel phi is not 0, if alpha is transcendental the simplest kernel phi is 0. And if alpha is algebraic, so suppose for the moment that alpha is algebraic, then kernel phi is actually a principal ideal generated by a MONIC. So, I will emphasize this words monic irreducible polynomial f of x, this is because when we discussed PID principal ideal domain we saw that polynomial ring in one variable over a field is what is called a PID. So, any ideal in that ring is a principal ideal, if alpha is further algebraic; that means, kernel phi is actually a nonzero ideal and remember how we figure out the generator of that ideal we simply look at the least degree polynomial content in that ideal. And that we can always assume is monic because we clear we can divide by the leading coefficient and make it monic.

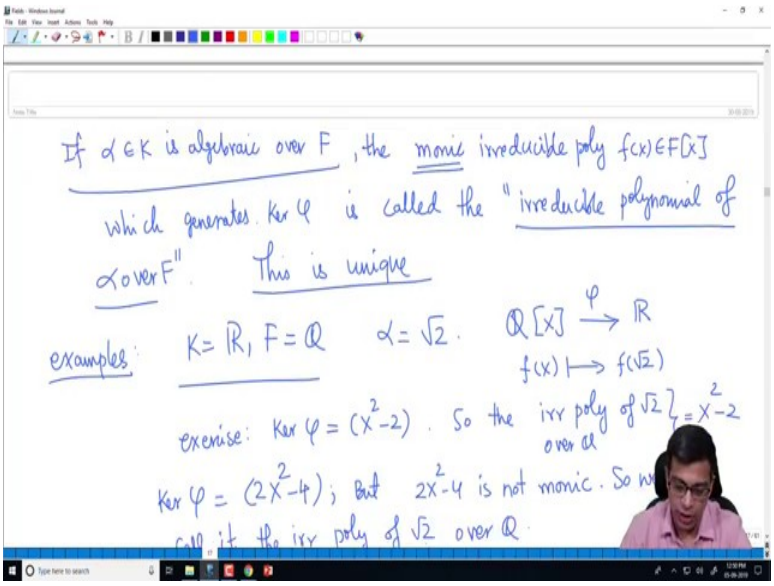
And then it becomes irreducible because if it is not irreducible, then it is product of two smaller degree, but positive degree polynomials. But then it they cannot be generated by that polynomial which as the least degree another way of saying this is, because K is a field F x mod kernel phi is isomorphic to a sub ring of K and as such it is an integral domain right.

(Refer Slide Time: 03:40)



And once it is an integral domain kernel phi is a prime ideal and hence it is generated by a monic irreducible polynomial this is also sort of revision of what we know already.

(Refer Slide Time: 04:02)

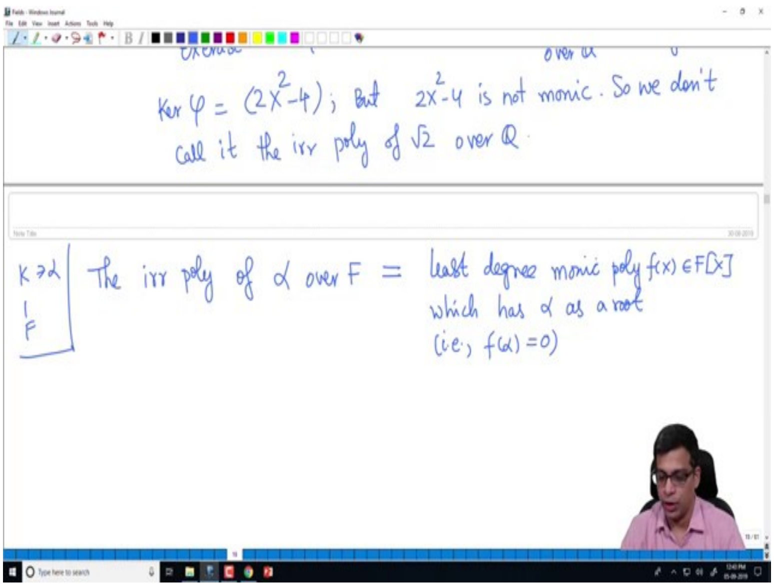


So, now this f x is very important for us, so if alpha is algebraic if alpha in K is algebraic over F the most important information that we want to attach to alpha is the following. The monic irreducible polynomial which generates polynomial F x and remember this is in capital F x which generates kernel phi, which I defined earlier phi defined earlier is called the irreducible polynomial irreducible polynomial of alpha over F this entire phrase is important.

So, it is called the irreducible polynomial of alpha over F ok. So, this is an important information that we have and remember this is unique that we know already. Because it is the generator of the kernel phi and once we insist that it is monic it is going to be unique because only way that we get another generator is multiplied by a unit. That means a field element, but it will you start with a monic polynomial and multiplied by a unit which is different from one it will no longer be monic. So, when we insist that it is monic we make it unique. So, let me give you a couple of quick examples to be clear about this idea. So, let us take K to be R and F to be Q this is a field extension and let us take alpha to be root 2. What is a monic irreducible polynomial of root 2 over Q, so for that we consider this map it sense F x to F root 2.

And it is not an easy it is an easy exercise to show that kernel phi is generated by x squared minus 2, x squared minus 2 is actually an irreducible polynomial because it is a degree 2 polynomial, all we need to check is that it has no roots and certainly it has no root because in Q. Of course, it is reducible in Q not over R it has no roots in Q, so it is irreducible in Q x. So, the irreducible polynomial of root 2 over Q is x squared minus 2.

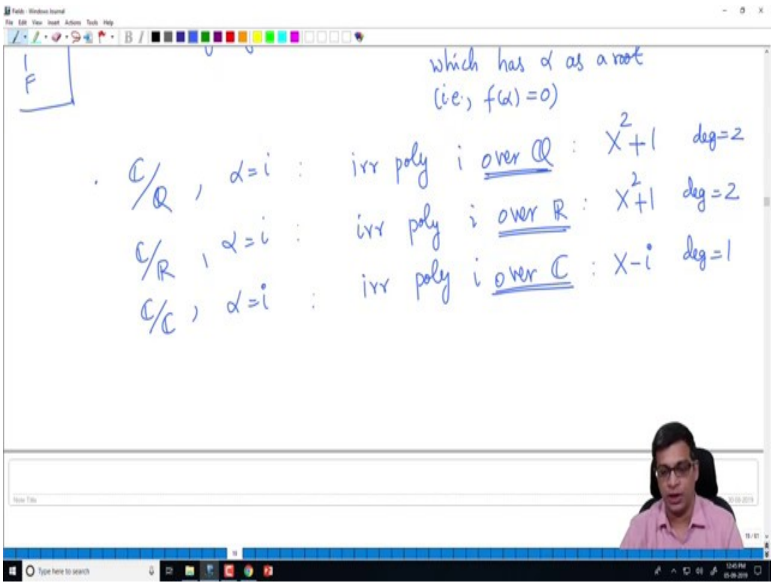
(Refer Slide Time: 06:53)



And let me emphasize that kernel phi is also generated by for example, 2 x squared minus 4 right, because all we are doing is multiplying by 2 which is the unit in Q, but 2 x squared minus 4 is not monic. So, we do not call it the irreducible polynomial root 2 over Q ok. So, it is a convention to make it unique; we want it to be monic.

So, what is in another words what are we really doing here, the irreducible polynomial of alpha over F in, I mean now I am writing in general capital F is any field K is a field extension and we have alpha in K that is the setup. The irreducible polynomial of alpha over F is the least degree monic polynomial F x in capital F x which as alpha as a root. That is the last thing is nothing but saying that F alpha is 0, because kernel phi that we have phi that we have earlier kernel phi is the set of all idea all polynomials that have alpha is a root. The least degree one among them is the generator and further insist on monic you get the irreducible polynomial of alpha over F.

(Refer Slide Time: 08:34)

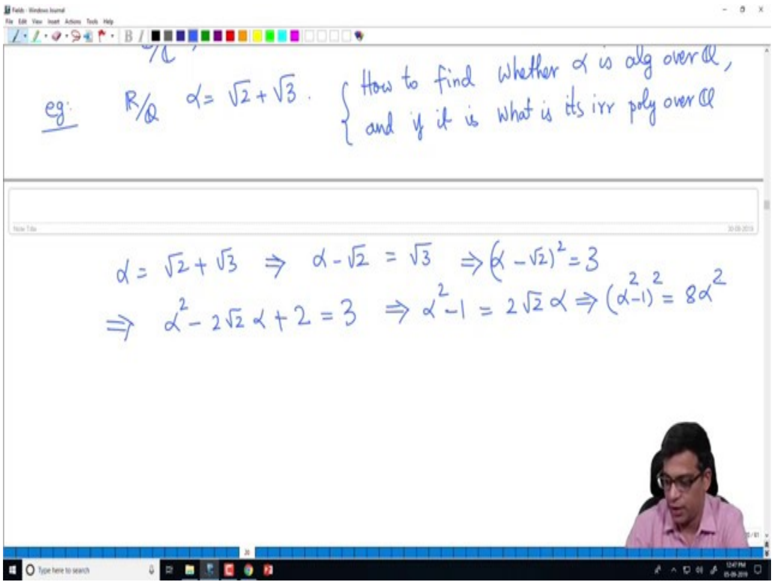


Another example: let us take C over Q and let us take alpha to be i, what is the irreducible polynomial of i over Q i is the square root of minus 1 always right i is the square root of minus 1, here it is just nothing but x square plus 1 ok.

Similarly, if you take R over Q C over R and alpha equal to i irreducible polynomial of i over R is actually the same it is x squared plus 1. On the other hand if you take the field extension C over C in other words both the fields are same what is the irreducible polynomial of i over C, say this is where over the best field is an important part of the information. What is irreducible polynomial of i over C? It is the least degree polynomial that has i has a root, of course x squared plus 1 has i as a root. And it is the least degree over

R or Q, but it is not the least degree polynomial over C it is simply x minus i ok. So, here degree is 2 here degree is 2, but here degree is 1. So, again this goes to show why it is very important to keep track of the base field whether something is algebraic or not changes, if you change the base field. Similarly if you have algebraic elements what is irreducible polynomial also changes if you change the base field.

(Refer Slide Time: 10:14)

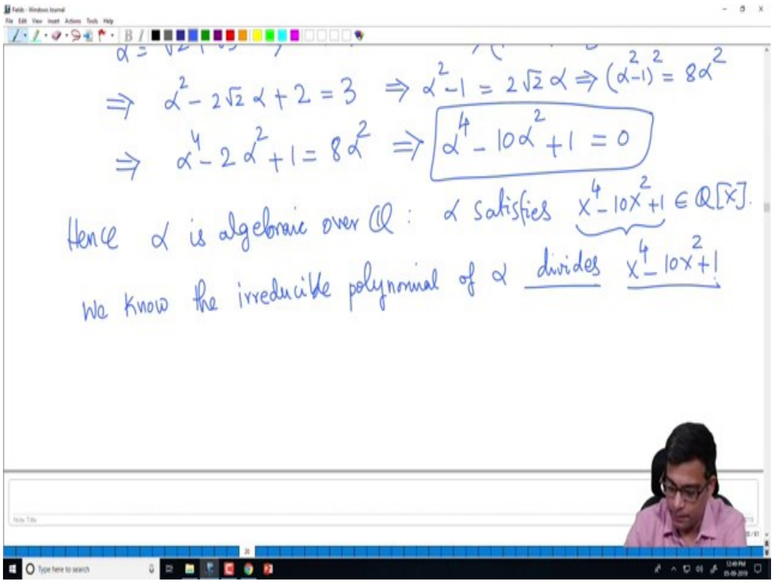


So, I will do one final example before we continue. So, let us take for example, R over Q and let us take root 2 plus root 3, technically speaking we do not even know if it is algebraic or not yet. So, how do we find whether it is algebraic or not and if so, how do you find its irreducible polynomial. This is just a technique that I might do again later, but let me quickly tell you how to find whether alpha is algebraic over we will see later, in this video or next video that some of algebraic elements is actually algebraic. So, it is algebraic and if it is what is it is irreducible polynomial over Q.

So, this is what I want quickly do in this example, so what we do is we consider alpha equals root 2 plus root 3. So, I will just do a series of calculations, so this means alpha minus root 2 is equal to root 3, that means alpha minus root 2 whole squared equal to 3. I will continue here that means, alpha squared minus 2 root 2 root alpha plus 2 is equal to 3.

So, the point is 2 square or take power suitably, so that we end up with the rational polynomial. So now, I am going to root this is three actually. So now, I am going to bring two root 2 alpha term on the other side. So, I have alpha squared minus 1 equals 2 root 2 alpha because 2 minus it is 1. Now I square both sides alpha squared minus 1 whole squared is 2 root 2 alpha whole squared that is 8 alpha squared right.

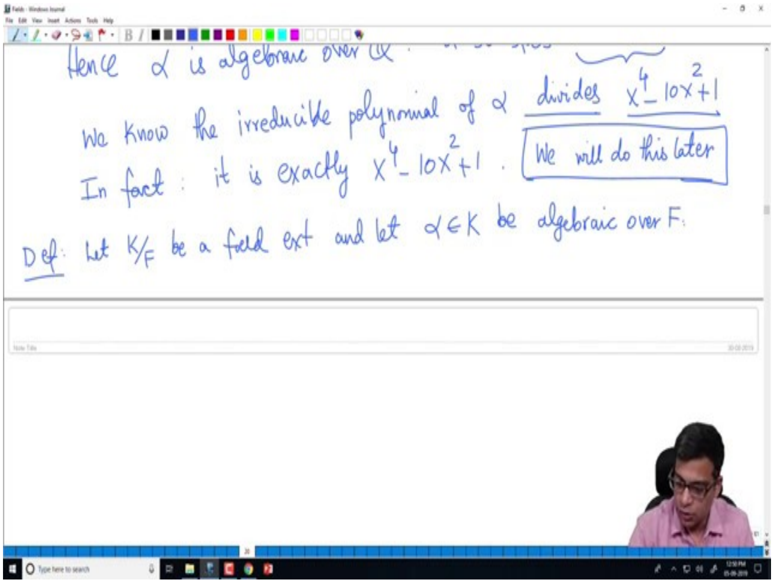
(Refer Slide Time: 12:11)



Because two root 2 squared is 8 and alpha squared, that means alpha power 4 minus 2 alpha squared plus 1 equals 8 alpha squared and finally putting everything on one side I have alpha to the fourth minus 10 alpha squared plus 1 equal to 0. So, immediately we know, hence what do, we know we know alpha is algebraic over Q. This is because alpha satisfies a rational polynomial. So, alpha satisfies this polynomial.

So, it is certainly algebraic and we know that the irreducible polynomial, see we all we can say at this point is the irreducible polynomial of alpha remember is the least degree monic polynomial that has alpha is a root. This is one such, this is a polynomial which as alpha has a root, it may or may not be irreducible polynomial of alpha. But we know that the irreducible polynomial of alpha at this point all we can say is it divides x power 4 minus 10 x squared plus 1 ok.

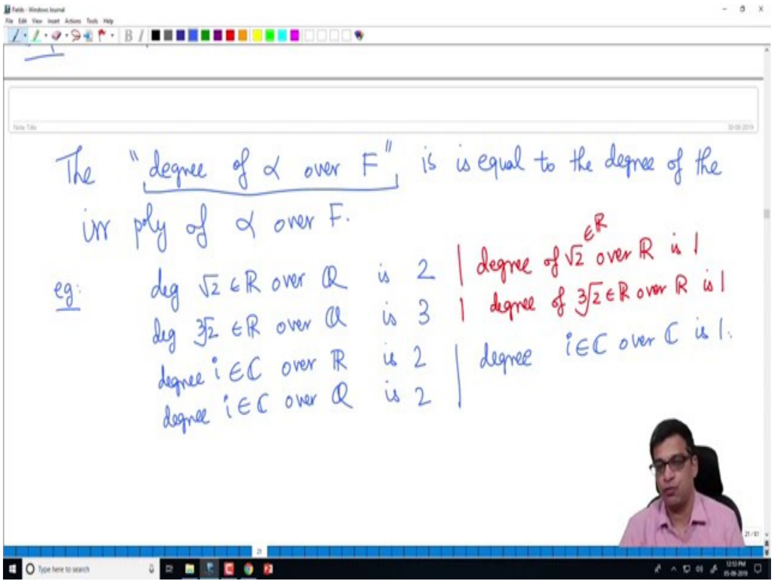
(Refer Slide Time: 13:33)



In fact, it is equal to the irreducible polynomial is it is exactly x power 4 minus 10 x squared plus 1, one way to do this is sure that this is irreducible. But that is not that easy because Eisenstein criterion does not apply and none of the other techniques that we know apply easily. So, what we need to do is something slightly more subtle and we will do this later in a couple of in the next video I think ok. So, once we talk about degree of field extensions and so on, it will follow that this is actually irreducible and we will come back to this, so this is to be done later.

So, and any way the hope right now is to just give you an idea of how to find whether something is irreducible or something is algebraic or not and try to find it is irreducible polynomial. Let me now continue so important definition now before I write the definition, let me just make one remark about transcendental elements. If you have a transcendental element there is no polynomial actually non zero polynomial that it satisfies, so we do not talk of irreducible polynomials ok. So, irreducible polynomials are only defined for algebraic elements. So, let K over F be a field extension and let alpha in K be algebraic over F; this is the definition now.

(Refer Slide Time: 15:13)

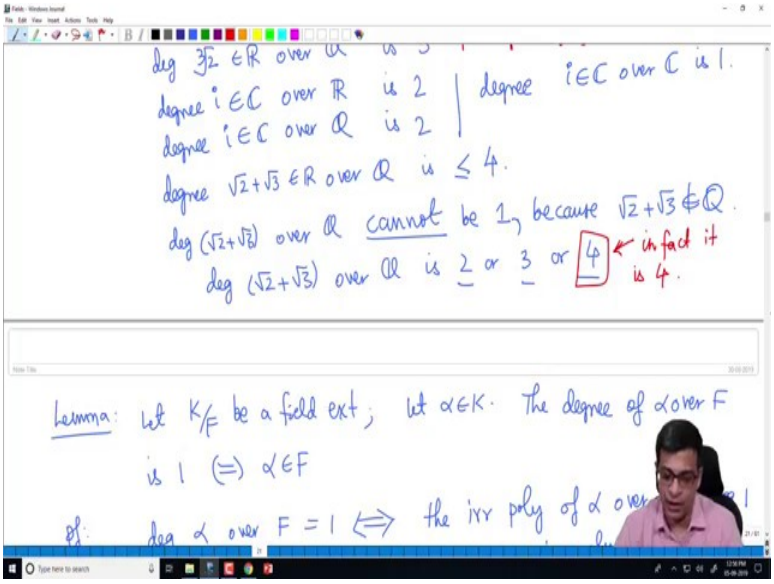


The degree of F the degree of alpha over K over F rather is simply define to be is equal to the degree of the irreducible polynomial of alpha over F very simple. The degree of an element are now defining the degree of an element over a base field is equal to the degree of the polynomial, irreducible polynomial remember irreducible polynomial is a unique polynomial that we attached to any algebraic element it is degree is call the degree of that element.

What is the degree of root 2 over root 2 which is a real number over Q. So, you have to be careful every time you talk about degree of an element, we have to specify the bigger field and the smaller field and it is over the smaller field degree of root 2 over Q is 2. Because that polynomial it satisfies x squared minus 2, which is in fact, the irreducible polynomial; what is a degree of root 3 over Q is 3 sorry I should say cube root of 2 over Q. On the other hand what is the degree of root 2 over R this is actually 1 because root 2 is in R. So, it is irreducible polynomial is actually x squared minus 2. So, it is one similarly what is the degree of cube root of 2 a real cube root of 2 over R, here also I should say is also one because it is irreducible polynomial is x minus cube root of 2. What is the degree of i which is a complex number over R this is 1 degree of the complex number i over Q is also 1 sorry this is not 1 this is 2.

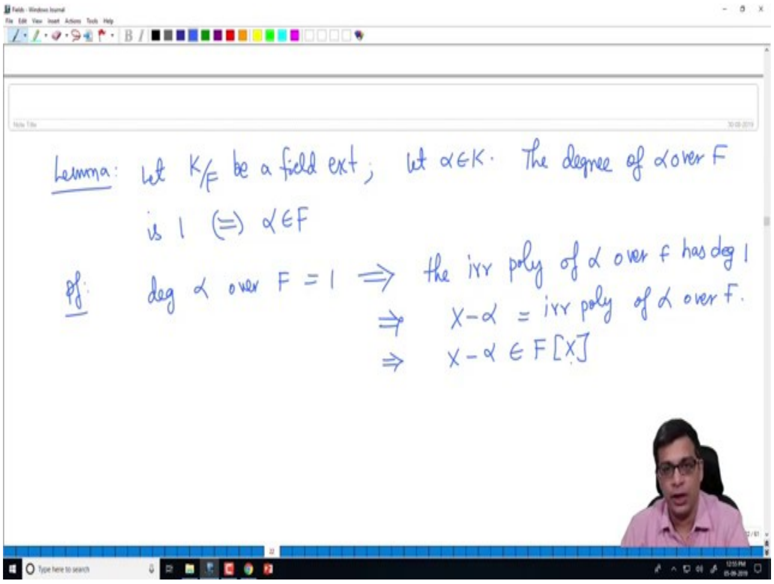
Because we saw that the irreducible polynomial that i satisfies over R or Q is x squared plus 1 and what is the degree of i over C itself that is 1 actually because the irreducible polynomial is x minus i.

(Refer Slide Time: 17:43)



And one final statement: what is the degree of root 2 plus root 3 over which is a real number over Q. We have seen that one polynomial that is satisfies is x power 4 minus ten x squared plus 1. So, at this point all we can say is that is the degree is less than or equal to 4. It is not necessarily for as of now, but it can be 4 3 2 or 1, but let me just rule out the possibility is that it is 1 degree of root 2 plus root 3 over Q cannot be 1 ok.

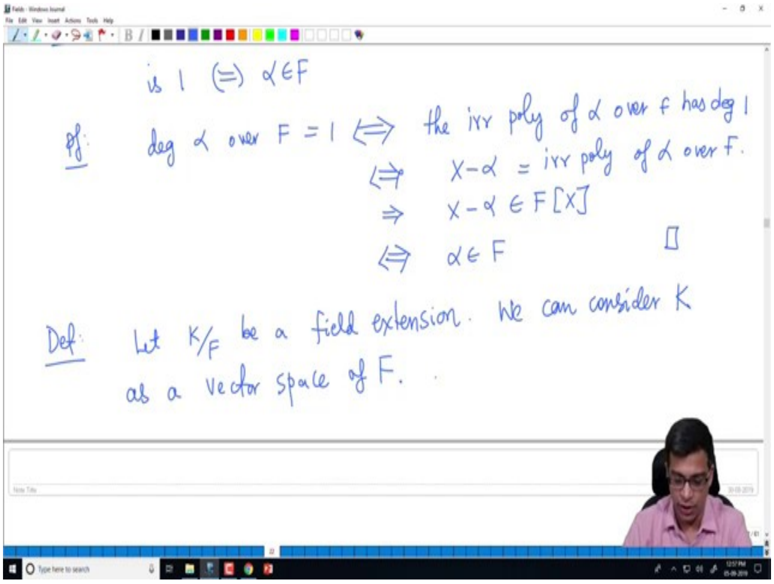
(Refer Slide Time: 18:33)



This is because a general statement I will make a simple lemma, let K over F be a field of extension as always um. Let alpha be in K the degree of alpha over F is 1 if and only if alpha is in F, so this is a simple statement why is this?

This is because suppose degree of alpha over F is 1, this implies the irreducible polynomial of alpha over F has degree 1. But this means x minus alpha is equal to the irreducible polynomial of alpha over F because it is degree of 1 it is monic. So, it has to be x plus something, but it also has to have alpha as a root, so the coefficient must be minus alpha. So, x minus alpha is irreducible polynomial of alpha over F, but remember irreducible polynomial of alpha over F lives over F, that means x minus alpha is actually in F x.

(Refer Slide Time: 19:51)

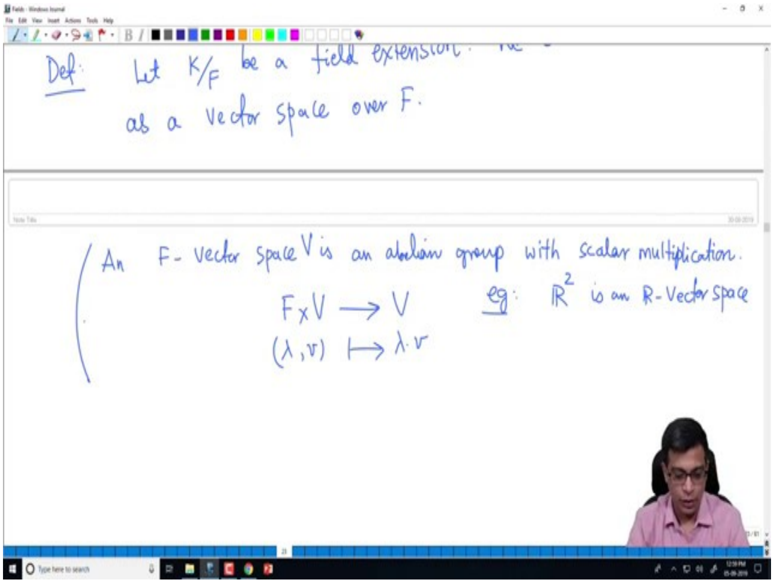


This means alpha is because if it is a polynomial over F all the coefficients are in F. So, minus alpha is in F obviously then alpha is F alpha is in F. And similarly converse is also true actually you can just go back everywhere, if alpha is in F x minus alpha is in F x minus alpha is a polynomial which has alpha is a root and degree cannot be anything smaller. So, it must be the irreducible polynomial of alpha over F hence it is degree is 1, that means it is degree is 1 so that finishes the proof.

Going over this going back to this degree of root 2 plus root 3 over Q cannot be 1 because, root 2 plus root 3 certainly we know very well is not in Q. So that means, degree of root 2 over root 2 plus root 3 over Q is 2 or 3 or 4 as of now we have three possibilities. We will comeback to this later and show that in fact it is 4. That is related to the fact that the polynomial that we computed earlier in this video x power 4 minus 10 x square plus 1 is actually irreducible, because of that irreducible the least degree polynomial has to be of degree 4 ok.

So now, we continue and define the degree of a field extension; this is the other important definition of this video; let K over F be a field extension. Let this be a field extension, we think of rather I will say we can consider K as a vector space over F. So, in this part of the course in the remaining videos we need a little bit of linear algebra, you need to know what are vector spaces, what are bases of vector spaces, when do we say set of vectors span a vector space or are linearly independent all these notions. You basic linear algebra that you covered in some earlier course will be required.

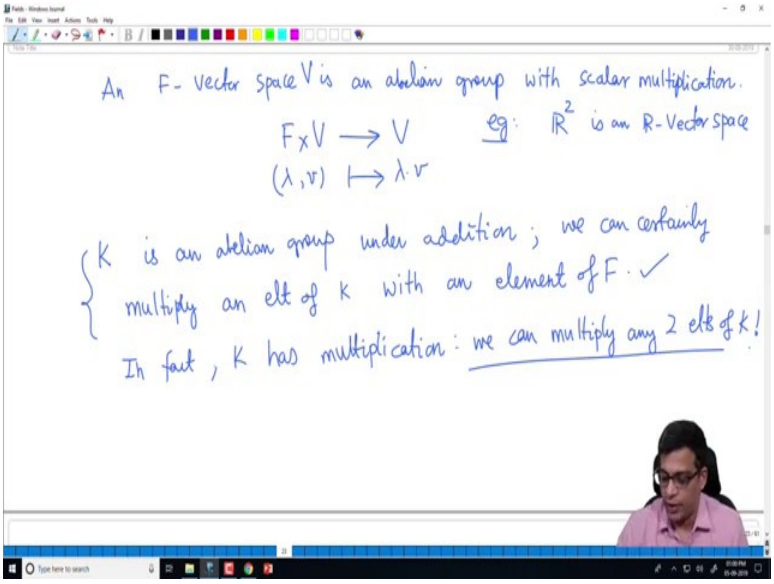
(Refer Slide Time: 22:16)



So, we can certainly think of K as a vector space of over I should not say of I should say over F, why is this how can we think of K as a vector space over F. So, let me quickly recall for you what is a vector space. An F vector space is an abelian group, an F vector space is an abelian group with scalar multiplication. So, I will simply write, this is not a formal definition as I said you only need to know basic linear algebra very little, not a lot just notions of what are vector spaces, what are bases, what are linearly independent vectors, what are spanning vectors and so on.

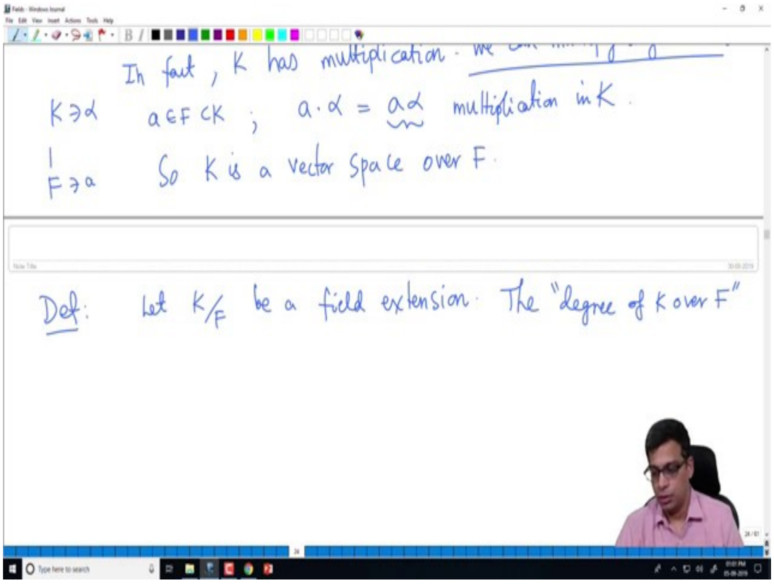
So, it is an abelian group which has a scalar multiplication, that means given an element of F which are called scalars and given a vector in V we need to know have the notion of lambda dot V. So, typical example is R 2 is an R vector space right, because R 2 is an abelian group by component wise addition and you can multiply any vector by a real number because you can multiply each coordinate by that vector. So, this is a quick review of what a vector space is.

(Refer Slide Time: 23:39)



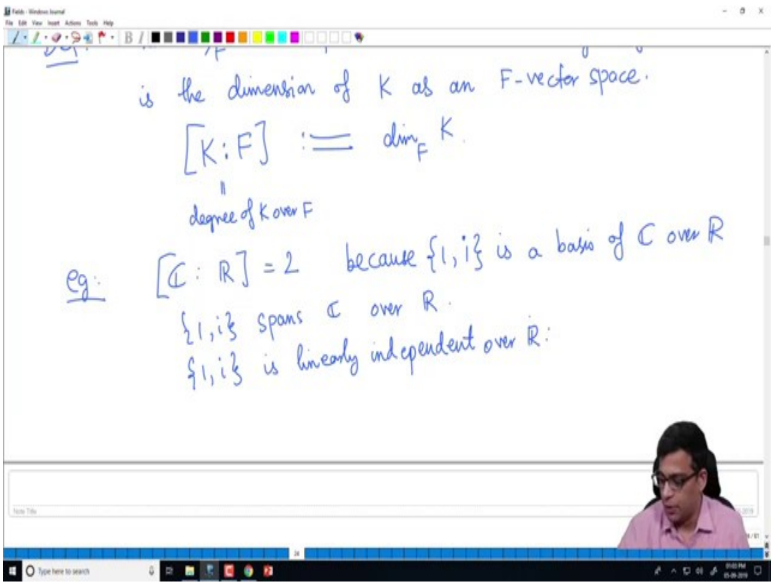
Now, K is certainly an abelian group under addition that is part of the definition of a ring, K is an abelian group under addition. So, that is the first condition for a vector space and we can certainly multiply an element of K with an element of F. Because remember that is what we need for a vector space. This is actually K has much more structure right, so in fact, K has multiplication so. In fact, it has a lot more structure than a vector space over F structure because you can multiply any two elements of K. Forget about multiplying an element of K with an element of F we can actually multiply any two elements of K, but when we think of K as a vector space we do not need that additional structure of K.

(Refer Slide Time: 25:00)



So, remember K contains F if you have some alpha here and some a here a is also in K. So, a dot alpha a is being thought of as a scalar alpha is being thought of as a vector is simply a dot alpha multiplication taking place in K ok. So, we have an abelian group with the scalar multiplication with scalars coming from F, so it is a vector space over F ok. So, this is an extremely important observation for us.

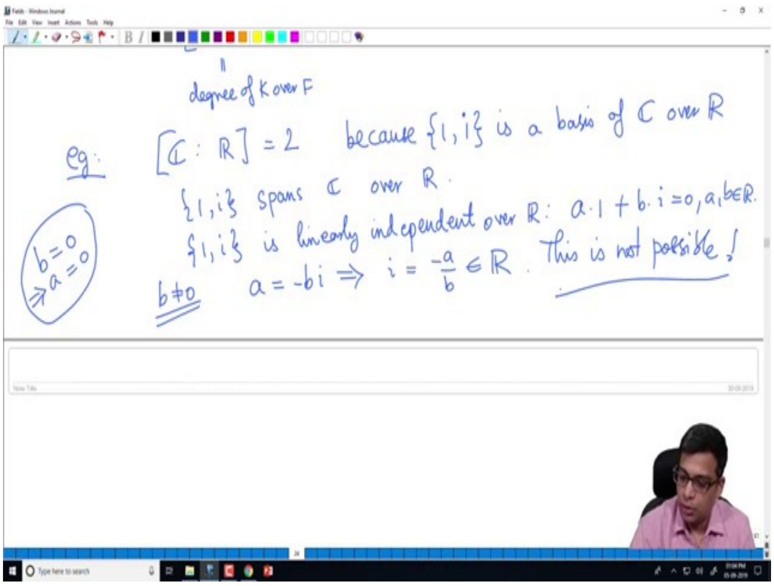
Every time you have a field extension we think of the bigger field as a vector space over F and we will elaborate on this in the future videos. But now let me actually give you the definition that I promised. Let K over F be a field extension.



Now, I am defining the degree of the entire field extension over F is simply the dimension of K as an F vector space ok. So, dimension of K as an F vector space, so the notation that we will use is K colon F in square brackets. So, this is the degree of K over F is by definition dimension of K as in F vector space.

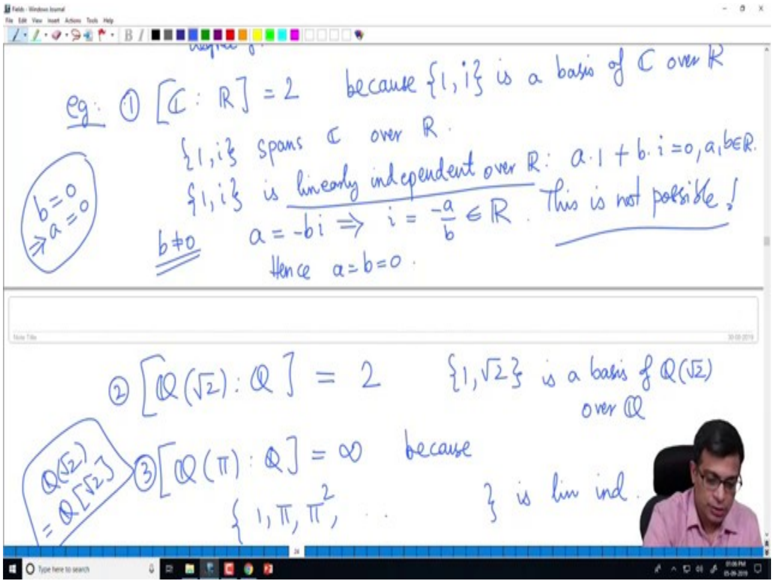
So, as I said I am going to elaborate on this and use this a lot in the future videos, let me now quickly give a couple of examples. If you take so if you take C colon R I claim is 2, because 1 comma i is a basis of R of C over R. Because what is an element of complex numbers it is of the form a plus i b where a and b are real numbers. So, in other words 1 comma i span C over R because every element of C is an R linear combination of 1 and i. But why do they form a basis because basis remember is spanning set which is also linearly independent set, we know that certainly they span why is it a linearly independent set. So, this certainly spans C over R. Why is it linearly independent set linearly independent, So let me write it here linearly independent over R because what does it mean?

(Refer Slide Time: 28:09)



If not, actually let us write like this a times 1 plus b times i is 0, let us I a b are in R; that means a is equal to minus b i. That means and suppose b is so if b is 0, that means a is 0. Also because b is 0 a times one is equal to 0. So, a is 0 supposed b is not 0, then we can write I as minus a by b which is of course in R this is obviously not possible right; the imaginary number i cannot be in R.

(Refer Slide Time: 28:55)

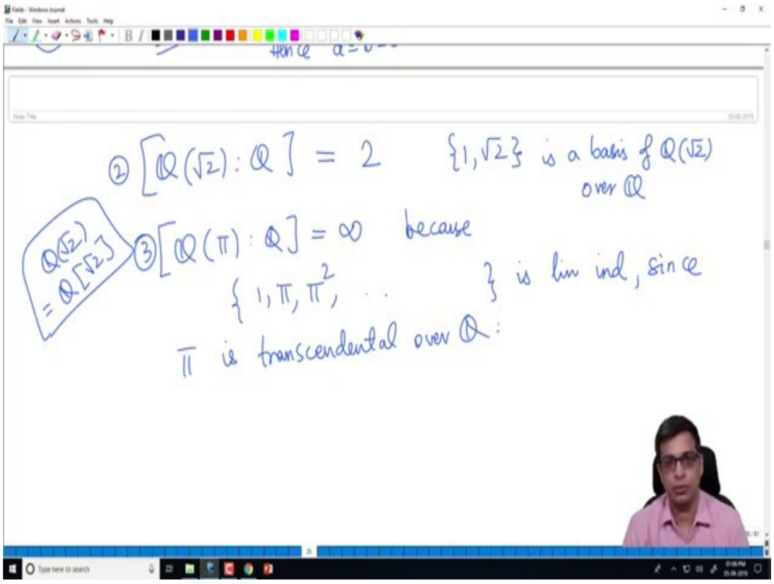


So that means, hence a and b are 0 which is exactly the linear independence right. If one comma I has a property that a times one plus b times is 0 than a and b are 0; that means, they are linearly independent. So, it is a basis so degree is 2. Now I will discuss this in the next video carefully, but I claim that this is also 2 the degree of the field extension Q root 2 over Q is 2.

Because here 1 comma root 2 is a basis of Q root 2 over Q remember because root 2 is algebra over Q root 2 is actually equal to Q square bracket root 2 and you want to say that this is all polynomials in root 2. But actually just degree two polynomials degree one polynomial means 1 and root 2 will suffice. And finally, I will also say Q adjoined pi over Q is infinite, because 1 comma pi is the transcendental element is linearly independent right. Because this all the powers of pi form a linearly independent set because, if they are not linearly independent then some finite linear combination is 0.

But if a finite linear combination of this is 0; that means, pi is algebraic over Q which it is not. So, there are three examples that I have done here please think about this carefully; first one I explained second one is very similar to the first one.

(Refer Slide Time: 30:44)



Third one is a consequence of transcendence of pi over Q. That means, you have, a you have an infinite linear independent set. That means, the degrees is in basis the dimension is infinite. So, the degree of Q pi over Q is infinite. So, let me stop the video here and the next video we are going to talk about degree of field extensions and do further properties of that invariant.

Thank you.