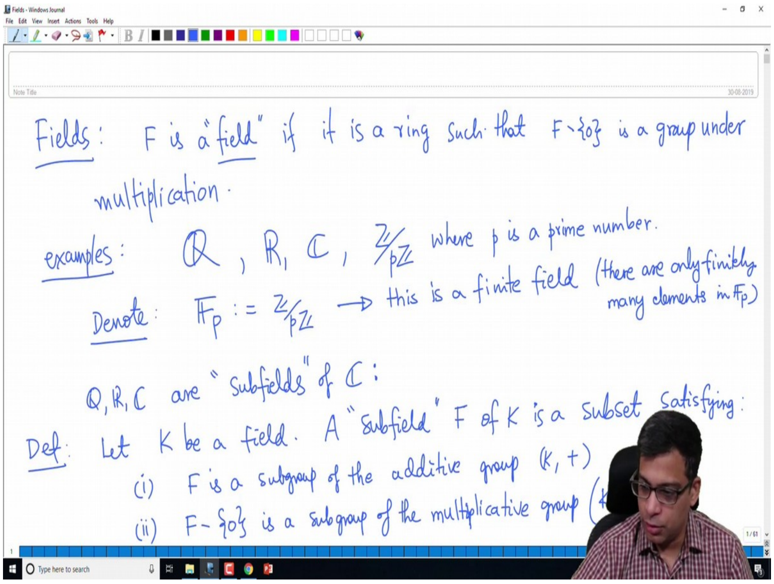
Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 33
Field extensions 1

We have so far covered ring theory in this course. Now in the remaining part of the course I will study fields.

(Refer Slide Time: 00:26)

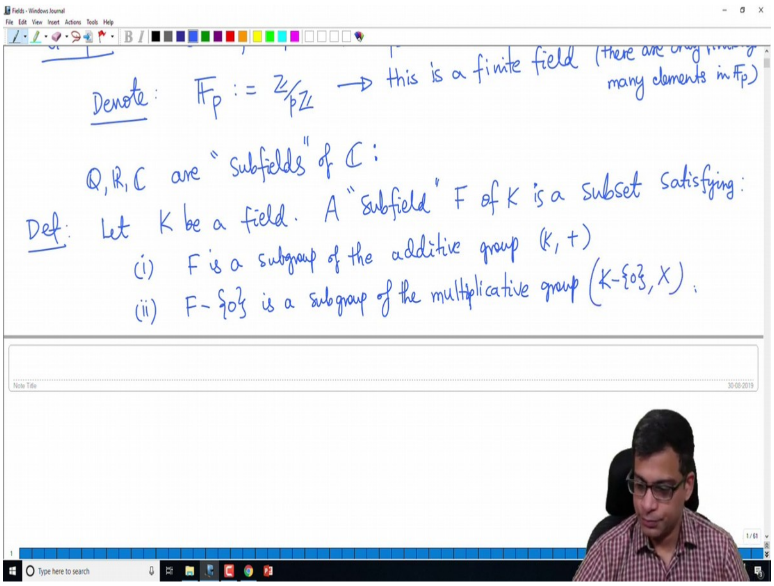


So, we already know what fields are. So let me remind you what fields are. Fields are special kinds of rings right. So, F is a field, if it is a ring in which or such that F minus 0; 0 is the additive identity element as always; F minus 0 is a group under multiplication. So, in the remaining course we are going to study rings which have this property. So, though these are just special cases of rings their study has a very different flavor from the study of rings, as we learn in these remaining the videos of the course.

So, let me first give you a collection of examples that we will be dealing with often before we continue and study more properties of fields. So, I am first part of this video I am going to study examples, the examples that we are already familiar with Q R C. we are also familiar with Z mod p Z where p is a prime number. Right in the beginning of the course I when I defined quotient rings and we discussed Z mod n, right we proved that Z mod n Z is a field if and only if n is a prime number. So, in the rest of the course we are going to use p to denote prime number. In this field we denote usually by F p, F written with this special symbol F p is Z mod p Z.

So, this is different from the remaining examples that I wrote here in the sense that this is a finite field. This is a finite field right finite here simply refers to the fact that there are only finitely many elements. So, that is all so the there are only finitely many elements in F p. We call it a finite field because of that, Q R and C the field of rational numbers the field of real numbers a field of complex numbers are not finite fields because certainly they have infinitely many elements.

(Refer Slide Time: 03:24)



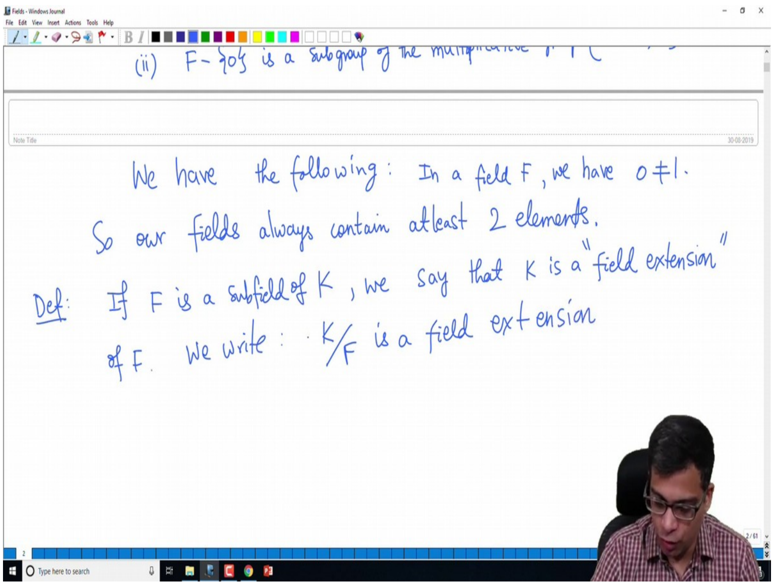
So, there are two classes of examples here I am discussing right. So, Q R C are subfields of C. So, unlike in the case of rings where we have subrings, but they did not feature prominently in our study of rings. There we looked at ideals, homomorphisms of rings, quotient rings, these were the important operations and objects in the study of rings, whereas in the study of fields we are often going to study subfields of a field.

So rather we are going to study pairs of fields where one contains the other. So, let me quickly tell you what a sub field is, this is something that you can guess. Just like a sub ring of a ring we say that a ring sub ring of a ring is a subset which is under addition it is an abelian sub group and it is closed under multiplication right.

So, it is basically the sub object in the category of rings. Here sub field is exactly the same so, a sub so, let define subfields more generally. Let K be a field the typical letters that I will use to denote fields are going to be K capital K capital F capital L and so on. So, this is the definition, let K be a field a subfield so, maybe I should write this separately this is a very important definition for us. So, definition, let K be a field. A subfield F of K is a subset of such that which is a so let me write satisfying the obvious properties right. 1 F is a subgroup of the additive group right.

So, F is a field in particular it is a ring so, it has two operations, we call them plus and times. So, it is a subgroup of the additive group K plus I should write, so, if you forget the multiplication on K and only consider the addition it is an abelian group F must be a subgroup of it F minus zero. So, because F is a subgroup of the additive group F contains 0, and if you remove it must be a subgroup of the multiplicative group K minus 0 cross ok. So, simple so, it is a subgroup in both senses it is an additive subgroup as it is and after removing 0 it is a multiplicative subgroup ok. So, now let me let me make some convention here.

(Refer Slide Time: 06:59)



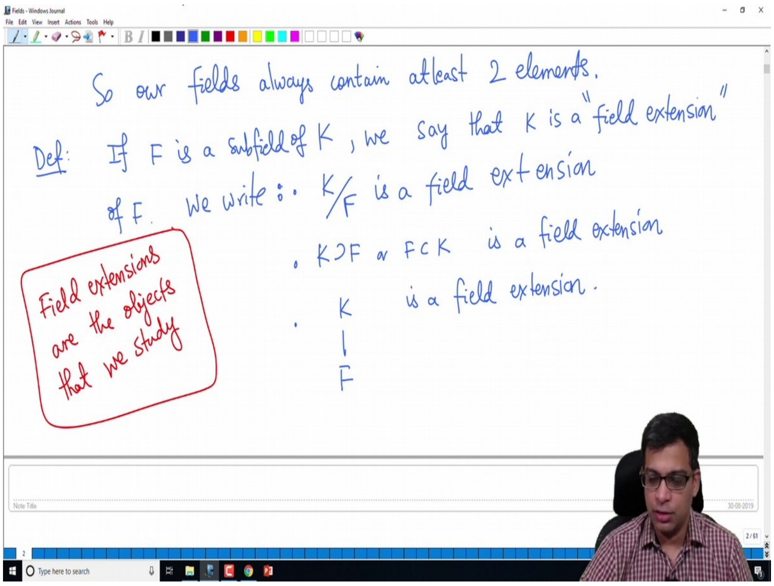
So, convention is or rather we always assume. So, remember a field is a ring and in this course our rings are commutative with one so, rings contain one and they multiplication there is always commutative. So, they these assumptions carry over to fields because our fields are also special classes of rings. Now in the in a ring it is conceivable that 0 which is the additive identity is equal to 1 which is the multiplicative identity. So, in other words you can have 0 equal to 1 in which case this ring is the 0 ring we will not consider that as a field. So, in a field F we have 0 is not equal to 1.

So, the additive identity is not same as the multiplicative identity. So, our fields always contain at least 2 elements right. So, this is an important statement you cannot have a field with only 1 element, because in that field 0 must be equal to one which we are eliminating. The point is when you remove 0 this follows the actually I should say we will always assume this. In fact, we will have this because it is of a ring such that F minus 0 is a group under multiplication. A group is supposed to be non empty so, if you remove 0 if it has to be a group it has to be non empty so, it must have identity.

So. In fact, it is not just it is not just that we have the following. So, I will write like we have the following right. So, that is not an assumption it is a consequence of our definition ok. So, now the most important terminology that we will use in the rest of the course when we study fields is, if F is a subfield of K, we say that K is a field extension of F. And we write we write this as K F is a field extension. So, various notations we will follow field we write K over F do not confuse this with the construction of a quotient ring this is not that.

So, it is somewhat confusing so, and I will generally try to avoid this notation, but you might see this sometimes K over F when we are talking about fields is just a notation it is just a short for K is a field excitation of F.

(Refer Slide Time: 10:05)



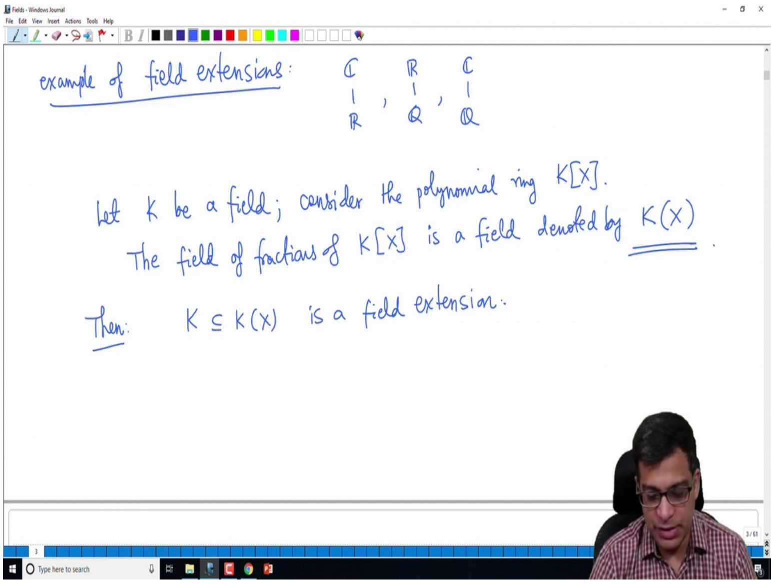
We will of course, write F K contains F or F contain F is contained in K is a field exten-sion. So, these are various notations that I will use, so, this 1 this 1 and another more pic-torial description is this, K and we put a vertical bar and we will put F is a field extension ok. So, as I said the study of fields has a very different flavor to the study of rings.

Where when we studied rings we looked at ideals in a ring, we looked at quotient rings, when we quotient on ideal, we looked at morphisms homomorphisms of rings and vari-ous other issues. Other constructions and objects and subrings were not that important right, if you go back and see the ring theory part of the course, we really did not talk much about sub rings though we learned what a sub ring is and we saw examples it was not a prominent aspect of ring theory.

Whereas, the entire field theory that we are going to study is really a study of field exten-sions. So, these are the important objects for us. Field extensions are the objects that we study. So, what I am trying to say is that we studied ring a ring on its own in some sense. Whereas, we do not study a field on its own, but we study its subfields or how a field sits inside in another sits inside another field and so on.

So, our objects are not just fields, but field extensions so; that means the pairs of fields. F is a subfield of K and we will say that as K is a extension field of F ok. So, now what I said earlier was that Q R and C R are subfields of C of course, they are.

(Refer Slide Time: 12:09)



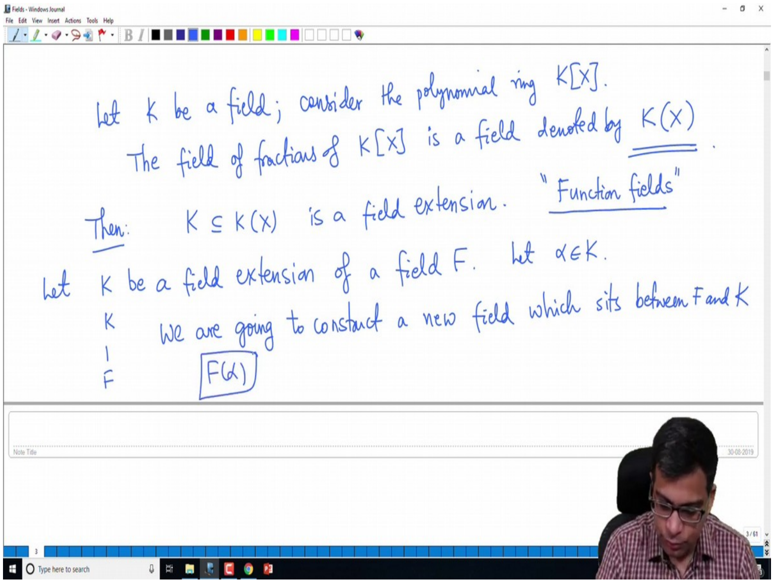
So, examples of field extensions: So, of course, we have C over R, R over C, we have C over sorry, R over Q we have C over Q. And we have not it is learned of any field extension of Z mod p Z right. So, there are field extensions of Z mod p Z and that is going to be discussed when we study finite fields explicitly we are going to study finite fields in a few videos. So, there we will study field extensions of Z mod p Z, but for now let us look at some other cases.

So, for example, you can have Q. So, I can introduce one obvious extension field of Z mod p Z in the following way. So, let K be a field consider the polynomial ring K x, the quotient field are the field of fractions in the language I used in the earlier part of the course. The field of fractions of K X is denoted by K round bracket X ok.

So, K square bracket X is the polynomial ring, K round bracket is X is its quotient field. So, this is called a function field, so, then of course, this is a field extension right so, this applies for any field case so, in particular we can consider Z mod p Z and include it in Z mod p Z bracket X. What is the typical element in K round bracket X it will be of the form F by g where F and g are polynomials in K square bracket X. So, this is always a field extension though if you start with Z mod p Z and you construct this new field it is no longer going to be finite field. It will have infinitely many elements because remember polynomial ring is already infinite ring.

So, when you take the field of fractions it is going to also be infinite. So, we will study later field extensions of Z mod p Z which are also finite fields, but this is an extension that we can construct for every field.

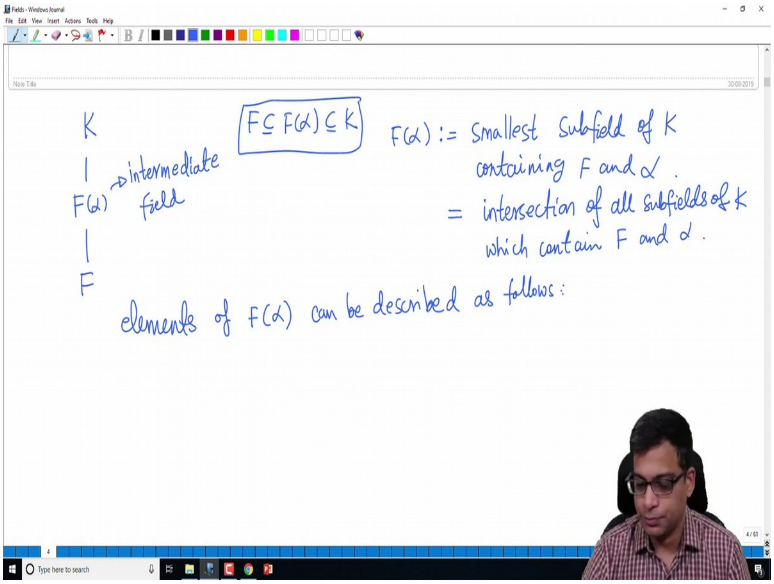
(Refer Slide Time: 15:00)



And this we are not going to study that much these are all examples of what are called function fields. The terminology comes from, algebraic geometry and analysis where these elements of this can be thought of as functions, because a polynomial is a function a ratio of 2 polynomials also is a function. But that is not going to be studied by us in detail. So, now another construction I want to give is. So, let us now start with an arbitrary field extension. Let K be a field extension of a field F, as I said my main object of study in this course in the field theory part is field extensions.

So, K is an arbitrary field extension of another field F. Typically I use F for the smaller field K for the bigger field. Now let us pick an element of K let us call alpha let alpha be an element of K. So, we are going to so, we have K and F here we are going to construct, construct or consider a new field which sits between F and K, and we are going to call this F alpha and what is this.

(Refer Slide Time: 16:29)

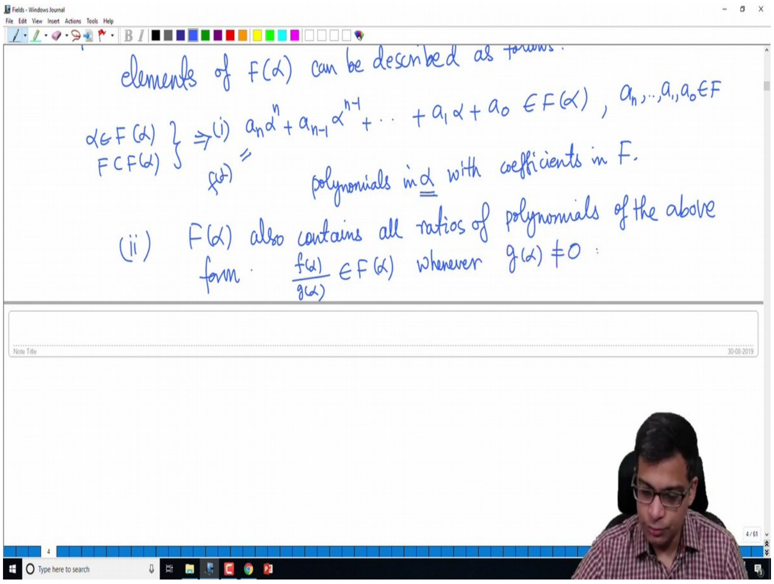


So, the picture will be K F alpha F. So, this is what we call an intermediate field. So, in particular when I write this or I what I mean is F is a subfield of F alpha and F alpha is a subfield of k. So, this data is represented like this. And what is F alpha F alpha is simply this smallest subfield of K containing F and alpha right.

So, this is a field that is supposed to contain F and also alpha and we look at the smallest such field. In fact, it is equal to the intersection of all fields that contain all subfields of K. I should say I should remain within K here I am only doing this between K and F.

So, intersection of all subfields of K which contain F and alpha, one can check that that intersection is actually a field, because if 2 elements are in that intersection those 2 elements are in every field; that means, the sum and the product is in every field the inverses are in every field. So, it there will be in the intersection yet another description of F alpha elements of F alpha can be described as: So, as follows let me write me like that and I will describe it now. So, let us construct such a field what are we supposed to make sure, we are supposed to make sure that capital F is contained in this and alpha is contained in this.

(Refer Slide Time: 18:44)

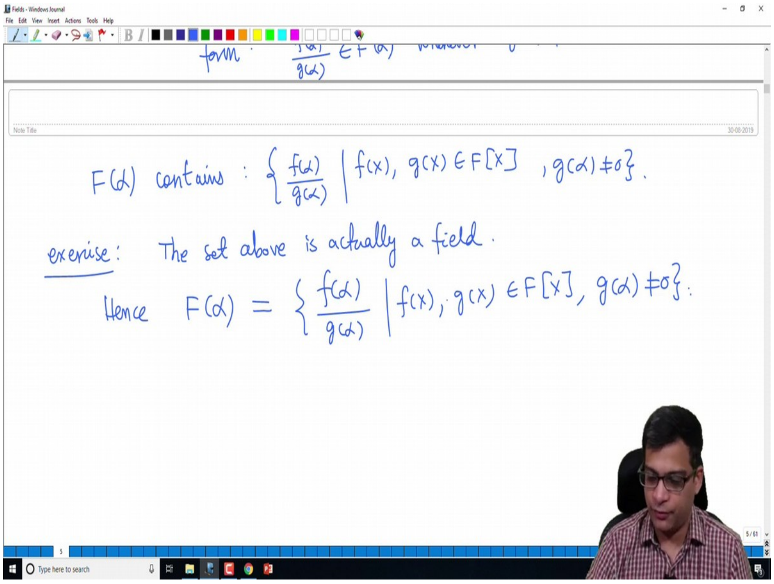


So, if alpha is in F alpha and F is in F alpha; that means, all expressions of the form a n alpha n a n minus 1 alpha n minus 1 a 1 a alpha plus a 0 are in F alpha with whenever a i or all of these coefficients a n a one a 0 or an F. This is clear right because if alpha is there F alpha is a field so, this alpha power n is there alpha power n minus 1 is there alpha is there are and F is inside it.

So, a n a n minus 1 a 1 a 0 are all there. So, they all linear combinations are like this are going to be there, this will happen as soon as it is a ring I am not looking at the smallest ring containing F and alpha so, I also must have ratios of this, so, not. So, these are polynomials, if you recall polynomials that we studied in ring theory these are polynomials in alpha with coefficients in F right. Exactly that is what this is these are polynomials in the element alpha with coefficient in f, but this is only one consequence of F alpha being a field. F alpha also contains all ratios of the of polynomials of the above form, why is that remember

Now, we are in the realm of fields it is any element that is non zero is going to contain its inverse also. So, F alpha is a field as soon as you have such a polynomial which is non zero one over that which is the multiplicative inverse is there; that means, we have to take all ratios of polynomials of course, denominator has to be non zero that goes without saying right. We take ratios of f by g small f by small g so, f alpha by g alpha so let us call this f alpha small f alpha; that means, you are thinking of a polynomial in a variable capital X a n X n a n minus 1 X n minus 1 and so on. Then you are plugging in alpha for X similarly you take g alpha whenever g alpha is non zero.

(Refer Slide Time: 21:33)

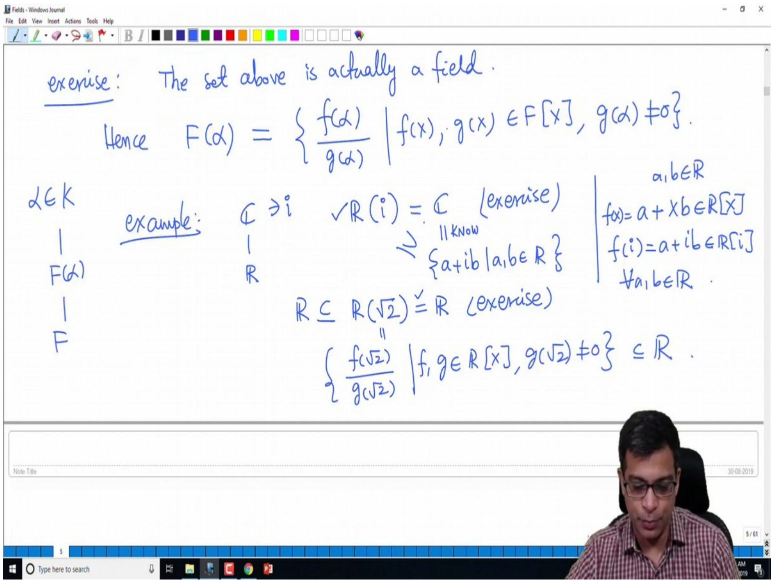


So, that is what we are saying is that F alpha contains this set F alpha g alpha where F X g X are polynomials in one variable over the field F and g alpha is non 0. This is forced for us because F alpha is supposed to contain capital F and alpha and it is supposed to be a field. So, it must contain all such ratios now the point is as an exercise: this. The set about is actually a field.

So, you take such ratios F alpha for a g alpha where F and g are polynomial polynomials in one variable over capital F and of course, g alpha is non zero then it is in fact, a field because 0 is there you can take the 0 polynomial for F and constant polynomial for 1 for g then you get 0 you can take F and g to be both 1 you get 1. If you take two such things you add them it is another polynomial ratio of another set of polynomials multiply them that is also rational polynomial.

So, it is very easy to check that it is. In fact, a field hence F alpha is equal to this right. It is supposed to be the smallest field that contains both F and alpha and we have described now the concrete description of elements of capital F alpha. So, this is a very important construction for us.

(Refer Slide Time: 23:17)



Every time you have a field extension and an element in the bigger field we have an intermediate field containing both F and alpha and in general it is smaller than K of course, in some examples it would be equal to K or equal to F even. So, what are the examples of this?

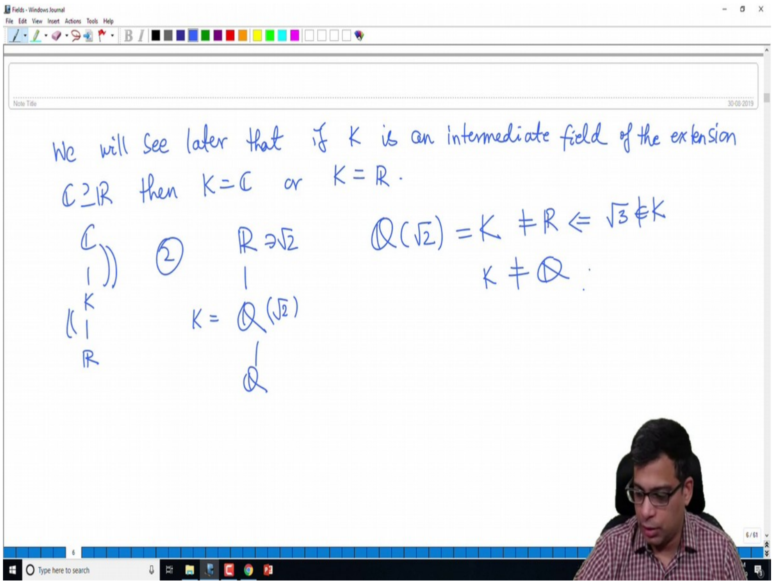
So, the for example, if you take C over R and you take i here the imaginary square root of minus one. What is R bracket i this in fact, I claim is C and I leave that as an exercise for you, because what is R bracket i in the description that we gave it is going to contain f i by g i, but every complex number is of the form a plus I b where a and b are real numbers right. So, C is already a plus I b this we know where a b are in R, but R I will certainly contain them because R i is you take all polynomials with rational coefficients in particular you can take the polynomial a plus X b right.

So, this is an R X because a b are in R, if you take this to be f x what is f i this is a plus i b. So, just taking the polynomials not even we do not even need to take ratios. This will be R i right so, for all a b in R. So, a plus i b is already in R I, but a plus i b is equal to c so, R I is equal to C, on the other hand what is R bracket square root 2.

R bracket square root 2 i claim is R and this is an exercise for you. R bracket square root is R because what is this these are ratios of polynomials by the description I gave there, these are ratios of polynomials in one variable such that g root 2 is non zero right, but remember if F is a real polynomial and you plug in root 2 you get nothing more than you get actually real numbers only.

So, this set is in R, but R obviously is contained in R root 2 by definition. So, R is contained in our root 2 R root 2 is contained in R so, this is the equality. So, I more or less finished completely solved these exercises, but this is these are simple examples and in fact, we will see later.

(Refer Slide Time: 26:11)

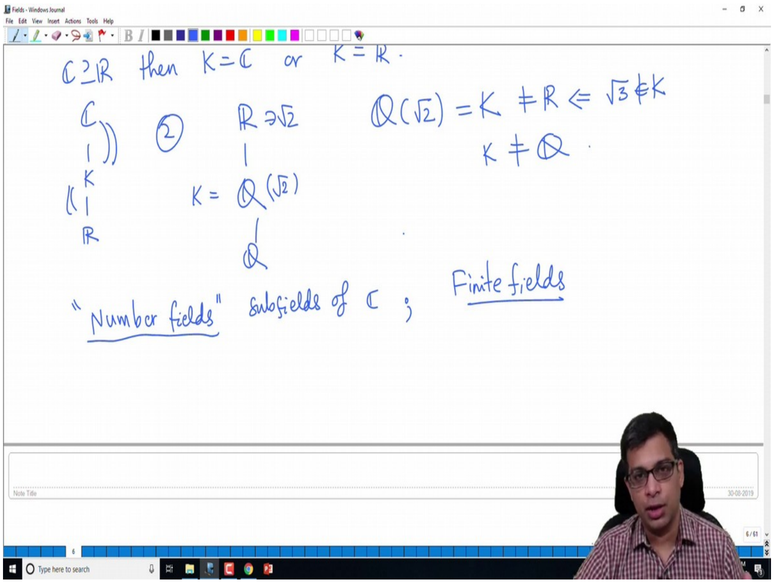


Then if K is an intermediate field of the extension C containing R then we must have that K is either C or K is an R. So, what I am saying is that if you have a field extension if you have the field extension C over R and K is in between either these are equal or these are equal ok. So, there is no field that is properly between C and R. So, some more examples let me do.

So, second example. So, you take R and Q you take R and Q, now you can take root two here which is not here and you can consider Q root that is K. So, Q root 2 will be an intermediate field and what we can do is we can describe the elements of Q root 2 as we have done before, but we will have a more convenient description more simple description later, but this is actually not equal to R that is all I will say for now and K is certainly not equal to Q. So, this is a proper intermediate field, and both of these statements are clear because root 2 is contained in K right root 2 is contained in K by definition, but root 2 is not in Q.

So, Q is strictly bigger than Q, K is strictly beginner Q I should say. Similarly R contains many real numbers which are not going to be expressed in terms of Q root 2 because Q root 2 is only things like this F root 2 by g root 2, where F and g are really rational polynomials for example, one can check quickly that root 3 is not in K. And similarly so, this implies this because root 3 is not in k, but it is in R ok. So, these are important subfields of C. So, the two classes of fields that we are going to study in detail in this field theory course is subfields of C; they are called number fields.

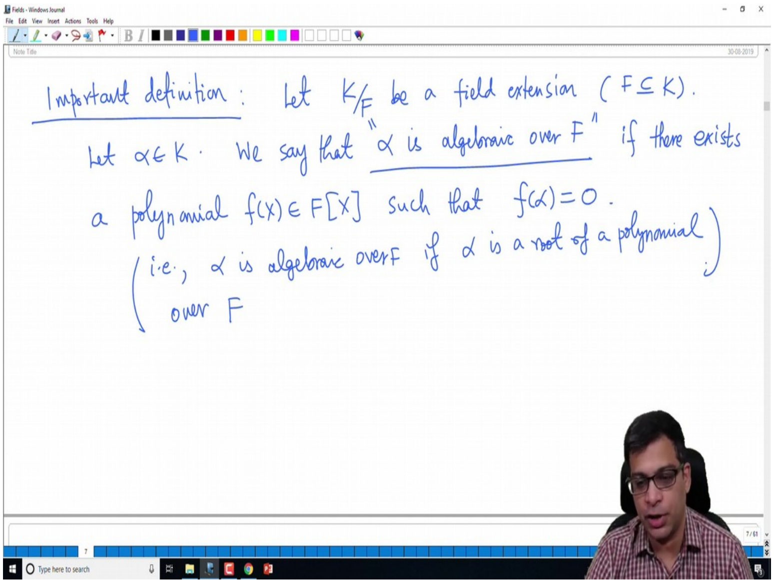
(Refer Slide Time: 28:36)



So, these are called subfield these are subfields of C. They are number fields because complex numbers. So, number refers to complex numbers these are fields containing numbers complex numbers and we are going to study finite fields. So, the two important classes of the fields that we are of fields that we are going to study are number fields and finite fields. Initially we will do some general study of properties of fields. Then we will look more closely at number fields and finite fields there are lots of other kinds of fields, but we will refer to them sometimes in examples, but our primary focus is going to be on number fields and finite fields ok.

So, let me now introduce a very important notion and then stop the video and we will continue with that notion next time. So, this is an important definition for us.

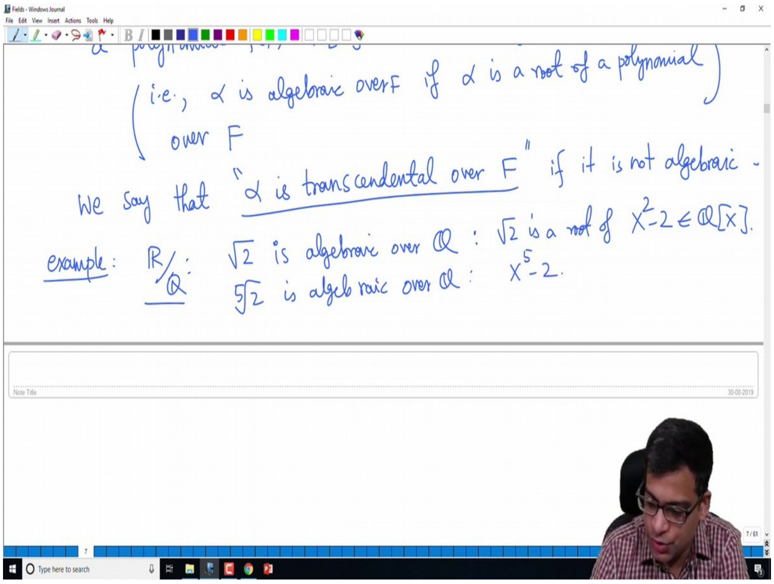
(Refer Slide Time: 29:40)



So, let K over F be a field extension so, this is the shortest way of writing and I want you to get used to this. Again let me remind you that we are not talking about quotients at all this is not the ring, quotients of rings that we learned earlier. This is just another short way of saying that F and K are fields and F is a subfield of K. So, let F K or F be a field extension and let us choose an element alpha in K. We say that alpha is algebraic over F, we say that alpha is algebraic over F if there exists a polynomial in one variable over capital F.

So, remember capital F X capital F square bracket X is a notation that we have been using in this course it stands for the polynomial ring in one variable X over capital F. So, there exists a polynomial small f X in capital F X such that, f alpha is 0 ok. So, algebraic if alpha is a root of a polynomial that is; alpha is algebraic over F, if alpha is a root of a polynomial, over F that is a convenient way of remembering this. And I want to stress again which I will do again and again that over capital F is an extremely important part of the terminology. Alpha is algebraic over capital F because the same element may be algebraic over some field and it may not be algebraic over another field ok.

(Refer Slide Time: 31:49)

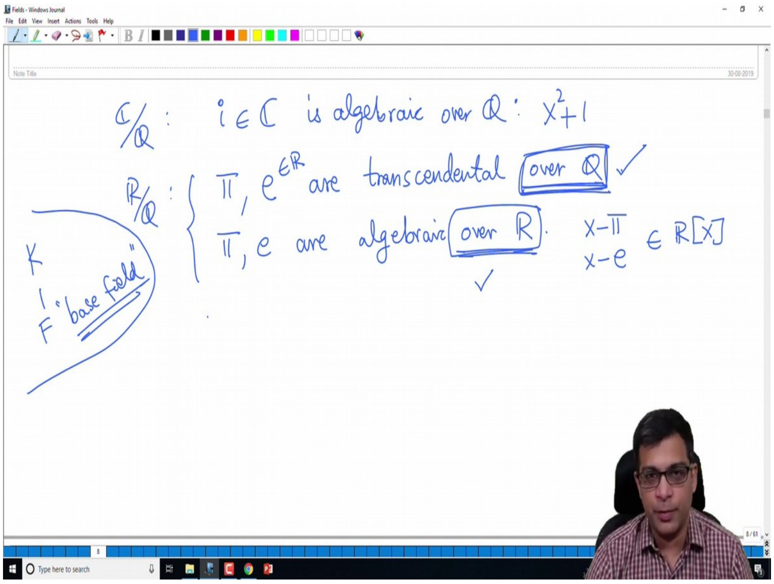


So, and continuing the definition: we say that alpha is transcendental over again F over is again over F is an important part of the transcendental, over capital F. If it is not algebraic that is all so, if there is no polynomial over capital F that alpha satisfies or in other words there is no polynomial or capital F for which alpha is a root we say alpha is transcendental over it ok.

So, now let me give a quick set of examples then we will stop. So, let us take the extension R over Q cut for this example, we say first that root 2 we see that root 2 is algebraic over Q: why is this because root 2 is a root of X squared minus 2 which is in Q X ok.

So, root 2 is a root of the polynomial X squared minus 2. Similarly root 5, 5th root of 2 is algebraic over F algebraic over Q, that is because we can consider the polynomial X power 5 minus 2 right.

(Refer Slide Time: 33:27)



Similarly, we can consider i. So, i of course, is not in R. So, if you consider the polynomial the field extension Q C over Q i in C is algebraic over Q. Remember all this study needs to fix a field extension a priori you fix a field extension you consider an element in the bigger field. And you look at polynomials over the lower field and look at any polynomial which may have the element as a root here it is of course, algebra because it is the root of this polynomial going back to R over Q you all know.

The elements pi and e that are defined using some geometric or analytic constructions these are not algebraic over Q. So, this is some this can be done it is it requires a proof these are consequence of some theorems. They are transcendental over Q. So, there is no polynomial for which have pi or e as roots and various other elements we one can write on the other hand pi and e are algebraic. So, they are in R right R algebraic over R right. So, this is where I am emphasizing the part about algebraic or transcendental or properties over a field. They are not intrinsic properties of an element their properties of an element with respect to a field while there is no polynomial over Q.

Which satisfies which has pi or e as roots there are polynomials over R for example, you can take X minus p pi and you can take X minus e. Which are both polynomials over R and of course, they have roots pi and e. When you substitute pi in the first polynomial you get 0, when you substitute e in the second polynomial you get 0. So, they are algebraic over R they are transcendent over Q. So, this is a good illustration of why it is very important to emphasize the base field. So, whenever you have a field extension the terminology is F is called the base field. So, in all these considerations base field is very important ok.

So, let me stop the video, here in this video we discussed the notion of subfields, field extensions and we talked about the sub if you have a field extension and an element in the bigger field. We considered the construction of an intermediate field which is the smallest field containing the base field and that element and we explicitly described.

What the elements of that intermediate field are; F alpha and we saw some examples and we are ending with an important definition of the notion of algebraic and transcendental elements, and let me emphasize again there is everything depends on the base field because whether an element is algebraic or not depends on the base field: pi is algebraic over R, but it is not algebraic over Q it is transcendental over Q. So, you have to keep stressing base field always.

So, let me stop the video here and we will continue in the next video with further study of algebraic extensions.

Thank you.