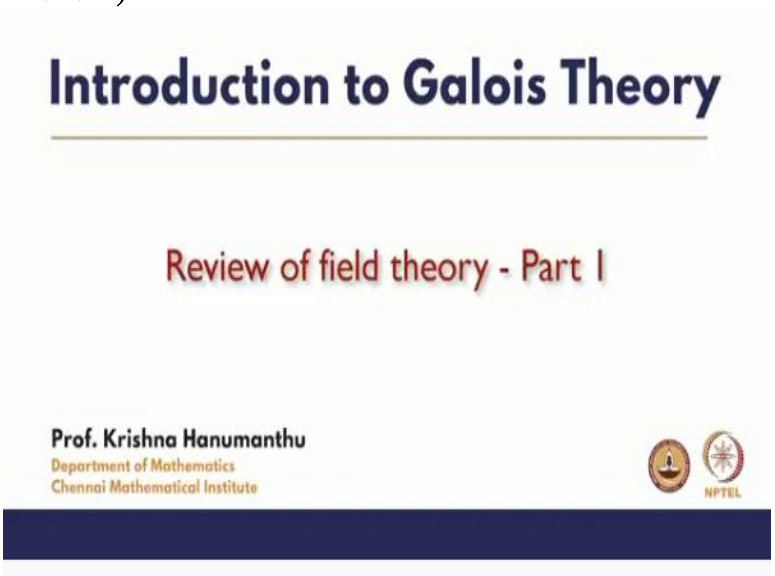
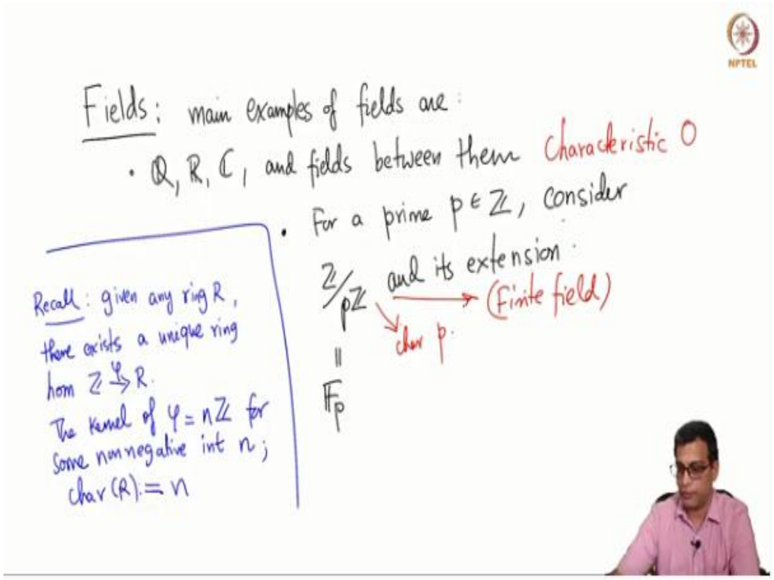
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Module: 01
Lecture 05: Review of field theory – Part I

(Refer Slide Time: 0:11)



Welcome to the course, so far, we have revised the basics of group theory, ring theory, in the last few videos, today I want to do the final topic of revision before we start Galois Theory and that is fields. So, I want to spend maybe one or two classes, just giving you a basic overview of the field theory that we are going to study.

(Refer Slide Time: 0:35)



So, we all know what fields are, I recall that definition. So the main examples of fields that I want to talk about today, and these are things that, things you should keep in mind are the following. So we will look at the fields of characteristic zero, namely Q, R, C and, and fields between them.

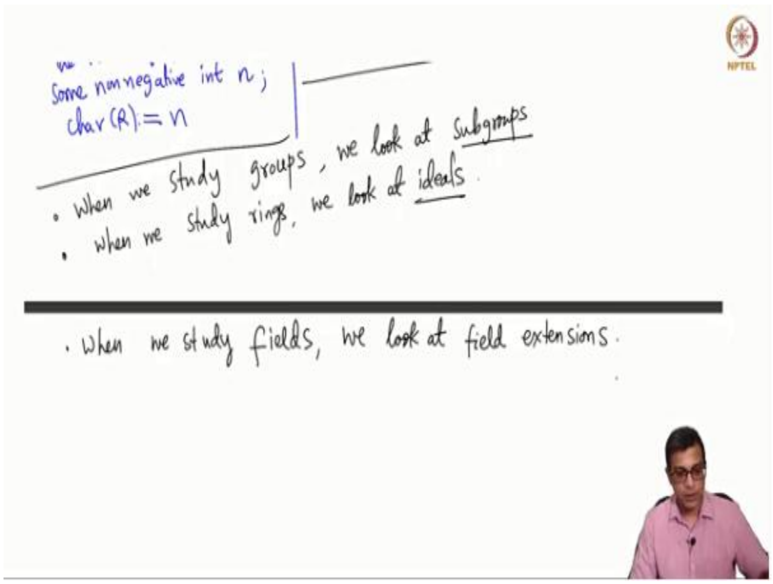
So I will explain in a minute what I mean by that. But these are fields that are contained let us say between Q and R. So these all have characteristic zero. So, if you recall from your ring theory and filed theory courses, characteristic means maybe I will just quickly recall this.

Given any ring and I will mention again though, this is a standard assumption throughout the course, ring for us is always commutative with unity, there exists a unique ring homomorphism from Z to R, the kernel of this which is, which is an ideal of Z, let us say phi is the form nZ for some positive integer n, then the characteristic of R is defined to be n that is the revision.

So, characteristic is, sorry some I should not say positive integer, I should say non negative integer because kernel could be zero ideal. So, n is a non negative integer characteristic is that, so, if you further now that R is a field in which case the kernel of, so image of this map (())(2:51) is an integral domain because the sub ring of a field is an integral domain. So, the kernel will be a prime ideal, so, it is either zero or generated by a prime number. So, the characteristic of a field is always zero or a prime number.

Now, the other important class of field is Z mod pZ, let us say p is a prime, consider Z mod pZ which we denote by Fp and its extensions. So, I am going to recall the main theorem of finite fields, later on, so this is characteristic p. So, this is a finite field in particular, this is a finite field, its extensions can be infinite but we, this class of finite fields is very important for us. So, these are the fields.

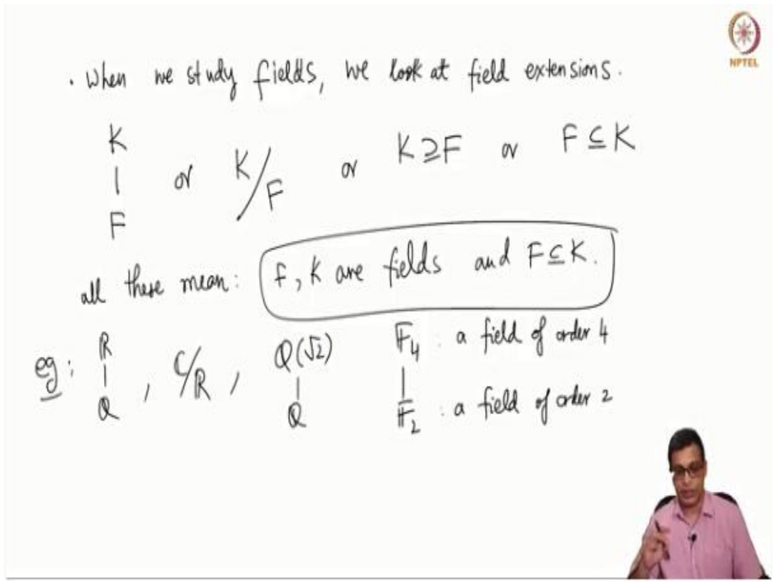
(Refer Slide Time: 4:01)



So, I sort of mentioned this in the previous video. So, when we study, when we study groups, we look at subgroups, this is the object that is often interesting for us, so to understand a group we look at its subgroups. When we study rings we look at ideals, sub rings not that interesting in ring theory.

So, we look at ideals and when we study fields, we also look at subfields but, unlike in the group case, the ambient ring and subgroups when you study them, ambient ring is the most important one, here we study field extensions, more so both the bigger field and the smaller field have equal importance. So we look at field extensions.

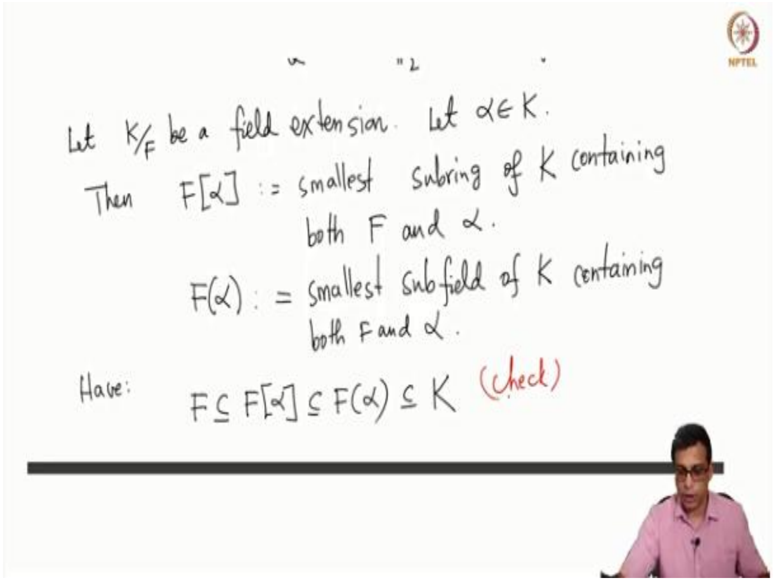
(Refer Slide Time: 5:13)



So, this is typically what, I mean the most important notation that we use when we study field, fields or field extensions, so I will write down all the kinds, different kinds of notations I am going to use. So, what do I mean by any of these symbols? So, all these mean F and K are fields and F is containing K. So, to illustrate that we write any of these symbols.

For example, we write, R over Q or C over R and Q root 2 over Q etcetera, so or F4 over F2, so this is a field of order 2, this is a field of order 4. So, these are all examples of field extensions, which is the primary object that we study in field theory. And in fact, that is a primary object that we are going to study in this course on Galois theory as well.

(Refer Slide Time 6:32)

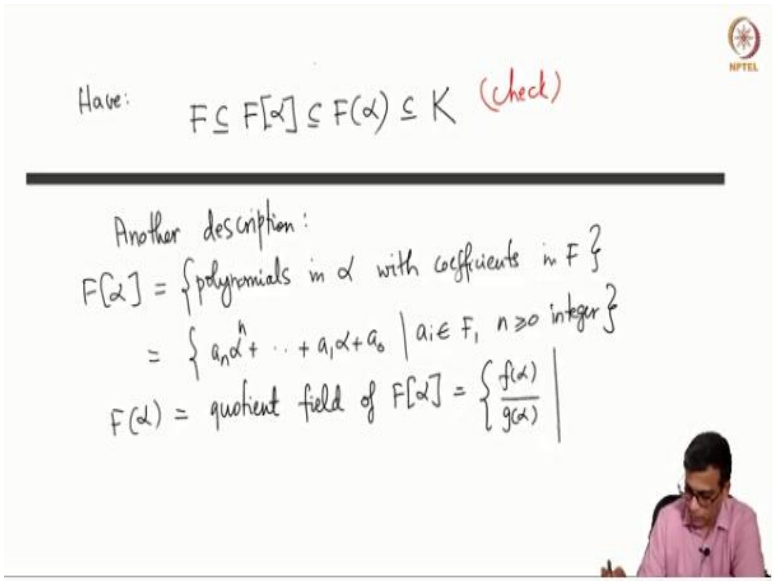


So, let me just quickly recall some of the fundamental things about this. So, let K over F be a field extension, by which I mean as I indicated here K and F are fields and F contains F is contained in K, the one in bottom is the smaller one, the one above is the bigger one and let alpha be an element of the bigger field, then we define two important things.

So F square bracket alpha is the smallest sub ring of K containing both F and alpha and other important sub ring, sorry, it is in fact a field is F round bracket alpha, it is this smallest sub field of K containing both F and alpha. So, these are two important things, so, we have always this chain of inclusions.

So, you have F, F square bracket alpha and contains F round bracket alpha because, if F square bracket alpha is the smallest sub ring containing F and alpha, F round bracket alpha is a smallest subfield, so, it is also a ring. So, it contains F square bracket alpha, this one can check okay.

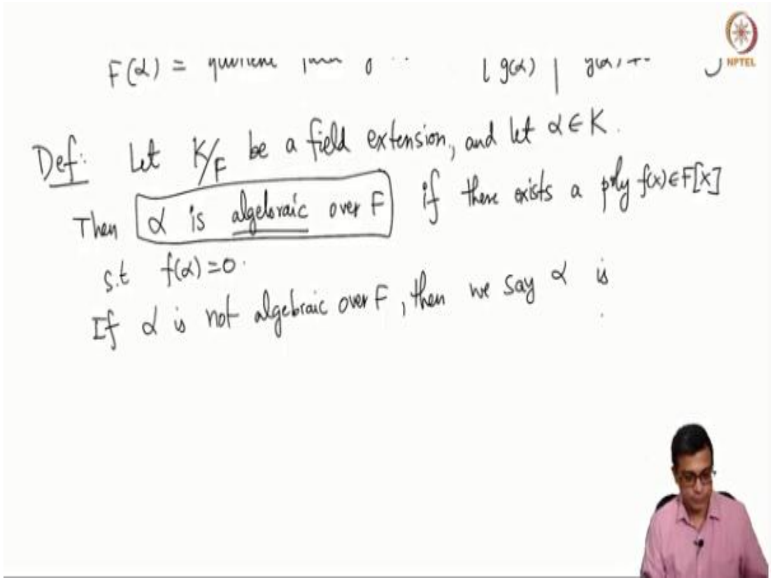
(Refer Slide Time 8:22)

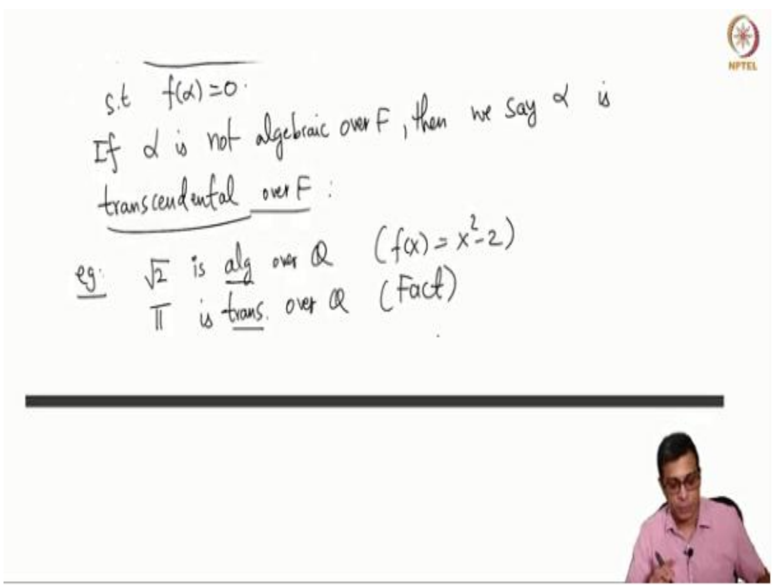


So, any sub ring of K containing both F and alpha contains F square bracket alpha and this is clear, another description of this is the following. F square bracket alpha consists of polynomials in alpha with coefficients in F. So, in other words it consists of all things of the form a n alpha power n a1 alpha plus a0 ai are in F and n is a non negative integer. That happens to be a ring, every ring that contains capital F and small alpha must contain all such polynomials and it happens to be a ring. So, this is the smallest sub ring containing this and this is the quotient field of F square bracket.

This is in fact ratios of polynomials. So, these are F alpha divided by G alpha, where F and G are in capital F X, so, there single variable polynomials over capital F and we want G alpha to be nonzero. So, this also justifies this chain of inclusions. Now, this is very general. What I now want to do is to understand a little bit more about what these sub rings and sub fields are.

(Refer Slide Time 10:10)



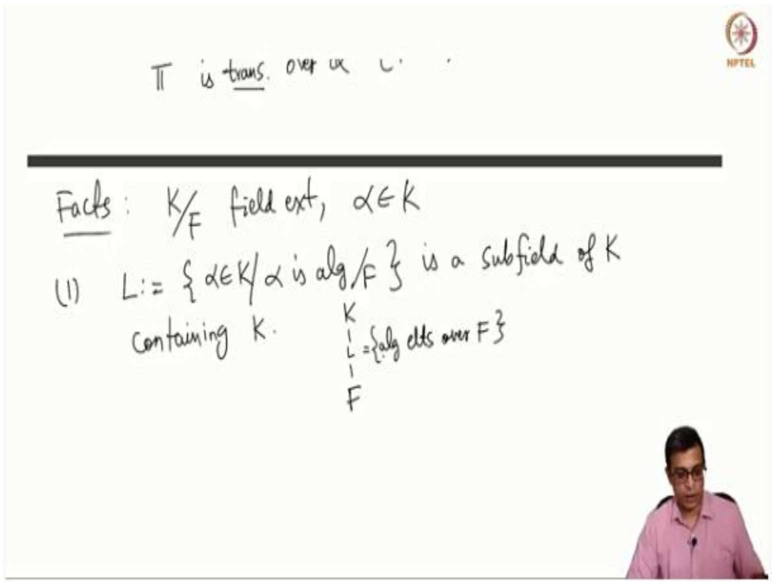


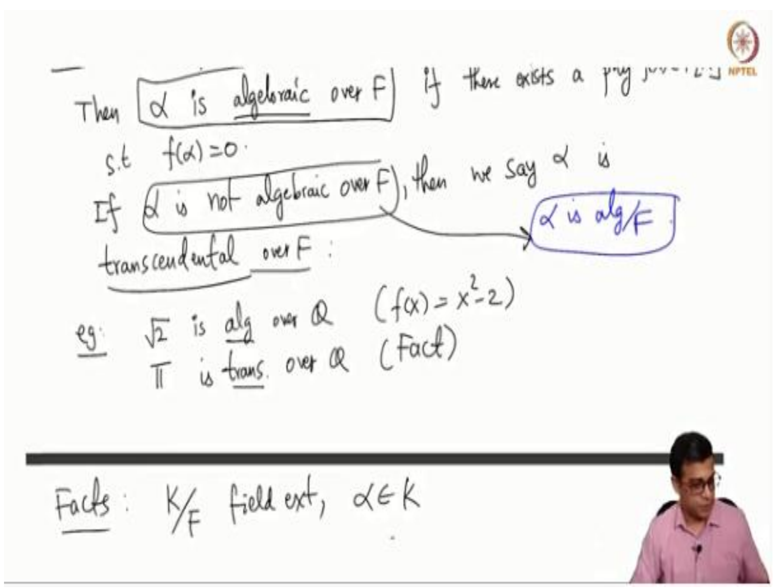
Now, an important definition. So, let again K over F be a field extension, everything that you study in a field theory starts with some statement like this, let K over a F be a field extension, because field theory is really a study of field extensions and let alpha be in K. So, you have an element in the bigger field.

Then alpha is algebraic over F if there exists a polynomial fx in capital FX such that F alpha is 0. So, we say that alpha is algebraic over F, this entire phrase is important, as we will see being algebraic is a statement about the element and the base field, if, so just to complete the definition, if alpha is not algebraic over F meaning there is no such polynomial which has alpha as a root, then we say alpha is transcendental over F.

So, examples, root 2 is algebraic over Q, take fx to be x square minus 2. Pi is transcendental over Q, this is a fact, it requires it is a theorem in mathematics that there is no algebraic, I mean there is no polynomial over rational numbers which satisfies alpha which, which has pi as a root. So, these are important notions for us.

(Refer Slide Time: 12:20)



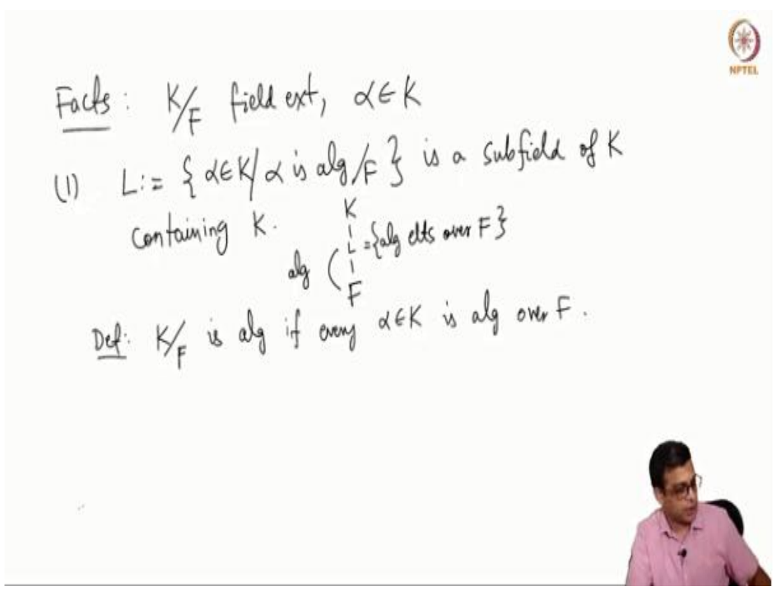


So, now I am going to write down a series of facts, which again you learn so, remember again, this is not supposed to be an exhaustive revision, I am just listing important facts so that it gives you a way of what kind of things we need from field theory so maybe I will just label them like this.

One, if alpha is so again, maybe I will just make a global assumption, K over F is a field extension, alpha is in F, sorry, alpha is in K. If you' define L to be alpha in K such that alpha is algebraic over F, this is my notation. So, we say, we write, for this we write alpha is algebraic over F, just a shortcut for me, so that I do not need to write the full sentence.

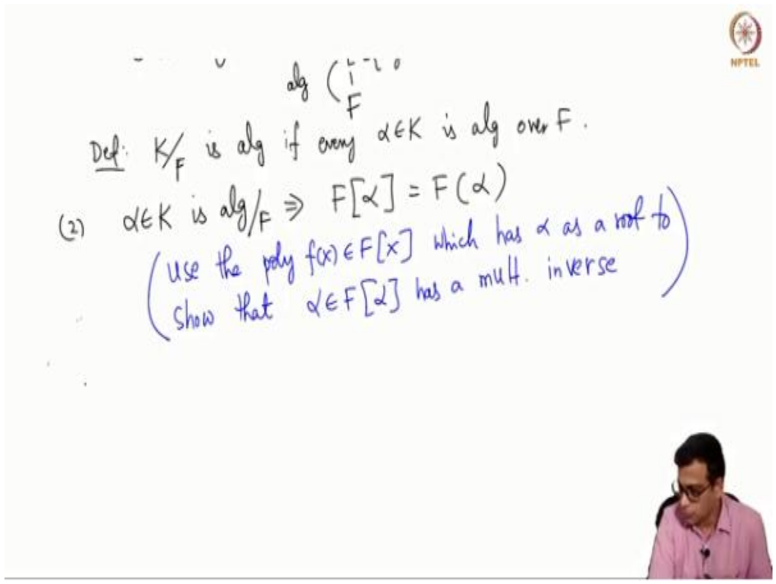
So, if alpha is algebraic over F, you take all such elements. So of course, F contains this, is a subfield so, the statement is that it is a field, this set is a field of K containing K. So, we always have given a field extension, we have L in between, in the middle. So this is a set of algebraic elements over F.

(Refer Slide Time: 13:59)



So, we say that definition, the field extension itself is algebraic, if every alpha in K is algebraic over F. So, so, this in particular is an algebraic extension, because everything in L is by definition algebraic over F. So, we say it is algebraic.

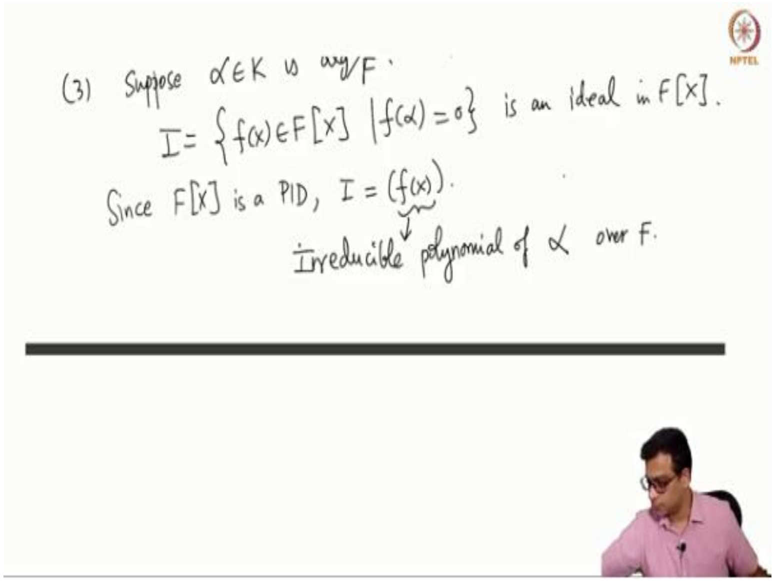
(Refer Slide Time: 14:28)



Second fact is, if alpha in K is algebraic over F, then the smallest field containing F and alpha is same as the smallest ring containing F and alpha. So, this is an important fact so, when we are dealing with algebraic elements, we do not do distinguish between square bracket and round bracket.

So, here, the idea is that use the polynomial F, I am not going to prove this fact, but I will simply say that, use the polynomial effects which has alpha as a root, to show that alpha in F square bracket alpha has an inverse, has a multiplicative inverse, as a multiplicative inverse, that means it is a unit. So F square bracket alpha already happens to be a field so, that is what we take.

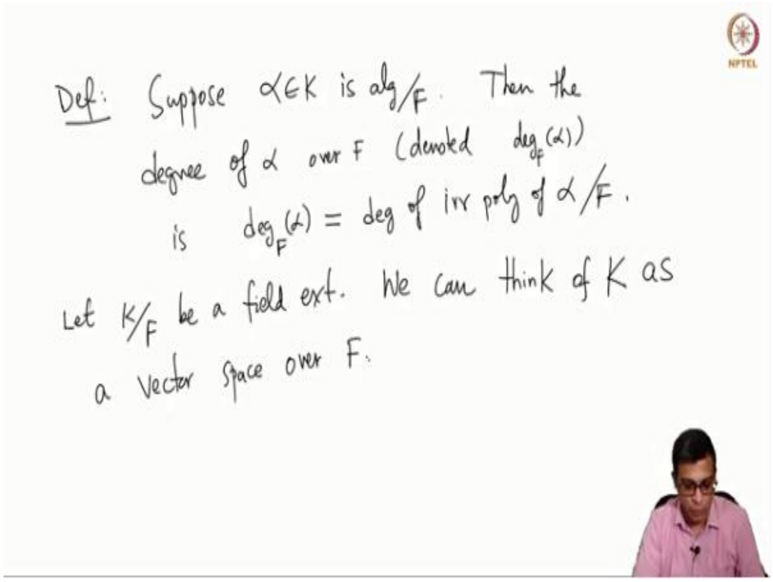
(Refer Slide Time: 15:37)



So now, so some other things, these are not facts really but I am introducing new things to you. So, let suppose alpha in K is algebraic over F so, then I equal to all polynomials in fx which have alpha as a root is an ideal in FX and from the previous videos we know that FX is a PID because F is a field the polynomial ring in one variable over a field is a PID.

So, I is generated by a single element and this is called the irreducible polynomial and that will be irreducible that is one, that is a fact one can check, it is the, it is called the irreducible polynomial of fx over capital F, sorry, irreducible polynomial of alpha over capital F.

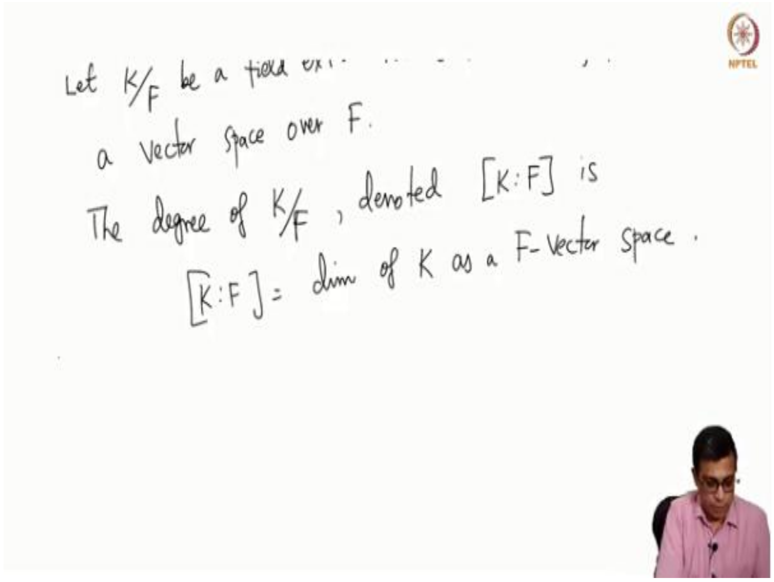
(Refer Slide Time: 16:56)



So, I am going to give examples of all these things and definition, degree if so, let suppose, suppose alpha in K is algebraic over F, then the degree of alpha, I am going to, degree sub F so, maybe I will first write it in words, degree of alpha over F, it is denoted degrees sub F of alpha is, is by definition degree of irreducible polynomial of alpha over F. So, that is a degree and let me just complete the review and then we will spend some time giving examples.

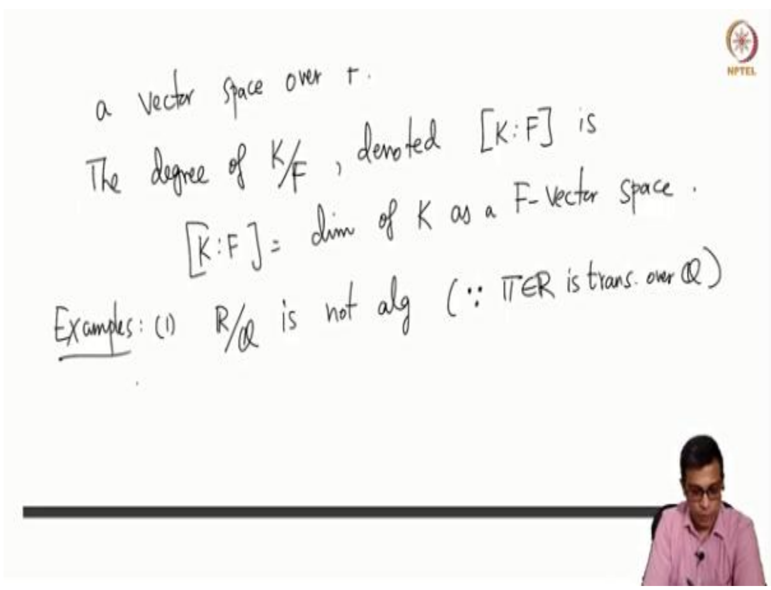
So, let us say K or F is a field extension. We can think of or we can consider K as a vector space over F because, what is an F vector space? F is a field and F vector space is an abelian group, which admits multiplication by F, elements of F, namely scalar multiplication. Of course, K is a field so, it is an abelian group and you can multiply two elements of K among themselves. So, certainly you can multiply an element of K by an element of F, so it is a K vector space.

(Refer Slide Time: 18:39)



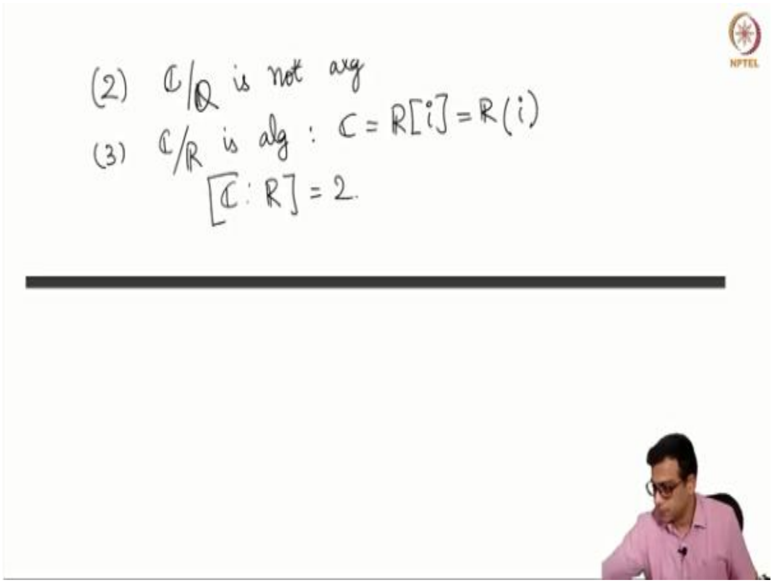
The degree of this field extension denoted by this symbol is dimension of K as a F vector space. So, that is the degree of field extensions, extension. So, I think I have essentially recalled the main things for now that I want to discuss. So, go ahead, let us go ahead and discuss various examples.

(Refer Slide Time: 19:17)



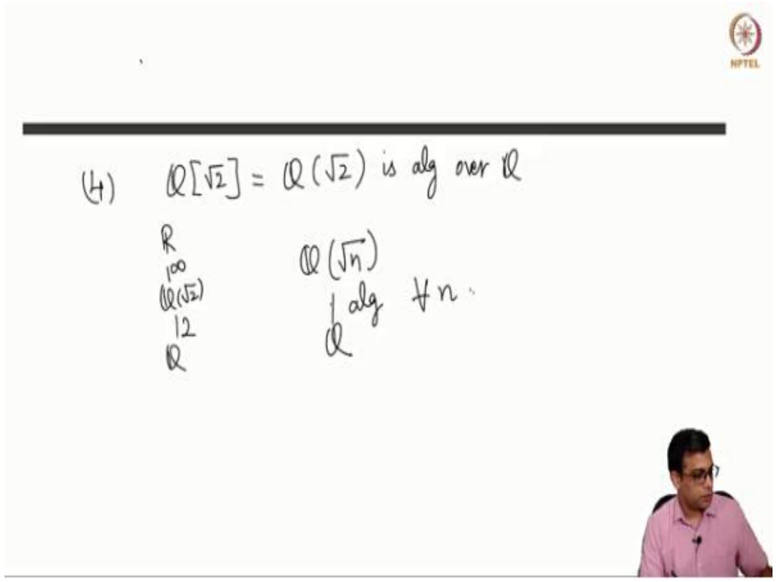
First one, we know that R over Q is not algebraic, the field extension R over Q is not algebraic. Remember an algebraic extension is an extension where every element of the bigger field is algebraic over the smaller field. So, even if there is one transcendental element, the extension will not be algebraic. So, the reason here is pi in R is, sorry, pi in the real numbers is transcendental over Q. So, what about C over R? So, first let us do C over Q, is also not algebraic, because pi is a complex number also.

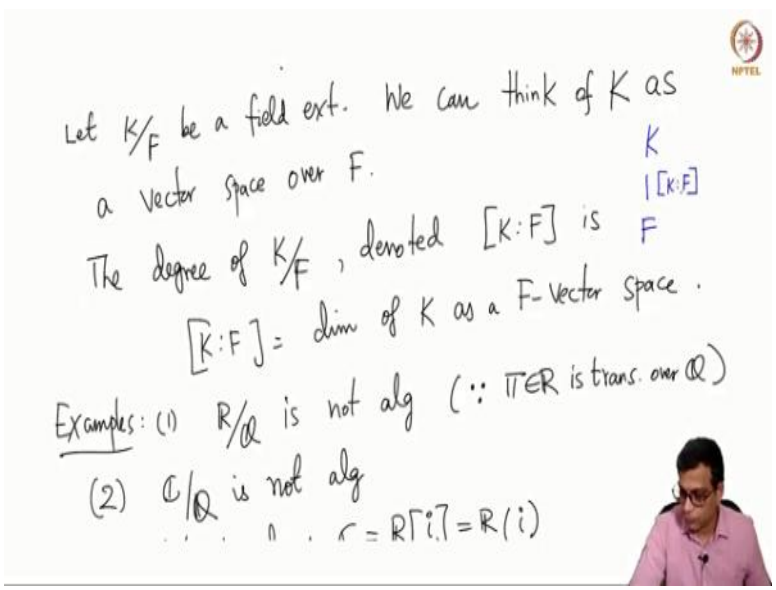
(Refer Slide Time: 20:08)

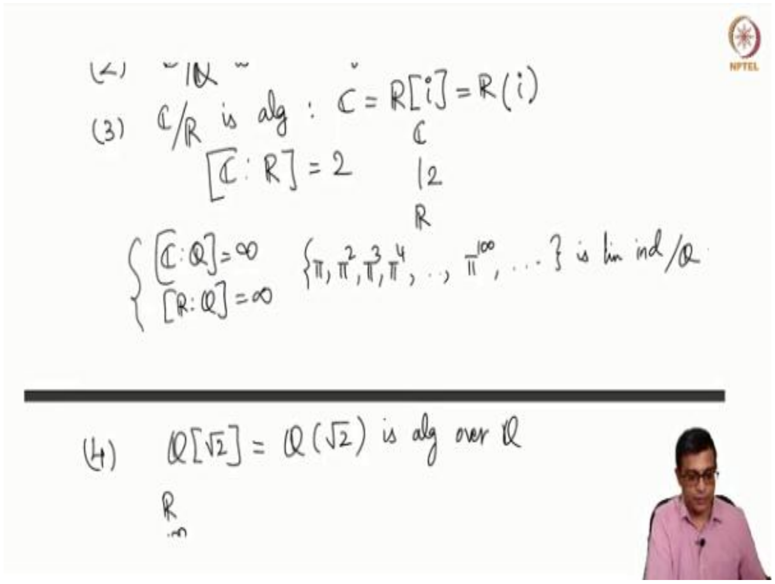


So, there is an transcendental element whereas C over R is algebraic. The reason is C is in fact R square bracket i, which we agree is the same as R round bracket i. In fact, we know that C colon R is just 2. So, this is the degree of that field extension.

(Refer Slide Time: 20:37)



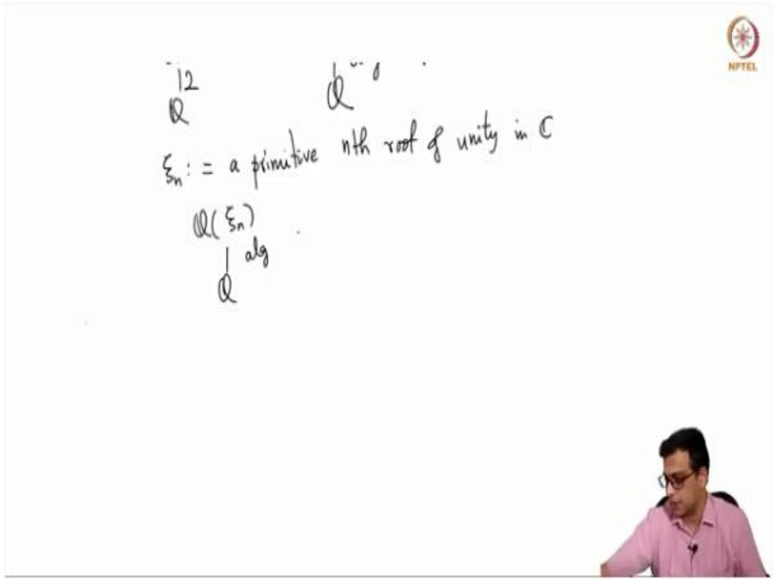




So, let us now continue so, Q square bracket root 2 is same as Q round bracket root 2, because root 2 is algebraic over Q, so, what we have is R Q root 2, Q and also when I defined the degree of a field extension, the terminology is that you put that number here. So, on the bar so, for example, here you will write C, R and 2 represents the fact that it is degree 2, so, this is 2 and this of course, is infinite.

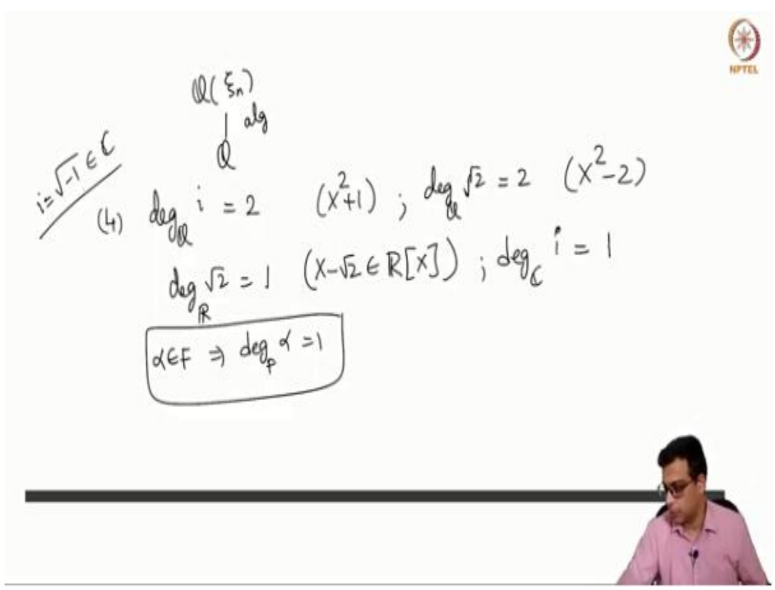
So, every time you have non algebraic extensions it is an infinite dimensional vector space. So, that is because pi, pi square, pi cube, pi power 4, pi power 100 and so, on the set is algebraic is linearly independent over Q, that is the meaning of being transcendental, if there is a linear relation that gives you a polynomial for which pi is a root. So, this is infinite dimensional vector spaces. So, similarly, this generalizes to Q is algebraic for all n.

(Refer Slide Time: 22:15)



So, some other examples, if you take zeta n be a primitive nth root of unity in C, so then that is a algebraic extension, we will learn later, what the degrees if n is prime, the degree is just n minus one but otherwise you have to, it is the Euler function, which at some point we will discuss.

(Refer Slide Time: 22:47)

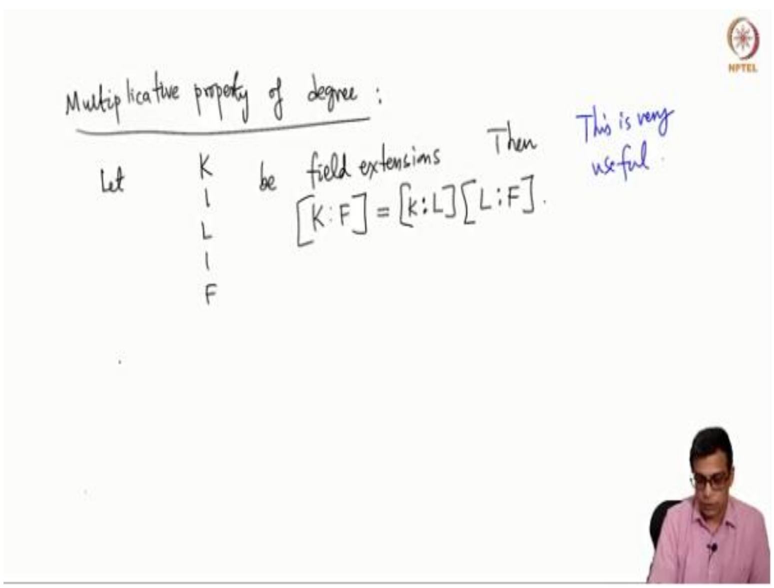


So now, let us talk about degrees on some specific elements. So I am going to recall what is degree of i over Q, i being the square root of minus one, complex square root of, one of the square root of minus one, degrees clearly two because irreducible polynomial here is X square plus 1.

What about degree of root 2 over Q? This is also 2, here irreducible polynomial is X square minus 2, what is the degree of root 2 over R? I claim this is 1 because X minus root 2 is a polynomial over the base field which satisfies root 2. So the degree of the irreducible polynomial is just 1.

So in general, of course, if you have alpha in F, then degree of alpha over F is always 1. So degree, sort of tells you how far away it is. If its degree is a positive number, its one means it is in the field itself. Similarly, degree of i over C is 1.

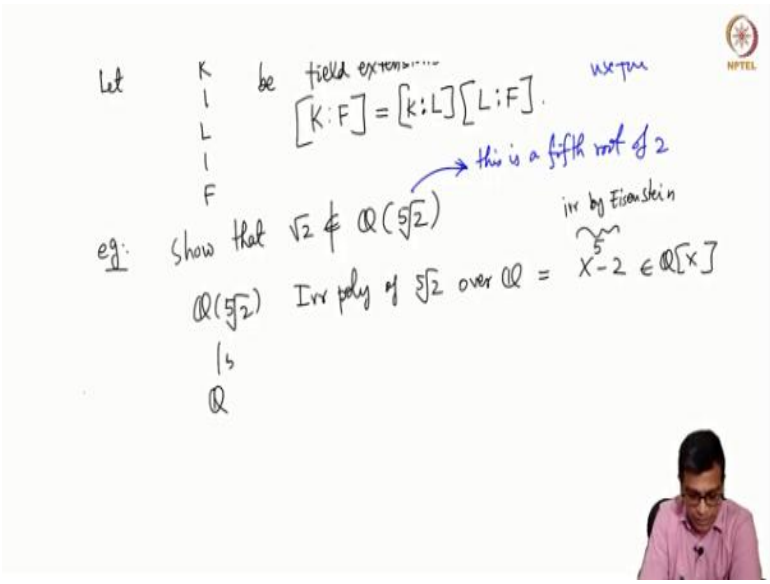
(Refer Slide Time: 24:04)



And the final thing that I want to mention here is the multiplicative property of degree. This is an important result for us, which we constantly use. So, this says that let you have K L, F, be field extensions, then what we have is the degree of K over F. So, remember this means K is a field containing L, L is a field containing F.

So, the degree of K over F is the product of degree of K over L times degree of L over F and this formula holds even if one of them is infinite, so, with the understanding that infinity times any number is infinity. So, if K colon F infinity, if this is infinity, one of these must be infinity. Otherwise, if these are both finite numbers, this is also finite number. So, this is most useful to us when everything is a finite extension and we constantly use this. So, and this tells you for example, useful this is very useful so, that is what I am saying, this is very useful.

(Refer Slide Time: 25:30)



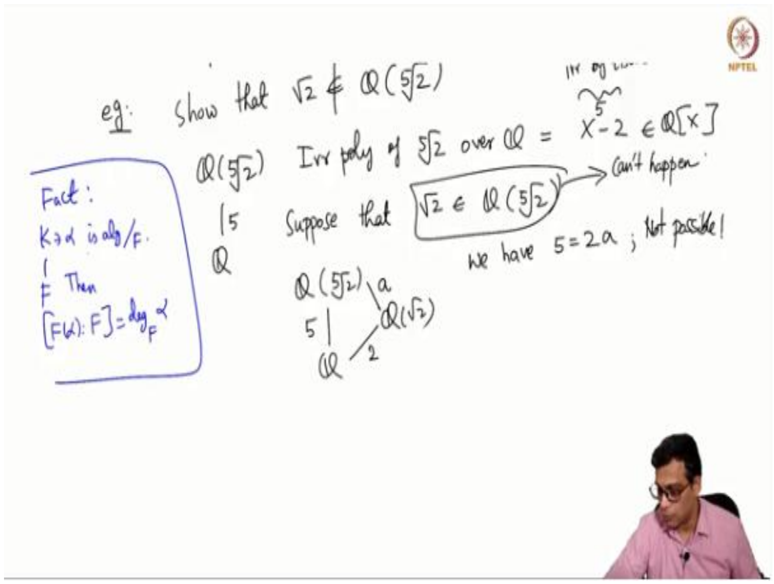
So, for example, let us apply this to the following situation, show that root 2 is not in Q adjoin fifth root of 2. So, this is a let us take this is a fifth root of, there are lots of fifth roots of 2 in C, I take one of them in fact, I can take real fifth root, I claim that root 2 is not there.

See this kind of statement if you try to do it from first principles, it is a bit tricky, because you have to work with arbitrary elements of Q adjoin fifth root of 2 and so that none of them has the property that it square is 2, whereas if you use the degree, multiplicativity of degree, this becomes very easy, because what is the degree of this extension? What is irreducible polynomial of fifth root of 2 over Q?

This is nothing but X square sorry, X power 5 minus 2, this is because X power 5 minus 2 is a polynomial in QX, which satisfies, which, which has fifth root of 2 as a root because if you apply, if you plug in X equal to fifth root of 2, you get zero and this is irreducible by Eisenstein criteria, which I recalled last week, last time.

So, this is irreducible, and it has a fifth root of 2 as a unit, it is monic which usually you take irreducible polynomial to be the monic because you can always multiply by a scalar it will be smallest degree polynomial having that as a root, so, you take the monic one, so this is the irreducible problem that means this degree is 5.

(Refer Slide Time: 27:28)



So here there is a fact. So, maybe I will write it here, fact is, so, you have K over F a given field extension, alpha is algebraic over F, then the degree of F alpha over F is same as degree of alpha over F, this is a simple fact you can check this. So, this says that it is 5.

Now, suppose that, suppose that root 2 is in Q root, Q adjoined 5 root of 2. So then that means you have this field extension, given field extension, but Q adjoins square root 2 is in between, this is 5, this we know is 2, that is clear. So whatever this number is, we must have 5 equals 2 here, because this is 5 is equal to 2 times here, just directly applying the, this formula here. But this of course, is not possible.

So, that means this cannot happen, so as you can see, this is a nice illustration of what we can say about field extensions and the multiplicative property of extension, degrees of extensions of fields, so let me stop this video here. In the next video, I am going to recall a few more things about fields and talk about finite fields, and then we will be ready to start Galois Theory. Thank you.