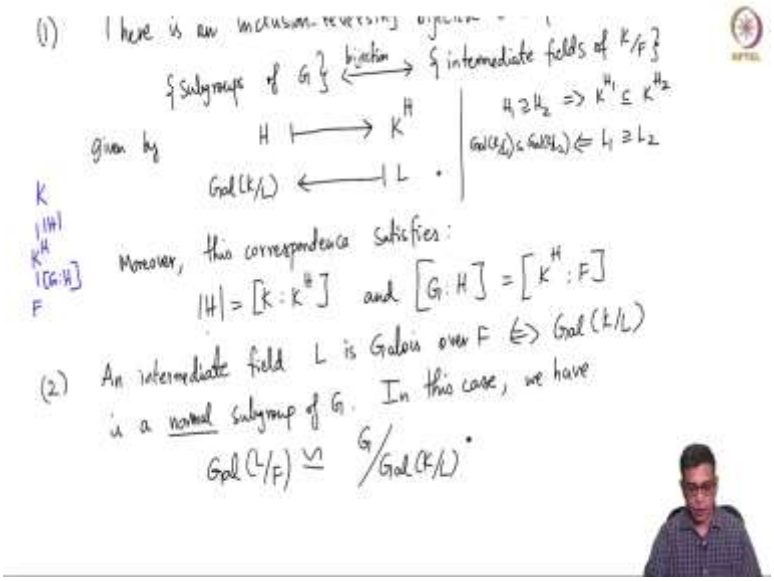
Introduction to Galois Theory
Professor Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute
Lecture 26
Fundamental Theorem of Algebra

(Refer Slide Time: 00:15)



Welcome back, in the last two classes, we proved the main theorem of Galois Theory, which as I told you then is the essential result in Galois Theory. So, the everything else follows from this, the statement itself is simple and the proof is also not difficult, but this statement has far reaching consequences as we will see in the rest of the course.

So, let me just quickly recall the statement of the main theorem. It says that if you start with a Galois extension; remember always, a Galois extension is a finite extension for us. So, K over F is a Galois extension, Galois group G, then there is an inclusion reversing bisection inclusion reversing refers to this statement between the subgroups of the Galois group and intermediate fields of the extension.

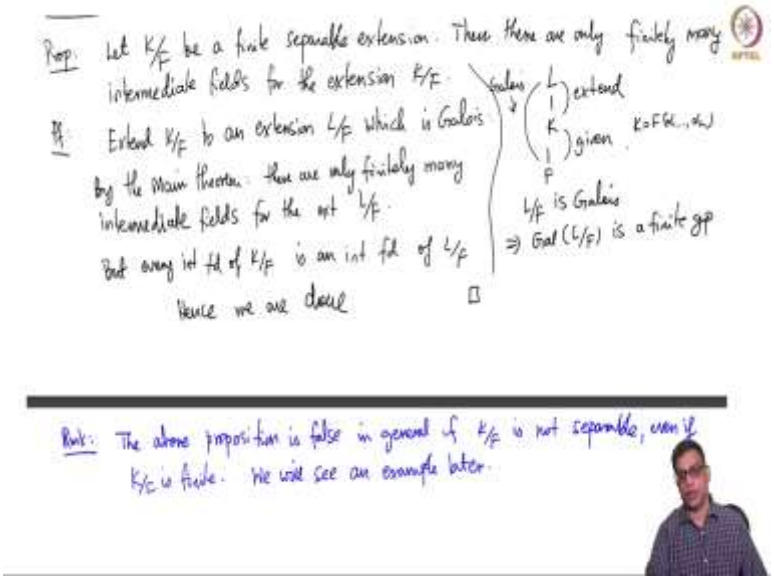
And the maps in either direction are given by take a group and take its fixed filed, take an intermediate field and take the Galois group of K over that intermediate field then these maps are well defined set maps and they are inverses of each other. And if you have a group H1 containing H2, there is the opposite inclusion among the fixed fields.

So, and knowing the order and the index of that group, you will know the degrees of the 2 field extensions with by you will get by putting this intermediate field in the middle and second statement, which is equally important is an intermediate field is Galois or not can be read of completely from the corresponding group.

So an intermediate field L is Galois or the base field F if and only if the corresponding group which is Galois K over L is a normal subgroup of G. And if that happens, the Galois group is the quotient group or G mod G Galois K over L. So, this is a very nice and compact set of statements and they have very strong implications.

And the proof was, as I said, relatively easy, given all the results that we have developed before this, so today, what I want to do is to give a nice proof of fundamental theorem of algebra, using the main theorem of Galois theory and after that, we will do a few problems and then we move on to other topics in the course.

(Refer Slide Time: 02:33)



So, the first so, these are really corollaries of the main theorem, but let me write it as a proposition. The first one is a simple statement that I want to highlight, before I move to the fundamental theorem of algebra, so, let K over F be a finite separable extension, then there are only a finitely many there are only finitely many intermediate fields for the extension K over F.

So, that means there are only finitely many fields L that live between K and F and the prove is rather simple. So, by an argument that I gave in an earlier class, given any separable extension, you can always extend that K to a bigger extension, which is Galois. So, extend K to a field extend K over F to an extension which is Galois. So, by which I mean the following. So, let me just write it down in pictorially.

So, you have this is given you extend here such that this whole thing is Galois. So, let me just orally say why thus is the case, this is because you take K you know K is of the form F alpha 1 through alpha n and each alpha i is separable, because the extension is given to be separable, then you take the irreducible polynomial of alpha 1 times irreducible polynomial of alpha 2 times irreducible polynomial of alpha n.

And so, that polynomial is F and you take the splitting field of that over K. So, L over F will be the splitting field of that polynomial that you obtained by multiplying the irreducible polynomials of alpha i and all of them are separable, so, their product is separable. So, L is a splitting field over F of a separable polynomial and hence it is Galois.

So, you can always extend a separable extension, finite separable extension to the Galois extension, you cannot do this if the given extension is not separable as we know because a Galois extension is separable and if a L over F is Galois and hence L over F is separable, hence K over F will be also separable. So, if K over F is given to be non-separable, you cannot do this.

And now by so now let us get back to the proof L over F is Galois by the main theorem of Galois Theory. So, which I will refer to simply as main theorem, there are only finitely many intermediate fields for the extension L over F because L over F is a Galois extension, it is a finite extension. So, of course, L over F is Galois implies is a finite group because that cardinality is exactly equal to the degree of L over F.

So, Galois's main theorem applies to the extension L over F and it says that the intermediate number of intermediate fields of L over F is exactly equal to the number of subgroups of the Galois group, but the Galois group is a finite group. So, there are only finitely many subgroups, and hence, there are only finitely many intermediate fields.

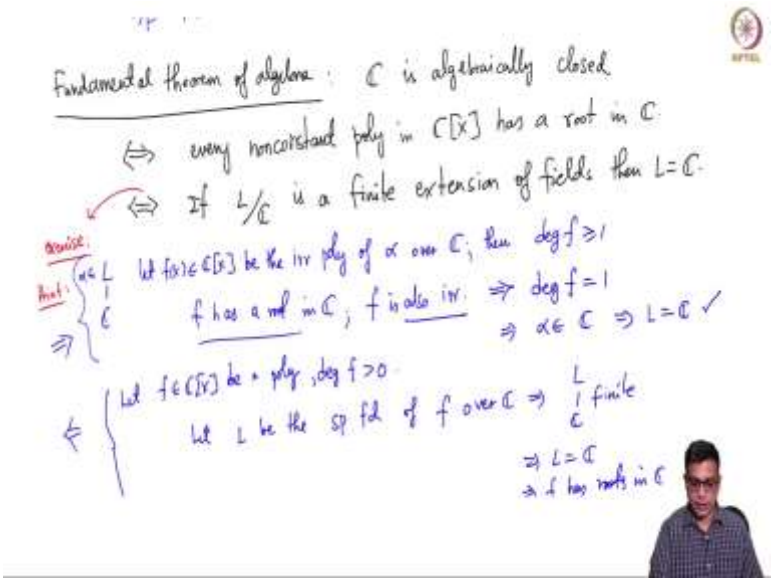
But now we are done every intermediate field of K over F is an intermediate field of L over F because if you have a field between K and F it is of course, a field between L and F. So, the set of intermediate fields of K over F is a subset of the set of intermediate fields of L over F. And the set of intermediate fields of L over F is finite. So, we are done.

So, in general, even if the extension is not Galois, the number of intermediate fields is finite. And this is an interesting statement, because, in general, it is not true. And it is tricky to prove this without Galois Theory. If you try to prove this, you can do it but it is significantly more work. So, you can see there a nice little application of the main theorem of Galois Theory.

So, let me just remark here and we will come back to this the above statement is false. In general, if K over F is not separable, of course, it is false if it is not finite, because then you can certainly construct infinitely many intermediate fields, but even if it is finite, if it is not separable, it may in general have infinitely many intermediate fields we will see an example later. So, I am going to do a few problems sessions later in which I will discuss this.

So, it is not in general true that a finite extension, it looks like how can it have infinitely many you have only a finite extension. How can it have many infinitely many. But they can be horizontal in some sense, they can be incomparable they can all infinitely many live in between. So, this we will discuss when we come to that example later. So, this is the first nice application of the main theorem.

(Refer Slide Time: 08:29)



But now, I want to do the main point of this video, which is the fundamental theorem of algebra. Fundamental theorem of algebra is famous for having lots of different proofs. There are proofs using complex analysis, topology, algebra and so on. So, we are going to give one with Galois Theory. So, what is the fundamental theorem of algebra? Firstly, let us recall that it says one way of saying that is C is algebraically closed equivalently every non constant polynomial in Cx has a root complex root that means as a root in C.

So, that means, every non constant polynomial so degree 1, 2, 3 and so on has a root. So, remember R is not algebraically closed because it has degree 2 polynomials, which do not have roots. So now, I am going to phrase this in terms that we will understand in view this course. It says that if so let me do this if L over C is a finite extension of fields then L equal to C so what I want to leave to you is, this is this implication is really a nice exercise.

So, if every non constant polynomial has a root in C then there cannot be any non-trivial finite extensions and conversely if there every non-finite extension is actually trivial extension, then every non constant polynomial has a root. So, let me just give you hints or rather it may be the full solution, but if you take an extension like this and you take alpha take the irreducible polynomial of that alpha.

So, then of course, degree is at least 1 because irreducible polynomial are by definition positive degree polynomials. So, so I am using this hypothesis that every non constant polynomial has a root. So, f has a root on the other hand f is also irreducible. Because it is the irreducible polynomial, so, it has a root, sorry, it is irreducible polynomial it is irreducible, but it has a root by hypothesis, this basically tells you that f has to be a linear polynomial.

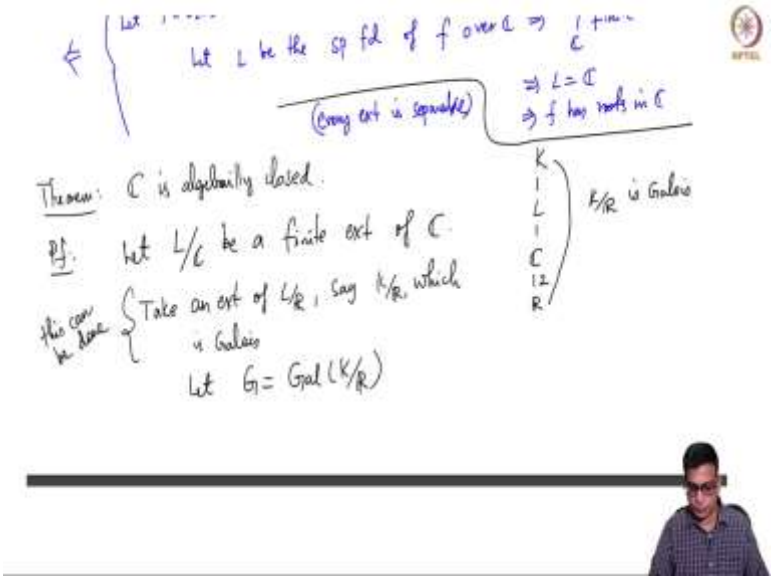
The only polynomial which is irreducible and has a root is degree one polynomials. So, that means alpha is in C. So, having an irreducible polynomial of degree 1 is equivalent to the statement that that element is in C itself. This of course, means L equal to C, because every element alpha, I am working with an arbitrary element here is in C, so, L itself is C that is one direction.

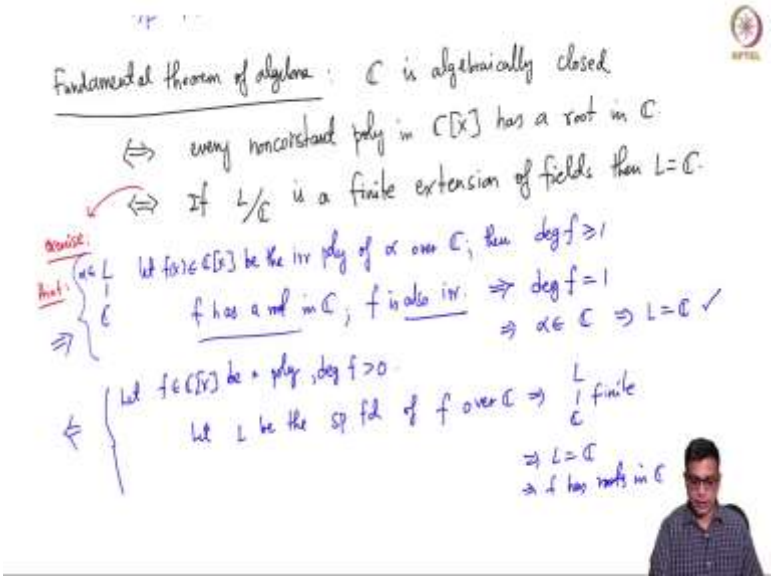
Now, if you take, I am really proving the whole thing, but if you take on the other hand, let f be an irreducible polynomial with degree positive, that means it is non constant. Actually, let f be an any polynomial degree f is positive; I want to show that it has a root. So, if let g be an irreducible, so maybe I do not need to do that so let us take the splitting field of that polynomial, let L be the splitting field of f or C.

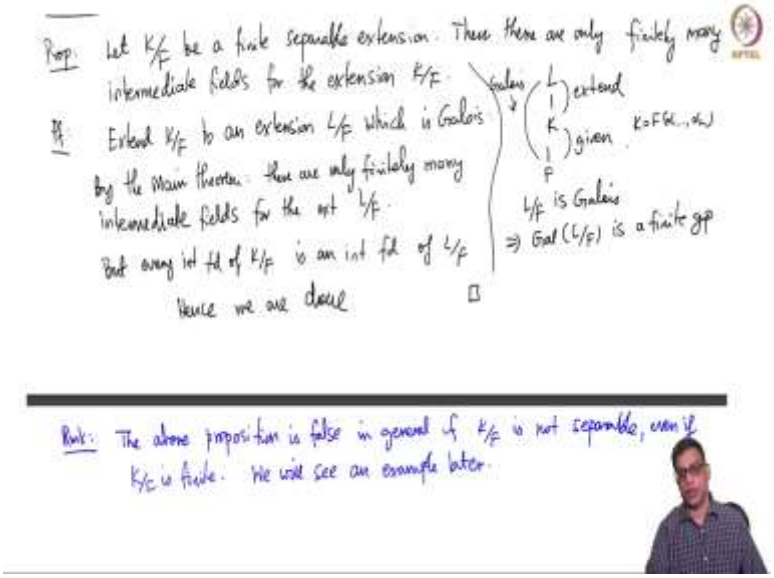
So, this implies L or C is a finite extension, because splitting field of any polynomial is generated by the roots, which are all algebraic, so it is finite extension, but then by hypothesis, L equal to C because here, every finite extension is trivial. So, I am not really breaking up the proof cleverly, but this is what this first part is the proof of forward direction, this is not proof the reverse direction, so L equal to C, which means f has roots in C.

Because L is supposed to contain the roots, but L is equal to C, so f has root. So, the statement that C is algebraically closed is equivalent to the statement that there are no non trivial finite extensions. And that is the theorem that we want to know prove.

(Refer Slide Time: 13:39)







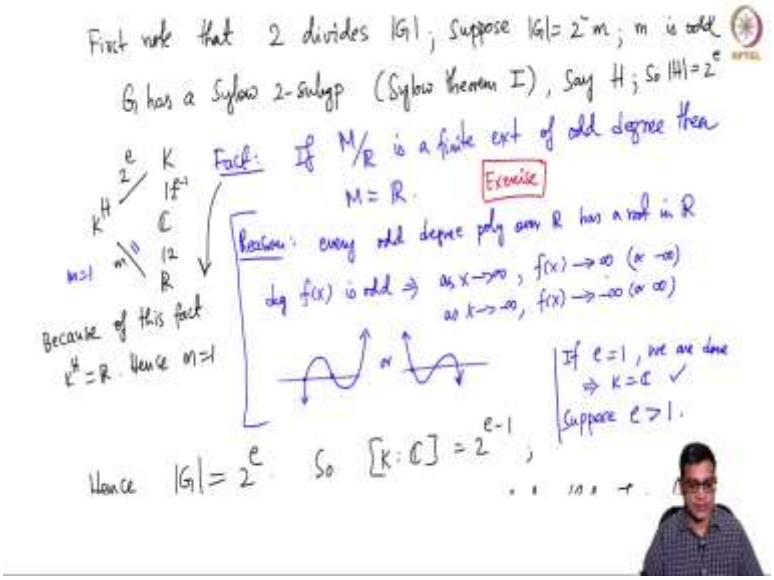
So, C is algebraically closed. So, let me prove this, the proof is quite nice. And it is rather straightforward. So, essentially uses the main theorem of Galois Theory. So, to prove this, we are going to use the third statement here, we are going to take a finite extension of C and prove that it is equal to C. So, let L over C be a finite extension of C.

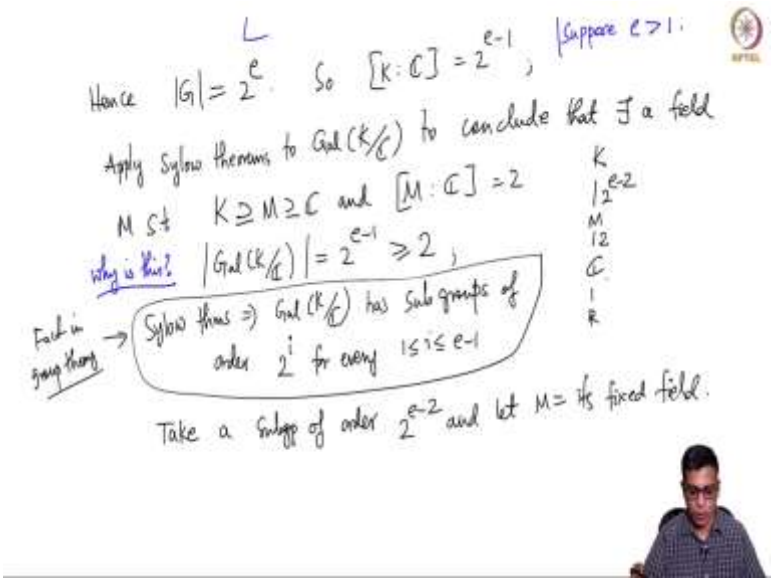
So, what we have is, so we have C here, L here and of course C contains R and this is a degree to extension. Now, take an extension of L over R say K over R, which is Galois. So, what I am really doing is K, so extend this I am going to put a line here. So, extend this. So, this K is some arbitrary extension, such that K over I want K over R to be Galois.

So, because I am not used that in, in particular, K over C will also be Galois, but I want to also assume that K over R is Galois, this we can do this can be done, as I indicated in the previous proof here, we can always extend a given separable extension to a Galois extension of course here everything is characteristic 0.

So, every extension here is I should remark this. So, every extension is separable, so, you any finite extension can be extended to a Galois extension, so, this is finite. So, this is finite and hence you can extend it to a Galois extension. So, now let G be the Galois group of K over R. Now, we are going to use some fairly advanced group theory.

(Refer Slide Time: 15:46)





So, what do we do, we first note that 2 divides the order of G, 2 divides the order of G, because that is clear, because order of G is equal to K colon R, which is equal to K colon C times C colon R and this is 2. So, two divides this. So suppose someone to look at Sylow 2 subgroups of G. So, suppose this is equal to 2e m. So, here of course, m is odd, because we are going to factor out the largest power of 2 in the order of G.

So, now, what we know is that G has a Sylow 2 subgroup. So, this is your first illustration of how deep theorems in group theory can shed light on field theory. So, this is Sylow theorems. If

I remember correctly, this is Sylow theorem 1, first Sylow theorem. So, sorry so say H. So, remember that this requires Sylow theorem we do not know that there is a Sylow 2 subgroup unless we use Sylow theorem. So, let us look at the fixed field of H.

So, I am going to redraw the, I am want to forget the given extension, we want to just directly prove that K equal to C. So, L will automatically be C so L disappears from the picture. So, then, if I take K power H. So, K power H is an intermediate field of K to R, it may or may not contain C. So, I want to write that separately and what are the degrees of these field extensions by the main theorem of Galois Theory, what we have is this is m, this is the index and this is the order.

So, remember so, order of H is 2 power e. So, that is 2 power e and this is m and m is odd, but, we can use a fact here if L over let us say M over R is a finite extension have odd degree then M equals R. So, R cannot have in fact any extension of degree different from 2 but that will come from fundamental theorem of algebra, but we can definitely show that it cannot have an odd degree and the reason for this which I will quickly do without getting into the details.

The reason is every odd degree polynomial has a polynomial over R has a root in R. This can be used for example, using the intermediate value theorem. So, an odd degree polynomial if you take degree is odd this implies as x goes to infinity fx goes to infinity as x goes to minus infinity fx goes to minus infinity.

This could also I mean if the leading term is negative this will be minus infinity but the point is as x goes to infinity and as x goes to minus infinity, the limits of fx are different. So, it either looks like this. So, or it looks like this. So, it goes to infinity as x goes to infinity or minus infinity. So, then it certainly will cross the x axis somewhere. So, this is bit of standard argument that you would have seen before.

And now I will not write anymore, but if this is granted, if you take an odd degree extension like this, and you take an alpha here and you take R alpha this degree is odd, because this it divides this. So, it cannot be even this is odd. So, the irreducible polynomial of alpha over R has odd degree, but then it cannot be it is also going to admit a root. So, it must be linear. So, just like in the previous case, R alpha equal to R, so, KH equals to K.

So, the conclusion is so, I am sorry that I went over this fast, but this is standard things. So, because of this fact. So, this is m by the way, because of this fact KH equals equal to R and hence so, let me leave this as an exercise. This is a very straight forward exercise and it uses this property of odd degree polynomial so were real numbers and once you admit this reason, the proof is similar to the proof that equivalence of these two statements.

So, if you have an odd degree extension and take an element, it is irreducible polynomial as degree odd so that irreducible polynomial must have a root but an irreducible polynomial which has a root as to be degree 1. So, it must be that arbitrary element alpha must be in R itself that means everything KH is in R so KH is equal to R.

So, this tells me that and hence. Now, let us proceed with the proof hence order of this is 2 power e. So, now order of this is 2 power e. So, there is no m, so, this m is 1. Now, this tells me that order of this. So, the degree of this extension is 2 power e minus 1. Because this is 2 and this is an equality. So, m equal to 1, so, this is 2 power e and this is 2 power e minus 1.

So, the product will be 2 power e. So, K is an extension of C of degree 2 power e minus 1. So, let us now apply Sylow theorem 2 the Galois group of K over C. So, apply theorem to Galois group of K over C to conclude, so, I will write the conclusion and I will explain why Sylow theorem applies here. To conclude that there exists a field M such that K it is an intermediate field of this and M colon C is 2.

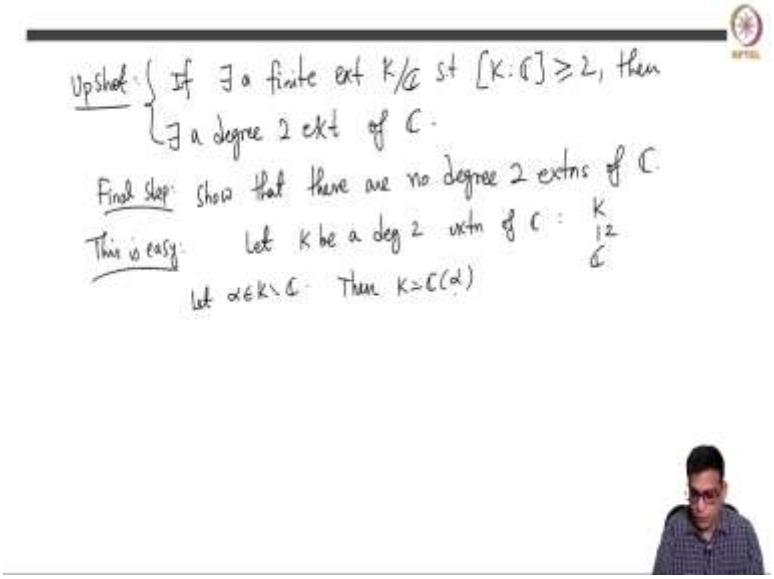
The reason for this is the following. So, we have K you have M, you have C you also have R but it is relevant for me. So, the point is I want to conclude this of course, this is assume that e is greater than 1, if e is equal to 1 we are done. Because then K equal to C. So, suppose e is greater than 1. So, that means e is at least 2 that means, K over C is at least 2 power e minus 1, so, that is at least 2.

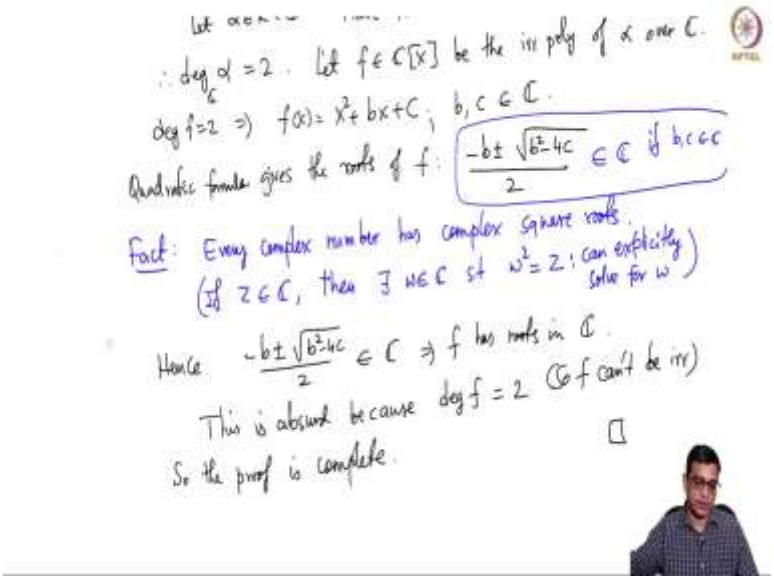
So, if K is this is already 2 then K equal to M, but otherwise I can always take a smaller extension with degree 2. So, why is this? The reason for this is G are the Galois group of K over C has order 2 power e minus 1 which is of course, at least 2. So, by Sylow theorems Galois K over C has sub groups of order 2 power i for every i from 1 to. So, this is the main application of Sylow theorem.

So, if you have a two group a group of order 2 power 10 for example, then there are sub groups of order 2 power 10, 2 power 9, 2 power 8, 2 power 3, 2 power 2, 2 power 1 for every power of 2 from 2 power 0 all the way to 2 power the cardinality the highest order. So, in this case 2 power i minus 1 so, this is a standard theorem of Sylow theorems. So, this is a fact in group theory. So, as I said we are going to use the fairly inward results in group theory.

So, this is also a result of Sylow theorems that Galois K over C has a subgroup of every order. So, all you need to do is take a subgroup of order 2 power e minus 2 and let M equal to its fixed field. So, if M is a fixed field of a group of order 2 power e minus 2 the degree of K over M will be 2 power e minus 2 and degree of M over C will be 2. So, hence we are guaranteed that there is a degree 2 extension of C.

(Refer Slide Time: 26:32)





So, upshot of all this is if there is a finite extension. So, so far, maybe it is good to write this. So, upshot if there exists a finite extension K over C, such that its index is at least 2, then there exists a degree 2 extension of C, that is the upshot. So, the entire slide, previous slide is proving this give me any finite extension, which is at least degree 2, then I can take a smaller extension, which is at least degree which is exactly degree 2.

And now, the final step is the following statement. So, the final step is show that there are no degree 2 extensions of C. So, this is a very special case of fundamental theorem of algebra, but this is straight forward, fundamental theorem says that there are no finite extension of C that means there is no degree 2 extension, there is no degree 3 extension, there is no degree 1000 extension, there is no degree 2000 extension and so on.

That is the full extent of fundamental theorem of algebra. But prove that there is no degree 2 extension is rather easy. So, this is easy. So, the proof proceeds in the following way, give me some finite extension of degree 100000. But I can construct a smaller extension of degree 2. And then I am going to argue in a very simple way that there cannot be a degree 2 extension of C.

So you are done. So, that means they cannot be finite extension of C. And this is, of course, something that I have seen before, I have sort of explained before. But let me just quickly explain this, let K be a degree 2 extension of C. So, now, I am going to just omit the entire notation from before and focus my attention on this situation.

So, you have K over C is a degree 2 extension. Now, let us choose alpha in K that has not in C of course, K is different from C because it is a degree 2 extension. If they are equal, it will be a degree 2 extension. So, we can always choose an alpha which is not in C, but it is in K. So, K will be C alpha that means degree of alpha over C is 2. So let f in complex numbers, f over complex numbers, be the irreducible polynomial of alpha over C.

So, degree of f is of course 2. So it will be of the form fx equals x square plus bx plus c. So, where b, c are complex numbers, but the quadratic formula tells us the roots of this. This are minus b plus or minus b square minus 4c by 2, because I am taking a monic polynomial. But here is the final fact that I am going to use. So, this proof works modulo some deep group theory and a fact about real degree odd degree polynomials and the following fact.

Every complex number has complex square roots. So, basically what I am saying is, if Z is in C, then there exists w, such that w square is Z, there exists w in C such that w square is Z. So, of course, w and minus w will be the roots of square roots of Z. So, every complex number has complex square root. This is a very small part of fundamental theorem of algebra.

But again, this is something you can write down. So, this you can explicitly can explicitly solve for w. So, you give me Z equals a plus a plus ib, you can explicitly solve for the square root. So, now let us compare to the quadratic formula. So, b and c are complex numbers. So, b square minus 4 is a complex number. So, it is square root is also a complex number. So, but these are in complex numbers. So this means f has roots in C.

But this is a problem. This is absurd, because only way that irreducible polynomial can have roots is if it is degrees 1, but degree of f is 2. So, f can be irreducible. So, this is a contradiction, because complex numbers have roots square complex square roots, this is in c, basically, if b, c are in c, see this is where it will not work, for example, for real numbers, because this could be negative and then square root will no longer be in R it will only be in C.

But if they are already complex numbers, the square roots are complex numbers and all operations will preserve complex numbers. So, this is absurd. So, that means there cannot be a degree to extension of C and hence, so the proof is complete. So, the proof is complete

essentially, key idea is of course, advanced group theory including Sylow theorems, but otherwise we are using some elementary facts about odd degree polynomials.

And we are proving that complex number has square roots we are using that. So, basically the proof reduces this entirety of fundamental theorem of algebra, which is a statement that every non constant polynomial has roots to the much simpler statement that every degree 2 complex polynomial as roots which is straight forward.

So, this using Galois Theory and some group theory, we have reduced fundamental theorem of algebra to a much more feasible statement, which we can proved directly and hence we get the fundamental theorem of algebra. So, this I have done this to just give you an idea of how to prove how to prove fundamental theorem of algebra using main theorem of Galois Theory. And to indicate to you that main theorem of Galois Theory has surprising applications.

So, let me stop this video here and in the next video, we will do some problems on all the material that we have covered so far. Thank you.