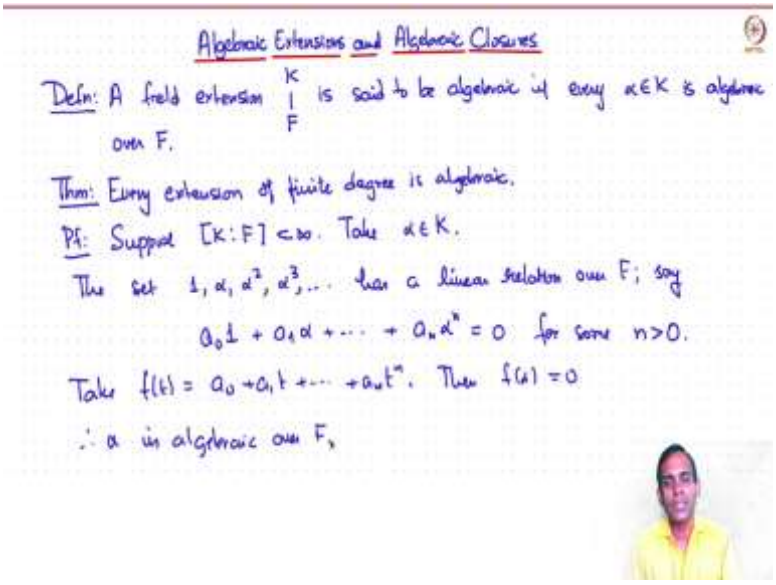
Algebra II
Professor – Amritanshu Prasad
The Institute of Mathematical Sciences
Algebraic Extensions and Algebraic Closures

(Refer Slide Time: 00: 14)



Today, we will talk about Algebraic Extensions and Algebraic Closures. Let us start with the definition of an algebraic extension. The field extension K over F is said to be algebraic, if every element is algebraic over F. So, a good example of an algebraic extension is a finite field extension. This is an easy theorem; every extension of finite degree, extension of finite degree is algebraic.

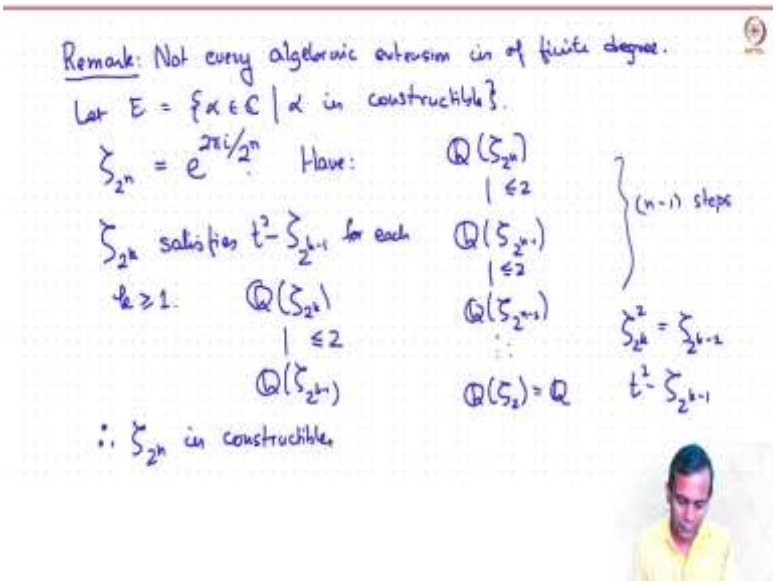
If you have been paying attention to the earlier lectures, you would find this quite easy to prove, the proof is as follows. So, suppose that you know K over F is an algebraic extension. So, K F is a finite, K is an extension of F at K over F. The degree of K over F is finite. Now, consider the infinite set, 1 and take alpha belonging to K.

We need to show that alpha satisfies a polynomial equation with coefficients in K, sorry in F. So, the set 1, alpha, alpha squared, alpha cubed and so on, this set is going to be, well it cannot be linearly independent. And therefore, there must be some linear relation between these elements, because K over F is a finite dimensional vector space over F, so has a linear relation over F.

Say, the first n of these would have a linear relation, because every linear relation has to be finite. So, a0 times 1 plus a1 times alpha plus an times alpha raised to n equals 0, for some

positive n. Now, this if we take the polynomial ft to be a0 plus a1t plus ant to the n. Then this linear relation is just saying that alpha is the root of the polynomial F. And therefore, alpha is algebraic over F. So, every extension of finite degree is algebraic.

(Refer Slide Time: 03: 43)



However, the converse is not true. Not every algebraic extension is of finite degree. Consider for example, E to be the set of all complex numbers, such that alpha is constructible, i.e., it can be constructed in a finite number of steps using a straightedge and a compass, as explained earlier. Then, we have elements zeta to the power 2 to the power n.

So, this is the 2 to the power nth primitive root of unity which I can take to just be the complex number E to the 2 pi i divided by 2 to the power n. Then we have, we have a tower of extensions, Q zeta to the power 2n. This contains Q zeta power 2n minus 1. Because this zeta power 2 to the n minus 1 is just the square of zeta power 2n. So, this element is contained in the field above.

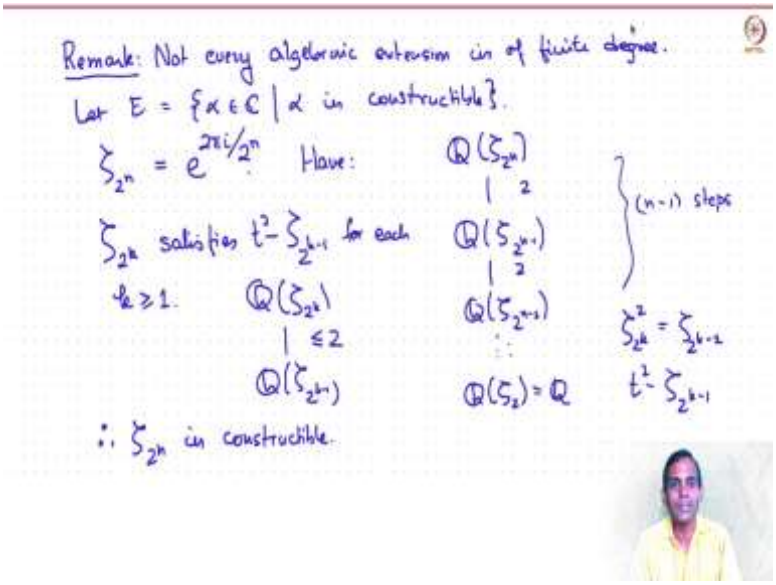
And therefore, this is a sub field of Q zeta power2n. And Q zeta power 2n minus 2, all the way down to, Q zeta 2 is just Q, because zeta 2 is just minus 1, and so Q zeta 2 is Q. And now, how many steps do we have in this? We have exactly n minus 1 steps here. And note that zeta to the power 2n whole squared is zeta to the power, maybe I should not say n here, let us say zeta to the power 2k whole squared is zeta power 2k minus 1.

If you take this element and square it, then you will get two times this, which is 2 pi i divided by 2 to the power n minus 1. And so, this element satisfies the polynomial t squared minus

zeta 2 to the k minus 2. So, what we are saying is that zeta 2 to the power k satisfies t squared minus zeta 2 to the power k minus 2, sorry k minus 1 for each k.

What that means is that, what that means is that this extension zeta 2 to the power k over Q zeta 2 to the power k minus 1, it has degree less than or equal to 2. So, this has degree less than or equal to 2, this has degree less than or equal to 2 and so on. And therefore, zeta 2 to the power n is constructible. If it has degree strictly less than 2, then those fields are the same. So, so in any case, this is a tower of quadratic extensions. Therefore, zeta 2 to the power n is constructible by our characterization of constructible numbers.

(Refer Slide Time: 07: 37)



But we also know a little more about zeta 2 the power n. We have shown that the minimal polynomial, the polynomial, the irreducible polynomial of zeta 2 to the power n is t to the power 2 to the power n minus 1 plus 1. See recall that zeta to the power 2n on the face of it satisfies the polynomial t to the power 2 power n minus 1 equals zero.

But this has a factorization t to the power 2 to the power n minus 1 minus 1 into t to the power n minus 1 plus 1. And this first term with a minus 1 that factorises further and further, but this thing turns out to be irreducible by applying Eisenstein's criterion after substituting t by t plus 1. So, this is an irreducible polynomial and it is satisfied by zeta 2 power n.

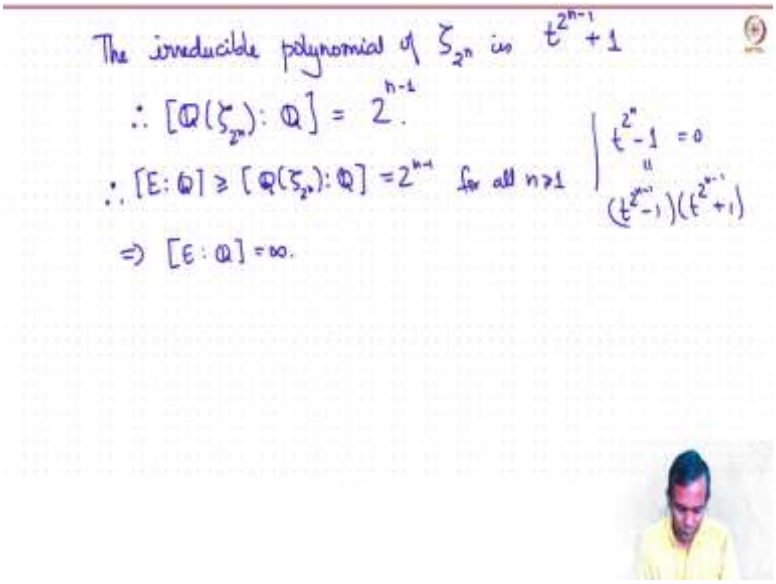
So, the irreducible polynomial of zeta 2 to the power n is t 2 to the power n minus 1 plus 1. And therefore, Q zeta to power n over Q is 2 to the power n minus 1, which means that, if we

look at this field of all constructible numbers, it contains Q zeta 2 to the power n. So, it's degree is greater than this over Q, which is 2 to the power n minus 1.

But this is true for all n greater than or equal to 1, which implies that the degree of E over Q has to be infinity. And another upshot of this exact computation of the degree of zeta 2 to the power n, the primitive 2 to the power nth root of unity is that we can go back here and replace each of these less than or equal to signs by equality.

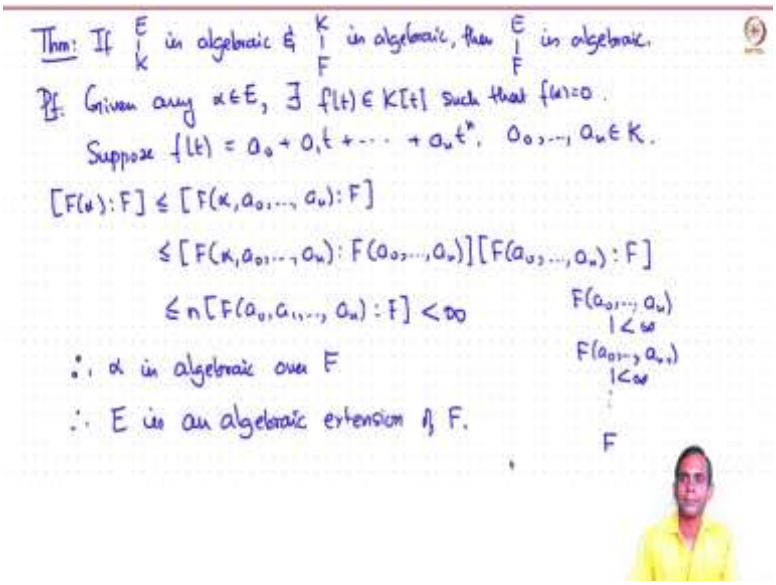
So, these extensions are each of degree exactly 2, because that is how you would get the total extension to have degree 2 to the power n minus 1. To summarise, the field of all complex numbers that are constructible is an infinite extension. But despite being infinite, it is an algebraic extension. Every constructible number is algebraic over the rationales. So, it is an algebraic extension of Q.

(Refer Slide Time: 10: 26)



We now come to a very useful result about algebraic, towers of algebraic extensions. We have seen that if you take a finite extension of a finite extension, then it is finite. And in fact, it is degree is given by the product of the degrees of the two extensions. Now, if you take an algebraic extension of an algebraic extension, it turns out that that is algebraic.

(Refer Slide Time: 10: 47)



So, the theorem states that if E over K is algebraic, and K over F is algebraic. Then E over F is algebraic. In order to prove this, we need to show that given any alpha in E alpha (satis) F alpha over F, that is this degree is finite. This is what we need to show. So, let us try to do that. So, firstly, given alpha in E, what we know is that there exists a polynomial ft in Kt, such that f of alpha is 0.

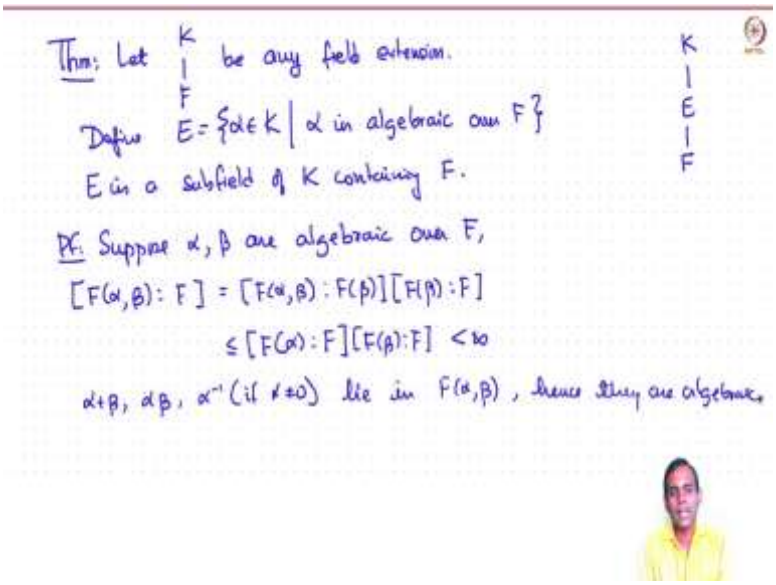
This is just because alpha is in E is algebraic over K. So, alpha is algebraic over K. And so, you have a polynomial coefficients in Kt. So, suppose we have ft is of the form a0 plus a1t plus an t to the power n, where a0 up to an, these all have to be elements of K. Now, what we want to show is that the degree of F alpha over F is finite.

Now surely this degree cannot be more than the degree of F alpha, a0, an over F because this is possibly larger field that F alpha, surely it contains the field F alpha. But this is less than or equal to the degree of F alpha, a0, an over F a0, an times the degree of F a0, an over F. Now this now is definitely less than or equal to n just because alpha satisfies a polynomial of degree n with coefficients in this field. This polynomial ft has coefficients in F a0, an.

And this is well, so, this fits into a tower of finite degree extensions. We have F a0, an over F a0, an minus 1 all the way down to F and the degree of this is less than or equal to the degree of an over F, because the degree of an over F a0, an minus 1 is less than or equal to the degree of an over F, because if it satisfies a polynomial of a certain degree in F it must, that polynomial can be regarded as a polynomial in F a0, an minus 1.

So, this is finite, all these steps are finite and so, this is finite. And so, what we have is that F alpha over F is finite, which means that alpha is algebraic over F, which means that E is algebraic over F, because we proved it for every alpha F, it is is an algebraic extension of F.

(Refer Slide Time: 15: 11)



We saw that all the complex numbers that are constructible form a field extension of Q, they form a field. The similar result holds for algebraic numbers in a much more general context. So, suppose you have any field extension K over F. And define a set E to be the set of those elements alpha in K such that alpha is algebraic over F.

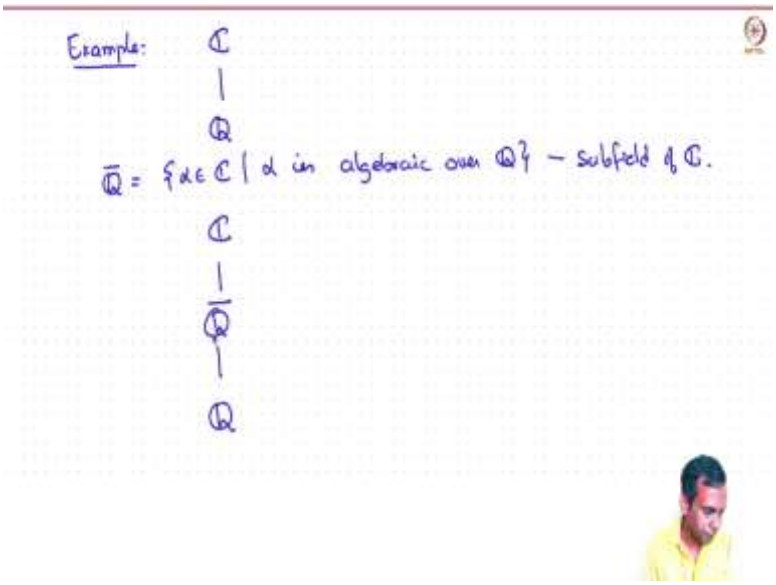
I have just defined it to be a set, the theorem is that E is a subfield of K, containing F. So, we have the situation you have K in between we have this field E and then we have F. The proof is not very difficult. So, suppose alpha and beta are algebraic over F. Then we can try to upper bound the degree of the field generated by alpha and beta over F. Well, by the tower theorem, this is the degree of F alpha beta over F beta times the degree of F beta over F.

But this F alpha beta over F beta it is degree is less than or equal to the degree of F alpha over F. This is just because, if beta satisfies a certain polynomial over F, then you can regard that polynomial is a polynomial with coefficients in F beta. And so, if alpha satisfies a polynomial with coefficients in F, you can regard that as a polynomial with coefficients in F beta. And alpha will satisfy that polynomial over F beta.

So, this degree is less than or equal to this degree, and this well of course, is what it is, but both these degrees are finite. And so, F alpha beta over F is a finite extension. Now, if you

take alpha plus beta alpha beta and alpha inverse at least if alpha is not equal to zero all lie in F alpha beta, which is a finite extension of F. Hence, they are algebraic.

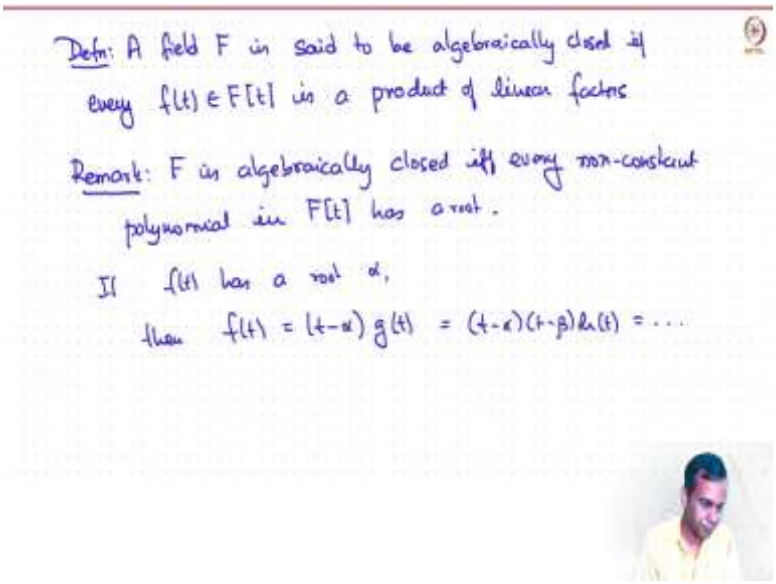
(Refer Slide Time: 18: 04)



And so, the sum product and inverse of algebraic numbers is algebraic, so they form a subfield. Nice example of this, you take the complex numbers over Q. And we define Q bar to be alpha in C such that alpha is algebraic over Q. So, we get this extension C over Q bar which lies over Q and this is a subfield of C.

This set of algebraic numbers is actually countable as we had discussed long ago. And so, this Q bar is a countable subfield of C, whereas, C has cardinality equal to the continuum. So, very few elements of C are actually in Q bar.

(Refer Slide Time: 19: 04)

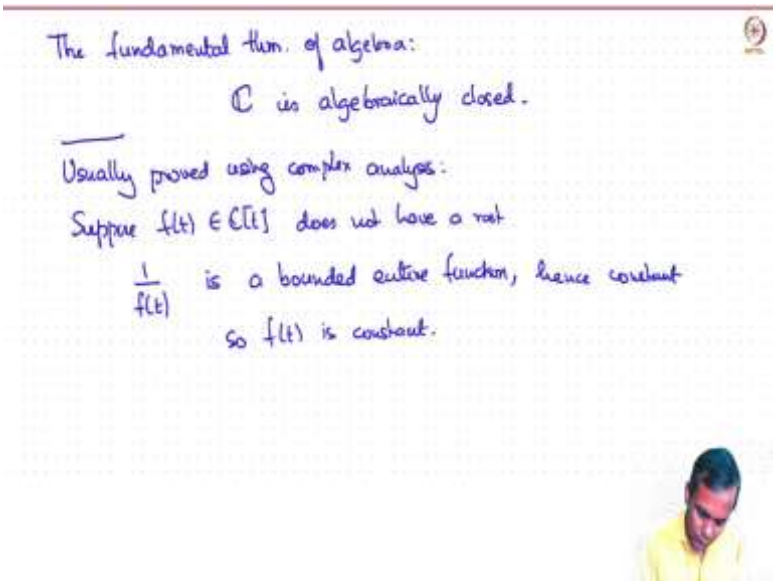


Now, let us talk about algebraically closed fields. So, definition, a field F is said to be algebraically closed if every polynomial with coefficients in F is a product of linear factors. Let me remark that F is algebraically closed if and only if every non constant polynomial has a root. Why is that?

Well, if a polynomial factor into linear factors, then each of those linear factors gives you a root. Conversely, suppose a polynomial has a root. So, if ft has a root alpha, then the factor theorem tells you that ft is t minus alpha times gt, for some polynomial gt whose degree is one less than the degree of ft.

And now, by our hypothesis, gt has a root and so, then gt can be written as t minus beta into ht and so on until finally, you get resolution of ft into a product of linear factors, the last thing will be a constant. And so, you will get a constant times linear factor in the form t minus alpha t minus beta and so on. So, to show that a field is algebraically closed, you do not need to show that every polynomial as linear factor, you just need to show that every non-constant polynomial not as a root.

(Refer Slide Time: 21: 41)

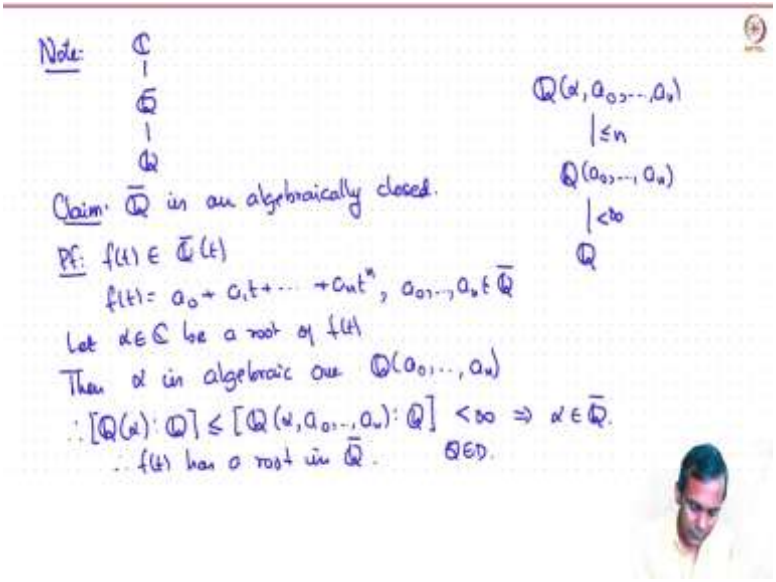


And very well-known theorem is the fundamental theorem of algebra. It says that, the field of complex numbers is algebraically closed. This is usually proved in the second form; you show that any non-constant polynomial has a root. So, this is usually proved using complex analysis. But it does not use all that much complex analysis, you can find a proof, a complete proof in Michael Orton's algebra book, which usually you prove using complex analysis, suppose ft is a polynomial with complex coefficients, and this does not have a root.

Then you can talk about 1 over ft. This makes sense as a function on the complex numbers. And it is what is in complex analysis known as a bounded, you have to show this, is a bounded entire function. And by Lobels theorem, this has to be constant. Which means that ft itself is constant. I am just outlining this here, it is always, it is usually done in complex analysis courses.

So, if ft is constant, so what it is saying is that if ft were not constant, then it would have a root. And therefore, using this inductive arguments that I described earlier, you could keep applying this and show that the polynomial is a product of linear factors. So, the complex numbers are algebraically closed.

(Refer Slide Time: 23: 54)



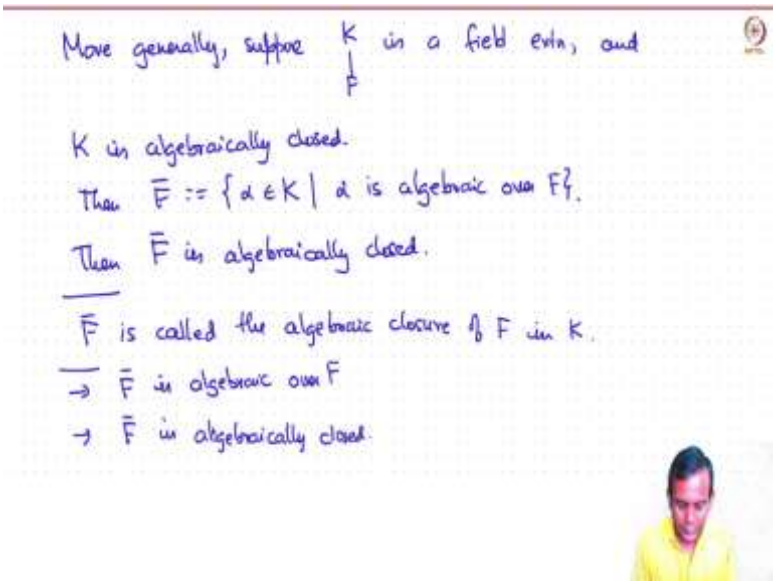
But we can say more. So, we have this situation, we have, we have complex numbers, we have the rationales down here, and in between we have Q bar. And what we can say is that Q bar is algebraically closed. It is much smaller than the complex numbers, but it is algebraically closed. And the proof, well, we just need to show that every polynomial non constant polynomial in Q bar t has a root.

So, suppose ft is equal to a0 plus a1t plus ant to the n. Now we will use the fact that the complex numbers are algebraically closed. Let alpha be a root of ft, ft is a polynomial with complex coefficients. So, it is also, so it has a root. And then alpha is algebraic over the field Q a0 an. So, we are using the same trick again of adjoining the coefficients of the polynomial. And so, we have this situation.

We have Q alpha, a0, an this sits over Q a0, an and this is of degree, I guess less than or equal to n, because alpha satisfies a polynomial of degree n in this field and this sits over Q and this is of course, finite by the fact that a0, a1, an belong to Q bar, so, they are algebraic. And so, this whole extension is finite.

And so, Q alpha over Q is less than or equal to as we did before Q alpha, a0, an over Q. And so, this as we argued before this is finite. And hence, alpha belongs to Q bar. So, what we have is at ft has a root in Q bar. And that is enough to show that Q bar is algebraically closed. Every polynomial has a root, every polynomial coefficients in Q bar has a root in Q bar.

(Refer Slide Time: 27: 14)



We can do this in more generality, we do not need to use complex numbers more generally. Suppose, we have a field extension and K is algebraically closed. Then you take F bar to be alpha in K such that alpha is algebraic over F. Then F bar is algebraically closed. So, F bar is called the algebraic closure of F in K. Sometimes this terminology is used even when K is not algebraically closed.

So, so then you just take the algebraic elements and that is called the algebraic closure of F in K. So, it is a relative, it is relative notion. It is not, it depends very much on what K you are looking at. But if K is algebraically closed, then F bar itself is algebraically closed. It has the two properties. So, it has the following two properties, F bar is algebraic over F.

And because case K is algebraically closed, this argument can be written more generally for any chain of extensions F bar is algebraically closed. These two properties characterise what are called algebraic closures in the abstract, and we will see them in the next lecture.