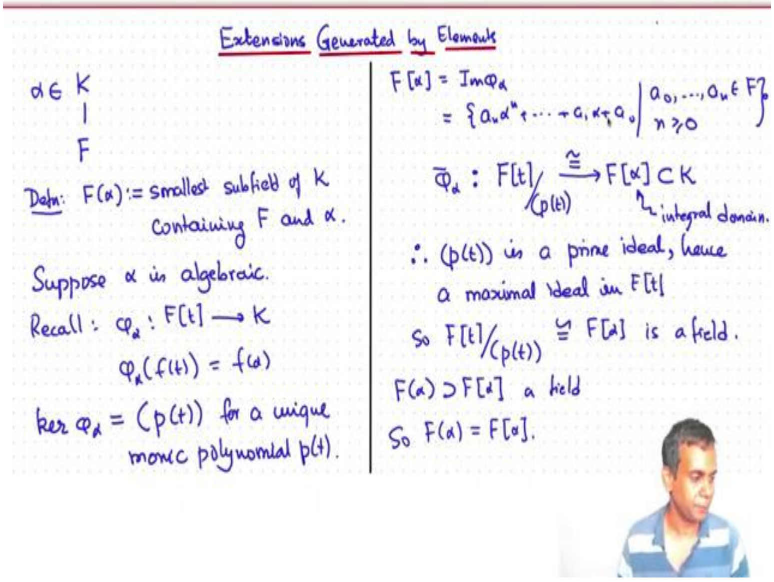
Algebra – II
Professor Amritanshu Prasad
Mathematics
The Institute of Mathematical Sciences
Lecture 2
Extensions Generated by Elements

(Refer Slide Time: 00:14)



Consider a field extension K over F and an element alpha of K, then we define F alpha to be the smallest subfield of K containing both F and alpha. Our objective is to understand this field. So, we concentrate on the case where alpha is algebraic. And we will use the substitution map, recall, we have this map phi subscript alpha from F t to K, the substitution map was defined by phi alpha of F t is just F of alpha. This is a ring homomorphism from F t to K. And now look at the kernel of phi alpha, kernel of phi alpha is an ideal in F t, F t is a Euclidean domain and therefore, a principle ideal domain. And so, the kernel of phi alpha is generated by a single polynomial.

Moreover, if we assume that this polynomial is monic, then it is going to be a uniquely determined polynomial. So, this is equal to the ideal generated by p t, for some, for a unique monic polynomial p t and let us make another definition, let us define F square brackets alpha just to be the image of phi alpha. Explicitly, the set is the set of all a n alpha to the n plus a1 alpha plus a0, where a0 up to a n up to just elements of F and n is some non-negative integer because after all, it is just the image, it is the values all possible values taken by polynomials evaluated at alpha.

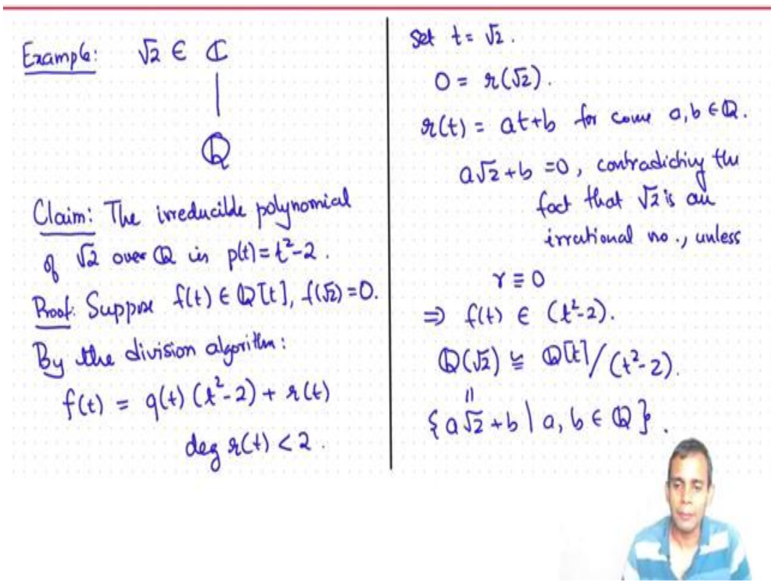
Now, we have this homomorphism from F t, phi alpha, and it goes from F t to K, but the image we have defined to be this subring F alpha of k. And the kernel is this prime ideal p t.

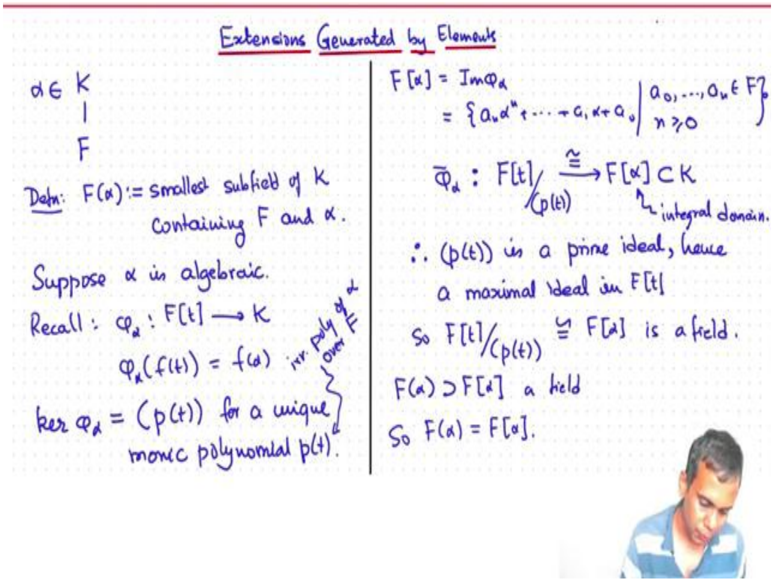
So, phi alpha induces an isomorphism, which we will call phi alpha bar from F t mod p t to F alpha, this is an isomorphism of rings. Now, F alpha is a sub ring of K and therefore, F alpha is an integral domain being a subring of an integral domain. Now, remember that if you have a commutative ring, and you go module in ideal and the quotient is an integral domain, then that ideal must be a prime ideal.

Now in F t, the prime ideals are generated by irreducible polynomials and in any principle ideal domain, in fact, the ideals generated by irreducible elements are actually maximal ideals. And so, that means, well the quotient of ring by a prime ideal is an integral domain whereas the quotient of ring by a maximal ideal is a field. So, we can conclude that F t mod p t which is isomorphic to F alpha is a field. Now, F round bracket alpha must contain F alpha because after all F square bracket alpha consists of elements of this form here a n alpha to the n plus dot dot dot a1 alpha plus a0.

Now a0, a1, all these are elements of F, and alpha is also an element of F round bracket alpha. So, everything in here, this expression here is a sum of products of elements of F round bracket alpha. And therefore, this must be contained in F round bracket alpha. So, what we see is that F alpha is contained in F round bracket alpha, but F alpha itself is a field. So, F alpha is a field that contains both F and alpha. So, therefore, F alpha is equal to F round bracket alpha. So, the field generated by alpha is the same as the values of all the polynomials evaluated at alpha. Let us look at an example.

(Refer Slide Time: 06:12)





Let us take for our field extension, the complex numbers over the rational numbers, and let us take alpha equals root 2. So, firstly, I claim that this polynomial here is called the irreducible polynomial of p t. So, this polynomial here is called the irreducible polynomial of Alpha over F. So, the irreducible polynomial, what is the irreducible polynomial of root 2 over Q?

Well, you can guess it is actually the polynomial t squared minus 2. Let us call this p t, how do I prove it? So, I need to show that if any polynomial vanishes at square root of 2, any polynomial with rational coefficients, then it is in fact, in the ideal generated by t squared minus 2. So, now, suppose f t belongs to Q t and f of square root 2 is 0. Now, apply the division algorithm in the polynomial ring Q t, Euclid's division algorithm, we have that f t is Q t times t squared minus 2 plus r t, where r t is some polynomial of degree less than 2 the degree of t squared minus 2.

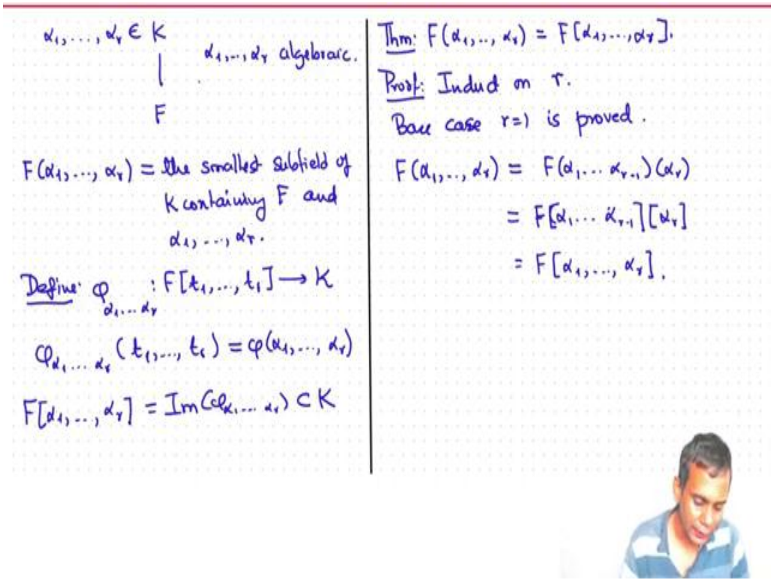
And now let us substitute square root 2 and what you get is 0, we assume that F of square root 2 is 0 is, now this t squared minus 2 also vanishes at t equals 0. And so, this is r of root 2. So, r is a polynomial of degree less than 2, which means that r is a t plus b for some a b in Q. And what we have is r of root 2 is 0 that means a root 2 plus b is 0, but this contradicts the fact that root 2 is an irrational number. Therefore, r has to be 0. Unless, of course, r is identically 0, that is a is 0 and b is 0. So, then this implies that f t is in the ideal generated by t squared minus 2.

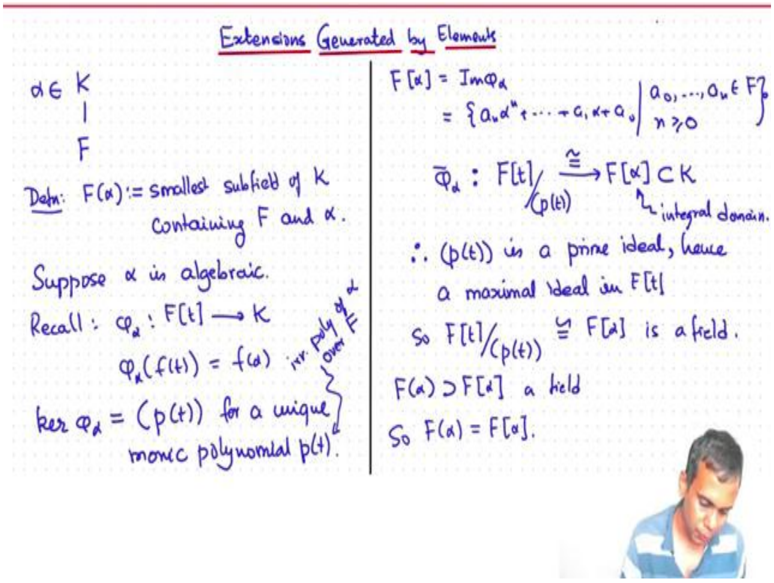
So, what we have is that Q root 2, the field generated by root 2 over the rational numbers, is isomorphic to Q t mod t squared minus 2. And we also know that as a subset of the complex numbers, this can be written as. Well, this is the same as Q square brackets root 2 which can be written as a root 2 plus b, where a, b are rational numbers. This is because you see it is Q square brackets root 2. But that is the set of all elements of this form.

But if you take even powers of square root 2, they will just give you integers. And so, every polynomial with rational coefficients when you evaluate it at root 2, it will give you something of form a root 2 plus b. Of course, anything of the form a root 2 plus b is a linear polynomial. So, it is an F alpha.

So here is a description of Q root 2, you can think about it two ways, one as a subset of complex numbers, it is all elements of the form a root 2 plus b, where a and b are rational, and the other is as a quotient of the polynomial ring, it is Q t mod r t squared minus 2.

(Refer Slide Time: 11:44)





Now let us consider a slightly more general situation. So as before, we have a field extension K over F but instead of one element, let us say we have r elements in K, then we can define in a similar manner, F round bracket, alpha 1, alpha r, to be the smallest subfield of K containing F and containing the elements, alpha 1, alpha 2 to alpha r. Now you can again define a substitution map, but from a multivariate polynomial ring.

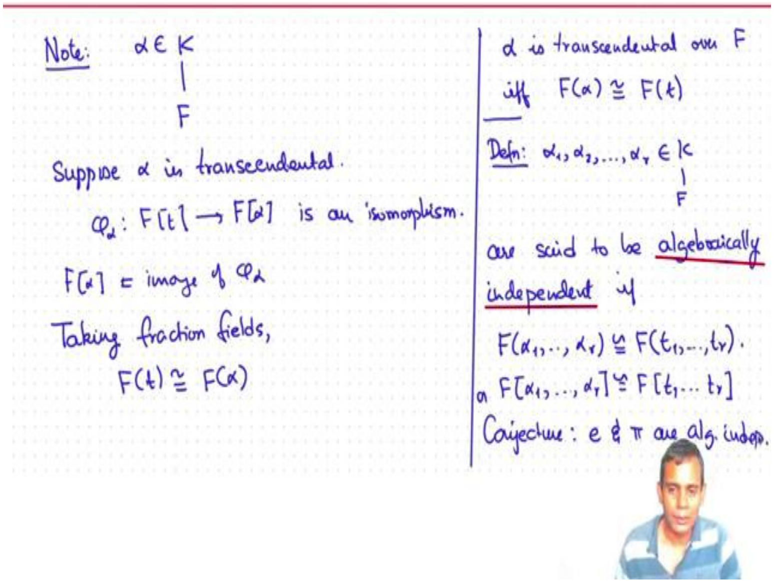
So define a substitution map, we will call it phi subscript alpha 1, alpha r, it is going to be a ring homomorphism from F with polynomial ring with r variables into K. And what it is going to do is phi alpha 1 alpha r, as you can guess, evaluated at t1 to tr, will just be the value of phi at alpha 1, alpha r. So, you substitute for ti, the value alpha i.

Now, I claim that in this case, also, the field is just given by the values of polynomials F, alpha 1, alpha r is equal to so let us just define this. We will define F square brackets, alpha 1 alpha r as the image phi alpha 1, alpha r, which is a subring of K. So, this is equal to F alpha 1, alpha r. The proof of this just goes by oops, alpha r. The proof of this goes by induction on r. So, the base case r equals 1, we have already proved over here.

So now, let us look at F alpha 1 alpha r. So there is a very simple trick to this, it is just to realize that this is to change this whole situation as F alpha 1, alpha r minus 1, alpha r, that this is just the smallest subfield of K containing this field F alpha 1 alpha r minus 1 and alpha r that turns out to be the same as the smallest subfield of K containing all the elements of alpha 1 up to alpha r.

But induction hypothesis this here is F alpha 1 alpha r minus 1. And of course, applying the base case, this is the same as polynomials in alpha r. So, this is a field and this whole thing is in fact a field, but this is the same as F alpha 1 up to alpha r. So, we also have the multivariate case, where the field generated by r elements is given by the values of polynomials. Of course, here we need to assume that all these elements are algebraic, otherwise, this does not work, because at each stage again, we are using the fact that alpha is algebraic, what happens when alpha is not algebraic?

(Refer Slide Time: 16:06)



So, let us just look at that case. Suppose, we have alpha in K over F. And suppose alpha is transcendental then we know by definition of transcendence that phi alpha from F t to K is injective. And in fact, the image suppose we define the image to again be phi alpha, then this is an isomorphism. And so, taking fraction fields F t is actually isomorphic to F alpha. So, this suggests an alternate definition of transcendence, which is that alpha is transcendental over F, if and only if F alpha is isomorphic to F t. The smallest field in K containing F and alpha is isomorphic to the field of rational functions with coefficients in F.

So, we can use this definition to sort of directly jump to the multivariate case and I will give you a definition here for the generalization of transcendence for n different elements, alpha 1, alpha 2, alpha r in K over F are said to be algebraically independent, if the smallest field containing alpha 1 alpha r is isomorphic to the field of rational functions in r variables, which is equivalent to saying that the polynomials in alpha 1 up to alpha r are isomorphic to polynomials in t1.

They are saying that they no algebraic relations between the elements alpha 1 alpha 2 and alpha r over F. So, it is again this algebraic it just as with transcendence, algebraic independence is a difficult problem. It is conjecture but not proved that e and pi are algebraically independent. But it is something that is not known, it is a big open problem.